



## **HS2310 Series Switches**

**Command Reference, Release 11.4(1)B90**

## **Copyright Statement**

Ruijie Networks©2023

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 11.9(6)B13P4.

## Audience

This manual is intended for:

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

## Obtaining Technical Assistance

- Ruijie Networks Website: <https://ruijie.co.jp/>
- Technical Support Website: <https://www.ruijie.co.jp/service>
- Inquiry & Repair: <https://www.ruijie.co.jp/service/post-sales>
- Technical Support Email: [support\\_jp@ruijienetworks.com](mailto:support_jp@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
<b>boldface font</b>	Commands, command options, and keywords are in <b>boldface</b> .
<i>italic font</i>	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 data.

---



## Ethernet Configuration Commands

---

1. Interface Commands
2. MAC Address Commands
3. Aggregate Port Commands
4. VLAN Commands
5. Protocol VLAN Commands(beta)
6. Private VLAN Commands(beta)
7. MSTP Commands(beta)
8. GVRP Commands(beta)
9. LLDP Commands(beta)
10. ERPS Commands(beta)

# 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 0/17
Ruijie(config-if-GigabitEthernet 0/17)# 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* **down** [ *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.
	<i>milliseconds</i>	(Optional) in the range from 0 to 60000 in the unit of milliseconds.
	<b>up</b>	(Optional) Configures the delay after which DCD changes from Down to Up in status.
	<b>down</b>	(Optional) Configures the delay after which DCD changes from Up to Down 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 or vice versa. 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 0/17
Ruijie(config-if-GigabitEthernet 0/17)# carrier-delay 5
```

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

```
Ruijie(config)# interface GigabitEthernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)#carrier-delay milliseconds 100
```

The following example sets the DCD delay from Down to Up in status to 100 milliseconds and from Up to Down to 200 milliseconds.

```
Ruijie(config)# interface GigabitEthernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# carrier-delay up milliseconds 100 down
milliseconds 200
```

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 0/17.

```
Ruijie# clear counters gigabitethernet 0/17
```

Related Commands	Command	Description
	<b>show interfaces</b>	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** The following example resets the interface gigabitethernet 0/17.

**Examples**

```
Ruijie# clear interface gigabitethernet 0/17
```

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

**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>	

**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 0/17
Ruijie(config-if-GigabitEthernet 0/17)# description GBIC-1
```

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

**Platform** N/A

**Description**

## 1.6 duplex

Use this command to specify the duplex mode for the interface. Use the **no** form of this command to restore the default setting.

**duplex { auto | full | half }**

**no duplex**

### Parameter Description

Parameter	Description
<b>auto</b>	Self-adaptive full duplex and half duplex
<b>full</b>	Full duplex
<b>half</b>	Half duplex

**Defaults** The default is **auto**,

**Command** Interface configuration mode.

### Mode

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

The feature is not supported by G.hn ports.

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

### Examples

```
Ruijie(config-if-GigabitEthernet 0/17)# duplex full
```

### Related Commands

Command	Description
<b>show interfaces</b>	Displays the interface information.

**Platform** N/A

### Description

## 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 0/17.

```
Ruijie(config)#interface GigabitEthernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# eee enable
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** N/A

## 1.8 errdisable recovery

Use this command to recover the interface in violation.

**errdisable recovery [ interval time ]**

**Parameter Description**

Parameter	Description
<b>interval time</b>	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 and Interface configuration mode.

**Usage Guide** Use the command to recover the port that triggers violation after being configured with the **violation shutdown** command.

**Configuration Examples** The following example recovers the violation interface gigabitethernet 0/17.

```
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# errdisable recovery
```

**Related Commands**

Command	Description
<b>switchport port-security violation shutdown</b>	Configures the port security violation to shutdown.

**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
<b>auto</b>	Self-negotiates the flow control.
<b>off</b>	Disables the flow control.
<b>on</b>	Enables the flow control.

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

**Command** Interface configuration mode.

**Mode**

**Usage Guide** Use the **show interfaces** command to display the flow control configuration. The feature is not supported by G.hn ports.

**Configuration** The following example enables flow control on GigabitEthernet port 0/17.

**Examples**

```
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# flowcontrol on
```

**Related Commands**

Command	Description
<b>show interfaces</b>	Displays the interface information.

**Platform** N/A

**Description**

## 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** Interface 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.

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

The following example enters configuration mode on GigabitEthernet 0/17.

```
Ruijie(config)# interface GigabitEthernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)#
```

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 Description** N/A

## 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>	
	<b>macro</b> <i>macro_name</i>	The macro name which represents the interface range.

**Defaults** The **interface range** command is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** Use the define interface-range command to define a range of interfaces as the macro name and then use the **interface range macro macro\_name** command to enter interface configuration mode on multiple interfaces.

**Configuration Examples** The following example enters interface configuration mode on multiple interfaces by setting the interface range.

```
Ruijie(config)# interface range gigabitEthernet 0/17, 0/18
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 0/17-18
Ruijie(config)# interface range macro routel
Ruijie(config-if-range)# bandwidth 100
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** N/A

## 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 0/17.

```
Ruijie(config)#interface gigabitEthernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)#line-detect
```

```

Interface : GigabitEthernet 0/17
start cable-diagnoses,please wait...
cable-daignoses end!this is result:
4 pairs
pair state      length(meters)
-----
A   Ok          1
pair state      length(meters)
-----
B   Ok          2
pair state      length(meters)
-----
C   Short       1
pair state      length(meters)
-----
D   Short       1
    
```

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 0/17** command is run.

```
3 minutes input rate 15 bits/sec, 0 packets/sec
3 minutes output rate 14 bits/sec, 0 packets/sec
```

**Configuration Examples** The following example sets the interval for calculating load on interface GigabitEthernet 0/1 to 180 seconds.

```
Ruijie(config)# interface gigabitEthernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# load-interval 180
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.14 logging

Use this command to print information on the interface.

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

Parameter Description	Parameter	Description
	<b>link-updown</b>	Prints the status change information.
	<b>error-frame</b>	Prints the error frame information.
	<b>link-dither</b>	Prints the 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  
Description** N/A

## 1.15 mtu

Use this command to set the MTU supported on the interface.

**mtu** *num*

**Parameter  
Description**

Parameter	Description
<i>num</i>	64 to 9216

**Defaults** The default is 1500.

**Command  
Mode** Interface configuration mode.

**Usage Guide** This command is used to set the maximum transmission unit (MTU) supported on the interface. The feature is not supported by G.hn ports.

**Configuration** The following example sets the MTU supported on interface `gigabitethernet 0/17` to 9000.

**Examples**

```
Ruijie(config)# interface GigabitEthernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# mtu 9000
```

**Related  
Commands**

Command	Description
show interfaces	Displays the interface information.

**Platform  
Description** N/A

## 1.16 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
<b>on</b>	Enables auto-negotiation.
<b>off</b>	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.  
The feature is not supported by G.hn ports.

**Configuration Examples** The following example enables auto-negotiation mode on interface GigabitEthernet 0/17.

```
Ruijie(config)# interface GigabitEthernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# negotiation mode on
```

### Related Commands

Command	Description
N/A	N/A

**Platform Description** N/A

## 1.17 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 Mode** Global configuration 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 Examples** The following example enables oscillation protection on the port.

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

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** N/A

## 1.18 protected-ports route-deny

Use this command to configure L3 routing between the protected ports. Use the **no** form of this command to restore the default setting.

**protected-ports route-deny**

**no protected-ports route-deny**

**Parameter Description**

Parameter	Description
N/A	N/A

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

**Command Mode** Global configuration mode.

**Usage Guide** The ports that are set as the protected ports can route on L3. Use this command to deny the L3 communication between protected ports. Use the **show running-config** command to display configuration.

**Configuration Examples** The following example configures L3 routing between the protected ports.

```
Ruijie(config)# protected-ports route-deny
```

**Related**

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

<b>Commands</b>	
	<b>show running-config</b> Displays the protected ports route-deny configuration.

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

## 1.19 show eee interfaces status

Use this command to display interface EEE status.

**show eee interfaces** { *interface-type interface-number* | *status* }

<b>Parameter Description</b>	<b>Parameter</b>	<b>Description</b>
	<i>interface-type</i> <i>interface-number</i>	Interface type and ID.
	<i>status</i>	All interface EEE status.

**Defaults** N/A

**Command Mode** Any CLI 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 0/17
Interface           : Gi0/17
EEE Support         : Yes
Admin Status       : Enable
Oper Status        : Enable
Remote Status      : Unknown
Trouble Cause      : None
```

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(config)#show eee interfaces status
Interface EEE      Admin   Oper    Remote  Trouble
           Support Status  Status Status  Cause
```

Ghn0/1	Yes	Enable	Enable	Unknown	None
Ghn0/2	Yes	Disable	Disable	Unknown	None
Ghn0/3	Yes	Disable	Disable	Unknown	None
Ghn0/4	Yes	Disable	Disable	Unknown	None
Ghn0/5	Yes	Disable	Disable	Unknown	None
Ghn0/6	Yes	Disable	Disable	Unknown	None
Ghn0/7	Yes	Disable	Disable	Unknown	None
Ghn0/8	Yes	Disable	Disable	Unknown	None
Ghn0/9	Yes	Disable	Disable	Unknown	None
Ghn0/10	Yes	Disable	Disable	Unknown	None
Ghn0/11	Yes	Disable	Disable	Unknown	None
Ghn0/12	Yes	Disable	Disable	Unknown	None
Ghn0/13	Yes	Disable	Disable	Unknown	None
Ghn0/14	Yes	Disable	Disable	Unknown	None
Ghn0/15	Yes	Disable	Disable	Unknown	None
Ghn0/16	Yes	Disable	Disable	Unknown	None
Gi0/17	Yes	Enable	Enable	Unknown	None
Gi0/18	Yes	Disable	Disable	Unknown	None
Te0/19	NO	-	-	-	-

#### Related Commands

Command	Description
N/A	N/A

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

## 1.20 show interfaces

Use this command to display the interface information and optical module information.

**show interfaces** [ *interface-type interface-number* ] [ **description** | **switchport** | **trunk** ]

#### Parameter Description

Parameter	Description
<i>interface-type</i> <i>interface-number</i>	Interface (including Ethernet interface, aggregate port, SVI or loopback interface).
<b>description</b>	The description of the interface, including the link status.
<b>switchport</b>	Layer 2 interface information.
<b>trunk</b>	Trunk port, applicable for physical port and aggregate port.

#### Defaults

**Command** Any CLI mode.  
**Mode**

**Usage Guide** This command is used to show all basic information if no parameter is specified.

**Configuration** The following example displays the interface information when the Gi0/17 is a Trunk port.

**Examples**

```
Ruijie#show interfaces gigabitEthernet 0/17
Index(dec):1 (hex):1
GigabitEthernet 0/17 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: 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 Gi0/17 is an Access port.

```
Ruijie#show interfaces gigabitEthernet 0/17
```

```

Index(dec):1 (hex):1
GigabitEthernet 0/17 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 Gi0/17 is a Hybrid port.

```

SwitchA#show interfaces gigabitEthernet 0/17
Index(dec):1 (hex):1
GigabitEthernet 0/17 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 Gi0/17.

```

Ruijie# show interfacesgigabitEthernet 0/17 switchport
Interface Switchport ModeAccess Native Protected VLAN lists
-----
GigabitEthernet 0/17 enabled Access 11 Disabled ALL
    
```

**Related  
Commands**

Command	Description
<b>duplex</b>	Duplex
<b>flowcontrol</b>	Flow control status.
<b>interface gigabitEthernet</b>	Selects the interface and enter the interface configuration mode.
<b>interface aggregateport</b>	Creates or accesses the aggregate port, and enters the interface configuration mode.
<b>interface vlan</b>	Creates or accesses the switch virtual interface (SVI), and enters the interface configuration mode.
<b>shutdown</b>	Disables the interface.



<b>speed</b>	Configures the speed on the port.
<b>switchport priority</b>	Configures the default 802.1q interface priority.
<b>switchport protected</b>	Configures the interface as a protected port.

**Platform** N/A

**Description**

## 1.21 show interfaces counters

Use this command to display the received and transmitted packet statistics.

**show interfaces** [ *interface-type interface-number* ] **counters** [ **increment** | **error** | **rate** | **summary** ]  
[ **up** | **down** ]

Parameter Description	Parameter	Description
	<i>interface-type</i> <i>interface-number</i>	(Optional) The interface type and ID.
	<b>increment</b>	Displays the packet statistics increased during the last sample interval.
	<b>error</b>	Displays error packet statistics.
	<b>rate</b>	Displays packet receiving and transmitting rate.
	<b>summary</b>	Displays packet statistics summary.
	<b>up</b>	(Optional) Displays the port up statistics.
	<b>down</b>	(Optional) Displays the port down statistics.

**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 Examples** The following example displays packet statistics on interface GigabitEthernet 0/17.

```
Ruijie#show interfaces GigabitEthernet 0/17 counters
Interface : GigabitEthernet 0/17
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 0/17 increased during the last sample interval.

```

Ruijie#show interfaces GigabitEthernet 0/17 counters increment
Interface : GigabitEthernet 0/17
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 0/17.

```
Ruijie#show interfaces GigabitEthernet 0/17 counters errors
Interface      UnderSize      OverSize      Collisions      Fragments
-----
Gi0/17         0              0              0              0
Interface      Jabbers        CRC-Align-Err  Align-Err        FCS-Err
-----
Gi0/17         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 0/17.

```
Ruijie#show interface gigabitEthernet 0/17 counters rate
Interface      Sampling Time      Input Rate      Input Rate      Output Rate
Output Rate
                (packets/sec)      (bits/sec)      (packets/sec)      (bits/sec)
-----
Gi0/17         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 0/17.

```
Ruijie#show interface gigabitEthernet 0/17 counters summary
```

Interface	InOctets	InUcastPkts	InMulticastPkts	InBroadcastPkts
Gi0/17	1475788005	1389	45880503	11886621
Interface	OutOctets	OutUcastPkts	OutMulticastPkts	OutBroadcastPkts
Gi0/17	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 Description** N/A

## 1.22 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> <i>interface-number</i>	The interface type and ID.

**Defaults** N/A

**Command Mode** Any CLI 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 0/17.

```
Ruijie# show interfaces GigabitEthernet 0/1 link-state-change statistics
```

Interface	Link state	Link state change times	Last change time
-----	-----	-----	-----
Gi0/17	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** N/A  
**Description**

## 1.23 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> <i>interface-number</i>	The interface type and ID.
	<b>status</b>	Displays interface status information, including speed and duplex.

**Defaults** N/A

**Command Mode** Any CLI mode

**Usage Guide** If you do not specify an interface, the status information of all interfaces is displayed.

**Configuration Examples** The following example displays the status information of interface GigabitEthernet 0/17.

```
Ruijie#show interfaces GigabitEthernet 0/17 status
```

Interface	Status	Vlan	Duplex	Speed	Type
-----	-----	-----	-----	-----	-----

```
GigabitEthernet 0/17    up          1          Full    1000M    copper
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description**

N/A

## 1.24 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>	(Optional) The interface type and ID.
<i>interface-number</i>	


**Defaults**

**Command Mode** Any CLI mode

**Usage Guide** If you do not specify an interface, violation status of all interfaces is displayed.

**Configuration Examples** The following example displays the violation status of interface GigabitEthernet 0/17.

```
Ruijie#show interface gigabitEthernet 0/17 status err-disabled
Interface                Status      Reason
-----
GigabitEthernet 0/17    err-disabled  BPDU Guard
```

 The violation status is displayed as **err-disabled**.

**Related Commands**

Command	Description
N/A	N/A

**Platform Description**

N/A

## 1.25 show interfaces transceiver

Use this command to display transceiver information of the interface.

**show interfaces** [ *interface-type interface-number* ] **transceiver** [ **alarm** | **diagnosis** ]

Parameter Description	Parameter	Description
	<i>interface-type</i> <i>interface-number</i>	The interface type and ID.
	<b>transceiver</b>	Displays the transceiver information.
	<b>alarm</b>	Displays the alarm message of the transceiver. If there is no alarm message, it is displayed as None.
	<b>diagnosis</b>	Displays the diagnostic parameters of the transceiver.

**Defaults** N/A

**Command Mode** Any CLI mode

**Usage Guide** If you do not specify an interface, the transceiver information of all interfaces is displayed. The feature is not supported by G.hn and GigabitEthernet ports.

**Configuration Examples** The following example displays the transceiver information of interface tenGigabitEthernet 0/19.

**Examples** Ruijie# show interfaces tenGigabitEthernet 0/19 transceiver

```
Transceiver Type      : 1000BASE-SX-SFP
Connector Type       : LC
Wavelength(nm)      : 850
Transfer Distance    :
    50/125 um OM2 fiber
    -- 550m
    62.5/125 um OM1 fiber
    -- 270m
Digital Diagnostic Monitoring : YES
Vendor Serial Number   : 101680093602489
```

The following example displays the alarm message of the transceiver of interface tenGigabitEthernet 0/19.

```
Ruijie#show interfaces tenGigabitEthernet 0/19 transceiver alarm
tenGigabitEthernet 0/19 transceiver current alarm information:
RX  loss of signal
```

The following example displays the diagnostic parameters of the transceiver of interface tenGigabitEthernet 0/19.

```
Ruijie#show interfaces tenGigabitEthernet 0/19 transceiver diagnosis
Current diagnostic parameters[AP:Average Power]:
Temp(Celsius)  Voltage(V)      Bias(mA)          RX power(dBm)    TX power(dBm)
```

38 (OK)	3. 20 (OK)	0. 04 (OK)	-40. 00 (alarm) [AP]
-40. 00 (alarm)			

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

**Platform Description** N/A

## 1.26 show interfaces usage

Use this command to display bandwidth usage of the interface.

**show interfaces** [ *interface-type interface-number* ] **usage** [ **up** | **down** ]

<b>Parameter Description</b>	Parameter	Description
	<i>interface-type</i> <i>interface-number</i>	(Optional) The interface type and ID.
	<b>up</b>	(Optional) Displays the port up statistics.
	<b>down</b>	(Optional) Displays the port down statistics.

**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 0/17.

Interface	Bandwidth	Average Usage	Output Usage	Input Usage
-----				
GigabitEthernet 0/17	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.

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



**Platform** N/A

**Description**

## 1.27 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 Mode**

Interface configuration 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.

You need to wait 15 seconds after execution under G.hn port for the chip to be ready

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

**Configuration Examples**

The following example disables an interface.

```
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
<b>clear interface</b>	Resets the hardware.
<b>show interfaces</b>	Displays the interface information.

**Platform** N/A

**Description**

## 1.28 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** Interface configuration mode.

**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** The following example disables the interface from sending LinkTrap on the interface.

**Examples**

```
Ruijie(config)# interface gigabitEthernet 0/17
```

```
Ruijie(config-if-GigabitEthernet 0/17)# no snmp trap link-status
```

The following example enables the interface to forward Link trap.

```
Ruijie(config)# interface gigabitEthernet 0/17
```

```
Ruijie(config-if-GigabitEthernet 0/17)# snmp trap link-status
```

Related Commands	Command	Description
	<b>snmp trap link-status</b>	Enables the interface to send LinkTrap on the interface.
	<b>no snmp trap link-status</b>	Disables the interface from sending LinkTrap on the interface.

**Platform** N/A

**Description**

## 1.29 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

**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

**Platform Description** N/A

## 1.30 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 ]**

Parameter Description	Parameter	Description
		<b>10</b>
	<b>100</b>	The transmission rate of the interface is 100Mbps.
	<b>1000</b>	The transmission rate of the interface is 1000Mbps.
	<b>auto</b>	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.

The feature is not supported by G.hn ports.

**Configuration** The following example sets the speed on interface gigabitethernet 0/17 to 100Mbps.

**Examples**

```
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# speed 100
```

**Related  
Commands**

Command	Description
<b>show interfaces</b>	Displays the interface information.

**Platform** N/A

**Description**

## 1.31 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 0/17 as a static access port and adds it to VLAN 2.

```
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# switchport access vlan 2
```

**Related  
Commands**

Command	Description
<b>switchport mode</b>	Configures the interface as Layer 2 mode (switch port mode).

<b>switchport trunk</b>	Configures a native VLAN and the allowed-VLAN list for the trunkport.
-------------------------	---

**Platform** N/A

**Description**

## 1.32 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
	<b>access</b>	Configures the switch port as an access port.
	<b>trunk</b>	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-if-GigabitEthernet 0/17)# switchport mode trunk
```

Related Commands	Command	Description
	<b>switchport access</b>	Configures an interface as a statics access port and assigns it to a VLAN.
	<b>switchport trunk</b>	Configures a native VLAN and the allowed-VLAN list for the trunk port.

**Platform** N/A

**Description**

## 1.33 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** Interface configuration mode.

### 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** The following example configures interface `gigabitethernet 0/17` as a protected port.

### Examples

```
Ruijie(config)#interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# switchport protected
```

### Related Commands

Command	Description
<b>show interfaces</b>	Displays the interface information.

**Platform** N/A

### Description

## 1.34 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 | only ] vlan-list } | native vlan vlan-id }**

**no switchport trunk { allowed vlan | native vlan }**

### Parameter Description

Parameter	Description
<b>allowed vlan</b> <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

	<p>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.</p> <p>all means that the allowed VLAN list contains all the supported VLANs;</p> <p>add means to add the specified VLAN list to the allowed VLAN list;</p> <p>remove means to remove the specified VLAN list from the allowed VLAN list;</p> <p>except means to add all the VLANs other than those in the specified VLAN list to the allowed VLAN list;</p>
<p><b>native vlan</b> <i>vlan-id</i></p>	<p>Configures the native VLAN.</p>

**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 removes port 0/17 from VLAN 2.

**Examples**

```
Ruijie(config)# interface GigabitEthernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# switchport trunk allowed vlan remove 2
Ruijie(config-if-GigabitEthernet 0/17)# end
Ruijie# show interfaces GigabitEthernet 0/17 switchport
Switchport is enabled
Mode is trunk port
Access vlan is 1,Native vlan is 1
Protected is disabled
Vlan lists is
1,3-4094
```

**Related Commands**

Command	Description
<b>show interfaces</b>	Displays the interface information.

<b>switchport access</b>	Configures an interface as a statics access port and assigns it to a VLAN.
--------------------------	--

**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	<b>dynamic</b>	Clears all the dynamic MAC addresses.
	<b>address</b> <i>mac-address</i>	Clears the specified dynamic MAC address.
	<b>interface</b> <i>interface-id</i>	Clears all the dynamic MAC addresses of the specified interface.
	<b>vlan</b> <i>vlan-id</i>	Clears all the dynamic MAC addresses of the specified VLAN, in the range from 1 to 4094.

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** Use the **show mac-address-table dynamic** command to display all the dynamic MAC addresses.

**Configuration** The following command clears all the dynamic MAC addresses.

**Examples** Ruijie# clear mac-address-table dynamic

Related	Command	Description
Commands	<b>show mac-address-table dynamic</b>	Displays dynamic MAC address.

**Platform Description** N/A

### 2.2 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
-----------	-----------	-------------

<b>Description</b>	N/A					
<b>Defaults</b>	The address learning function is enabled.					
<b>Command Mode</b>	Interface configuration mode.					
<b>Usage Guide</b>	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.					
<b>Configuration Examples</b>	The following example disables the port address learning function.					
<b>Examples</b>	<pre>Ruijie(config-if-GigabitEthernet 0/1)# no mac-address-learning</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					

## 2.3 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 Description	Parameter	Description
	<b>enable</b>	Enables MAC address learning globally.
	<b>disable</b>	Disables MAC address learning globally.

<b>Defaults</b>	The <b>mac-address-learning enable</b> command is enabled by default.
<b>Command Mode</b>	Global configuration mode
<b>Usage Guide</b>	When this function is enabled, the MAC address is learned in global configuration mode the same as learned in interface configuration mode.
<b>Configuration Examples</b>	The following example disables MAC address learning globally.
<b>Examples</b>	<pre>Ruijie(config)# mac-address-learning disable</pre>

Related	Command	Description
Commands	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	Parameter	Description
Description	<i>seconds</i>	Aging time of the dynamic MAC address (in seconds). The range is from 10 to 630. The value can be set to 0, indicating no aging.

**Defaults** The default is 300.

**Command Mode** Global configuration mode.

**Usage Guide** Use **show mac-address-table aging-time** to display configuration.

**Configuration Examples** The following example sets the aging time of the dynamic MAC address to 500 seconds.

```
Ruijie(config)# mac-address-table aging-time 500
```

Related	Command	Description
Commands	<b>show mac-address-table aging-time</b>	Displays the aging time of the dynamic MAC address.
	<b>show mac-address-table dynamic</b>	Displays dynamic MAC address.

**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 1.

**Examples** Ruijie(config)#mac-address-table filtering 0000.0202.0303 vlan 3

Related Commands	Command	Description
	<b>clear mac-address-table filtering</b>	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	<b>interval</b> <i>value</i>	Sets the interval of sending the MAC address trap message, 1 second by default.
	<b>history-size</b> <i>value</i>	Sets the maximum number of the entries in the MAC address notification table, 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
<b>snmp-server enable traps</b>	Sets the method of handling the MAC address trap message.
<b>show mac-address-table notification</b>	Displays the MAC address notification configuration and the MAC address trap notification table.
<b>snmp trap mac-notification</b>	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-address* **vlan** *vlan-id* **interface** *interface-id*

**default mac-address-table static** *mac-address* **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 Examples** N/A

Related Commands	Command	Description
	<b>show mac-address-table static</b>	Displays the static MAC address.

**Platform Description** N/A

## 2.8 max-dynamic-mac-count

Use this command to set the maximum number of MAC address learned dynamically on the VLAN or interface. Use the **no** or **default** form of this command to restore the default setting.

- max-dynamic-mac-count** *num*
- no max-dynamic-mac-count**
- default max-dynamic-mac-count**

Parameter Description	Parameter	Description
	<i>num</i>	Sets the maximum number of MAC addresses. The range is from 1 to 16000.

**Defaults** The maximum number is not set by default.

**Command Mode** VLAN configuration mode / Interface configuration mode

**Usage Guide** This command is used to set the maximum number of MAC addresses learned dynamically on the VLAN or interface.

If the number of MAC addresses dynamically learned on the VLAN or interface reaches the upper limit, MAC address learning is disabled on the VLAN or interface.

If the number of MAC addresses reaches the upper limit when this command is configured, the surplus MAC addresses are not cleared. Instead, they remain and then age. MAC address learning is disabled on the VLAN or interface.

Use the **show mac-address-table max-dynamic-mac-count** command to display the maximum number of MAC addresses learned dynamically on the VLAN or interface.

**Configuration Examples** The following example sets the maximum number of MAC addresses dynamically learned on interface GigabitEthernet 0/17.

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#interface GigabitEthernet 0/17
```

```
Ruijie(config-if-GigabitEthernet 0/17)#max-dynamic-mac-count 160
```

Related Commands	Command	Description
	N/A	N/A

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

## 2.9 show mac-address-learning

Use this command to display the MAC address learning.

### show mac-address-learning

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** All modes.

**Usage Guide** N/A

**Configuration Examples** The following example displays the MAC address learning.

```
Ruijie#show mac-address-learning
Ghn 0/1          learning ability: enable
Ghn 0/2          learning ability: enable
Ghn 0/3          learning ability: enable
Ghn 0/4          learning ability: enable
Ghn 0/5          learning ability: enable
Ghn 0/6          learning ability: enable
Ghn 0/7          learning ability: enable
Ghn 0/8          learning ability: enable
Ghn 0/9          learning ability: enable
Ghn 0/10         learning ability: enable
Ghn 0/11         learning ability: enable
Ghn 0/12         learning ability: enable
Ghn 0/13         learning ability: enable
Ghn 0/14         learning ability: enable
Ghn 0/15         learning ability: enable
Ghn 0/16         learning ability: enable
GigabitEthernet 0/17 learning ability: enable
GigabitEthernet 0/18 learning ability: enable
TenGigabitEthernet 0/19 learning ability: enable
```

```
AggregatePort 1      learning ability: enable
Ruijie#
```

Related Commands	Command	Description
	N/A	N/A

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

## 2.10 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-address ] [ interface interface-id ] [ vlan vlan-id ]
```

Parameter Description	Parameter	Description
	address <i>mac-address</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** N/A

**Configuration Examples** The following example displays the MAC address.

```
Ruijie# show mac-address-table
```

Vlan	MAC Address	Type	Interface	Live Time
1	00d0.f800.1001	STATIC	GigabitEthernet 0/17	-

Vlan	MAC Address	Type	Interface	Live Time
1	00d0.f800.1001	STATIC	GigabitEthernet 0/17	-
1	00d0.f800.1002	DYNAMIC	GigabitEthernet 0/17	-
1	00d0.f800.1003	OTHER	GigabitEthernet 0/17	-
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.
Live Time	The live time of MAC address.

Related Commands	Command	Description
	N/A	N/A

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

## 2.11 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 Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** All modes.

**Usage Guide** N/A

**Configuration Examples** The following example displays the aging time of the dynamic MAC address.

```
Ruijie# show mac-address-table aging-time
Aging time : 300
```

Related Commands	Command	Description
	<b>mac-address-table aging-time</b>	Sets the aging time of the dynamic MAC address.

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

## 2.12 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 Description	Parameter	Description
	<b>interface</b> <i>interface-id</i>	Interface ID
	<b>vlan</b> <i>vlan-id</i>	VLAN ID, in the range from 1 to 4094.

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** The **show mac-address-table count** command is used to display the number of entries based on the type of MAC address entry.

The **show mac-address-table count interface** command is used to display the number of entries based on the interface associated with the MAC address entry.

The **show mac-address-table count vlan** command is used to display the number of entries based on the VLAN of MAC address entries.

**Configuration** The following example displays the number of MAC address entries.

**Examples**

```
Ruijie#show mac-address-table count
Dynamic Address Count : 0
Static Address Count : 0
Filtering Address Count: 1
Other Address Count : 0
Total Mac Addresses : 1
Total Mac Address Space Available: 16383
```

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
Other Address Count : 0
Total Mac Addresses : 7
```

The following example displays the number of MAC addresses on interface gi 0/17.

```
Ruijie# show mac-address-table count interface gi 0/17
Dynamic Address Count : 10
Static Address Count : 0
Filter Address Count : 0
Other Address Count : 0
Total Mac Addresses : 10
```

Field	Discription
Dynamic Address Count	Number of dynamic addresses
Static Address Count	Number of static addresses
Filter Address Count	Number of filter addresses
Other Address Count	Number of other addresses
Total Mac Addresses	Number of total MAC addresses

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

<b>Commands</b>	<b>show mac-address-table static</b>	Displays the static address.
	<b>show mac-address-table filtering</b>	Displays the filtering address.
	<b>show mac-address-table dynamic</b>	Displays the dynamic address.
	<b>show mac-address-table address</b>	Displays all the address information of the specified address.
	<b>show mac-address-table interface</b>	Displays all the address information of the specified interface.
	<b>show mac-address-table vlan</b>	Displays all the address information of the specified vlan.

**Platform** N/A

**Description**

## 2.13 show mac-address-table dynamic

Use this command to display the dynamic MAC address.

**show mac-address-table dynamic** [ **address** *mac-add r*] [ **interface** *interface-id*] [ **vlan** *vlan-id*]

Parameter	Parameter	Description
<b>Description</b>	<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	Live Time
1	0000.0000.0001	DYNAMIC	gigabitethernet 0/17	1d 00:19:00
1	0001.960c.a740	DYNAMIC	gigabitethernet 0/17	1d 00:28:00
1	0007.95c7.dff9	DYNAMIC	gigabitethernet 0/17	1d 00:38:00
1	0007.95cf.eee0	DYNAMIC	gigabitethernet 0/17	1d 00:42:00
1	0007.95cf.f41f	DYNAMIC	gigabitethernet 0/17	1d 00:45:00
1	0009.b715.d400	DYNAMIC	gigabitethernet 0/17	1d 00:58:00
1	0050.bade.63c4	DYNAMIC	gigabitethernet 0/17	1d 00:59:00

Field	Description
Vlan	The interface address.

	MAC Address	The MAC address.
	Type	The MAC address type.
	Interface	The interface corresponding to the MAC address.
	Live Time	The live time of MAC address.
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>clear mac-address-table dynamic</b>	Clears the dynamic MAC address.

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

## 2.14 show mac-address-table filtering

Use this command to display the filtering MAC address.

**show mac-address-table filtering [ address *mac-address* ] [ vlan *vlan-Id* ]**

<b>Parameter Description</b>	<b>Parameter</b>	<b>Description</b>
	<i>mac-address</i>	Destination MAC address of the entry
	<i>vlan-id</i>	VLAN ID of the entry, in the range from 1 to 4094.

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays the filtering MAC address.

```
Ruijie# show mac-address-table filtering
Vlan   MAC Address   Type   Interface   Live Time
-----
1      0000.2222.2222  FILTER Not available  -
```

Field	Description
Vlan	The interface address.
MAC Address	The MAC address.
Type	The MAC address type.
Interface	The interface corresponding to the MAC address.
Live Time	The live time of MAC address.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>mac-address-table filtering</b>	Configures the filtering MAC address.

**Platform** N/A

**Description**

## 2.15 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
<b>Description</b>	<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.

**Mode**

**Usage Guide** N/A

**Configuration Examples** The following example displays all the MAC addresses on interface gigabitethernet 0/17.

**Examples**

```
Ruijie# show mac-address-table interface gigabitethernet 0/17
Vlan  MAC Address  Type  Interface          Live Time
-----
1     00d0.f800.1001  STATIC  gigabitethernet 0/17  -
1     00d0.f800.1002  STATIC  gigabitethernet 0/17  -
1     00d0.f800.1003  STATIC  gigabitethernet 0/17  -
1     00d0.f800.1004  STATIC  gigabitethernet 0/17  -
```

Field	Description
Vlan	The interface address.
MAC Address	The MAC address.
Type	The MAC address type.
Interface	The interface corresponding to the MAC address.
Live Time	The live time of MAC address.

**Related Commands**

Command	Description
<b>show mac-address-table static</b>	Displays the static MAC address.
<b>show mac-address-table filtering</b>	Displays the filtering MAC address.
<b>show mac-address-table dynamic</b>	Displays the dynamic MAC address.
<b>show mac-address-table address</b>	Displays all types of MAC addresses.

<b>show mac-address-table vlan</b>	Displays all types of MAC addresses of the specified VLAN.
<b>show mac-address-table count</b>	Displays the address counts in the MAC address table.

**Platform** N/A

**Description**

## 2.16 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
<b>Description</b>	<b>interface</b>	Displays the MAC address notification configuration on all interfaces.
	<b>interface</b> <i>interface-id</i>	Displays the MAC address notification configuration on a specific interface.
	<b>history</b>	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
```

Related	Command	Description
<b>Commands</b>	<b>mac-address-table notification</b>	Enables MAC address notification.
	<b>snmp trap mac-notification</b>	Enables the MAC address trap notification function on the specified interface.

**Platform** N/A

**Description**

## 2.17 show mac-address-table static

Use this command to display the static MAC address.

**show mac-address-table static** [**address** *mac-address*] [**interface** *interface-Id*] [**vlan** *vlan-id*]

Parameter	Parameter	Description
Description	<i>mac-address</i>	Destination MAC address of the entry
	<i>vlan-id</i>	VLAN ID of the entry, within the range from 1 to 4094.
	<i>interface-id</i>	Interface of the entry physical interface or aggregate port

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays the static MAC addresses

```
Ruijie# show mac-address-table static
Vlan    MAC Address    Type    Interface    Live Time
-----
1 00d0.f800.1001  STATIC  gigabitethernet 0/17 -
1 00d0.f800.1002  STATIC  gigabitethernet 0/17 -
1 00d0.f800.1003  STATIC  gigabitethernet 0/17 -
```

Field	Description
Vlan	The interface address.
MAC Address	The MAC address.
Type	The MAC address type.
Interface	The interface corresponding to the MAC address.
Live Time	The live time of MAC address.

Related Commands	Command	Description
	<b>mac-address-table static</b>	Configures the static MAC address.

**Platform** N/A

**Description**

## 2.18 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, in 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          Live Time
-----
1     00d0.f800.1001  STATIC gigabitethernet 0/17 -
1     00d0.f800.1002  STATIC gigabitethernet 0/17 -
1     00d0.f800.1003  STATIC gigabitethernet 0/17 -
    
```

Field	Description
Vlan	The interface address.
MAC Address	The MAC address.
Type	The MAC address type.
Interface	The interface corresponding to the MAC address.
Live Time	The live time of MAC address.

Related Commands	Command	Description
	<b>show mac-address-table static</b>	Displays static addresses.
	<b>show mac-address-table filtering</b>	Displays filtered addresses.
	<b>show mac-address-table dynamic</b>	Displays dynamic addresses.
	<b>show mac-address-table address</b>	Displays all address information about the specified address.
	<b>show mac-address-table interface</b>	Displays all address information about the specified interface.
	<b>show mac-address-table count</b>	Displays the number of addresses in the address table.

**Platform Description** N/A



## 2.19 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** The following example enables the MAC address trap notification on interface gigabitethernet 0/17.

### Examples

```
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# snmp trap mac-notification added
```

Related	Command	Description
Commands	<b>mac-address-table notification</b>	Enables MAC address notification.
	<b>show mac-address-table notification</b>	Displays the MAC address notification configuration and the MAC address notification table.

**Platform** N/A

### Description

## 3 Aggregate Port Commands

### 3.1 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-mac | src-mac | src-dst-mac | dst-ip | src-ip | src-dst-ip | dst-l4port | src-dst-l4port | src-l4port | src-port }**

**no aggregateport load-balance**

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

<b>Description</b>	<b>dst-mac</b>	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.
	<b>src-mac</b>	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.
	<b>src-dst-ip</b>	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.
	<b>dst-ip</b>	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.
	<b>src-ip</b>	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.
	<b>src-dst-mac</b>	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.
	<b>dst-l4port</b>	Load balance based on the L4 destination port number.
	<b>src-dst-l4port</b>	Load balance based on the L4 source port number and L4 destination port number.
	<b>src-l4port</b>	Load balance based on the L4 source port number.
	<b>src-port</b>	Load balance based on the source port.

**Defaults** The default load balance mode is **src-dst-mac**.

**Command Mode** Global configuration mode

**Usage Guide** To restore the default settings, run the **no aggregateport load-balance** command in global configuration mode.  
The feature is not supported by G.hn ports.

**Configuration Examples** The following example configures a load-balance algorithm globally based on the destination MAC address.

```
Ruijie(config)# aggregateport load-balance dst-mac
```

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

<b>Commands</b>	<b>show aggregateport load-balance</b>	Displays aggregate port configuration.
-----------------	--	--

**Platform** N/A

**Description**

## 3.2 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
<b>Description</b>	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**

## 3.3 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
<b>Description</b>	<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)# interface aggregateport 5
Ruijie(config-if-Aggregateport 5)# end
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** N/A

### 3.4 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>	The LACP port priority, in the range from 0 to 65535.

**Defaults** The default is 32768.

**Command Mode** Interface configuration mode

**Usage Guide** N/A  
The feature is not supported by G.hn ports.

**Configuration Examples** This example sets the LACP port priority of interface Gi0/17 to 4096.

```
Ruijie(config)# interface gigabitEthernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# lacp port-priority 4096
```

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

**Platform Description** N/A

### 3.5 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**

<b>Parameter Description</b>	Parameter	Description
	N/A	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.  
 The G.hn port does not support this function.

**Configuration Examples** The following example configures the short-timeout mode for the LACP AP member port.

```
Ruijie(config)# interface gigabitEthernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# lacp short-timeout
```

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

**Platform Description** N/A

### 3.6 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 Examples** The following example sets the LACP system priority to 4096.

```
Ruijie(config)# lacp system-priority 4096
```

Related Commands	Command	Description
	<b>port-group</b> <i>key mode</i> { <b>active</b>   <b>passive</b> }	Enables the LACP on the port and specifies the aggregation group ID and operation mode.
	<b>lacp port-priority</b>	Sets the LACP port priority.

**Platform** N/A

#### Description

### 3.7 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 Description	Parameter	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.
<b>active</b>	Places a port into an active negotiating state, in which the port initiates negotiations with remote ports by sending LACP packets.
<b>passive</b>	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.  
The feature is not supported by G.hn ports.

**Configuration** The following example specifies the Ethernet interface 0/17 as a member of the static AP 3.

**Examples**

```
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# port-group 3
```

The following example specifies the Ethernet interface 0/17 as a member of the LACP AP4 and set the aggregation mode to active.

```
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# port-group 4 mode active
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

### 3.8 show aggregateport

Use this command to display the aggregate port configuration.

**show aggregateport** { [ *aggregate-port-number* ] **summary** | **load-balance** }

Parameter Description	Parameter	Description
	<i>aggregate-port-number</i>	Number of the aggregate port.
	<b>load-balance</b>	Displays the load-balance algorithm on the aggregate port.
	<b>summary</b>	Displays the summary of the aggregate port.

**Defaults** N/A

**Command** Any mode

**Mode**

**Usage Guide** If the aggregate port number is not specified, all the aggregate port information will be displayed.

**Configuration** The following example displays the aggregate port configuration.

**Examples**

```
Ruijie# show aggregateport 1 summary
AggregatePort MaxPorts SwitchPort Mode Ports
-----
Ag1           8      Enabled  ACCESS Gi0/17
```

Related Commands	Command	Description
	<b>aggregateport load-balance</b>	Configures a load-balance algorithm of AP.

**Platform** N/A

**Description**

### 3.9 show lacp summary

Use this command to display the LACP aggregation information.

**show lacp summary [ key ]**

Parameter Description	Parameter	Description
	<i>key</i>	Specifies the aggregation group id to show. If it is not specified, all aggregation group information is displayed by default.

**Defaults** N/A

**Command Mode** Any mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays the LACP aggregation information.

```
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:
Port          Flags    State    LACP port  Oper  Port  Port
Port          Flags    State    Priority   Key   Number State
-----
Gi0/17       SA      bndl     4096       0x3   0x1   0x3d
```



Gi0/18	SA	bndl	4096	0x3	0x2	0x3d
Partner information:						
		LACP port		Oper	Port	Port
Port	Flags	Priority	Dev ID	Key	Number	State
-----						
Gi0/17	SA	61440	00d0.f800.0002	0x3	0x1	0x3d
Gi0/18	SA	61440	00d0.f800.0002	0x3	0x2	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
<b>port-group key mode</b>	Enables the LACP on the port and specifies the aggregation group ID and operation mode.

**Platform Description**

N/A

## 4 VLAN Commands

### 4.1 add interface

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.
	<b>range</b> <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 0/17 to VLAN20.

```
Ruijie# configure terminal
SwitchA(config)#vlan 20
SwitchA(config-vlan)#add interface GigabitEthernet 0/17
Ruijie# show interface GigabitEthernet 0/17 switchport
Interface  Switchport  Mode  Access  Native  Protected  VLAN lists
-----  -
GigabitEthernet 0/17  enabled  ACCESS  20  1  Disabled  ALL
```

The following example adds the interface range GigabitEthernet 0/17-18 to VLA1200.

```
Ruijie# configure terminal
SwitchA(config)#vlan 100
SwitchA(config-vlan)#add interface range GigabitEthernet 0/17-18
```

```
Ruijie# show vlan
Ruijie#show vlan
VLAN      Name                               Status  Ports
-----
          1 VLAN0001                        STATIC  Ghn0/1, Ghn0/2, Ghn0/3, Ghn0/4
                                                Ghn0/5, Ghn0/6, Ghn0/7, Ghn0/8
                                                Ghn0/9, Ghn0/10, Ghn0/11, Ghn0/12
                                                Ghn0/13, Ghn0/14, Ghn0/15, Ghn0/16
                                                Te0/19, Ag5, Ag2
          20 VLAN0020                    STATIC
          100 VLAN0100                   STATIC  Gi0/17, Gi0/18
          4094 VLAN4094                   STATIC  Ag1
```

The following example adds the AggregatePort10 to VLAN20.

```
Ruijie# configure terminal
SwitchA(config)#vlan 20
SwitchA(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
<b>show interface switchport</b>	Displays the layer-2 interfaces.

**Platform** N/A

**Description**

## 4.2 interface vlan

Use this command to create a Switch Virtual Interface and enter the SVI configuration mode.

**interface vlan** *vlan-id*

**Parameter Description**

Parameter	Description
<i>vlan-id</i>	VLAN ID

**Defaults** By default, no SVI is configured.

**Command** Global configuration mode

**Mode**

**Usage Guide** N/A

**Configuration** The following example enters the SVI configuration mode on VLAN 1.

**Examples**

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

Related Commands	Command	Description
	N/A	N/A

## 4.3 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
	<b>show vlan</b>	

**Platform Description** N/A

## 4.4 show vlan

Use this command to display member ports of the VLAN.

**show vlan [ id *vlan-id* ]**

Parameter Description	Parameter	Description
	id <i>vlan-id</i>	VLAN ID

**Defaults** N/A

**Command mode** All modes

**Usage Guide** N/A

**Configuration Examples** The following command displays the status of VLAN 20.

```
Ruijie(config-vlan)#show vlan id 20
VLAN Name                Status    Ports
-----
 20 VLAN0020              STATIC    Ag10
```

The following command displays the status of all VLANs.

```
Ruijie(config-vlan)#show vlan
VLAN    Name                Status    Ports
-----
 1 VLAN0001          STATIC    Ghn0/1, Ghn0/2, Ghn0/3, Ghn0/4
                                                Ghn0/5, Ghn0/6, Ghn0/7, Ghn0/8
                                                Ghn0/9, Ghn0/10, Ghn0/11, Ghn0/12
                                                Ghn0/13, Ghn0/14, Ghn0/15, Ghn0/16
                                                Te0/19, Ag5, Ag2
 10 vlan10           STATIC
 20 VLAN0020         STATIC    Ag10
 100 VLAN0100        STATIC    Gi0/17, Gi0/18, Ag1, Ag8
 4094 VLAN4094       STATIC
```

Related Commands	Command	Description
	name	VLAN name.

**Platform Description** N/A

## 4.5 switchport access vlan

Use this command to configure an interface as a static access port and assign it to a VLAN. Use the **no** 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.

**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 port to the VLAN. If the port is a trunk port, the operation does not take effect.

**Configuration Examples**

```
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# switchport access vlan 2
```

Related Commands	Command	Description
	<b>switchport mode</b>	Specifies the interface as Layer 2 mode (switch port mode).

**Platform Description** N/A

## 4.6 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** }

**no switchport mode**

**default switchport mode**

Parameter Description	Parameter	Description
	<b>access</b>	Configures the switch port as an access port.

<b>trunk</b>	Configures the switch port as a trunk 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.

**Configuration** The following example configures port 17 as an access port.

**Examples**

```
Ruijie(config)#interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# switchport
Ruijie(config-if-GigabitEthernet 0/17)# switchport mode access
```

The following example configures port 17 as a trunk port.

```
Ruijie(config)#interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# switchport
Ruijie(config-if-GigabitEthernet 0/17)# switchport mode trunk
```

**Related Commands**

Command	Description
<b>switchport</b>	Configures a Layer 2 interface.

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

## 4.7 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
<b>all</b>	Adds the trunk/uplink port to all VLANs.
<b>add</b> <i>vlan-list</i>	Adds the trunk/uplink port to the specified VLAN.
<b>remove</b> <i>vlan-list</i>	Removes the trunk/uplink port from the specified VLAN.
<b>except</b> <i>vlan-list</i>	Removes the trunk/uplink port from the specified VLAN and adds the

	port to all the other VLANs.
<b>only</b> <i>vlan-list</i>	Adds the trunk/uplink port to the specified VLAN and removes the port from the VLANs not on the VLAN list.

**Defaults** The trunk port is in all VLANs by default.

**Command mode** Interface configuration mode.

**Usage Guide** A trunk 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** The following example removes trunk port GigabitEthernet 0/17 from VLAN 2.

**Examples**

```
Ruijie(config)# interface gigabitEthernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/17)# switchport trunk allowed vlan remove 2
```

The following example removes trunk port GigabitEthernet 0/17 from VLAN 2.

```
Ruijie(config)# interface gigabitEthernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# switchport trunk allowed vlan except 10
```

**Related Commands**

Command	Description
<b>switchport mode</b>	Specifies an interface as a Layer 2 interface (switch port mode).

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

## 4.8 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>	Native VLAN ID.

**Defaults** By default, the native VLAN for the trunk/uplink port is VLAN 1.

**Command** Interface configuration mode



**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** The following example configures VLAN 10 as the native VLAN for trunk port GigabitEthernet 0/17.

**Examples**

```
Ruijie(config)#interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/17)# switch trunk native vlan 10
```

The following example configures VLAN 10 as the native VLAN for unlinK port GigabitEthernet 0/17.

```
Ruijie(config)#interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# switchport mode uplink
Ruijie(config-if-GigabitEthernet 0/17)# switch trunk native vlan 10
```

**Related Commands**

Command	Description
<b>switchport mode</b>	Specifies an interface as a Layer 2 interface (switch port mode).

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

## 4.9 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.
<b>range</b> <i>vlan-range</i>	VLAN ID range.

**Defaults** The default is static VLAN.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration** The following example creates VLAN 10.

**Examples**

```
Ruijie(config)# vlan 10
```

```
Ruijie(config-vlan)#
```

**Related  
Commands**

Command	Description
<b>show vlan</b>	Displays member ports of the VLAN.

**Platform  
Description**

N/A

## 5 Protocol VLAN Commands(beta)

### 5.1 protocol-vlan ipv4 mask vlan

Use this command to configure VLAN for the specified subnet.

**protocol-vlan ipv4** *address mask address vlan vlan-id*

Use this command to remove VLAN configuration for the specified subnet.

**no protocol-vlan ipv4** *address mask address*

Use this command to remove VLAN configuration for all subnets.

**no protocol-vlan ipv4**

Parameter Description	Parameter	Description
	<b>ipv4</b> <i>address</i>	IP address in the A.B.C.D format.
	<b>mask</b> <i>mask</i>	IP subnet mask in the A.B.C.D format.
	<b>vlan</b> <i>vlan-id</i>	VLAN ID. The value ranges from 1 to 4094.

**Defaults** It is disabled by default.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example configures VLAN 100 for the specified subnet.

```
Ruijie(config)# protocol-vlan ipv4 192.168.100.3 mask 255.255.255.0 vlan 100
```

Related Commands	Command	Description
	<b>show protocol-vlan ipv4</b>	N/A

**Platform** N/A

**Description**

### 5.2 protocol-vlan ipv4

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

**protocol vlan ipv4**

**no protocol vlan ipv4**

Parameter Description	Parameter	Description
	N/A	N/A

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

**Command mode** Interface configuration mode.

**Usage Guide** An interface must work in Trunk/Hybrid mode.  
The feature is not supported by G.hn ports.

**Configuration** The following example enables the subnet VLAN.

**Examples**

```
Ruijie(config)# interface GigabitEthernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# switchport
Ruijie(config-if-GigabitEthernet 0/17)# switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/17)# protocol-vlan ipv4
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 5.3 protocol-vlan profile

Use this command to configure the profile for the VLAN.

**protocol-vlan profile** *number* **frame-type** { **EtherII** *ether-type type* | **SNAP** *ether-type type* | **LLC** **dsap** *value* **ssap** *value* }

Use this command to delete the specified profile.

**no protocol-vlan profile** *number*

Use this command to delete all profiles.

**no protocol-vlan profile**

Parameter Description	Parameter	Description
	<b>profile</b> <i>number</i>	Profile indexes. The value ranges from 1 to 16.
	<b>frame-type</b>	Type of message, including <b>EtherII</b> , <b>SNAP</b> and <b>LLC</b> .
	<b>ether-type</b> <i>type</i>	Type of Ethernet II or SNAP. The value ranges from 1501 to 65535.
	<b>dsap</b> <i>value</i> <b>ssap</b> <i>value</i>	Service access point type. The value ranges from 0 to 255.

**Defaults** It is disabled by default.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration** The following example configures the profile for the VLAN.

```
Ruijie(config)# protocol-vlan profile 1 frame-type ETHERII ether-type aarp
Ruijie(config)# protocol-vlan profile 2 frame-type LLC DSAP 255 SSAP 255
```

Related Commands	Command	Description
		show protocol-vlan

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

## 5.4 protocol-vlan profile vlan

Use this command to apply some profile to an interface.

**protocol-vlan profile** *number* **vlan** *vlan-id*

Use this command to clear the specified profile on the port.

**no protocol-vlan profile** *number*

Use this command to clear all profiles on the port.

**no protocol-vlan profile**

Parameter Description	Parameter	Description	
		<i>number</i>	Profile indexes. The value ranges from 1 to 16.
		<i>vlan id</i>	VLAN ID. The value ranges from 1 to 4094.

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

**Command mode** Interface mode.

**Usage Guide** The interface must be in Trunk or Hybrid mode.  
 The feature is not supported by G.hn ports.

**Configuration** The following example applies profile 1 to VLAN 101.

```
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# protocol-vlan profile 1 vlan 101
```

Related Commands	Command	Description
		<b>show protocol-vlan</b>

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

## 5.5 show protocol-vlan

Use this command to display a protocol VLAN.

**show protocol-vlan [ profile [ number ] | ipv4 ]**

Parameter Description	Parameter	Description
		<b>profile [ number ]</b>
	<b>ipv4</b>	Display the VLAN for the specified subnet.

**Defaults** N/A

**Command mode** Privileged EXEC mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays the configuration of protocol VLAN.

```
Ruijie#show protocol-vlan

ip          mask          vlan
-----
1.2.1.0    255.255.255.0    5

interface          ipv4 status
-----
Gi0/17             enable

profile frame-type      ether-type/DSAP+SSAP  interface  vlan
-----
1      ETHERII      0x5fa                                Gi0/17    12
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform  
Description**

## 6 Private VLAN Commands(beta)

### 6.1 debug bridge pvlan

Use this command to enable private VLAN debugging. Use the **no** or **default** form of this command to restore the default setting.


**debug bridge pvlan**  
**no debug bridge pvlan**


Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** Debugging is disabled by default.

**Command mode** Privileged EXEC mode

**Usage Guide** Debugging information includes error and prompt messages appearing during private VLAN configuration.  
 This command can be used to troubleshoot VLAN and interface configuration failure.

 With private VLAN debugging enabled, all super VLAN configuration and packet processing on SVI is displayed.

 Debugging information helps troubleshooting and fault location.

**Configuration** The following example enables private VLAN debugging.

**Examples** Ruijie# debug bridge pvlan

The following example disables private VLAN debugging.

Ruijie# no debug bridge pvlan

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

### 6.2 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
	<b>community</b>	Sets the community VLAN.
	<b>isolated</b>	Sets the isolated VLAN.
	<b>primary</b>	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**

### 6.3 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** { [ **add** ] *secondary-vlan-list* | **remove** *secondary-vlan-list* }  
**no private-vlan association**  
**default private-vlan association**

Parameter Description	Parameter	Description
	<b>add</b> <i>secondary-vlan-list</i>	Adds the associated secondary VLAN.
	<b>remove</b> <i>secondary-vlan-list</i>	Removes the associated secondary VLAN.

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

**Command mode** VLAN configuration Mode.

**Usage Guide** N/A

**Configuration Examples** The following example associates the secondary VLAN with the primary VLAN on layer 2.

```
Ruijie(config)# vlan 22
Ruijie(config-vlan)# private-vlan association add 24-26
```

The following example removes the association between the secondary VLAN with the primary VLAN.

```
Ruijie(config)# vlan 22
Ruijie(config-vlan)# private-vlan association remove 24
```

Related Commands	Command	Description
	<b>show vlan private-vlan</b>	N/A

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

### 6.4 private-vlan mapping

Use this command to associate the secondary VLAN with the primary VLAN on layer 3. Use the **no** or **default** form of this command to restore the default setting.

**private-vlan mapping** { [ **add** ] *secondary-vlan-list* | **remove** *secondary-vlan-list* }  
**no private-vlan mapping**  
**default private-vlan mapping**

Parameter Description	Parameter	Description
	[ <b>add</b> ] <i>secondary-vlan-list</i>	Adds the associated secondary VLAN.
	<b>remove</b> <i>secondary-vlan-list</i>	Removes the associated secondary VLAN.

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

**Command mode** The interface mode corresponding to the primary VLAN

**Usage Guide** N/A

**Configuration Examples** The following example associates the secondary VLAN with the primary VLAN on layer 3.

```
Ruijie(config)# interface vlan 22
Ruijie(config-if-VLAN 22)# private-vlan mapping add 24-26
```

Related Commands	Command	Description
	<b>show vlan private-vlan</b>	N/A

**Platform Description** N/A

## 6.5 show vlan private-vlan

Use this command to display the private VLAN configuration.

**show vlan private-vlan** [ **community** | **primary** | **isolated** ]

Use this command to display all the private VLANs configuration.

**show vlan private-vlan**

Parameter Description	Parameter	Description
	<b>primary</b>	Displays the primary VLAN information.
	<b>community</b>	Displays the community VLAN information.
	<b>isolated</b>	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
30	primary	inactive	Enabled		
31	isolated	inactive	Disabled		No Association
90	primary	active	Disabled		91-92
91	isolated	active	Disabled		90
92	community	active	Disabled	Gi0/17	90

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** N/A

## 6.6 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**

**default switchport mode**

**Parameter Description**

Parameter	Description
<b>host</b>	Host mode of the private VLAN
<b>promiscuous</b>	Promiscuous mode of the private VLAN

**Defaults** The port is an access port by default.

**Command mode** Interface configuration mode.

**Usage Guide** Before a port is configured as an isolated port or promiscuous port, and the port mode must be configured as the host port mode.

The port mode must be configured as the promiscuous mode.

**Configuration** The following example applies the private host mode to the interface.

**Examples**

```
Ruijie(config)# interface gigabitEthernet0/17
Ruijie(config-if-GigabitEthernet 0/17)# switchport mode private-vlan host
```

The following example applies the promiscuous mode to the interface.

```
Ruijie(config)# interface gigabitEthernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)#sw mode private-vlan promiscuous
```

**Related Commands**

Command	Description
<b>show vlan private-vlan</b>	N/A

**Platform** N/A

**Description**

## 6.7 switchport private-vlan association trunk

Use this command to configure the trunk port as an isolated trunk port and associate it with a primary VLAN and its associated isolated VLAN on layer 2. Use the **no** or **default** form of this command to restore the default settings.

**switchport private-vlan association trunk** *primary-vlan-id isolated-vlan-id*

**no switchport private-vlan association trunk** [*primary-vlan-id isolated-vlan-id*]

**default switchport private-vlan association trunk** [*primary-vlan-id isolated-vlan-id*]

**Parameter Description**

Parameter	Description
<i>primary-vlan-id</i>	The ID of the primary VLAN associated with an isolated VLAN. The VLAN ID ranges from 2 to 4094.
<i>isolated-vlan-id</i>	The ID of the isolated VLAN associated with a primary VLAN. The VLAN ID ranges from 2 to 4094.

**Defaults** The trunk port is not an isolated trunk port and associated with no VLAN by default.

**Command mode** Interface configuration mode.

**Usage Guide** Configure a trunk port as an isolated trunk port.  
 Associate the isolated VLAN with the primary VLAN on layer 2.  
 A private VLAN contains up to one isolated VLAN. So a private VLAN can be associated with up to one primary VLAN and its associated isolated VLAN.  
 More than one private VLANs are supported. So an isolated port can be configured with more than

one primary VLANs and their associated isolated VLANs.

**Configuration Examples** The following example configures GigabitEthernet 0/17 as an isolated trunk port associated with two primary VLANs and their associated isolated VLANs,

```
Ruijie> enable
Ruijie# configure terminal
Ruijie(config)# vlan 5
Ruijie(config-vlan)# private-vlan isolated
Ruijie(config-vlan)# exit
Ruijie(config)# vlan 2
Ruijie(config-vlan)# private-vlan primary
Ruijie(config-vlan)# private-vlan association add 5
Ruijie(config-vlan)# exit
Ruijie(config)# vlan 9
Ruijie(config-vlan)# private-vlan isolated
Ruijie(config-vlan)# exit
Ruijie(config)# vlan 6
Ruijie(config-vlan)# private-vlan primary
Ruijie(config-vlan)# private-vlan association add 9
Ruijie(config-vlan)# exit
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# switchport
Ruijie(config-if-GigabitEthernet 0/17)# switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/17)# switchport private-vlan association trunk 2 5
Ruijie(config-if-GigabitEthernet 0/17)# switchport private-vlan association trunk 6 9
```

Related Commands	Command	Description
		show vlan private-vlan

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

## 6.8 switchport private-vlan host-association

Use this command to associate the secondary VLAN with the primary VLAN. Use the **no** or **default** form of this command to restore the default setting.

**switchport private-vlan host-association** *primary-vlan-id secondary-vlan-id*

**no switchport private-vlan host-association**

**default switchport private-vlan host-association**

Parameter Description	Parameter	Description
		<i>primary-vlan-id</i>

<i>secondary-vlan-id</i>	Secondary VLAN ID.
--------------------------	--------------------

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

**Command mode** Interface configuration mode.

**Usage Guide** Before a port is configured as an isolated port or promiscuous port, and the port mode must be configured as the host port mode.  
 Whether a port is configured as an isolated port or community port depends on the *secondary-vlan-id* parameter.  
*primary-vlan-id* and *secondary-vlan-id* must be respectively the IDs of the primary VLAN and secondary VLAN in a PVLAN pair, on which Layer-2 association is performed.  
 One host port can be associated with only one PVLAN pair.

**Configuration** The following example associates the secondary VLAN with the primary VLAN on the host port.

```
Ruijie(config)# interface gigabitEthernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# switchport mode private-vlan host
Ruijie(config-if-GigabitEthernet 0/17)# switchport private-vlan host-association 22 23
Ruijie(config-if-GigabitEthernet 0/17)# default switchport private-vlan host-association
Ruijie(config-if-GigabitEthernet 0/17)# switchport private-vlan host-association 22 25
```

Related Commands	Command	Description
	<b>show vlan private-vlan</b>	N/A

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

## 6.9 switchport private-vlan mapping

Use this command to associate the promiscuous port with a primary VLAN and its associated secondary VLANs.. Use the **no** or **default** form of this command to restore the default settings.

**switchport private-vlan mapping** *primary-vlan-id* { [ **add** ] *secondary-vlan-list* | **remove** *secondary-vlan-list* }

**no switchport private-vlan mapping**

**default switchport private-vlan mapping**

Parameter Description	Parameter	Description
	<i>primary-vlan-id</i>	Primary VLAN ID.
	[ <b>add</b> ] <i>secondary-vlan-list</i>	Adds a list of secondary VLANs.

<code>remove secondary-vlan-list</code>	Removes a list of secondary VLANs.
---	------------------------------------

**Defaults** The promiscuous port is associated with no VLAN by default.

**Command mode** Interface configuration mode

**Usage Guide** The port should be a promiscuous port.  
The primary VLAN and secondary VLAN should be associated on layer 2.

**Configuration Examples** The following example configures GigabitEthernet 0/17 as a promiscuous port and associates it with primary VLAN 22 and secondary VLANs 23–25.

```
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# switchport mode private-vlan promiscuous
Ruijie(config-if-GigabitEthernet 0/17)# switchport private-vlan mapping 22 add 23-25
```

**Related Commands**

Command	Description
<code>show vlan private-vlan</code>	N/A

**Prompt** 1. If the specified VLAN is not a primary VLAN.

```
Operation is not supported on interface GigabitEthernet 0/1: the primary vlan doesn't exist!
```

2. If the primary VLAN and secondary VLAN are not associated on layer 2.

```
The vlan pair(22-23) is invalid!
```

**Common** 1. The primary VLAN and secondary VLAN are not associated on layer 2.

**Error** 2. The associated primary VLAN and secondary VLAN have no private VLAN attribute or attribute is wrong.

## 6.10 switchport private-vlan promiscuous trunk

Use this command to configure the trunk port as a promiscuous trunk port and associate it with a primary VLAN and its associated isolated VLAN on layer 2. Use the **no** or **default** form of this command to restore the default settings.

**switchport private-vlan promiscuous trunk** *primary-vlan-id secondary-vlan-list*

**no switchport private-vlan promiscuous trunk** *primary-vlan-id secondary-vlan-list*

**default switchport private-vlan promiscuous trunk** *primary-vlan-id secondary-vlan-list*

**Parameter Description**

Parameter	Description
<i>primary-vlan-id</i>	The ID of the primary VLAN associated with a secondary VLAN. The VLAN ID ranges from 2 to 4094.
<i>secondary-vlan-list</i>	The list of the secondary VLANs associated with a primary VLAN. The VLAN ID ranges from 2 to 4094. Use commas(,) to separate



	VLANs and use a hyphen (-) to connect consecutive VLANs.
--	--

**Defaults** The trunk port is not a promiscuous trunk port and associated with no VLAN by default.

**Command mode** Interface configuration mode

**Usage Guide** Configure a trunk port as a promiscuous trunk port.  
 Associate the secondary VLAN with the primary VLAN on layer 2.  
 A promiscuous port can be configured with more than one primary VLANs and their associated secondary VLANs.

**Configuration Examples** The following example configures GigabitEthernet 0/17 as a promiscuous trunk port associated with primary VLAN 202 and its associated isolated VLAN 203.

```
Ruijie> enable
Ruijie# configure terminal
Ruijie(config)# vlan 202
Ruijie(config-vlan)# private-vlan primary
Ruijie(config-vlan)# exit
Ruijie(config)# vlan 203
Ruijie(config-vlan)# private-vlan isolated
Ruijie(config-vlan)# exit
Ruijie(config)# vlan 202
Ruijie(config-vlan)# private-vlan association add 203
Ruijie(config-vlan)# exit
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# switchport
Ruijie(config-if-GigabitEthernet 0/17)# switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/17)# switchport private-vlan promiscuous trunk 202 203
```

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

**Platform Description** N/A

## 7 MSTP Commands(beta)

### 7.1 bpdu src-mac-check

Use this command to enable the BPDU source MAC address check function on the interface. Use the **no** form of this command to disable the BPDU source MAC address check function on the interface.

**bpdu src-mac-check** *mac-address*

**no bpdu src-mac-check**

Parameter Description	Parameter	Description
	<i>mac-address</i>	Indicates that only the BPDU messages from this MAC address are received. The input format is H.H.H.

**Defaults** The BPDU messages from any MAC address are received 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 0/17 .

```
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# bpdu src-mac-check 00d0.f800.1e2f
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 7.2 bridge-frame forwarding protocol bpdu

Use this command to enable BPDU transparent transmission. Use the **no** form of this command to disable BPDU transparent transmission.

**bridge-frame forwarding protocol bpdu**  
**no 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

## 7.3 clear spanning-tree counters

Use this command to clear the statistics of the sent and received STP packets.

**clear spanning-tree detected-protocols [ interface interface-type interface-number ]**

Parameter Description	Parameter	Description
	<b>interface interface-type interface-number</b>	ID of the interface

**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 GigabitEthernet 0/1.

Ruijie# clear spanning-tree counters interface gigabitethernet 0/1

**Related Commands**

Command	Description
<b>show spanning-tree counters</b>	Displays the statistics of STP transceived packets.

**Platform Description** N/A

## 7.4 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
<b>interface <i>interface-type interface-number</i></b>	ID of the interface

**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**

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

<b>Commands</b>		
	<b>show spanning-tree interface</b>	Displays the STP configuration of the interface.

**Platform** N/A

**Description**

## 7.5 clear spanning-tree mst topochange record

Use this command to clear STP topology change record.

**clear spanning-tree mst *instance-id* topochange record**

<b>Parameter Description</b>	<b>Parameter</b>	<b>Description</b>
	<i>instance-id</i>	Instance ID. 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   GI0/17         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.
    
```

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

**Platform** N/A

**Description**

## 7.6 instance

Use this command to map VLANs to an instance. 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 64
	<b>vlan</b> <i>vlan-range</i>	VLAN range, in the range from 1 to 4094.

**Defaults** By default, only instance 0 exists and all VLANs are in instance 0.

**Command Mode** MST configuration mode

**Usage Guide** **instance** *instance-id* **vlan** *vlan-range*: Add VLAN to MST instance. Instance-ID is in the range from 0 to 64 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. Use the no form of this command to remove VLAN from instance 1-64. If you create 64 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 Examples** This example enters MST mode and maps VLAN 3 and 5-10 to MST instance1.

```
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
	<b>show spanning-tree mst configuration</b>	Displays MST region information.

**Platform** N/A

**Description**

## 7.7 l2protocol-tunnel stp

Use this command to enable BPDU TUNNEL globally. Use the **no** form of this command to disable this function.

**l2protocol-tunnel stp**  
**no l2protocol-tunnel stp**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** If you want to BPDU TUNNEL globally, enable BPDU TUNNEL on the interface first.

**Configuration Examples** The following example enables BPDU TUNNEL globally.

```
Ruijie(config)# l2protocol-tunnel stp
Ruijie(config)# show l2protocol-tunnel stp

L2protocol-tunnel: stp Enable
L2protocol-tunnel destination mac address: 01d0.f800.0005
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 7.8 l2protocol-tunnel stp enable

Use this command to enable BPDU TUNNEL on the interface. Use the **no** form of this command to disable this function.

**l2protocol-tunnel stp enable**  
**no l2protocol-tunnel stp enable**

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

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

**Defaults** N/A

**Command Mode** Interface configuration mode

**Usage Guide** If you want to BPDU TUNNEL globally, enable BPDU TUNNEL on the interface first.

**Configuration Examples** The following example enables BPDU TUNNEL on the interface.

```
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# l2protocol-tunnel stp enable
Ruijie(config-if-GigabitEthernet 0/17)# show l2protocol-tunnel stp

L2protocol-tunnel: stp Enable
L2protocol-tunnel destination mac address: 01d0.f800.0005
GigabitEthernet 0/17 l2protocol-tunnel stp enable
```

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 7.9 l2protocol-tunnel stp tunnel-dmac

Use this command to configure the STP address for transparent transmission through BPDU TUNNEL. Use the **no** form of this command to restore the default setting.

**l2protocol-tunnel stp tunnel-dmac mac-address**  
**no l2protocol-tunnel stp tunnel-dmac**

**Parameter Description**

Parameter	Description
<i>mac-address</i>	The STP address for transparent transmission. The available STP addresses include 01d0.f800.0005, 011a.a900.0005, 010f.e200.0003, 0100.0ccd.cdd0, 0100.0ccd.cdd1, and 0100.0ccd.cdd2.

**Defaults** The default is 01d0.f800.0005.

**Command Mode** Global configuration mode



**Usage Guide** N/A

**Configuration Examples** The following example configures the STP address for transparent transmission through BPDU TUNNEL.

```
Ruijie(config)# l2protocol-tunnel stp tunnel-dmac 011a.a900.0005
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** N/A

## 7.10 name

Use this command to set the 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 Mode** MST configuration mode

**Usage Guide** N/A

**Configuration Examples** This example sets MST name to region1.

```
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)#
```

<b>Related Commands</b>	Command	Description
	<b>show spanning-tree mst configuration</b>	Displays MST region information

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

## 7.11 revision

Use this command to set the revision number of MSTP region. Use the **no** form of the command to restore the default setting.

**revision** *version*  
**no revision**

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

**Configuration Examples** 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)#
```

<b>Related Commands</b>	Command	Description
	<b>show spanning-tree mst configuration</b>	Displays MST region information

**Platform** N/A

**Description**

## 7.12 show l2protocol-tunnel stp

Use this command to display BPDU TUNNEL configuration.

**show l2protocol-tunnel stp**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

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

**Usage Guide** N/A

**Configuration** The following example displays BPDU TUNNEL configuration.

**Examples**

```
Ruijie# show l2protocol-tunnel stp

L2protocol-tunnel: stp Enable
L2protocol-tunnel destination mac address:011a.a900.0005
GigabitEthernet 0/17 l2protocol-tunnel stp enable
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 7.13 show spanning-tree

Use this command to display the global spanning-tree configuration.

**show spanning-tree [ counters | forward-time | hello-time | inconsistentports | max-age | max-hops | mst *instance-id* | pathcost method | summary | tx-hold-count ]**

Parameter Description	Parameter	Description
	<b>counters</b>	Displays the statistics of STP transceived packets.
	<b>forward-time</b>	Displays BridgeForwardDelay.

<b>hello-time</b>	Displays BridgeHelloTime.
<b>inconsistentports</b>	Displays the blocked port due to root guard or loop guard.
<b>max-age</b>	Displays BridgeMaxAge.
<b>max-hops</b>	Displays the maximum hops of an instance.
<b>mst <i>instance-id</i></b>	Displays MSTP information of an instance.
<b>pathcost method</b>	Displays the method used for calculating path cost.
<b>summary</b>	Displays the information of MSTP instances and forwarding status of the interfaces.
<b>tx-hold-count</b>	Displays TxHoldCount.

**Defaults** N/A

**Command Mode** Privileged EXEC mode, global configuration mode and interface configuration mode.

**Usage Guide** N/A

**Configuration** The following example displays the global spanning-tree configuration.

**Examples** 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 0/17          0          122594

----- STP TC or TCN count -----
MSTID   Port                Receive      Send
0       GigabitEthernet 0/17          0            0
```

Related Commands	Command	Description
	<b>spanning-tree pathcost method</b>	Configures the pathcost method.
	<b>spanning-tree</b>	Configures STP basic settings globally

**Platform Description** N/A

## 7.14 show spanning-tree interface

Use this command to display the STP configuration of the interface, including the optional spanning tree.

**show spanning-tree [ mst *instance-id* ] interface *interface-type interface-number* [ bpdupfilter |**

**bpduguard | link-type | portfast ]**

Parameter Description	Parameter	Description
	<b>mst</b> <i>instance-id</i>	Displays the instance ID, in the range from 0 to 64.
	<b>interface</b> <i>interface-type interface-number</i>	Displays the interface ID.
	<b>bpdufilter</b>	Displays the status of BPDU filter.
	<b>bpduguard</b>	Displays the status of BPDU guard.
	<b>link-type</b>	Displays the link type of an interface.
	<b>portfast</b>	Displays the status of portfast.

**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 STP configuration on interface GigabitEthernet 0/17.

```
Ruijie# show spanning-tree interface gigabitethernet 0/17
```

```
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
```

Related Commands	Command	Description
	<b>spanning-tree bpdudfilter</b>	Enables the BPDU filter feature someone the interface.
	<b>spanning-tree portfast</b>	Enables the portfast on the interface.
	<b>spanning-tree bpduguard</b>	Enables the BPDU guard on the interface.
	<b>spanning-tree link-type</b>	Configures the link type of the interface to point-to-point.

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

### 7.15 show spanning-tree mst configuration

Use this command to display the information of MST and instances.

**show spanning-tree mst configuration**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

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

**Usage Guide** N/A

**Configuration Examples** The following example displays the information of MST and instances.

```
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
	<b>spanning-tree mst configuration</b>	Configures the MST region.
	<b>instance</b>	Configures instance and VLAN mapping relations
	<b>name</b>	Configures the MST name
	<b>revision</b>	Configures the revision number of MSTP region.

**Platform** N/A

**Description**

## 7.16 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>

**Defaults** N/A

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

**Usage Guide** N/A

**Configuration** The following example displays the STP topology change record of instance 0.

### 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  Gi0/17          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: <ul style="list-style-type: none"> <li>● Normal: UP/DOWN state change on the interface,</li> <li>● LoopGuard Block: Loop-inconsistence causes the interface to be blocked.</li> </ul>

	<ul style="list-style-type: none"> <li>● RootGuard Block: Root-inconsistence causes the interface to be blocked.</li> <li>● Inferior Block: Receiving inferior BPDU frames causes the interface to be blocked.</li> <li>● LoopGuard Unblock: The interface returns to Forward status from loop-inconsistence. RootGuard Unblock: The interface returns to Forward status from root-inconsistence.</li> <li>● Inferior Unblock-The interface returns to Forward status after not receiving inferior BPDU frames.</li> </ul>
--	--

**Related Commands**

Command	Description
N/A	N/A

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

## 7.17 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** *forward* | **hello-time** *hello* | **max-age** *age* | **max-hops** *hop-count* | **tx-hold-count** *tx-hold-count* ]

**no spanning-tree** [ **forward-time** | **hello-time** | **max-age** / **max-hops** / **tx-hold-count** ]

**Parameter Description**

Parameter	Description
<b>forward-time</b> <i>forward</i>	Interval at which the port status changes, in the range from 4 to 30 in the unit of seconds. The default is 15.
<b>hello-time</b> <i>hello</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.
<b>max-age</b> <i>age</i>	Maximum aging time of the BPDU message, in the range from 6 to 40 in the unit of seconds. The default is 20.
<b>max-hops</b> <i>hop-count</i>	Number of hops in a region that the BPDU message passes before being dropped. The value range is from 1 to 40 in the unit of hops. The default is 20.
<b>tx-hold-count</b> <i>tx-hold-count</i>	Maximum number of the BPDU messages sent in one second, in the range from 1 to 10. The default is 3.

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

**Command** Global configuration mode.



**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.

$$2x(\text{Hello Time}+1.0 \text{ second}) \leq \text{Max-Age Time} \leq 2x(\text{Forward-Delay}-1.0 \text{ second})$$

If the values do not according with the condition, the settings do not work.

In the region, the BPDU message sent by the root bridge includes a Hot 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 timed out. The device will drop the BPDU message whose Hop Count is 0.

Use parameter **max-hops** *hop-count* to set the maximum number of hops(Max-hopsCount) of the BPDU message in the global configuration mode. Use the **no** form of this command to restore the default setting. This parameter takes effect for all instances.

Use parameter **tx-hold-count** *tx-hold-count* to configure the TxHoldCount of the STP. Use the **no** form of this command to restore the default setting.

**Configuration** The following example enables the spanning-tree function.

**Examples** Ruijie(config)# spanning-tree

The following example configures the BridgeForwardDelay.

Ruijie(config)# spanning-tree forward-time 10

The following example sets the max-hops of the spanning tree to 10 for all instances.

Ruijie(config)# spanning-tree max-hops 10

The following example sets the maximum number of the BPDU messages sent in one second.

Ruijie(config)# spanning-tree tx-hold-count 5

**Related Commands**

Command	Description
<b>show spanning-tree</b>	Displays the global STP configuration.

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

## 7.18 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
<b>disabled</b>	Disabled Autoedge on the interface.

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

**Command** Interface configuration mode.

**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 0/17
Ruijie(config-if-GigabitEthernet 0/17)# spanning-tree autoedge disabled
```

**Related  
Commands**

Command	Description
<b>show spanning-tree interface</b>	Displays the STP configuration information of the interface.

**Platform** N/A

**Description**

## 7.19 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
<b>enabled</b>	Enables BPDU filter on the interface.
<b>disabled</b>	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 GigabitEthernet 0/17.

**Examples**

```
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# spanning-tree bpdudfilter enable
```

Related Commands	Command	Description
		<b>show spanning-tree interface</b>

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

## 7.20 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
		<b>enabled</b>
	<b>disabled</b>	Disables BPDU guard on the interface.

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

**Command Mode** Interface configuration 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 time ]** 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 0/17
Ruijie(config-if-GigabitEthernet 0/17)# spanning-tree bpduguard enable
```

Related Commands	Command	Description
		<b>show spanning-tree interface</b>

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

## 7.21 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**

Parameter Description	Parameter	Description
	N/A	N/A

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

**Command Mode** Interface configuration mode.

**Usage Guide** 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.

**Configuration Examples** The following example enables the compatibility mode on interface GigabitEthernet 0/17.

```
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)#spanning-tree compatible enable
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 7.22 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
	<b>mst instance-id</b>	Instance ID in the range from 0 to 64. The default instance-id is 0.
	<b>cost cost</b>	Path cost in the range from 1 to 200,000,000.

**Defaults** The default value is calculated by the link rate of the interface automatically based on the IEEE 802.1T Long standard.

- 1000 Mbps—20000
- 100 Mbps—200000
- 10 Mbps—2000000

**Command Mode** Interface configuration mode.

**Usage Guide** A higher cost value means a higher path cost.  
 You can verify your settings by running the **show spanning-tree [ mst instance-id ] interface interface-type interface-number** command in the privileged EXEC mode.

**Configuration Examples** This example sets the path cost to 400 on the interface associated with instances 3.

```
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# spanning-tree mst 3 cost 400
```

Related Commands	Command	Description
		<b>show spanning-tree interface</b>

**Platform Description** N/A

## 7.23 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 bpdu. 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

**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** The following example enables **loop guard** on interface GigabitEthernet 0/17.

**Examples**

```
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# spanning-tree guard loop
```

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

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

## 7.24 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**

<b>Parameter Description</b>	Parameter	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 **guard** on interface GigabitEthernet 0/17.

```
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# spanning-tree guard none
```

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

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

## 7.25 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**

Parameter Description	Parameter	Description
	N/A	N/A

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

**Command Mode** Interface configuration mode.

**Usage Guide**

1. If root guard is enabled, the current root bridge will not change due to incorrect configuration or illegal packet attacks.
2. 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 0/17
Ruijie(config-if-GigabitEthernet 0/17)# spanning-tree guard root
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 7.26 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** Interface configuration mode.

**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 0/17
Ruijie(config-if-GigabitEthernet 0/17)# spanning-tree ignore tc
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 7.27 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 link; 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 0/17
Ruijie(config-if-GigabitEthernet 0/17)# 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**

## 7.28 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 bpdu. 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 Mode** Global configuration 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**

## 7.29 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	Parameter	Description
-----------	-----------	-------------

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**

## 7.30 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**

**Command** Global configuration mode.

**Mode**

**Usage Guide** 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 MSTP Region parameters:

- **instance** *instance-id* **vlan** *vlan-range*: Adds the VLANs to the MST instance.
- **name** *name*: Specifies the MST name, a string of up to 32 characters.
- **revision** *version*: Sets the MST versions in the range 0 to 65535.

Run the **show spanning-tree mst configuration** command to display the information of the MST region.

**Configuration** This example enters the MST configuration mode.

**Examples**

```
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)# instance 1 vlan 3, 5-10
Ruijie(config-mst)# name region1
Ruijie(config-mst)# revision1
Ruijie(config-mst)# show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name      : region1
Revision  : 1Instance  Vlans Mapped
-----
0         1-2, 4, 11-4094
1         3, 5-10
-----
Ruijie(config-mst)# exit
Ruijie(config)#
```

**Related Commands**

Command	Description
<b>show spanning-tree mst configuration</b>	Displays the MST region configuration.
<b>instance</b>	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**

### 7.31 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>	Adopts the 802.1t standard (long) to configure path cost. The cost of a port path ranges from 1 to 200000000. Aggregate Port Cost = Physical Port Cost * 95%.
<b>long standard</b>	Adopts the 802.1t standard (long standard) to configure path cost. The cost of the port path ranges from 1 to 200000000. Aggregate Port Cost = Physical Port Cost / Linkupcnt.
<b>short</b>	Adopts the 802.1d standard to configure path cost. The cost of a port path ranges from 1 to 65535. Aggregate Port Cost = Physical Port Cost * 95%

**Defaults** 802.1T standard (**long**) is adopted to set path cost by default.

**Command** Global configuration mode.

**Mode**

**Usage Guide** When the path cost method of the port is **long standard**, the cost of the aggregate port changes as the number of member ports changes, which changes the network topology.

- If an aggregate port is static, the value of Linkupcnt in the table is the number of active member ports.
- If an aggregate port is an LACP AP, the value of Linkupcnt in the table is the number of member ports forwarding AP data.

If no member port in the aggregate port goes up, the value of Linkupcnt is 1.

**Configuration** The following example configures the path cost of the port.

**Examples**

```
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# 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**

### 7.32 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 Mode** Interface configuration 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 0/17
Ruijie(config-if-GigabitEthernet 0/17)# spanning-tree portfast
```

**Related Commands**

Command	Description
<b>show spanning-tree interface</b>	Displays the STP configuration of the interface.

**Platform Description** N/A

### 7.33 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	N/A

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

**Command Mode** Global configuration mode.

**Usage Guide** 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**

## 7.34 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 Description	Parameter	Description
		N/A

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

**Command Mode** Global configuration 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 Examples** The following example enables the GPDU guard globally.

```
Ruijie(config)# spanning-tree portfast bpduguard default
```

Related Commands	Command	Description
		<b>show spanning-tree interface</b>

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

## 7.35 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 Description	Parameter	Description
		N/A

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

**Command Mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example enables the portfast feature on all interfaces globally.

```
Ruijie(config)# spanning-tree portfast default
```

Related Commands	Command	Description
		<b>show spanning-tree interface</b>

**Platform Description** N/A

### 7.36 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 Description	Parameter	Description
		<b>mst instance-id</b>
	<b>port-priority priority</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 port priority is 128.

**Command Mode** Interface configuration mode.

**Usage Guide** 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 0/17 to 0 in instance 20.

**Examples**

```
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# spanning-tree mst 20 port-priority 0
```

**Related  
Commands**

Command	Description
<b>show spanning-tree interface</b>	Displays the global STP configuration.

**Platform** N/A

**Description**

## 7.37 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  
Description**

Parameter	Description
<b>mst <i>instance-id</i></b>	Instance ID, in the range of 0 to 64. The default instance ID is 0.
<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 device priority is 32768.

**Command** Global configuration mode.

**Mode**

**Usage Guide** 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** The following example sets the device priority of the Instance to 8192.

**Examples**

```
Ruijie(config)# spanning-tree mst 20 priority 8192
```

You can verify your settings by entering the **show spanning-tree mst summary** command in the privileged EXEC mode.

**Related**

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



Commands	
<b>show spanning-tree</b>	Displays the global STP configuration.

Platform N/A

Description

## 7.38 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 Global configuration mode.

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

## 7.39 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** Interface configuration mode.

**Usage Guide** Enable TC guard to prevent TC packets from spreading

**Configuration Examples** The following example enables **tc-guard** on the interface to prevent the spread of TC messages.

```
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# spanning-tree tc-guard
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

### 7.40 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**

## 7.41 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** The following example enables tc-guard to prevent TC packets from being flooded.

**Examples** Ruijie(config)# spanning-tree tc-protection tc-guard

Related Commands	Command	Description
	N/A	N/A

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

## 8 GVRP Commands(beta)

### 8.1 bridge-frame forwarding protocol gvrp

Use this command to enable GVRP PDUs transparent transmission. Use the **no** form of this command to restore the default setting.

**bridge-frame forwarding protocol gvrp**  
**no bridge-frame forwarding protocol gvrp**

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, the MAC address 01-80-C2-00-00-21 of GVRP PDUs is reserved for future standardization. In other words, the device following the IEEE 802.1Q standard does not forward GVRP PDUs frames. However, in actual network deployment, GVRP PDUs transparent transmission may be required. For example, the device not enabled with GVRP needs to transmit GVRP PDUs frames transparently to ensure proper GVRP topology calculation.

**Configuration Examples** The following example enables GVRP PDUs transparent transmission.

```
Ruijie(config)# bridge-frame forwarding protocol gvrp
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

### 8.2 clear gvrp statistic

Use this command to clear the GVRP statistics for re-counting.

**clear gvrp statistics** { *interface-type interface-number* | **all** }

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

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

**Defaults** N/A

**Command mode** Privileged EXEC mode.

**Usage Guide** Use the **show gvrp statistics** to display the statistics.

**Configuration** The following example clears GVRP statistics.

**Examples**

```
Ruijie# clear gvrp statistics all
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

### 8.3 gvrp applicant state

Use this command configures the GVRP advertisement mode on the interface. Use the **no** form of this command to restore default setting.

**gvrp applicant state { normal | non-applicant }**  
**no gvrp applicant state**

Parameter Description	Parameter	Description
	<b>normal</b>	The interface sends VLAN advertisement.
<b>non-applicant</b>	The interface does not send VLAN advertisement.	

**Defaults** The interface sends GVRP advertisement by default.

**Command mode** Interface configuration mode.

**Usage Guide** N/A

**Configuration** The following example configures the GVRP advertisement mode on the interface.

**Examples**

```
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# gvrp applicant state normal
```

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

Commands	
<b>show gvrp configuration</b>	Displays the GVRP configurations.

**Platform** N/A

**Description**

## 8.4 gvrp dynamic-vlan-creation enable

Use this command to enable dynamic VLAN creation. Use the **no** form of this command to restore the default setting.

**gvrp dynamic-vlan-creation enable**

**no gvrp dynamic-vlan-creation enable**

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

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

**Command mode** Global configuration mode.

**Usage Guide** Use the **show gvrp configuration** to display the configuration.

**Configuration Examples** The following example enables dynamic VLAN creation.

```
Ruijie(config)# gvrp dynamic-vlan-creation enable
```

Related Commands	Command	Description
	<b>show gvrp configuration</b>	Displays the GVRP configurations.

**Platform** N/A

**Description**

## 8.5 gvrp enable

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

**gvrp enable**

**no gvrp enable**

Parameter	Parameter	Description
<b>Description</b>		

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

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

**Command mode** Global configuration mode

**Usage Guide** This command is used to display the configuration.

**Configuration Examples** The following example enables the GVRP function.

```
Ruijie(config)#gvrp enable
```

Related Commands	Command	Description
	<b>show gvrp configuration</b>	Displays the GVRP configurations.

**Platform Description** N/A

## 8.6 gvrp registration mode

Use this command to set the registration mode to control whether to enable dynamic VLAN creation/registration/canceling on the port. Use the **no** form of this command to restore the default setting.

```
gvrp registration mode { normal | disabled }  
no gvrp registration mode
```

Parameter Description	Parameter	Description
	<b>normal</b>	Enables dynamic VLAN creation/registration/canceling on the port.
	<b>disabled</b>	Disables dynamic VLAN creation/registration/canceling on the port.

**Defaults** Dynamic VLAN creation/registration/canceling is enabled by default,

**Command mode** Interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example sets the registration mode.

```
Ruijie(config)# interface gigabitethernet 0/17  
Ruijie(config-if-GigabitEthernet 0/17)# gvrp registration mode normal
```

Related Commands	Command	Description
		<b>show gvrp configuration</b>

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

## 8.7 gvrp timer

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

**gvrp timer** { **join** *hold* | **leave** *leave* | **leaveall** *leaveall* }  
**no gvrp timer**

Parameter Description	Parameter	Description
		<b>join</b> <i>hold</i>
	<b>leave</b> <i>leave</i>	Controls the waiting time before removing the VLAN from the port with the Leave Message received. If the Join Message is received again within this time range, the port-VLAN relation still exists and the timer becomes invalid. If no Join Message is received on the port, the port status will be the Empty and removed from the VLAN member list. The value ranges from 600 to 9999 in the unit of milliseconds.
	<b>leave all</b> <i>leaveall</i>	Controls the minimum interval of sending the LeaveAll Message on the port. If the LeaveAll Message is received before the timer expires, the timer re-counts. If the timer expires, send the LeaveAll Message on the port and also send this Message to the port, so that the Leave timer begins counting. The actual sending interval ranges from <i>leaveall</i> to <i>leaveall</i> + <i>join</i> . The value ranges from 601 to 2147483647 in the unit of milliseconds.

**Defaults** By default, Join timer is 200 milliseconds, Leave timer is 600 milliseconds, and Leaveall timer is 10000 milliseconds.

**Command mode** Global configuration mode

**Usage Guide** Use the **show gvrp configuration** to display the configuration.  
 Use the **no gvrp timer** command to restore **join**, **leave** and **leaveall timer** to default settings.

**Configuration** The following example configures the join timer.

**Examples**

```
Ruijie(config)# gvrp timer join 200
```



<b>Related Commands</b>	Command	Description
	<b>show gvrp configuration</b>	Displays the GVRP configuration.

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

## 8.8 l2protocol-tunnel gvrp

Use this command to enable global GVRP PDUs TUNNEL globally. Use the **no** form of this command to restore the default setting.

**l2protocol-tunnel gvrp**  
**no l2protocol-tunnel gvrp**

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

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

**Command mode** Global configuration mode

**Usage Guide** If you want to enable global GVRP PDUs TUNNEL, enable GVRP PDUs TUNNEL on the interface first.

**Configuration Examples** The following example enables GVRP PDUs TUNNEL globally.

```
Ruijie(config)# l2protocol-tunnel gvrp
Ruijie(config)# show l2protocol-tunnel gvrp

L2protocol-tunnel: Gvrp Disable
L2protocol-tunnel destination mac address:01d0.f800.0006
```

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

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

## 8.9 I2protocol-tunnel gvrp enable

Use this command to enable GVRP PDUs TUNNEL on the interface. Use this command to restore the default setting.

**I2protocol-tunnel gvrp enable**

**no I2protocol-tunnel gvrp enable**

Parameter Description	Parameter	Description
	N/A	N/A

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

**Command mode** Interface configuration mode

**Usage Guide** If you want to enable global GVRP PDUs TUNNEL, enable GVRP PDUs TUNNEL on the interface first.

**Configuration** The following example enables GVRP PDUs TUNNEL on the interface.

**Examples**

```
Ruijie(config)# interface gigabitEthernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# l2protocol-tunnel gvrp enable
Ruijie(config-if-GigabitEthernet 0/17)# show l2protocol-tunnel gvrp

L2protocol-tunnel: Gvrp Disable
L2protocol-tunnel destination mac address:01d0.f800.0006
GigabitEthernet 0/17 l2protocol-tunnel gvrp enable
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 8.10 I2protocol-tunnel gvrp tunnel-dmac

Use this command to configure the MAC address for transparent transmission in GVRP PDUs TUNNEL. Use the **no** form of this command to restore the default setting.

**I2protocol-tunnel gvrp tunnel-dmac mac-address**

**no I2protocol-tunnel gvrp tunnel-dmac**

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

<b>Description</b>		
	<i>mac-address</i>	The MAC address for transparent transmission in GVRP PDUs TUNNEL. The available GVRP PDUs TUNNEL addresses include 01d0.f800.0006 and 011a.a900.0006.

**Defaults** The default is 01d0.f800.0006.

**Command mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example configures the MAC address for transparent transmission in GVRP PDUs TUNNEL.

```
Ruijie(config)# l2protocol-tunnel gvrp tunnel-dmac 011a.a900.0006
```

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

**Platform Description** N/A

## 8.11 show gvrp configuration

Use this command to display the GVRP configuration.

**show gvrp configuration**

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

**Defaults** N/A

**Command mode** Privileged EXEC mode.

**Usage Guide** Use the **show gvrp configuration** to display the configuration.

**Configuration Examples** The following example displays GVRP configuration.

```
Global GVRP Configuration:
GVRP Feature:enabled
GVRP dynamic VLAN creation:enabled
```

```

Join Timers(ms):200
Leave Timers(ms):600
Leaveall Timers(ms):1000
Port based GVRP Configuration:
      PORT           Applicant Status       Registration Mode
-----
GigabitEthernet 0/17       normal           normal
    
```

Field	Description
GVRP Feature	Whether to enable GVRP
GVRP dynamic VLAN creation	Whether to enable dynamic VLAN creation
Join Timers	Join timer
Leave Timers	Leave timer
Leaveall Timers	Leaveall timer
PORT	Port
Applicant Status	Advertisement mode
Registration Mode	Registration mode

Related Commands	Command	Description
	N/A	N/A

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

## 8.12 show gvrp statistics

Use this command to display the GVRP statistics of one interface or all interfaces.

```
show gvrp statistics { interface-type interface-number | all }
```

Parameter Description	Parameter	Description
	<i>interface-type interface-number</i>	Interface ID. Display the statistics of one interface.
	<b>all</b>	Display the statistics of all interfaces.

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** Ruijie# show gvrp statistics gigabitethernet 0/17

**Examples**

```

Interface      GigabitEthernet 0/17
RecValidGvrpPdu      0
RecInvalidGvrpPdu    0
RecJoinEmpty  0
RecJoinIn      0
RecEmpty       0
RecLeaveEmpty   0
RecLeaveIn      0
RecLeaveAll     0
SentGvrpPdu    0
SentJoinEmpty  0
SentJoinIn     0
SentEmpty      0
SentLeaveEmpty  0
SentLeaveIn     0
SentLeaveAll    0
JoinIndicated  0
LeaveIndicated  0
JoinPropagated 0
LeavePropagated 0
    
```

Field	Description
RecValidGvrpPdu	Number of received valid GPDU packets.
RecInvalidGvrpPdu	Number of received unvalid GPDU packets.
RecJoinEmpty/ SentJoinEmpty	Number of received/sent JoinEmpty messages.
RecJoinIn/ SentJoinIn	Number of received/sent JoinIn messages.
RecEmpty/SentEmpty	Number of received/sent Empty messages.
RecLeaveEmpty/SentLeaveEmpty	Number of received/sent LeaveEmpty messages,
RecLeaveIn/ SentLeaveIn	Number of received/sent LeaveIn messages.
RecLeaveAll/SentLeaveAll	Number of received/sent LeaveAll messages.
SentGvrpPdu	Number of sent GPDU messages.
JoinIndicated/ LeaveIndicated	Number of Join/Leave service requests.
JoinPropagated / LeavePropagated	Number of Join/Leave topology update requests.

**Related Commands**

Command	Description
<b>clear gvrp statistics</b>	Clears the statistics of one interface or all interfaces.

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

### 8.13 show gvrp status

Use this command to display all dynamic VLAN ports generated by GVRP and the dynamic VLAN ports added to the static VLAN.

**show gvrp status**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command mode** Privileged EXEC mode.

**Usage Guide** Use the **show gvrp status** command to display the GVRP status.

**Configuration Examples** The following example displays the GVRP status.

```
Ruijie# show gvrp status
VLAN 1
Dynamic Ports:
DVLAN 2
Dynamic Ports:
```

Field	Description
VLAN	Static VLAN
DVLAN	Dynamic VLAN
Dynamic Ports	Dynamic ports.

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

### 8.14 show I2protocol-tunnel gvrp

Use this command to display GVRP PDUs TUNNEL configuration.

**show I2protocol-tunnel gvrp**

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

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

**Defaults** N/A

**Command mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** N/A

**Configuration** The following example displays GVRP PDUs TUNNEL configuration.

**Examples**

```
Ruijie# show l2protocol-tunnel gvrp

L2protocol-tunnel: Gvrp Enable
L2protocol-tunnel destination mac address:011a.a900.0006
GigabitEthernet 0/17 l2protocol-tunnel gvrp enable
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** N/A

## 9 LLDP Commands(beta)

### 9.1 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** The common address of a device is not configured by default.

**Command Mode** LLDP Civic address configuration mode

**Usage Guide** This command is used to configure a common LLDP address in LLDP Civic address configuration mode.

The **show lldp location civic-location { identifier *id* | interface *interface-type interface-number* | static }** command can be used to display the information about an LLDP Civic address.

**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</b>	Displays the information about an LLDP Civic address.

**Platform** N/A

**Description**

## 9.2 clear lldp statistics

Use this command to clear LLDP statistics.

**clear lldp statistics [ interface *interface-type interface-number* ]**

Parameter	Parameter	Description
<b>Description</b>	<b>interface <i>interface-type interface-number</i></b>	Clear the LLDP statistics of the specified interface

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example clears LLDP statistics of interface 1.

**Examples**

```
Ruijie# clear lldp statistics interface GigabitEthernet 0/17
```

```
Ruijie# show lldp statistics interface GigabitEthernet 0/17
Lldp statistics information of port [GigabitEthernet 0/17]
-----
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**

### 9.3 clear lldp table

Use this command to clear LLDP neighbor information.

**clear lldp table** [ **interface** *interface-type interface-number* ]

Parameter	Parameter	Description
Description	<b>interface</b> <i>interface-type interface-number</i>	Clears the LLDP neighbor information of the specified interface.

**Defaults** N/A

**Command Mode** Privileged EXEC 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 Examples** The following example clears the LLDP neighbor information on interface 17.

```
Ruijie# show lldp neighbors interface GigabitEthernet 0/17
Lldp statistics information of port [GigabitEthernet 0/17]
-----
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
Ruijie# clear lldp table interface GigabitEthernet 0/17
Ruijie# show lldp neighbors interface GigabitEthernet 0/17
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 9.4 device-type

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

**device-type** *device-type*

**no device-type**

Parameter	Parameter	Description
<b>Description</b>	<i>device-type</i>	Device type. The value ranges from 0 to 2. 0: The device type is DHCP Server. 1: The device type is switch. 2: The device type is LLDP MED terminal.

**Defaults** The device type is not configured by default.

**Command Mode** LLDP Civic address configuration mode

**Usage Guide** This command is used to configure the device type in a common LLDP address in LLDP Civic address configuration mode.  
The **show lldp location civic-location { identifier *id* | interface *interface-type interface-number* | static }** command can be used to display the information about an LLDP Civic address.

**Configuration Examples** The following example sets the device type to switch.

```
Ruijie#config
Ruijie(config)# lldp location civic-location identifier 1
Ruijie(config-lldp-civic)# device-type 1
```

Related Commands	Command	Description
	<b>show lldp location</b>	Displays the information about an LLDP Civic address.

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

## 9.5 Ildp enable

Use this command to enable the LLDP globally or on the interface. Use **no** form of this command to disable this function.

**Ildp enable**  
**no Ildp enable**

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

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

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

**Usage Guide** LLDP takes effect on an interface only when LLDP is enabled globally.  
 The feature is not supported by G.hn ports.

**Configuration Examples** The following example disables LLDP globally and on the interface.

```
Ruijie#config
Ruijie(config)#no lldp enable
Ruijie(config)#interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# no lldp enable
```

Related Commands	Command	Description
	<b>show Ildp status</b>	Displays LLDP status information.

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

## 9.6 Ildp encapsulation snap


Use this command to configure the encapsulation format of LLDP packets. Use the **no** form of this command to restore the default setting.


**Ildp encapsulation snap**  
**no Ildp encapsulation snap**

Parameter	Parameter	Description
<b>Description</b>	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.

 The feature is not supported by G.hn ports.

**Configuration Examples** The following example sets LLDP packet encapsulation format to SNAP.

```
Ruijie#config
Ruijie(config)#interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)#lldp encapsulation snap
```

Related Commands	Command	Description
	show lldp status	Displays LLDP status information.

**Platform Description** N/A

## 9.7 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** form of this command to disable this function.

**lldp error-detect**

**no lldp error-detect**

Parameter Description	Parameter	Description
	N/A	N/A

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

**Command Mode** Interface configuration 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.  
The feature is not supported by G.hn ports.

**Configuration** The following example configures LLDP error detection.

**Examples**

```
Ruijie#config
Ruijie(config)#interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)#lldp error-detect
```

**Related  
Commands**

Command	Description
<b>show interface status</b>	Displays LLDP status information.

**Platform** N/A

**Description**

## 9.8 Ildp 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** form of this command to restore the default setting.

**lldp fast-count** *fast-count-value*

**no lldp fast-count**

**Parameter  
Description**

Parameter	Description
<i>fast-count-value</i>	The number of fast sent LLDP packets, in the range from 1 to 10.

**Defaults** The default is 3.

**Command  
Mode** Global configuration mode.

**Usage Guide** N/A

**Configuration** The following example sets the number of fast sent LLDP packets to 5.

**Examples**

```
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**

## 9.9 Ildp hold-multiplier

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

**Ildp hold-multiplier** *tvl-value*

**no Ildp hold-multiplier**

Parameter	Parameter	Description
<b>Description</b>	<i>tvl-value</i>	TTL multiplier, in the range from 2 to 10.

**Defaults** The default is 4.

**Command** Global configuration mode.

**Mode**

**Usage Guide** The value of Time To Live (TLV) in LLDP packet = TTL multiplier × LLDP packet transmit interval + 1. Therefore, the TTL of local device information on the neighbor device can be controlled by adjusting TTL multiplier.

**Configuration** The following example sets TTL multiplier to 5.

**Examples**

```
Ruijie#config
Ruijie(config)#lldp hold-multiplier 5
```

Related	Command	Description
<b>Commands</b>	<b>show lldp status</b>	Displays LLDP status information.

**Platform** N/A

**Description**

## 9.10 Ildp 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** form of this command to delete the address.

**Ildp location civic-location identifier** *id*

**no Ildp 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.

**Defaults** The common address of a device is not configured by default.

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

**Usage Guide** This command can be used to enter the LLDP Civic Address configuration mode.  
The **show lldp location civic-location { identifier *id* | interface *interface-type interface-number* | static }** command can be used to display the information about an LLDP Civic address.

**Configuration Examples** The following example creates the Civic Address information in LLDP MED-TLV as follows: set *id* to 1.

```
Ruijie#config
Ruijie(config)#lldp location civic-location identifier 1
Ruijie(config-lldp-civic)#
```

Related Commands	Command	Description
	<b>show lldp location</b>	Displays the LLDP Civic Address information.

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

## 9.11 lldp location elin identifier

Use this command to set an emergency number encapsulated in a Location Identification TLV. Use the **no** form of this command to delete the number.

**lldp location elin identifier *id* elin-location *tel-number***  
**no lldp location elin identifier *id***

Parameter	Parameter	Description
<b>Description</b>	<i>id</i>	ID of an emergency number, in the range from 1 to 1024.
	<i>tel-number</i>	Emergency number, in the range from 10 to 25 bytes.

**Defaults** The emergency telephone number of a device is not configured by default.  
The **show lldp location elin-location { identifier *id* | interface *interface-type interface-number* | static }** command can be used to display the LLDP emergency number.

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

**Usage Guide** This command is used to configure an emergency number.

**Configuration Examples** The following example sets an emergency number.

**Examples**

```
Ruijie#config
Ruijie(config)#lldp location elin identifier 1 elin-location 085283671111
```



Related	Command	Description
Commands	<b>show lldp location elin-location</b> { <b>identifier</b> <i>id</i>   <b>interface</b> <i>interface-type interface-number</i>   <b>static</b> }	Displays an LLDP emergency number.

**Platform** N/A

**Description**

## 9.12 lldp management-address-tlv

Use this command to configure the management address advertised in LLDP packets. Use the **no** form of this command to disable the advertisement of management address.

**lldp management-address-tlv** [*ip-address*]

**no lldp management-address-tlv**

Parameter	Parameter	Description
Description	<i>ip-address</i>	The management address advertised in LLDP packets.

**Defaults** 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.

If the IPv4 address is still not found, the IPv6 address of the lowest-ID VLAN carried on the port will be tried.

If the IPv6 address is still not found, the MAC address of the device will be advertised as the management address.

**Command Mode** Interface configuration mode.

**Usage Guide** In global configuration mode, the command **lldp management-address-tlv** *ip-address* can be used to configure the management address advertised in LLDP packets.

The feature is not supported by G.hn ports.

**Configuration Examples** The following example configures the management address advertised in LLDP packets to 192.168.1.1.

```
Ruijie#config
Ruijie(config)#interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)#lldp management-address-tlv 192.168.1.1
```

Related	Command	Description
Commands	<b>show lldp local-information</b>	Displays LLDP local information

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

## 9.13 lldp mode

Use this command to configure the LLDP operating mode. Use **no** form of this command to restore the default setting.

**lldp mode** { **rx** | **tx** | **txrx** }  
**no lldp mode**

Parameter	Parameter	Description
<b>Description</b>	<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. The feature is not supported by G.hn ports.

**Configuration Examples** The following example sets LLDP operating mode to tx on the interface.

```
Ruijie#config
Ruijie(config)#interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)#lldp mode tx
```

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

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

## 9.14 lldp network-policy profile

Use this command to create an LLDP network policy and enter the LLDP network policy configuration mode. Use the **no** form of this command to delete the policy.

**lldp network-policy profile** *profile-num*  
**no lldp network-policy profile** *profile-num*

Parameter	Parameter	Description
Description	<i>profile-num</i>	ID of an LLDP network policy, in the range from 1 to 1024.

**Defaults** There is no LLDP network policy by default.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to enter the LLDP network policy configuration mode. When this command is run, the policy ID must be specified.

In LLDP network-policy mode, the { **voice** | **voice-signaling** } **vlan** command can be used to configure the specific network policy.

The **show lldp network-policy profile** [ *profile-num* ] command can be used to display the LLDP network policy.

**Configuration Examples** The following example creates an LLDP network policy whose ID is 1.

```
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>	Displays an LLDP network policy.

**Platform Description** N/A

## 9.15 lldp notification remote-change enable

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

**lldp notification remote-change enable**  
**no lldp notification remote-change enable**

Parameter	Parameter	Description
Description	N/A	N/A

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

**Command Mode** Interface configuration 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.

The feature is not supported by G.hn ports.

**Configuration** The following example configures LLDP Trap.

**Examples**

```
Ruijie#config
Ruijie(config)#interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)#lldp notification remote-change enable
```

Related	Command	Description
Commands	show lldp status	Displays LLDP status information.

**Platform** N/A

**Description**

## 9.16 lldp timer notification-interval

Use this command to set an interval of sending LLDP Traps. Use the **no** form of this command to restore the default setting.

**lldp timer notification-interval** *trap*

**no lldp timer notification-interval**

Parameter	Parameter	Description
Description	<i>trap</i>	Interval of sending LLDP Traps, in the range from 5 to 3600 in the unit of seconds.

**Defaults** The default is 5.

**Command** Global configuration mode.

**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** The following example sets the interval of sending LLDP Traps to 10 seconds.

**Examples**

```
Ruijie#config
Ruijie(config)#lldp timer notification-interval 10
```

Related Commands	Command	Description
	<b>show lldp status</b>	Displays LLDP status information.

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

## 9.17 lldp timer reinit-delay

Use this command to set port initialization delay. Use the **no** form of this command to restore the default setting.

**lldp timer reinit-delay** *reinit-delay*

**no lldp timer reinit-delay**

Parameter Description	Parameter	Description
	<i>reinit-delay</i>	Port initialization delay, in the range from 1 to 10 in the unit of seconds.

**Defaults** The default is 2.

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

## 9.18 lldp timer tx-delay

Use this command to set LLDP packet transmission delay. Use the **no** form of this command to restore the default setting.

**lldp timer tx-delay** *tx-delay*

**no lldp timer tx-delay**

Parameter	Parameter	Description
<b>Description</b>	<i>tx-delay</i>	LLDP packet transmission delay, in the range from 1 to 8192 in the unit of seconds.
<b>Defaults</b>	The default is 2.	
<b>Command Mode</b>	Global configuration mode.	
<b>Usage Guide</b>	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.	
<b>Configuration Examples</b>	The following example sets LLDPDU transmission delay to 3 seconds.	
	<pre>Ruijie#config Ruijie(config)#lldp timer tx-delay 3</pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show lldp status</b>	Displays LLDP status information.
<b>Platform Description</b>	N/A	

## 9.19 lldp timer tx-interval

Use this command to set the interval of sending the LLDP packets. Use **no** form of this command to restore the default setting.

**lldp timer tx-interval** *tx-interval*

**no lldp timer tx-interval**

Parameter	Parameter	Description
<b>Description</b>	<i>tx-interval</i>	Interval of sending the LLDP packets, in the range from 5 to 32768 in the unit of seconds.
<b>Defaults</b>	The default is 30.	
<b>Command Mode</b>	Global configuration mode.	
<b>Usage Guide</b>	N/A	
<b>Configuration</b>	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 Commands	Command	Description
	<b>show lldp status</b>	Displays LLDP status information.

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

## 9.20 lldp tlv-enable basic-tlv

Use this command to configure the optional basic management TLVs to be advertised.  
 Use the **no** form of this command to remove the optional basic management TLVs to be advertised.

**lldp tlv-enable basic-tlv { all | port-description | system-capability | system-description | system-name }**  
**no lldp tlv-enable basic-tlv { all | port-description | system-capability | system-description | system-name }**

Parameter Description	Parameter	Description
	<b>all</b>	All optional basic management TLVs
	<b>port-description</b>	Port Description TLV
	<b>system-capability</b>	System Capabilities TLV
	<b>system-description</b>	System Description TLV
	<b>system-name</b>	System Name TLV

**Defaults** All optional basic management TLVs are advertised on an interface by default.

**Command Mode** Interface configuration mode

**Usage Guide** The mandatory basic management TLVs must be advertised in LLDPDU.  
 You do not need to run this command to configure the mandatory basic management TLVs to be advertised.  
 You cannot run the **no** form of this command to remove the mandatory basic management TLVs to be advertised.  
 The feature is not supported by G.hn ports.

**Configuration Examples** The following example configures all optional basic management TLVs to be advertised.

```
Ruijie# configure terminal
Ruijie(config)#interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)#lldp tlv-enable basic-tlv all
```

Related	Command	Description
Commands	<code>show lldp tlv-config interface</code>	Displays the attributes of advertisable TLVs.

Platform N/A

Description

## 9.21 lldp tlv-enable dot1-tlv

Use this command to configure the IEEE 802.1 TLVs to be advertised.

Use the **no** form of this command to remove the IEEE 802.1 TLVs to be advertised.

**lldp tlv-enable dot1-tlv** { **all** | **port-vlan-id** | **protocol-vlan-id** [ *vlan-id* ] | **vlan-name** [ *vlan-id* ] }

**no lldp tlv-enable dot1-tlv** { **all** | **port-vlan-id** | **protocol-vlan-id** | **vlan-name** }

Parameter	Parameter	Description
Description	<b>all</b>	The Port VLAN ID TLV, the Port and Protocol VLAN ID TLV, and the VLAN Name TLV
	<b>port-vlan-id</b>	Port VLAN ID TLV
	<b>protocol-vlan-id</b> [ <i>vlan-id</i> ]	Port and Protocol VLAN ID TLV
	<b>vlan-name</b> [ <i>vlan-id</i> ]	VLAN Name TLV. VLAN ID corresponding to the specified VLAN name

**Defaults** All IEEE 802.1 TLVs are advertised on an interface by default.

**Command** Interface configuration mode

**Mode**

**Usage Guide** The feature is not supported by G.hn ports.

**Configuration** The following example configures all IEEE 802.1 TLVs to be advertised.

**Examples**

```
Ruijie# configure terminal
Ruijie(config)#interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)#lldp tlv-enable dot1-tlv all
```

Related	Command	Description
Commands	<code>show lldp tlv-config interface</code>	Displays the attributes of advertisable TLVs.

Platform N/A

Description

## 9.22 lldp tlv-enable dot3-tlv

Use this command to configure the IEEE 802.3 TLVs to be advertised.

Use the **no** form of this command to remove the IEEE 802.3 TLVs to be advertised.



```
lldp tlv-enable dot3-tlv { all | link-aggregation | mac-physic | max-frame-size | power }
no lldp tlv-enable dot3-tlv { all | link-aggregation | mac-physic | max-frame-size | power }
```

Parameter	Parameter	Description
Description	<b>all</b>	All IEEE 802.3 TLVs
	<b>link-aggregation</b>	Link Aggregation TLV
	<b>mac-physic</b>	MAC/PHY Configuration/Status TLV
	<b>max-frame-size</b>	Maximum Frame Size TLV
	<b>power</b>	Power Via MDI TLV

**Defaults** All the IEEE 802.3 TLVs are not advertised on an interface by default.

**Command Mode** Interface configuration mode

**Usage Guide** When configuring LLDP-MED Capability TLVs, configure LLDP 802.3 MAC/PHY TLVs first.  
When removing LLDP 802.3 MAC/PHY TLVs, remove LLDP-MED Capability TLVs first.  
The feature is not supported by G.hn ports.

**Configuration Examples** The following example configures all IEEE 802.3 TLVs to be advertised.

```
Ruijie# configure terminal
Ruijie(config)#interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)#lldp tlv-enable dot3-tlv all
```

Related Commands	Command	Description
	<b>show lldp tlv-config interface</b>	Displays the attributes of advertisable TLVs.

**Platform Description** N/A

## 9.23 lldp tlv-enable med-tlv

Use this command to configure the LLDP MED TLVs to be advertised.

Use the **no** form of this command to remove the LLDP MED TLVs to be advertised.

```
lldp tlv-enable med-tlv { all | capability | inventory | location civic-location identifier id | location
elin identifier id | network-policy profile [ profile-num ] | power-over-ethernet }
no lldp tlv-enable med-tlv { all | capability | inventory | location civic-location identifier id |
location elin identifier id | network-policy profile [ profile-num ] | power-over-ethernet }
```

Parameter	Parameter	Description
Description	<b>all</b>	All LLDP-MED TLVs except Location Identification TLVs
	<b>capability</b>	LLDP-MED Capabilities TLV
	<b>inventory</b>	Inventory management TLVs, including hardware revision

	TLVs, firmware revision TLVs, software revision TLVs, serial number TLVs, manufacturer name TLVs, model name TLVs, and asset ID TLVs.
<b>location civic-location identifier</b> <i>id</i>	Common address information about the network device in Location Identification TLVs. The policy ID ranges from 1 to 1024.
<b>location elin identifier</b> <i>id</i>	Emergency number in Location Identification TLVs. The policy ID ranges from 1 to 1024.
<b>network-policy profile</b> [ <i>profile-num</i> ]	Network Policy TLV. The network policy ID ranges from 1 to 1024.
<b>power-over-ethernet</b>	Extended Power-via-MDI TLV

**Defaults** All types of LLDP-MED TLVs are not advertised on an interface by default.

**Command** Interface configuration mode

**Mode**

**Usage Guide** When configuring LLDP-MED Capability TLVs, configure LLDP 802.3 MAC/PHY TLVs first. When removing LLDP 802.3 MAC/PHY TLVs, remove 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. When removing LLDP-MED TLVs, remove LLDP-MED TLVs of other types first, so that LLDP-MED capability TLVs can be removed. If a device connects to an IP phone supporting LLDP-MED, the network policy TLV can be configured to deliver policies to the IP phone. The feature is not supported by G.hn ports.

**Configuration** The following example applies LLDP network policy 1 on the 0/17 interface.

**Examples**

```
Ruijie#config
Ruijie(config)#interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)#lldp tlv-enable med-tlv network-policy profile 1
```

The following example applies the LLDP Civic Address (ID: 1) configuration on the 0/17 interface.

```
Ruijie#config
Ruijie(config)#interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)#lldp tlv-enable med-tlv location civic-location identifier 1
```

The following example applies the emergency number (ID: 1) on the 0/17 interface.

```
Ruijie#config
Ruijie(config)#interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)#lldp tlv-enable med-tlv 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**

## 9.24 show lldp local-information

Use this command to display the LLDP information of local device. The information will be encapsulated in the TLVs and sent to the neighbor device.

**show lldp local-information** [ **global** | **interface** *interface-type interface-number* ]

Parameter	Parameter	Description
<b>Description</b>	<b>global</b>	Display the global LLDP information to be sent.
	<b>interface</b> <i>interface-type interface-number</i>	Displays the LLDP information to be sent out from the specified interface.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** If no parameter is specified, all LLDP information is displayed, including global and interface-based LLDP information.

**Configuration Examples** The following example displays the device information to be sent to neighbor device.

```
Ruijie#show lldp local-information
Global LLDP local-information:
  Chassis ID type           : MAC address
  Chassis ID                : 00e0.4c00.215c
  System name               : Ruijie
  System description        : Ruijie Full Gigabit Security Intelligence Access
Switch(RG-HS2310-16GH2GT1XS) By Ruijie Networks
  System capabilities supported : Repeater, Bridge, Router
  System capabilities enabled   : Repeater, Bridge, Router

  LLDP-MED capabilities       : LLDP-MED Capabilities, Network Policy, Location
Identification, Inventory
  Device class               : Network Connectivity
  HardwareRev                : 1.00
  FirmwareRev                : HS2310_RGOS 11.4(1)B90, Release(10221711)
  SoftwareRev                 : HS2310_RGOS 11.4(1)B90, Release(10221711)
  SerialNum                   : MACC942570105
  Manufacturer name           : RUIJIE
```

```
Asset tracking identifier      :
```

Description of fields in the command output is as follows:

Field	Description
Chassis ID type	Chassis ID type for identifying the Chassis ID field
Chassis ID	Used to identify the device, and is generally represented with MAC address
System name	Name of the sending device
System description	Description of the sending device, including hardware/software version, operating system and etc.
System capabilities supported	Capabilities supported by the system
System capabilities enabled	Capabilities currently enabled by the system
LLDP-MED capabilities	LLDP-MED capabilities supported by the system
Device class	MED device class, which is divided into 2 categories: network connectivity device and terminal device. Network connectivity device Class I: normal terminal device Class II: media terminal device; besides Class I capabilities, it also supports media streams. 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: PSE (power sourcing equipment) PD (powered device)
Power-via-MDI power source	Power source type
Power-via-MDI power priority	Power supply priority
Power-via-MDI power value	Available power on port
Model name	Name of model

Related	Command	Description
Commands	N/A	N/A

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

## 9.25 show lldp location

Use this command to display the common LLDP address or emergency number of the local device.  
**show lldp location** { **civic-location** | **elin** } { **identifier** *id* | **interface** *interface-type interface-number* | **static** }

Parameter	Parameter	Description
<b>Description</b>	<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. <i>id</i> indicates the policy ID of configured information.
	<b>Interface</b> <i>interface-type interface-number</i>	Displays the address or emergency number on an interface.
	<b>static</b>	Displays all addresses or emergency numbers configured.

**Defaults** N/A

**Command Mode** 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
civic location information:
-----
Identifier          :1
country             :CH
city                :Fuzhou
```

The following example displays all emergency numbers.

```
Ruijie#show lldp location elin-location static
elin location information:
-----
Identifier          :1
elin number         :085283671111
```

Related Commands	Command	Description
	N/A	N/A

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

## 9.26 show lldp neighbors

Use this command to display the LLDP information about a neighboring device.

**show lldp neighbors** [ **interface** *interface-type interface-number* ] [ **detail** ]

Parameter	Parameter	Description
<b>Description</b>	<b>interface</b> <i>interface-type interface-number</i>	Interface name
	<b>detail</b>	All detailed information about a neighboring device

**Defaults** N/A

**Command Mode** Privileged EXEC mode

- Usage Guide** If the **detail** parameter is not specified, the brief information about a neighboring device is displayed.  
 If the **detail** parameter is specified, the detailed information about a neighboring device is displayed.  
 If the **interface** 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 0/17]
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 0/17
Port description     :

802.1 organizationally information
Port VLAN ID       : 1
Port and protocol VLAN ID(PPVID) : 1
PPVID Supported    : YES
PPVID Enabled      : NO
VLAN name of VLAN 1 : VLAN0001
Protocol Identity  :

802.3 organizationally information
```

```

Auto-negotiation supported : YES
Auto-negotiation enabled  : YES
PMD auto-negotiation advertised : 1000BASE-T full duplex mode, 100BASE-TX full duplex mode,
100BASE-TX half duplex mode, 10BASE-T full duplex mode, 10BASE-T half duplex mode
Operational MAU type      : speed(1000)/duplex(Full)
PoE support               : NO
Link aggregation supported : YES
Link aggregation enabled  : NO
Aggregation port ID      : 0
Maximum frame Size       : 1500
LLDP-MED organizationally information
Power-via-MDI device type :
Power-via-MDI power source :
Power-via-MDI power priority :
Power-via-MDI power value :

```

Description of fields in the command output is as follows:

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	<p>MED device type: network connectivity device and terminal device</p> <p>Network connectivity device:</p> <p>Class I: general terminal device</p> <p>Class II: media terminal device, including capabilities of Class I and supporting media stream</p> <p>Class III: communication terminal device, including capabilities of Class I and Class II and supporting IP communication</p>



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	Command	Description
Commands	N/A	N/A

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

## 9.27 show lldp network-policy

Use this command to display the information about an LLDP network policy.

```
show lldp network-policy { profile [ profile-num ] | interface interface-type interface-number }
```

Parameter	Parameter	Description
Description	<b>profile</b> [ <i>profile-num</i> ]	The information about the specified network policy is displayed.The network policy ID ranges from 1 to 1024.
	<b>interface</b> <i>interface-type interface-number</i>	Interface name
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	If no parameter is specified, the information about all network policies is displayed.	
Configuration Examples	<p>The following example displays the information about a network policy.</p> <pre>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</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

## 9.28 show lldp statistics

The following example displays LLDP statistics.

**show lldp statistics** [ **global** | **interface** *interface-type interface-number* ]

Parameter	Parameter	Description
Description	<b>global</b>	Displays the global LLDP statistics.
	<b>interface</b> <i>interface-type interface-number</i>	Displays the LLDP statistics of the specified interface.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	If no parameter is specified, the information about all LLDP statistics is displayed.	
Configuration Examples	<p>The following example displays all LLDP statistics.</p> <pre>Ruijie# show lldp statistics</pre>	

```

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 0/17]
-----

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
    
```

Description of fields in the command output is as follows:

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 Description  
N/A

## 9.29 show lldp status

Use this command to display LLDP status information.

**show lldp status** [ **interface** *interface-type interface-number* ]

Parameter	Parameter	Description
Description	<b>interface</b> <i>interface-type interface-number</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, the LLDP status information of all ports is displayed.

**Configuration** The following example displays LLDP status information of all ports.

### Examples

```
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 0/17]
-----
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
```

Description of fields in the command output is as follows:

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**

### 9.30 show lldp tlv-config

Use this command to display the advertisable TLV configuration of a port.

**show lldp tlv-config** [ **interface** *interface-type interface-number* ]

Parameter Description	Parameter	Description
	<b>interface</b> <i>interface-type interface-number</i>	Displays the LLDP TLV configuration of the specified interface.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** If no parameter is specified, the LLDP TLV configuration of all ports is displayed.

**Configuration Examples** The following example displays TLV information of port 17.

```
Ruijie# show lldp tlv-config interface GigabitEthernet 0/17
LLDP tlv-config of port [GigabitEthernet 0/17]
```

```
-----
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**

### 9.31 voice vlan

Use this command to configure the LLDP network policy. Use the **no** form of this command to delete the policy.

**{ voice | voice-signaling } vlan { { { vlan-id | dot1p } [ cos cos | dscp dscp ] } | none | untagged }  
no { voice | voice-signaling } vlan**

Parameter Description	Parameter	Description
	<b>voice</b>	Voice application
	<b>voice-signaling</b>	Voice-signaling application
	<i>vlan-id</i>	(Optional) The tagged frame is sent in the voice VLAN in VoIP. The tagged frame includes user_priority and VLAN ID. The VLAN ID of voice flow ranges from 1 to 4094.

<b>dot1p</b>	(Optional) The tagged frame is sent in the voice VLAN in VoIP. The tagged frame contains only user_priorit. The VLAN ID is 0.
<b>cos cos</b>	(Optional) The tagged frame is sent in the voice VLAN in VoIP. The CoS (Class of service) value of the voice flow ranges from 0 to 7. The default value is 5.
<b>dscp dscp</b>	(Optional) The tagged frame is sent in the voice VLAN in VoIP. The DSCP (Differentiated services code point) value of the voice flow ranges from 0 to 63. The default value is 46.
<b>none</b>	(Optional) The network policy is not advertised. VoIP determines the network policy based on its configuration.
<b>untagged</b>	(Optional) The untagged frame is sent in the voice vlan in VoIP. In this case, the value of vlan id and cos are ignored.

**Defaults** The network policy is not advertised. VoIP determines the network policy based on its configuration.

**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 *Configuring QoS*. For details about how to configure the security channel, see *Configuring ACL*.

The **show lldp network-policy profile [ profile-num ]** command can be used to display the LLDP network policy.

**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	Command	Description
Commands	show lldp network-policy profile	Displays the LLDP network policy.

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



## 10 ERPS Commands(beta)

### 10.1 associate sub-ring

Use this command to associate the Ethernet ring with its sub-rings.

**associate sub-ring raps-vlan** *sub-ring-vlan-list*

**no associate sub-ring raps-vlan** *sub-ring-vlan-list*

Parameter Description	Parameter	Description
	<i>sub-ring-vlan-list</i>	Sub-rings' R-APS VLAN. The VLAN ID ranges from 1 to 4094.

**Defaults** By default, Ethernet ring is not associated with its sub-rings.

**Command** ERPS configuration mode.

**Mode**

**Usage Guide** You need to configure this command on all nodes of the Ethernet ring, so as to transmit its sub-ring's ERPS protocol packets in the Ethernet ring.

Configuring the association is mainly to make the sub-ring's protocol packets transmit in the Ethernet ring. Users can also adopt the configuration command provided by the VLAN module to configure elaborately the VLAN and the relation between ports and VLAN, so as to transmit the sub-ring's protocol packets in other Ethernet rings and not leak the packets to the user network.

The feature is not supported by G.hn ports.

**Configuration** The following example associates the Ethernet sub-ring with other Ethernet rings:

**Examples** 1. Enter the privileged EXEC mode and configure the link mode of the Ethernet ring port and the default VLAN.

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/17)# exit
Ruijie(config)# interface GigabitEthernet 0/18
Ruijie(config-if-GigabitEthernet 0/18)# switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/18)# exit
```

2. Enter the erps configuration mode and add the ports that participate in the ERPS protocol computing to the Ethernet ring.

```
Ruijie(config)# erps raps-vlan 4093
Ruijie(config-erps4093)# ring-port west GigabitEthernet 0/17 east GigabitEthernet 0/18
```

3. Configure the Ethernet subring.

```
Ruijie(config)# erps raps-vlan 100
Ruijie(config)# interface TenGigabitEthernet 0/19
```

```
Ruijie(config-if-TenGigabitEthernet 0/19)# switchport mode trunk
Ruijie(config-if-TenGigabitEthernet 0/19)# exit
Ruijie(config)# erps raps-vlan 100
Ruijie(config-erps100)# ring-port west TenGigabitEthernet 0/19 east virtual-channel
Ruijie(config-if-TenGigabitEthernet 0/19)# exit
```

4. Associate the subring with other Ethernet rings.

```
Ruijie(config)# erps raps-vlan 4093
Ruijie(config-erps4093)# associate sub-ring raps-vlan 100
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description**

N/A

## 10.2 erps enable

Use this command to enable the ERPS function in the global configuration mode. Use the **no** form of this command to restore the default setting.

**erps enable**  
**no erps enable**

**Parameter Description**

Parameter	Description
N/A	N/A

**Defaults**

ERPS is enabled by default.

**Command Mode**

Global configuration mode.

**Usage Guide**

The ERPS protocol of the specified ring will begin running truly only after the global ERPS protocol and the ERPS protocol of the specified ring are both enabled. After entering the ERPS configuration mode of the specified ring, configure the **state enable** command to enable the ERPS protocol of this specified ring.

**Configuration Examples**

The following example enables the ERPS protocol globally:

**Examples**

1. Enter the privileged EXEC mode, enable the ERPS function globally.

```
Ruijie# configure terminal
Ruijie(config)# erps enable
```

2. Enter the ERPS configuration mode and enable the ERPS function for the specified ring.

```
Ruijie(config)# erps raps-vlan 4093
```

```
Ruijie(config-erps4093)# state enable
```

<b>Related Commands</b>	Command	Description
	<b>state enable</b>	Enables the ERPS protocol of the specified ring in the ERPS mode of the specified ring.

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

### 10.3 erps monitor link-state by oam

Use this command to configure the method of monitoring the ERPS link state.

**erps monitor link-state by oam vlan** *vlan-id*

**no erps monitor link-state by oam**

<b>Parameter Description</b>	Parameter	Description
	<i>vlan-id</i>	Indicates the VLAN that monitors link state. The VLAN ID ranges from 1 to 4094.

**Defaults** By default, it adopts the directly monitoring the link physical state (up or down) rather than the oam method.

**Command Mode** Global configuration mode.

**Usage Guide** For the link state monitoring, use the method of directly monitoring the link physical state (up or down), also monitor the logic state (unidirectional fault, bidirectional fault or normal) of the link by the OAM. By default, the former is adopted. If the OAM method is used, the inefficient link state monitoring may cause the convergence time longer when the topology changes.

**Configuration Examples** The following example configures the method of monitoring the link state.

1. Enter the privileged EXEC mode and configure the method of monitoring the link state.

```
Ruijie# configure terminal
Ruijie(config)# erps monitor link-state by oam vlan 100
```

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

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

## 10.4 erps raps-vlan

Use this command to configure the R-APS VLAN of Ethernet ring.

**erps raps-vlan** *vlan-id*

**no erps raps-vlan** *vlan-id*

Parameter Description	Parameter	Description
	<i>vlan-id</i>	R-APS VLAN ID. The VLAN ID ranges from 1 to 4094.

**Defaults** No R-APS VLAN is configured by default.

**Command Mode** Global configuration mode.

**Usage Guide** The R-APS VLAN must be the VLAN that is not used on the device. Cannot set the VLAN1 to the R-APS VLAN.  
 The same Ethernet ring of different devices needs the same R-APS VLAN.  
 If you want to transparently transmit the ERPS protocol packets on a device without the ERPS function configured, make sure that only the two ports connected to the Ethernet ring on this device allow the R-APSA VLAN packets corresponding to this ERPS ring passing through. Otherwise, the other VLAN packets may enter the R-APS VLAN through the transparent transmission, causing the shock to the ERPS ring.

**Configuration Examples** The following example configures the R-APS VLAN globally.

```
Ruijie# configure terminal
Ruijie(config)# erps raps-vlan 4093
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 10.5 protected-instance

Use this command to specify the instance protected by the Ethernet ring to implement the load balance function.

**protected-instance** *instance-id-list*

**no protected-instance**

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

<b>Description</b>		
	<i>instance-id-list</i>	ID of the instance protected by this Ethernet ring. The instance ID ranges from 0 to 64.

**Defaults** All instances are protected by default.

**Command Mode** EPRS configuration mode.

**Usage Guide** The protected VLAN consists of the R-APS VLAN of this Ethernet ring and the data VLAN protected by this Ethernet ring.  
Run the **instance** *instance-id* **vlan** *vlan-range* command to map VLANs to an instance before running the **protected-instance** *instance-id-list* command to specify the instance protected by the Ethernet ring. You can implement load balance by configuring more than one Ethernet ring to protect different instances.  
If no instance is specified, all VLANs will be protected. If the instance is specified but no VLAN are mapped to the instance, no VLAN will be protected..

**Configuration Examples** Suppose that the ERP1 and ERP2 are configured on the switch to implement the load balance. The R-APS VLAN of the ERPS1 is 100, the protected data VLAN is in the range of 1 to 99 and 101-2000, the R-APS VLAN of the ERPS2 is 4093, and the protected data VLAN is in the range of 2001 to 4092 and 4094. The following example configures load balance.

1. Enter the privileged EXEC mode.

```
Ruijie# configure terminal
```

2. Configure the VLAN configured by the ERP1.

```
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)# instance 1 vlan 100, 1-99, 101-2000
Ruijie(config-mst)# exit
Ruijie(config)# erps raps-vlan 100
Ruijie(config-erps100)#protected-instance 1
```

3. Configure the VLAN configured by the ERP2.

```
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)# instance 2 vlan 4093, 2001-4092, 4094
Ruijie(config-mst)# exit
Ruijie(config)# erps raps-vlan 4093
Ruijie(config-erps4093)#protected-instance 2
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>instance</b>	Configures instance and VLAN mapping relations.

**Platform Description** N/A

## 10.6 ring-port

Use this command to configure the ERPS ring.

**ring-port west** { *interface-type interface-number* | **virtual-channel** } **east** { *interface-type interface-number* | **virtual-channel** }

**no ring-port**

Parameter Description	Parameter	Description
	<b>west</b> <i>interface-type interface-number</i>	Specifies an interface as the West port of the ERPS ring.
	<b>west virtual-channel</b>	Specifies the virtual interface as the West port of the ERPS ring.
	<b>east</b> <i>interface-type interface-number</i>	Specifies an interface as the East port of the ERPS ring.
	<b>east virtual-channel</b>	Specifies the virtual interface as the East port of the ERPS ring.

**Defaults** No ERPS ring is configured by default.

**Command Mode** EPRS configuration mode.

- Usage Guide**
- After adding the port to the ERP ring, the trunk attribute of the port is not allowed to be modified any more.
  - If the ring port is configured on the virtual-channel, this ring will be considered as a sub-ring.
  - Ports running the ERPS do not participate in the STP computing. ERPS, RERP and REUP do not share the port.
  - The feature is not supported by G.hn ports.

**Configuration** The following example configures the ERPS ring.

**Examples**

1. Enter the privileged EXEC mode.

```
Ruijie# configure terminal
```

2. Configure the link mode of the Ethernet ring port and the default VLAN.

```
Ruijie(config)# interface GigabitEthernet 0/17
```

```
Ruijie(config-if-GigabitEthernet 0/17)# switchport mode trunk
```

```
Ruijie(config-if-GigabitEthernet 0/17)# exit
```

```
Ruijie(config)# interface GigabitEthernet 0/18
```

```
Ruijie(config-if-GigabitEthernet 0/18)# switchport mode trunk
```

```
Ruijie(config-if-GigabitEthernet 0/18)# exit
```

3. Enter the ERPS configuration mode and add the ports that participate in the ERPS protocol computing to the Ethernet ring.

```
Ruijie(config)# erps raps-vlan 4093
```

```
Ruijie(config-erps4093)# ring-port west GigabitEthernet 0/18 east GigabitEthernet 0/18
```

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

Commands	
<b>state enable</b>	Enables the ERPS protocol of the specified ring in the ERPS mode of the specified ring.
<b>switchport mode</b>	Configures the L2 interface (switch port) mode to be Trunk

**Platform** N/A

**Description**

## 10.7 rpl-port

Use this command to configure the RPL port and RPL owner.

**rpl-port { west | east } [ rpl-owner ]**

**no rpl-port**

Parameter	Parameter	Description
<b>Description</b>	<b>west</b>	Specifies the West port as the RRL port.
	<b>east</b>	Specifies the East port as the RRL port.

**Defaults** No RPL port and RPL owner are configured.

**Command** EPRS configuration mode.

**Mode**

**Usage Guide** Up to one RPL link and one RPL owner node are needed and configurable for each ring. The feature is not supported by G.hn ports.

**Configuration** The following example configures the RPL port and RPL owner.

**Examples**

1. Enter the privileged EXEC mode.

```
Ruijie# configure terminal
```

2. Configure the link mode of the Ethernet ring port and the default VLAN.

```
Ruijie(config)# interface GigabitEthernet 0/17
```

```
Ruijie(config-if-GigabitEthernet 0/17)# switchport mode trunk
```

```
Ruijie(config-if-GigabitEthernet 0/17)# exit
```

```
Ruijie(config)# interface GigabitEthernet 0/18
```

```
Ruijie(config-if-GigabitEthernet 0/18)# switchport mode trunk
```

```
Ruijie(config-if-GigabitEthernet 0/18)# exit
```

3. Enter the ERPS configuration mode.

```
Ruijie(config)# erps raps-vlan 4093
```

4. Add the ports that participate in the ERPS protocol computing to the Ethernet ring.

```
Ruijie(config-erps4093)# ring-port west GigabitEthernet 0/17 east GigabitEthernet 0/18
```

5. Specify the port where the RPL link is and the RPL owner.

```
Ruijie(config-erps4093)# rpl-port west rpl-owner
```

**Related Commands**

Command	Description
<b>ring-port</b>	Configures the specified ERP ring in the ERPS configuration mode of the specified ring.
<b>state enable</b>	Enables the ERPS protocol of the specified ring in the ERPS configuration mode of the specified ring.

**Platform** N/A

**Description**

## 10.8 show erps

Use this command to show the parameters and states of the ERPS.

**show erps [ global | raps\_vlan *vlan-id* [ sub-ring ] ]**

**Parameter Description**

Parameter	Description
<b>global</b>	Displays global ERPS information.
<b>raps_vlan <i>vlan-id</i></b>	Displays specified ERPS information. The VLAN ID ranges from 1 to 4094.
<b>sub-ring</b>	Displays specified sub ring information.

**Defaults** N/A

**Command Mode** Any mode.

**Usage Guide** N/A

**Configuration** The following example shows the use of this command.

**Examples**

```
Ruijie# show erps
ERPS Information
Global Status           : Disabled
Link monitored by      : Oam
Oam monitored vid      : 1000
-----
R-APS VLAN              : 1000
Ring Status             : Disabled
West Port               : Te0/19      (Link Normal)
East Port               : Virtual Channel
RPL Port                : None
Protected VLANs        : ALL
```



```

RPL Owner          : Disabled
Holdoff Time       : 0 milliseconds
Guard Time         : 500 milliseconds
WTR Time           : 2 minutes
Current Ring State : initialize
Associate R-APS VLAN :
-----
R-APS VLAN         : 2000
Ring Status        : Disabled
West Port          : None
East Port          : None
RPL Port           : None
Protected VLANs    : ALL
RPL Owner          : Disabled
Holdoff Time       : 0 milliseconds
Guard Time         : 500 milliseconds
WTR Time           : 2 minutes
Current Ring State : initialize
Associate R-APS VLAN :
-----
R-APS VLAN         : 4093
Ring Status        : Disabled
West Port          : Gi0/17      (Link Normal)
East Port          : Gi0/18      (Link Normal)
RPL Port           : West Port
Protected VLANs    : None
RPL Owner          : Enabled
Holdoff Time       : 0 milliseconds
Guard Time         : 500 milliseconds
WTR Time           : 2 minutes
Current Ring State : initialize
Associate R-APS VLAN : 1000
    
```

Description of fields in the command output is as follows:

Field	Description
Global Status	Global ERPS status <ul style="list-style-type: none"> <li>● Enabled: Global ERPS is enabled.</li> <li>● Disabled: Global ERPS is disabled.</li> </ul>
Link monitored by	<ul style="list-style-type: none"> <li>● Not Oam: The ERPS link is not monitored by OAM. Oam: The ERPS link is monitored by OAM.</li> </ul>
Oam monitored vid	ID of the VLAN whose link connectivity is monitored by OAM.
R-APS VLAN	The R-APs VALN ID
Ring Status	<ul style="list-style-type: none"> <li>● Enabled: ERPS ring is enabled.</li> <li>● Disabled: ERPS ring is disabled.</li> </ul>

West Port	The West port of the ERPS ring.
East Port	The East port of the ERPS ring.
RPL Port	<ul style="list-style-type: none"> <li>West Port: The West port is specified as the RPL port.</li> <li>East Port: The East port is specified as the RPL port. None: No RPL port is configured.</li> </ul>
Protected VLANs	<ul style="list-style-type: none"> <li>ALL: All VLANs are protected.</li> <li>1-4094: Some VLANs are protected.</li> <li>None: No VLAN is protected.</li> </ul>
RPL Owner	<ul style="list-style-type: none"> <li>Enabled: The current device is the RPL owner of the Ethernet ring.</li> <li>Disabled: The current device is not the RPL owner of the Ethernet ring.</li> </ul>
Holdoff Time	The Holdoff timer is used to delay topology switchover upon link failure. Range: 1-100. This value, multiplied by 100 milliseconds, equals the Holdoff time.
Guard Time	The Guard timer is used to delay response to SF R-APS packets after the failed link recovers. Range: 1-200. This value, multiplied by 10 milliseconds, equals the Guard time.
WTR Time	The WTR timer is used to delay re-blocking the RPL Owner port after the failed link recovers. <ul style="list-style-type: none"> <li>Range: 1-12 minutes.</li> </ul>
Current Ring State	<ul style="list-style-type: none"> <li>Idle: No failure on the ring; the node is performing normally.</li> <li>Protection: A failure occurs on the ring.</li> </ul>
Sub-Ring R-APS VLANs	ID of the R-APS VLAN of the subring.
TC Propagation State	<ul style="list-style-type: none"> <li>Enable: Enables notification upon subring topology change.</li> <li>Disable: Disables notification upon subring topology change.</li> </ul>

**Related Commands**

Command	Description
<code>erps enable</code>	Enables the global ERPS protocol.

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

### 10.9 state enable

Use this command to enable the ERPS ring. Use the **no** form of this command to disable the specified ERPS ring.

- state enable**
- no state enable**

**Parameter Description**

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

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

**Defaults** Disabled

**Command Mode** EPRS configuration mode.

**Usage Guide** Only after the global ERPS protocol and the ERPS protocol of the specified ring are both enabled, the ERPS protocol of the specified ring will begin truly running.

**Configuration Examples** The following example enables the specified ERPS ring:

1. Enter the privileged EXEC mode.

```
Ruijie# configure terminal
```

2. Configure the link mode of the Ethernet ring port and the default VLAN.

```
Ruijie(config)# interface GigabitEthernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/17)# exit
Ruijie(config)# interface GigabitEthernet 0/18
Ruijie(config-if-GigabitEthernet 0/18)# switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/18)# exit
```

3. Enter the ERPS configuration mode. Add the ports that participate in the ERPS protocol computing to the Ethernet ring. Enable the ERPS function for the specified ring.

```
Ruijie(config)# erps raps-vlan 4093
Ruijie(config-erps4093)# ring-port west GigabitEthernet 0/17 east GigabitEthernet 0/18
Ruijie(config-erps4093)# state enable
```

4. Enable the global ERPS function.

```
Ruijie(config-erps4093)# exit
Ruijie(config)# erps enable
```

**Related Commands**

Command	Description
<b>erps enable</b>	Enables the global ERPS protocol.

**Platform** N/A

**Description**

### 10.10 sub-ring tc-propagation

Use this command to specify the devices corresponding to the crossing node on the crossing ring whether to send out the notification when the subring topology changes.

**sub-ring tc\_propagation enable**

**no sub-ring tc\_propagation**

**Parameter**

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

<b>Description</b>	
	<b>enable</b> Enables notification upon subring topology change.

**Defaults** By default, the topology changing notification is not sent.

**Command** EPRS configuration mode.

**Mode**

**Usage Guide** This command is just needed to be configured on the crossing nodes on the crossing ring.

**Configuration** The following example enables notification upon subring topology change.

**Examples**

```
Ruijie> enable
Ruijie# configure terminal
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/17)# exit
Ruijie(config)# interface gigabitethernet 0/18
Ruijie(config-if-GigabitEthernet 0/18)# switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/18)# exit
Ruijie(config)# erps raps-vlan 4093
Ruijie(config-erps 4093)# ring-port west gigabitethernet 0/17 east gigabitethernet 0/18
Ruijie(config-erps 4093)# associate sub-ring raps-vlan 100
Ruijie(config-erps 4093)# state enable
Ruijie(config-erps 4093)# exit
Ruijie(config)# interface tengigabitethernet 0/19
Ruijie(config-if-TenGigabitEthernet 0/19)# switchport mode trunk
Ruijie(config-if-TenGigabitEthernet 0/19)# exit
Ruijie(config)# erps raps-vlan 100
Ruijie(config-erps 100)# ring-port west tengigabitethernet 0/19 east virtual-channel
Ruijie(config-erps 100)# sub-ring tc-propagation enable
Ruijie(config-erps 100)# state enable
Ruijie(config-erps 100)# exit
Ruijie(config)# erps enable
```

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

**Platform** N/A

**Description**

## 10.11 timer

Use this command to configure the timer of the ERPS protocol.

**timer** { **holdoff-time** *holdoff* | **guard-time** *guard* | **wtr-time** *wtr* }  
**no timer** { **holdoff-time** | **guard-time** | **wtr-time** }

**Parameter Description**

Parameter	Description
<b>holdoff-time</b> <i>holdoff</i>	Value of the Holdoff timer in 100 milliseconds, the valid range is 0 to 100.
<b>guard-time</b> <i>guard</i>	Value of the Guard timer in 10 milliseconds, the valid range is 1 to 200.
<b>wtr-time</b> <i>wtr</i>	Value of the WTR in minute, the valid range is 1 to 12.

**Defaults**

Holdoff timer: 0 milliseconds.  
 Guard timer: 500 milliseconds.  
 WTP timer: 2 seconds.

**Command Mode**

ERPS configuration mode.

**Usage Guide**

**Holdoff timer:** This timer is used to avoid the ERPS from topology switching continuously due to the link intermittent fault. With this timer configured, if the link fault is detected, the ERPS does not perform the topology switching immediately until the timer times out and the link fault is verified.

**Guard timer:** This timer is used to prevent the device receiving the timed-out R-APS messages. When the device detects the recovery from failure of the link, it sends out the message of link recovery and starts up the Guard timer. Before the Guard times out, except for the flush packets indicating the subring topology change, other packets are discarded directly without being handled.

**WTR (Wait-to-restore) timer:** This timer is only valid for the RPL owner device. It is mainly used to prevent the RPL owner making the erroneous judgment to the ring network status. When the RPL detects the fault recovery, it does not perform the topology switching immediately until the WTR times out and the Ethernet ring indeed recovers from the fault. If the ring network fault is checked again before the WTR times out, then the WTR timer will be canceled and topology switching will be not executed any longer.

**Configuration**

The following example configures the timer of the ERPS protocol.

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# erps raps-vlan 4093
Ruijie(config-erps4093)# timer holdoff-time 10
Ruijie(config-erps4093)# timer guard-time 10
Ruijie(config-erps4093)# timer wtr-time 10
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description**

N/A



## ACL & QoS Configuration Commands

---

1. ACL Commands
2. QoS Commands

# 1 ACL Commands

## 1.1 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.

1. Standard IP access list (1 to 99, 1300 to 1999)

```
access-list acl-id { deny | permit } { source-ipv4-address source-ipv4-wildcard | any | host
source-ipv4-address } [ time-range time-range-name ] [ log ]
```

2. Extended IP access list (100 to 199, 2000 to 2699)

```
access-list acl-id { deny | permit } protocol { source-ipv4-address source-ipv4-wildcard | any | host
source-ipv4-address } [ eq port | gt port | lt port | neq port | range lower upper ]
{ destination-ipv4-address destination-ipv4-wildcard | any | host destination-ipv4-address } [ dscp
dscp ] [ fragment ] [ precedence precedence ] [ tos tos ] [ eq port | gt port | lt port | neq port | range
lower upper ] [ match-all tcp-flag | established ] [ time-range time-range-name ] [ log ]
```

3. 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 ] [ cos [ cos ]
[ inner cos ] ] [ time-range time-range-name ]
```

4. Extended expert access list (2700 to 2899)

```
access-list acl-id { deny | permit } [ protocol | [ ethernet-type ] [ cos [ cos ] [ inner cos ] ] ] [ VID [ vid ]
[ inner vid ] ] { source-ipv4-address source-ipv4-wildcard | any | host source-ipv4-address }
{ source-mac-address mask | any | host source-mac-address } [ eq port | gt port | lt port | neq port |
range lower upper ] { destination-ipv4-address destination-ipv4-wildcard | any | host
destination-ipv4-address } { any | host destination-mac-address } [ eq port | gt port | lt port | neq port |
range lower upper ] [ dscp dscp ] [ precedence precedence ] [ tos tos ] [ fragment ] [ match-all
tcp-flag | established ] [ time-range time-range-name ]
```

- When you select the Ethernet-type field or cos field:

```
access-list acl-id { deny | permit } { ethernet-type | cos [ cos ] [ inner cos ] } [ VID [ vid ] [ inner vid ] ]
{ source-mac-address mask | any | host source-mac-address } { any | host
destination-mac-address } [ time-range time-range-name ]
```

- When you select the protocol field:

```
access-list acl-id { deny | permit } protocol { source-ipv4-address source-ipv4-wildcard | any | host
source-ipv4-address } { source-mac-address mask | any | host source-mac-address } [ eq port | gt
port | lt port | neq port | range lower upper ] { destination-ipv4-address destination-ipv4-wildcard | any
| host destination } { any | host destination-mac-address } [ eq port | gt port | lt port | neq port | range
lower upper ] [ dscp dscp ] [ precedence precedence ] [ tos tos ] [ fragment ] [ match-all tcp-flag |
established ] [ time-range time-range-name ]
```

- Extended expert ACLs of some important protocols:

**Internet Control Message Protocol (ICMP)**

```
access-list acl-id { deny | permit } icmp { source-ipv4-address source-ipv4-wildcard | any | host
source-ipv4-address } { source-mac-address mask | any | host source-mac-address }
```

{ *destination-ipv4-address destination-ipv4-wildcard* | **any** | **host** *destination-ipv4-address* } { **any** | **host** *destination-mac-address* } [ *icmp-type* ] [ [ *icmp-type* [ *icmp-code* ] ] | [ *icmp-message* ] ] [ **dscp** *dscp* ] [ **precedence** *precedence* ] [ **tos** *tos* ] [ **fragment** ] [ **time-range** *time-range-name* ]

**Transmission Control Protocol (TCP)**

**access-list** *acl-id* { **deny** | **permit** } **tcp** { *source-ipv4-address source-ipv4-wildcard* | **any** | **host** *source-ipv4-address* } { *source-mac-address mask* | **any** | **host** *source-mac-address* } [ **eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper* ] { *destination-ipv4-address destination-ipv4-wildcard* | **any** | **host** *destination-ipv4-address* } { **any** | **host** *destination-mac-address* } [ **eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper* ] [ **dscp** *dscp* ] [ **precedence** *precedence* ] [ **tos** *tos* ] [ **fragment** ] [ **match-all** *tcp-flag* | **established** ] [ **time-range** *time-range-name* ]

**User Datagram Protocol (UDP)**

**access-list** *acl-id* { **deny** | **permit** } **udp** { *source-ipv4-address source-wildcard* | **any** | **host** *source-ipv4-address* } { *source-mac-address mask* | **any** | **host** *source-mac-address* } [ **eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper* ] { *destination-ipv4-address destination-ipv4-wildcard* | **any** | **host** *destination-ipv4-address* } { **any** | **host** *destination-mac-address* } [ **eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper* ] [ **dscp** *dscp* ] [ **precedence** *precedence* ] [ **tos** *tos* ] [ **fragment** ] [ **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, 2700 to 2899, and 700 to 799
<b>deny</b>	If not matched, access is denied
<b>permit</b>	If matched, access is permitted
<i>source-ipv4-address</i>	Specify the source IP address (host address or network address)
<i>source-ipv4-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-ipv4-address</i>	Specify the destination IP address (host address or network address)
<i>destination-ipv4-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>dscp</b>	Differentiated service code point
<i>dscp</i>	Code point value, ranging from 0 to 63
<b>precedence</b>	Specify the packet priority
<i>precedence</i>	Packet precedence value (0 to 7)
<b>eq</b>	Equal operator
<b>gt</b>	Greater operator
<b>lt</b>	Smaller operator
<b>neq</b>	Unequal operator
<i>port</i>	Layer4 port number
<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)
<i>icmp-type</i>	ICMP message type (0 to 255)
<i>icmp-code</i>	ICMP message type code (0 to 255)
<i>icmp-message</i>	ICMP message type name
<b>host</b> <i>source-mac-address</i>	Source physical address
<b>host</b> <i>destination-mac-address</i>	Destination physical address
<b>cos</b> <i>cos</i>	Match the specified cos field in the outer tag
<b>inner</b> <i>cos</i>	Match the specified cos field in the inner tag
<b>VID</b> <i>vid</i>	Match the specified VLAN ID field in the outer tag
<b>inner</b> <i>vid</i>	Match the specified VLAN ID field in the inner tag
<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>log</b>	Logs will be periodically output if packets matching the ACEs are found

**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.

The extended expert access list (2700 to 2899) is a combination of the above and can match and filter the VLAN ID.

For the layer-3 routing protocols including the unicast routing protocol and multicast routing protocol, the following parameters are not supported by the ACL: **precedence** *precedence/tos* *tos/fragments/range* *lower upper/time-range* *time-range-name*

The TCP Flag includes part or all of the following:

- urg
- ack
- psh

- rst
- syn
- fin

The packet precedence is as below:

- critical
- flash
- flash-override
- immediate
- internet
- network
- priority
- routine

The service types are as below:

- max-reliability
- max-throughput
- min-delay
- min-monetary-cost
- normal

The ICMP message types are as below:

- administratively-prohibited
- dod-host-prohibited
- dod-net-prohibited
- echo
- echo-reply
- fragment-time-exceeded
- general-parameter-problem
- host-isolated
- host-precedence-unreachable
- host-redirect
- host-tos-redirect
- host-tos-unreachable
- host-unknown
- host-unreachable
- information-reply
- information-request
- mask-reply
- mask-request
- mobile-redirect
- net-redirect
- net-tos-redirect
- net-tos-unreachable

- net-unreachable
- network-unknown
- no-room-for-option
- option-missing
- packet-too-big
- parameter-problem
- port-unreachable
- precedence-unreachable
- protocol-unreachable
- redirect
- device-advertisement
- device-solicitation
- source-quench
- source-route-failed
- time-exceeded
- timestamp-reply
- timestamp-request
- ttl-exceeded
- unreachable

The TCP ports are as follows. A port can be specified by port name and port number:

- bgp
- chargen
- cmd
- daytime
- discard
- domain
- echo
- exec
- finger
- ftp
- ftp-data
- gopher
- hostname
- ident
- irc
- klogin
- kshell
- ldp
- login
- nntp
- pim-auto-rp
- pop2
- pop3

- smtp
- sunrpc
- syslog
- tacacs
- talk
- telnet
- time
- uucp
- whois
- www

The UDP ports are as follows. A UDP port can be specified by port name and port number.

- biff
- bootpc
- bootps
- discard
- dnsix
- domain
- echo
- isakmp
- mobile-ip
- nameserver
- netbios-dgm
- netbios-ns
- netbios-ss
- ntp
- pim-auto-rp
- rip
- snmp
- snmptrap
- sunrpc
- syslog
- tacacs
- talk
- tftp
- time
- who
- xdmcp

The Ethernet types are as below:

- aarp
- appletalk
- decnet-iv
- diagnostic

- etype-6000
- etype-8042
- lat
- lavc-sca
- mop-console
- mop-dump
- mumps
- netbios
- vines-echo
- xns-idp

**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 0/17. The configuration procedure is as below:

```
Ruijie(config)# access-list 702 deny host 00d0f8000c0c any aarp
```

```
Ruijie(config)# interface gigabitEthernet0/17
```

```
Ruijie(config-if-GigabitEthernet 0/17)# mac access-group 702 in
```

4. Example of the extended expert ACL

The following example shows how to create and display an extended expert ACL. This expert ACL denies all the TCP packets with the source IP address 192.168.12.3 and the source MAC address 00d0.f800.0044.

```
Ruijie(config)# access-list 2702 deny tcp host 192.168.12.3 0.0.0.0 00d0.f800.0044
0000.0000.0000 any any
```

```
Ruijie(config)# access-list 2702 permit any any any any
```

```
Ruijie(config)# show access-lists
```

```
expert access-list extended 2702
```

```
10 deny tcp host 192.168.12.3 host 00d0.f800.0044 any any
```

```
10 permit any any any any
```

**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**

## 1.2 access-list list-remark

Use this command to write a helpful comment (remark) for an access list. Use the **no** form of this command to remove the remark.

**access-list** *acl-id* **list-remark** *comment*

**no access-list** *acl-id* **list-remark**

Parameter Description	Parameter	Description
	<i>acl-id</i>	Access list number. Standard IP ACL: 1 to 99, 1300 to 1999. Extended IP ACL: 100 to 199. 2000 to 2699. Extended MAC ACL: 700 to 799. Extended Expert ACL: 2700 to 2899.
	<i>comment</i>	Comment that describes the access list.

**Defaults** The access lists have no remarks by default.

**Command Mode** Global configuration mode

**Usage Guide** You can use this command to write a helpful comment for a specified access list. If the specified access list does not exist, the command will create the access list, then add remarks for the access list.

**Configuration Examples** The following example writes a comment of "this acl is to filter the host 192.168.4.12" for ACL100.

```
Ruijie(config)# ip access-list extended 100
```

```
Ruijie(config)# access-list 100 list-remark this acl is to filter the host 192.168.4.12
```

Related Commands	Command	Description
	<b>show access-lists</b>	Displays all access lists, including the remarks for the access lists.

**Platform Description**

## 1.3 access-list remark

Use this command to write a helpful comment (remark) for an entry in a numbered access list. Use

the **no** form of this command to remove the remark.

**access-list** *acl-id* **remark** *comment*

**no access-list** *acl-id* **remark** *comment*

**Parameter  
Description**

Parameter	Description
<i>acl-id</i>	Access list number. Standard IP ACL: 1 to 99, 1300 to 1999. Extended IP ACL: 100 to 199. 2000 to 2699. Extended MAC ACL: 700 to 799. Extended Expert ACL: 2700 to 2899.
<i>comment</i>	Comment that describes the access list entry.

**Defaults** The access list entries have no remarks by default.

**Command  
Mode** Global configuration mode

**Usage Guide** You can use this command to write a helpful comment for an entry in a specified access list. If the specified access list does not exist, the command will create the access list, then add remarks for the access entry.

**Configuration** The following example writes a comment for an entry in ACL102.

**Examples** Ruijie(config)# access-list 102 remark deny-host-10.1.1.1

**Related  
Commands**

Command	Description
<b>show access-lists</b>	Displays all access lists, including the remarks for the access list entries.

**Platform  
Description**

## 1.4 clear access-list counters

Use this command to clear counters of packets matching the deny entries in ACLs.

**clear access-list counters** [*acl-id* | *acl-name* ]

**Parameter  
Description**

Parameter	Description
<i>acl-id</i>	Access list number

<i>acl-name</i>	Access list name
-----------------	------------------

**Defaults****Command** Privileged EXEC mode**Mode****Usage Guide** This command is used to clear the counters of packets matching the deny entries in ACLs.**Configuration** The following example clears the packet matching counter of ACL No. 1:**Examples** Before configuration:

```
Ruijie# show access-lists
ip access-list standard 1
 10 deny host 50.1.1.2 (10 matches)
 20 permit host 60.1.1.2 (15 matches)
(10 packets filtered)
```

## After configuration:

```
Ruijie# clear access-list counters
Ruijie# show access-lists
ip access-list standard 1
 10 deny host 50.1.1.2 (10 matches)
 20 permit host 60.1.1.2 (15 matches)
```

**Related  
Commands**

Command	Description
N/A	N/A

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

## 1.5 clear counters access-list

Use this command to clear counters of packets matching ACLs.

**clear counters access-list** [*acl-id* | *acl-name* ]**Parameter  
Description**

Parameter	Description
<i>acl-id</i>	Access list number
<i>acl-name</i>	Access list name

**Defaults**



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

**Usage Guide** This command is used to clear the counters of packets matching the specified or all ACLs.

**Configuration** The following example clears the packet matching counter of ACL No. 2700:

**Examples**

```
Ruijie #show access-lists 2700
expert access-list extended 2700
    10 permit ip VID 4 host 192.168.3.55 any host 192.168.99.6 any (88 matches)
    20 deny tcp any any eq login any any (33455 matches)
    30 permit tcp any any host 192.168.6.9 any (10 matches)

Ruijie# clear counters access-list 2700
Ruijie# show access-lists 2700
expert access-list extended 2700
    10 permit ip VID 4 host 192.168.3.55 any host 192.168.99.6 any
    20 deny tcp any any eq login any any
    30 permit tcp any any host 192.168.6.9 any
```

**Related Commands**

Command	Description
N/A	N/A

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

## 1.6 deny

One or multiple **deny** conditions are used to determine whether to forward or discard the packet. In ACL configuration mode, you can modify the existent ACL or configure according to the protocol details.

1. Standard IP ACL

```
[ sn ] deny { source-ipv4-address source-ipv4-wildcard | any | host source-ipv4-address }
[ time-range time-range-name ] [ log ]
```

2. Extended IP ACL

```
[ sn ] deny protocol { source-ipv4-address source-ipv4-wildcard | any | host source-ipv4-address }
[ eq port | gt port | lt port | neq port | range lower upper ] { destination-ipv4-address
destination-ipv4-wildcard | any | host destination-ipv4-address } [ dscp dscp ] [ fragment ]
[ precedence precedence ] [ tos tos ] [ eq port | gt port | lt port | neq port | range lower upper ]
[ match-all tcp-flag | established ] [ time-range time-range-name ] [ log ]
```

Extended IP ACLs of some important protocols:

- Internet Control Message Protocol (ICMP)

```
[ sn ] deny icmp { source-ipv4-address source-ipv4-wildcard | any | host source-ipv4-address }
{ destination-ipv4-address destination-ipv4-wildcard | any | host destination-ipv4-address }
```

[ *icmp-type* ] [ [ *icmp-type* [ *icmp-code* ] ] | [ *icmp-message* ] ] [ **dscp** *dscp* ] [ **precedence** *precedence* ] [ **tos** *tos* ] [ **fragment** ] [ **time-range** *time-range-name* ]

- Transmission Control Protocol (TCP)

[ *sn* ] **deny tcp** { *source-ipv4-address* *source-wildcard* | **any** | **host** *source-ipv4-address* } [ **eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper* ] { *destination-ipv4-address* *destination-ipv4-wildcard* | **any** | **host** *destination-ipv4-address* } [ **eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper* ] [ **dscp** *dscp* ] [ **precedence** *precedence* ] [ **tos** *tos* ] [ **fragment** ] [ **match-all** *tcp-flag* | **established** ] [ **time-range** *time-range-name* ]

- User Datagram Protocol (UDP)

[ *sn* ] **deny udp** { *source-ipv4-address* *source-wildcard* | **any** | **host** *source-ipv4-address* } [ **eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper* ] { *destination-ipv4-address* *destination-ipv4-wildcard* | **any** | **host** *destination-ipv4-address* } [ **eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper* ] [ **dscp** *dscp* ] [ **precedence** *precedence* ] [ **tos** *tos* ] [ **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* ] [ **cos** [ *cos* ] [ **inner** *cos* ] ] [ **time-range** *time-range-name* ]

### 4. Extended expert ACL

[ *sn* ] **deny** [ *protocol* | [ *ethernet-type* ] [ **cos** [ *cos* ] [ **inner** *cos* ] ] ] [ **VID** [ *vid* ] [ **inner** *vid* ] ] { *source-ipv4-address* *source-ipv4-wildcard* | **any** | **host** *source-ipv4-address* } { *source-mac-address* *mask* | **any** | **host** *source-mac-address* } [ **eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper* ] { *destination-ipv4-address* *destination-ipv4-wildcard* | **any** | **host** *destination-ipv4-address* } { **any** | **host** *destination-mac-address* } [ **eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper* ] [ **dscp** *dscp* ] [ **precedence** *precedence* ] [ **tos** *tos* ] [ **fragment** ] [ **match-all** *tcp-flag* | **established** ] [ **time-range** *time-range-name* ]

- When you select the *ethernet-type* field or *cos* field:

[ *sn* ] **deny** { *ethernet-type* | **cos** [ *cos* ] [ **inner** *cos* ] } [ **VID** [ *vid* ] [ **inner** *vid* ] ] { *source-mac-address* *mask* | **any** | **host** *source-mac-address* } { **any** | **host** *destination-mac-address* } [ **time-range** *time-range-name* ]

- When you select the *protocol* field:

[ *sn* ] **deny** *protocol* [ **VID** [ *vid* ] ] { *source-ipv4-address* *source-ipv4-wildcard* | **any** | **host** *source-ipv4-address* } { *source-mac-address* *mask* | **any** | **host** *source-mac-address* } [ **eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper* ] { *destination-ipv4-address* *destination-ipv4-wildcard* | **any** | **host** *destination-ipv4-address* } { **any** | **host** *destination-mac-address* } [ **eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper* ] [ **dscp** *dscp* ] [ **precedence** *precedence* ] [ **tos** *tos* ] [ **fragment** ] [ **match-all** *tcp-flag* | **established** ] [ **time-range** *time-range-name* ]

- Extended expert ACLs of some important protocols

#### Internet Control Message Protocol (ICMP)

[ *sn* ] **deny icmp** [ **VID** [ *vid* ] ] { *source-ipv4-address* *source-ipv4-wildcard* | **any** | **host** *source-ipv4-address* } { *source-mac-address* *mask* | **any** | **host** *source-mac-address* } { *destination-ipv4-address* *destination-ipv4-wildcard* | **any** | **host** *destination-ipv4-address* } { **any** | **host** *destination-mac-address* } [ *icmp-type* ] [ [ *icmp-type* [ *icmp-code* ] ] | [ *icmp-message* ] ] [ **dscp** *dscp* ] [ **precedence** *precedence* ] [ **tos** *tos* ] [ **fragment** ] [ **time-range** *time-range-name* ]

#### Transmission Control Protocol (TCP)

```
[ sn ] deny tcp [ VID [ vid ] { source-ipv4-address source-ipv4-wildcard | any | host
source-ipv4-address } { source-mac-address mask | any | host source-mac-address } [ eq port | gt
port | lt port | neq port | range lower upper ] { destination-ipv4-address destination-ipv4-wildcard | any
| host destination-ipv4-address } { any | host destination-mac-address } [ eq port | gt port | lt port |
neq port | range lower upper ] [ dscp dscp ] [ precedence precedence ] [ tos tos ] [ fragment ]
[ match-all tcp-flag | established ] [ time-range time-range-name ]
```

#### User Datagram Protocol (UDP)

```
[ sn ] deny udp [ VID [ vid ] [ inner vid ] ] { source-ipv4-address source-ipv4-wildcard | any | host
source-ipv4-address } { source-mac-address mask | any | host source-mac-address } [ eq port | gt
port | lt port | neq port | range lower upper ] { destination-ipv4-address destination-ipv4-wildcard | any
| host destination-ipv4-address } { any | host destination-mac-address } [ eq port | gt port | lt port |
neq port | range lower upper ] [ dscp dscp ] [ precedence precedence ] [ tos tos ] [ fragment ]
[ time-range time-range-name ]
```

#### 5. ACL80

```
[ sn ] deny hex hex-mask offset
```

#### 6. Extended IPv6 ACL

```
[ sn ] deny ipv6-protocol { any | host source-ipv6-address } [ eq port | gt port | lt port | neq port |
range lower upper ] { any | host destination-ipv6-address } [ eq port | gt port | lt port | neq port |
range lower upper ] [ dscp dscp ] [ flow-label flow-label ] [ fragment ] [ match-all tcp-flag |
established ] [ time-range time-range-name ] [ log ]
```

Extended IPv6 ACLs of some important protocols:

#### Internet Control Message Protocol (ICMP)

```
[ sn ] deny icmp { any | host source-ipv6-address } { any | host destination-ipv6-address }
[ icmp-type ] [ [ icmp-type [ icmp-code ] ] [ icmp-message ] ] [ dscp dscp ] [ flow-label flow-label ]
[ fragment ] [ time-range time-range-name ] [ log ]
```

#### Transmission Control Protocol (TCP)

```
[ sn ] deny tcp { any | host source-ipv6-address } [ eq port | gt port | lt port | neq port | range lower
upper ] { any | host destination-ipv6-address } [ eq port | gt port | lt port | neq port | range lower
upper ] [ dscp dscp ] [ flow-label flow-label ] [ fragment ] [ match-all tcp-flag | established ]
[ time-range time-range-name ] [ log ]
```

#### User Datagram Protocol (UDP)

```
[ sn ] deny udp { any | host source-ipv6-address } [ eq port | gt port | lt port | neq port | range lower
upper ] { any | host destination-ipv6-address } [ eq port | gt port | lt port | neq port | range lower
upper ] [ dscp dscp ] [ flow-label flow-label ] [ fragment ] [ time-range time-range-name ] [ log ]
```

#### Parameter Description

Parameter	Description
<i>sn</i>	ACL entry sequence number
<b>deny</b>	If matched, access is denied.
<i>source-ipv4-address</i>	Specify the source IP address (host address or network address).
<i>source-ipv4-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-ipv4-address</i>	Specify the destination IP address (host address or network address).
<i>destination-ipv4-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>dscp</b>	Differentiated service code point
<i>dscp</i>	Code point value, ranging from 0 to 63
<b>precedence</b>	Specify the packet priority.
<i>precedence</i>	Packet precedence value (0 to 7)
<b>eq</b>	Equal operator
<b>gt</b>	Greater operator
<b>lt</b>	Smaller operator
<b>neq</b>	Unequal operator
<i>port</i>	Layer4 port number
<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>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
<b>host</b> <i>source-mac-address</i>	Source physical address
<b>host</b> <i>destination-mac-address</i>	Destination physical address
<b>cos</b> <i>cos</i>	Match the specified cos field in the outer tag
<b>inner</b> <i>cos</i>	Match the specified cos field in the inner tag
<b>VID</b> <i>vid</i>	Match the specified VLAN ID field in the outer tag
<b>inner</b> <i>vid</i>	Match the specified VLAN ID field in the inner tag
<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.
<i>prefix-length</i>	Prefix mask length
<i>source-ipv6-address</i>	Source IPv6 address
<i>destination-ipv6-address</i>	Destination IPv6 address
<b>flow-label</b>	Flow label
<i>flow-label</i>	Flow label value, within the range of 0 to 1048575.
<i>ipv6-protocol</i>	For the IPv6, the field can be <code>ipv6   icmp   tcp   udp</code> and number in the range 0 to 255
<b>time-range</b>	Time range of the packet filtering
<i>time-range-name</i>	Time range name of the packet filtering

<b>log</b>	Logs will be periodically output if packets matching the ACEs are found
------------	---

**Defaults** No entry

**Command mode** ACL configuration mode.

**Usage Guide** Use this command to configure the filtering entry of ACLs in ACL configuration mode.

**Configuration Examples** The following example shows how to create and display an extended expert ACL. This expert ACL denies all the TCP packets with the source IP address 192.168.4.12 and the source MAC address 001300498272.

```
Ruijie(config)# expert access-list extended 2702
Ruijie(config-exp-nacl)# deny tcp host 192.168.4.12 host 0013.0049.8272 any any
Ruijie(config-exp-nacl)# permit any any any any
Ruijie(config-exp-nacl)# show access-lists
expert access-list extended 2702
10 deny tcp host 192.168.4.12 host 0013.0049.8272 any any
20 permit any any any any
Ruijie(config-exp-nacl)#
```

This example shows how to use the extended IP ACL. The purpose is to deny the host with the IP address 192.168.4.12 to provide services through the TCP port 100 and apply the ACL to Interface GigabitEthernet 0/17. 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 0/17
Ruijie(config-if-GigabitEthernet 0/17)# 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 0/17. The configuration procedure is as below:

```
Ruijie(config)# mac access-list extended macl
Ruijie(config-mac-nacl)# deny host 0013.0049.8272 any aarp
Ruijie(config-mac-nacl)# show access-lists
mac access-list extended macl
10 deny host 0013.0049.8272 any aarp
Ruijie(config-mac-nacl)# exit
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# mac access-group macl 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 0/17
Ruijie(config-if-GigabitEthernet 0/17)# ip access-group 34 in
```

This example shows how to use the extended IPv6 ACL. The purpose is to deny the host with the IP address 192.168.4.12 and apply the rule to Interface GigabitEthernet 0/1. The configuration procedure is as below:

```
Ruijie(config)# ipv6 access-list v6-acl
Ruijie(config-ipv6-nacl)# 11 deny ipv6 host 2001::1 any
Ruijie(config-ipv6-nacl)# show access-lists
ipv6 access-list extended v6-acl
11 deny ipv6 host 2001::1 any
Ruijie(config-ipv6-nacl)# exit
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 traffic-filter v6-acl in
```

#### Related Commands

Command	Description
<b>show access-lists</b>	Displays all ACLs.
<b>ip access-list</b>	Defines an IP ACL.
<b>mac access-list</b>	Defines an extended MAC ACL.
<b>expert access-list</b>	Defines an extended expert ACL.
<b>ipv6 access-list</b>	Defines an extended IPv6 ACL.

**Platform** N/A

**Description**

## 1.7 expert access-group

Use this command to apply the specified expert access list globally or on the specified interface. Use the **no** form of the command to remove the application.

**expert access-group** { *acl-id* | *acl-name* } **in**

**no expert access-group** { *acl-id* | *acl-name* } **in**

#### Parameter Description

Parameter	Description
<i>acl-id</i>	Expert access list number: 2700 to 2899
<i>acl-name</i>	Name of the expert access list

<b>in</b>	Specifies filtering on inbound packets.
-----------	---

**Defaults** No expert access list is applied globally or on the interface.

**Command mode** Global or interface configuration mode.

**Usage Guide** This command is used to apply the specified access list globally or on the interface to control the input and output data streams. Use the **show access-group** command to view the setting.

**Configuration Examples** The following example shows how to apply the **access-list accept\_00d0f8xxxxxx** only to Gigabit interface 0/17:

```
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# expert access-group accept_00d0f8xxxxxx_only in
```

**Related Commands**

Command	Description
<b>show access-group</b>	Displays the ACL configuration.

**Platform Description** N/A

## 1.8 expert access-list advanced

Use this command to create an advanced expert access list and place the device in expert advanced access list configuration mode. Use the **no** form of this command to remove the advanced expert access list.

**expert access-list advanced** *acl-name*

**no expert access-list advanced** *acl-name*

**Parameter Description**

Parameter	Description
<i>acl-name</i>	Name of the advanced expert access list

**Defaults** N/A

**Command mode** Global configuration mode

**Usage Guide** Use this command to create an advanced expert access list (namely, ACL80) to match your custom fields.

**Configuration Examples** The following example creates an advanced expert access list named adv-acl.

```
Ruijie(config)# expert access-list advanced adv-acl
```

```
Ruijie(config-exp-dacl)# show access-lists
expert access-list advanced adv-acl
```

**Related Commands**

Command	Description
<b>show access-lists</b>	Displays all access lists.

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

### 1.9 expert access-list counter

Use this command to enable the counter of packets matching the specified expert access list. Use the **no** form of this command to disable this function.

```
expert access-list counter { acl-id | acl-name }
no expert access-list counter { acl-id | acl-name }
```

**Parameter Description**

Parameter	Description
<i>acl-id</i>	Expert access list number: 2700 to 2899.
<i>acl-name</i>	Name of the access list.

**Defaults** The counter of the packets matching the expert access list is disabled.

**Command mode** Global configuration mode

**Usage Guide** Use this command to enable the counter of packets matching the specified expert access list, so that you can analyze the counters to learn whether the network is attacked by the illegal packets.

**Configuration Examples** The following example enables the counter of packets matching the extended expert access list named exp-acl:

```
Ruijie(config)# expert access-list counter exp-acl
Ruijie(config)# show access-lists
expert access-list extended exp-acl
 10 permit ip VID 4 host 192.168.3.55 any host 192.168.99.6 any (16 matches)
 20 deny tcp any any eq login any any (78 matches)
```

The following example disables the counter of packets matching the extended expert access list named exp-acl.

```
Ruijie(config)# no expert access-list counter exp-acl
Ruijie(config)# show access-lists
expert access-list extended 2700
```



```
10 permit ip VID 4 host 192.168.3.55 any host 192.168.99.6 any
20 deny tcp any any eq login any any
```

**Related  
Commands**

Command	Description
<b>show access-lists</b>	Displays the extended expert ACL.

**Platform  
Description**

N/A

## 1.10 expert access-list extended

Use this command to create an extended expert access list. Use the **no** form of the command to remove the ACL.

**expert access-list extended** { *acl-id* | *acl-name* }

**no expert access-list extended** { *acl-id* | *acl-name* }

**Parameter  
Description**

Parameter	Description
<i>acl-id</i>	Extended expert access list number: 2700 to 2899
<i>acl-name</i>	Name of the extended expert access list

**Defaults**

N/A

**Command  
mode**

Global configuration mode.

**Usage Guide**Use the **show access-lists** command to display the ACL configurations.

**Configuration** Create an extended expert ACL named exp-acl:

**Examples**

```
Ruijie(config)# expert access-list extended exp-acl
Ruijie(config-exp-nacl)# show access-lists expert access-list extended exp-acl
Ruijie(config-exp-nacl)#
```

Create an extended expert ACL numbered 2704:

```
Ruijie(config)# expert access-list extended 2704
Ruijie(config-exp-nacl)# show access-lists access-list extended 2704
Ruijie(config-exp-nacl)#
```

**Related  
Commands**

Command	Description
<b>show access-lists</b>	Displays the extended expert ACLs

**Platform  
Description**

N/A

## 1.11 expert access-list new-fragment-mode

Use this command to switch the matching mode of fragmentation packets. Use the **no** form of this command to restore the default matching mode of fragmentation packets.

**expert access-list new-fragment-mode** { *acl-id* | *acl-name* }

**no expert access-list new-fragment-mode** { *acl-id* | *acl-name* }

Parameter Description	Parameter	Description
	<i>acl-id</i>	Expert access list number: 2700 to 2899.
	<i>acl-name</i>	Name of the expert access list.

**Defaults** Use the default matching mode of fragmentation packets. By default, if the access rule is tagged with fragment, it will match all packets except for the first fragmentation packet. If the access rule is not tagged with fragment, all packets including the first and all subsequent fragmentation packets will be matched.

**Command mode** Global configuration mode

**Usage Guide** Use this command to switch and control the matching mode of access rules to fragmentation packets.

**Configuration Examples** The following example switches the matching mode of fragmentation packets for the ACL 2700 from the default mode to a new matching mode:

```
Ruijie(config)# expert access-list new-fragment-mode 2700
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.12 expert access-list resequence

Use this command to resequence an expert access list. Use the **no** form of this command to restore the default order of access entries.

**expert access-list resequence** { *acl-id* | *acl-name* } *start-sn* *inc-sn*

**no expert access-list resequence** { *acl-id* | *acl-name* }

Parameter Description	Parameter	Description
	<i>acl-id</i>	Expert access list number: 2700 to 2899.

<i>acl-name</i>	Name of the expert access list
<i>start-sn</i>	Start sequence number. Range: 1 to 2147483647
<i>inc-sn</i>	Increment of the sequence number. Range: 1 to 2147483647

**Defaults**      *start-sn*: 10  
*inc-sn*: 10

**Command mode**      Global configuration mode

**Usage Guide**      Use this command to change the order of the access entries.

**Configuration Examples**      The following example resequences entries of expert access list “exp-acl”:

**Examples**      Before the configuration:

```
Ruijie# show access-lists
expert access-list extended exp-acl
 10 permit ip any any any any
 20 deny ip any any any any
```

After the configuration:

```
Ruijie# config
Ruijie(config)# expert access-list resequence exp-acl 21 43
Ruijie(config)# exit
Ruijie# show access-lists
expert access-list extended exp-acl
 21 permit ip any any any any
 64 deny ip any any any any
```

Related Commands	Command	Description
	<b>show access-lists</b>	Displays all access lists.

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

### 1.13 global access-group

Use this command to apply the global access list on the interface. Use the **no** form of this command to remove the global access list from the interface.

**global access-group**  
**no global access-group**

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

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

**Defaults** By default, the global access list is applied on the interface.

**Command mode** Interface configuration mode

**Usage Guide** N/A

**Configuration** The following example applies the global access list on interface GigabitEthernet 0/17.

**Examples**

```
Ruijie(config)# interface gigaEthernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# global access-group
```

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 1.14 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: 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 or interface configuration mode.

**Usage Guide** Use this command to control access to a specified interface, globally.

**Configuration** The following example applies the ACL 120 on interface gigaEthernet 0/17 to filter the incoming packets:

**Examples**

```
Ruijie(config)# interface gigaEthernet 0/17
```

```
Ruijie(config-if-GigabitEthernet 0/17)# 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

## 1.15 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: Standard: 1 to 99, 1300 to 1999; Extended: 100 to 199, 2000 to 2699.
<i>acl-name</i>	Name of the access list

**Defaults** N/A

**Command mode** Global configuration mode

**Usage Guide** Configure a standard access list if you need to filter on source address only. If you want to filter on anything other than source address, you need to create an extended access list. Refer to **deny** or **permit** in the two modes. Use the **show access-lists** command to display the ACL configurations.

**Configuration Examples** The following example creates a standard access list named std-acl.

```
Ruijie(config)# ip access-list standard std-acl
Ruijie(config-std-nacl)# show access-lists
ip access-list standard std-acl
```

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>

**Platform** N/A

**Description**

## 1.16 ip access-list counter

Use this command to enable the counter of packets matching the standard or extended IP access list.

Use the **no** form of this command to disable the counter.

**ip access-list counter** { *acl-id* | *acl-name* }

**no ip access-list counter** { *acl-id* | *acl-name* }

Parameter Description	Parameter	Description
		<i>acl-id</i>
	<i>acl-name</i>	Name of the IP access list.

**Defaults** The counter of packets matching the standard or extended IP access list is disabled by default.

**Command mode** Global configuration mode

**Usage Guide** N/A

**Configuration** The following example enables the counter of packets matching the standard access list:

```
Ruijie(config)# ip access-list counter std-acl
Ruijie(config-std-nacl)# show access-lists
ip access-list standard std-acl
 10 permit 195.168.6.0 0.0.0.255 (999 matches)
 20 deny host 5.5.5.5 time-range tm (2000 matches)
```

The following example disables the counter of packets matching the standard access list:

```
Ruijie(config)# no ip access-list counter std-acl
Ruijie(config-std-nacl)# show access-lists
ip access-list standard std-acl
 10 permit 195.168.6.0 0.0.0.255
 20 deny host 5.5.5.5 time-range tm
```

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

<b>show access-lists</b>	Displays all access lists.
--------------------------	----------------------------

**Platform**  
**Description**

N/A

## 1.17 ip access-list log-update interval

Use this command to configure the interval at which the IPv4 access list log is updated. Use the **no** form of this command to restore the default interval.

**ip access-list log-update interval** *time*

**no ip access-list log-update interval**

**Parameter**  
**Description**

Parameter	Description
<i>time</i>	For the access rule with the <b>log</b> option, a packet hit is output at the interval of ACL logging output. The interval ranges from 0 to 1440 minutes, and the default value is 5 minutes, indicating that the ACL matching log of a specified flow is output every 5 minutes. 0 indicates that no ACL logging is output.

**Defaults** The default interval at which the IPv4 access list log is updated is 5 minutes.

**Command mode** Global configuration mode

**Usage Guide** Use this command to configure the interval at which the IPv4 access list log is updated.

**Configuration Examples** The following example configures the interval for the IPv4 access list log update to 10 minutes:

```
Ruijie# configure terminal
Ruijie(config)# ip access-list log-update interval 10
```

**Related Commands**

Command	Description
<b>ip access-list</b>	Defines an IPv4 access list.

**Platform**  
**Description**

N/A

## 1.18 ip access-list new-fragment-mode

Use this command to switch the matching mode of fragmentation packets of standard or extended IP access list. Use the **no** form of this command to restore the default matching mode of fragmentation packets.

**ip access-list new-fragment-mode** { *acl-id* | *acl-name* }

**no ip access-list new-fragment-mode** { *acl-id* | *acl-name* }

Parameter Description	Parameter	Description
	<i>acl-id</i>	IP access list number: Standard IP access list: 1 to 99, 1300 to 1999; Extended IP access list: 100 to 199, 2000 to 2699.
	<i>acl-name</i>	Name of the standard or extended IP access list

**Defaults** Use the default matching mode of fragmentation packets. By default, if the access rule is tagged with fragment, it will match all packets except for the first fragmentation packet. If the access rule is not tagged with fragment, all packets including the first and all subsequent fragmentation packets will be matched.

**Command mode** Global configuration mode

**Usage Guide** This command is used to switch and control the fragmentation packet matching mode of access rules.

**Configuration Examples** The following example switches the fragmentation packet matching mode of the ACL 100 from the default mode to a new mode:

```
Ruijie(config)# ip access-list new-fragment-mode 100
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.19 ip access-list resequence

Use this command to resequence a standard or extended IP access list. Use the **no** form of this command to restore the default order of access entries.

**ip access-list resequence** { *acl-id* | *acl-name* } *start-sn* *inc-sn*

**no ip access-list resequence** { *acl-id* | *acl-name* }

Parameter Description	Parameter	Description
	<i>acl-id</i>	IP access list number: Standard IP access list: 1 to 99, 1300 to 1999; Extended IP access list: 100 to 199, 2000 to 2699.
	<i>acl-name</i>	Name of the standard or extended IP access list



<i>start-sn</i>	Start sequence number. Range: 1 to 2147483647
<i>inc-sn</i>	Increment of the sequence number. Range: 1 to 2147483647

**Defaults**      *start-sn*: 10  
*inc-sn*: 10

**Command mode**      Global configuration mode

**Usage Guide**      Use this command to change the order of the access entries.

**Configuration**      The following example resequences entries of ACL1:

**Examples**      Before the configuration:

```
Ruijie# show access-lists
ip access-list standard 1
10 permit host 192.168.4.12
20 deny any any
```

After the configuration:

```
Ruijie# config
Ruijie(config)# ip access-list resequence 1 21 43
Ruijie(config)# exit
Ruijie# show access-lists
ip access-list standard 1
21 permit host 192.168.4.12
64 deny any any
```

**Related Commands**

Command	Description
<b>show access-lists</b>	Displays all access lists..

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

## 1.20 ipv6 access-list

Use this command to create an IPv6 access list and to place the device in IPv6 access list configuration mode. Use the **no** form of this command to remove the access list.

**ipv6 access-list** *acl-name*

**no ipv6 access-list** *acl-name*

**Parameter Description**

Parameter	Description
<i>acl-name</i>	Name of the IPv6 access list.

<b>Defaults</b>	N/A
<b>Command mode</b>	Global configuration mode
<b>Usage Guide</b>	To filter the IPv6 packets through the access list, you need to define an IPv6 access list by using the <b>ipv6 access-list</b> command.

**Configuration** The following example creates an IPv6 access list named v6-acl:

```
Ruijie(config)# ipv6 access-list v6-acl
Ruijie(config-ipv6-nacl)# show access-lists
ipv6 access-list extended v6-acl
```

<b>Related Commands</b>	Command	Description
	<b>show access-lists</b>	Displays all access lists.

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

## 1.21 ipv6 access-list counter

Use this command to enable the counter of packets matching the IPv6 access list. Use the **no** form of this command to disable the counter.

```
ipv6 access-list counter acl-name
no ipv6 access-list counter acl-name
```

<b>Parameter Description</b>	Parameter	Description
	<i>acl-name</i>	Name of the IPv6 access list.

**Defaults** -

**Command mode** Global configuration mode

**Usage Guide** Use this command to enable the counter of packets matching the IPv6 access list to monitor the IPv6 packets matching and filtering.

**Configuration** The following example enables the counter of packets matching the IPv6 access list named v6-acl:

```
Ruijie(config)# ipv6 access-list counter v6-acl
Ruijie(config)# show access-lists
ipv6 access-list acl-v6
```

```
10 permit icmp any any (7 matches)
20 deny tcp any any (7 matches)
```

The following example disables the counter of packets matching the IPv6 access list named v6-acl:

```
Ruijie(config)# no ipv6 access-list counter v6-acl
Ruijie(config-ipv6-nacl)# show access-lists
ipv6 access-list acl-v6
 10 permit icmp any any
 20 deny tcp any any
```

#### Related Commands

Command	Description
<b>show access-lists</b>	Displays all access lists.

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

## 1.22 ipv6 access-list log-update interval

Use this command to configure the interval at which the IPv6 access list log is updated. Use the **no** form of this command to restore the default interval.

**ipv6 access-list log-update interval *time***  
**no ipv6 access-list log-update interval**

#### Parameter Description

Parameter	Description
<i>time</i>	For the access rule with the <b>logging</b> option, a packet hit is output at the interval of ACL logging output. The interval ranges from 0 to 1440 minutes, and the default value is 5 minutes, indicating that the ACL matching log of a specific flow is output every 5 minutes. 0 indicates that no ACL logging is output.

**Defaults** By default, it is 5 minutes.

**Command mode** Global configuration mode

**Usage Guide** Use this command to configure the interval at which the IPv6 access list log is updated.

**Configuration Examples** The following example configures the interval for the IPv6 access list log update to 10 minutes:

```
Ruijie# configure terminal
Ruijie(config)# ipv6 access-list log-update interval 10
```

#### Related

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

Commands	
<code>ipv6 access-list</code>	Defines an IPv6 access list.

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

## 1.23 ipv6 access-list resequence

Use this command to resequence an IPv6 access list. Use the **no** form of this command to restore the default order of access entries.

**ipv6 access-list resequence** *acl-name start-sn inc-sn*

**no ipv6 access-list resequence** *acl-name*

Parameter Description	Parameter	Description
	<i>acl-name</i>	Name of the IPv6 access list
	<i>start-sn</i>	Start sequence number. Range: 1 to 2147483647
	<i>inc-sn</i>	Increment of the sequence number. Range: 1 to 2147483647

**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 IPv6 access list "v6-acl":

**Examples** Before the configuration:

```
Ruijie# show access-lists
ipv6 access-list v6-acl
 10 permit ipv6 any any
 20 deny ipv6 any any
```

After the configuration:

```
Ruijie# config
Ruijie(config)# ipv6 access-list resequence v6-acl 21 43
Ruijie(config)# exit
Ruijie# show access-lists
ipv6 access-list v6-acl
 21 permit ipv6 any any
 64 deny ipv6 any any
```

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

<b>Commands</b>		
	<b>show access-lists</b>	Displays all access lists.

**Platform** N/A

**Description**

## 1.24 ipv6 traffic-filter

Use this command to apply an IPv6 access list on the specified interface. Use the **no** form of the command to remove the IPv6 access list from the interface/VXLAN.

**ipv6 traffic-filter** *acl-name* **in**

**no ipv6 traffic-filter** *acl-name* **in**

<b>Parameter Description</b>	<b>Parameter</b>	<b>Description</b>
	<i>acl-name</i>	Name of IPv6 access list
	<b>in</b>	Specifies filtering on inbound packets

**Defaults** By default, it is not disabled.

**Command mode** Interface configuration mode.

**Usage Guide** Use this command to apply the IPv6 access list to a specified interface to filter the inbound or outbound packets.

**Configuration Examples** The following example applies the IPv6 access list named **v6-acl** to interface GigabitEthernet 0/1:

```
Ruijie(config)# interface GigaEthernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# ipv6 traffic-filter v6-acl in
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show access-group</b>	Displays ACL configurations on the interface.

**Platform** N/A

**Description**

## 1.25 list-remark

Use this command to write a helpful comment (remark) for an access list. Use the **no** form of this command to remove the remark.

**list-remark** *comment*

**no list-remark**

Parameter Description	Parameter	Description
	<i>comment</i>	Comment that describes the access list.

**Defaults** The access lists have no remarks by default.

**Command mode** ACL configuration mode

**Usage Guide** You can use this command to write a helpful comment for a specified access list.

**Configuration Examples** The following example writes a comment of “this acl is to filter the host 192.168.4.12” for ACL102.

```
Ruijie(config)# ip access-list extended 102
Ruijie(config-ext-nacl)# list-remark this acl is to filter the host
192.168.4.12
Ruijie(config-ext-nacl)# show access-lists
ip access-list extended 102
deny ip host 192.168.4.12 any
1000 hits
this acl is to filter the host 192.168.4.12
Ruijie(config-ext-nacl)#
```

Related Commands	Command	Description
	<b>show access-lists</b>	Displays all access lists.
	<b>ip access-list</b>	Defines an IPv4 access list.
	<b>access-list list remark</b>	Adds a helpful comment for an access list in global configuration mode.

**Platform** N/A

**Description**

## 1.26 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.

**Command mode** Global or interface configuration mode.

**Usage Guide** 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.

**Configuration Examples** The following example applies the MAC access-list **accept\_00d0f8xxxxx\_only** to interface GigabitEthernet 0/1:

```
Ruijie(config)# interface gigabitEthernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# mac access-group accept_00d0f8xxxxx_only in
```

**Related Commands**

Command	Description
<b>show access-group</b>	Displays the ACL configuration on the interface.

**Platform** N/A

**Description**

## 1.27 mac access-list counter

Use this command to enable the counter of packet matching the extended MAC access list. Use the **no** form of this command to disable the counter.

**mac access-list counter** { *acl-id* | *acl-name* }

**no mac access-list counter** { *acl-id* | *acl-name* }

**Parameter Description**

Parameter	Description
<i>acl-id</i>	Extended MAC access list number. The range is from 700 to 799.
<i>acl-name</i>	Name of the extended MAC access list

**Defaults** The counter is disabled by default.

**Command mode** Global configuration mode

**Usage Guide** Use this command to enable the counter of packets matching the MAC access list to monitor the packets matching and filtering.

**Configuration Examples** The following example enables the counter of packet matching the extended MAC access list named mac-acl:

```
Ruijie(config)# mac access-list counter mac-acl
Ruijie(config)# show access-lists
mac access-list extended mac-acl
 10 permit host 0023.56ac.8965 any (170 matches)
 20 deny any any etype-any cos 6 (239 matches)
```

The following example disables the counter of packet matching the extended MAC access list named `mac-acl`:

```
Ruijie(config)# no mac access-list counter mac-acl
Ruijie(config)# show access-lists
mac access-list extended mac-acl
 10 permit host 0023.56ac.8965 any
 20 deny any any etype-any cos 6
```

<b>Related Commands</b>	Command	Description
	<b>show access-lists</b>	Displays all access lists.

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

## 1.28 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>	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

**Defaults** N/A

**Command mode** Global configuration mode.

**Usage Guide** To filter the packets based on the MAC address, you need to define a MAC access list by using the **mac access-list extended** command.

**Configuration** The following command creates an extended MAC access list named `mac-acl`:

```
Examples Ruijie(config)# mac access-list extended mac-acl
```



```
Ruijie(config-mac-nacl)# show access-lists
mac access-list extended mac-acl
```

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**

## 1.29 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":

**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 mac-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**

## 1.30 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-ipv4-address source-ipv4-wildcard | any | host source-ipv4-address }
[ time-range time-range-name ] [ log ]
```

- Extended IP ACL

```
[ sn ] permit protocol { source-ipv4-address source-ipv4-wildcard | any | host source-ipv4-address }
[ eq port | gt port | lt port | neq port | range lower upper ] { destination-ipv4-address
destination-ipv4-wildcard | any | host destination-ipv4-address } [ dscp dscp ] [ fragment ]
[ precedence precedence ] [ tos tos ] [ eq port | gt port | lt port | neq port | range lower upper ]
[ match-all tcp-flag | established ] [ time-range time-range-name ] [ log ]
```

Extended IP ACLs of some important protocols:

Internet Control Message Protocol (ICMP)

```
[ sn ] permit icmp { source-ipv4-address source-ipv4-wildcard | any | host source-ipv4-address }
{ destination-ipv4-address destination-ipv4-wildcard | any | host destination-ipv4-address }
[ icmp-type ] [ [ icmp-type [ icmp-code ] ] | [ icmp-message ] ] [ dscp dscp ] [ precedence
precedence ] [ tos tos ] [ fragment ] [ time-range time-range-name ]
```

Transmission Control Protocol (TCP)

```
[ sn ] permit tcp { source-ipv4-address source-ipv4-wildcard | any | host source-ipv4-address } [ eq
port | gt port | lt port | neq port | range lower upper ] { destination-ipv4-address
destination-ipv4-wildcard | any | host destination-ipv4-address } [ eq port | gt port | lt port | neq port |
range lower upper ] [ dscp dscp ] [ precedence precedence ] [ tos tos ] [ fragment ] [ match-all
tcp-flag | established ] [ time-range time-range-name ]
```

User Datagram Protocol (UDP)

```
[ sn ] permit udp { source-ipv4-address source-ipv4-wildcard | any | host source-ipv4-address } [ eq port | gt port | lt port | neq port | range lower upper ] { destination-ipv4-address destination-ipv4-wildcard | any | host destination-ipv4-address } [ eq port | gt port | lt port | neq port | range lower upper ] [ dscp dscp ] [ precedence precedence ] [ tos tos ] [ fragment ] [ time-range time-range-name ]
```

### 3. 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 ] [ cos [ cos ] [ inner cos ] ] [ time-range time-range-name ]
```

### 4. Extended expert ACL

```
[ sn ] permit [ protocol | [ ethernet-type ] [ cos [ cos ] [ inner cos ] ] ] [ VID [ vid ] [ inner vid ] ] { source-ipv4-address source-ipv4-wildcard | any | host source-ipv4-address } { source-mac-address mask | any | host source-mac-address } [ eq port | gt port | lt port | neq port | range lower upper ] { destination-ipv4-address destination-ipv4-wildcard | any | host destination-ipv4-address } { any | host destination-mac-address } [ eq port | gt port | lt port | neq port | range lower upper ] [ dscp dscp ] [ precedence precedence ] [ tos tos ] [ fragment ] [ match-all tcp-flag | established ] [ time-range time-range-name ]
```

When you select the Ethernet-type field or cos field:

```
[ sn ] permit { ethernet-type | cos [ cos ] [ inner cos ] } [ VID [ vid ] [ inner vid ] ] { source-mac-address mask | any | host source-mac-address } { any | host destination-mac-address } [ time-range time-range-name ]
```

When you select the protocol field:

```
[ sn ] permit protocol [ VID [ vid ] [ inner vid ] ] { source-ipv4-address source-ipv4-wildcard | any | host source-ipv4-address } { source-mac-address mask | any | host source-mac-address } [ eq port | gt port | lt port | neq port | range lower upper ] { destination-ipv4-address destination-ipv4-wildcard | any | host destination-ipv4-address } { any | host destination-mac-address } [ eq port | gt port | lt port | neq port | range lower upper ] [ dscp dscp ] [ precedence precedence ] [ tos tos ] [ fragment ] [ match-all tcp-flag | established ] [ time-range time-range-name ]
```

Extended expert ACLs of some important protocols:

Internet Control Message Protocol (ICMP)

```
[ sn ] permit icmp [ VID [ vid ] [ inner vid ] ] { source-ipv4-address source-ipv4-wildcard | any | host source-ipv4-address } { source-mac-address mask | any | host source-mac-address } { destination-ipv4-address destination-ipv4-wildcard | any | host destination-ipv4-address } { any | host destination-mac-address } [ icmp-type ] [ [ icmp-type [ icmp-code ] ] ] [ icmp-message ] [ dscp dscp ] [ precedence precedence ] [ tos tos ] [ fragment ] [ time-range time-range-name ]
```

Transmission Control Protocol (TCP)

```
[ sn ] permit tcp [ VID [ vid ] [ inner vid ] ] { source-ipv4-address source-ipv4-wildcard | any | host source-ipv4-address } { source-mac-address mask | any | host source-mac-address } [ eq port | gt port | lt port | neq port | range lower upper ] { destination-ipv4-address destination-ipv4-wildcard | any | host destination-ipv4-address } { any | host destination-mac-address } [ eq port | gt port | lt port | neq port | range lower upper ] [ dscp dscp ] [ precedence precedence ] [ tos tos ] [ fragment ] [ match-all tcp-flag | established ] [ time-range time-range-name ]
```

User Datagram Protocol (UDP)

```
[ sn ] permit udp [ VID [ vid ] [ inner vid ] ] { source-ipv4-address source-ipv4-wildcard | any | host
```

```
source-ipv4-address } { source-mac-address mask | any | host source-mac-address } [ eq port | gt
port | lt port | neq port | range lower upper ] { destination-ipv4-address destination-ipv4-wildcard | any
| host destination-ipv4-address } { any | host destination-mac-address } [ eq port | gt port | lt port |
neq port | range lower upper ] [ dscp dscp ] [ precedence precedence ] [ tos tos ] [ fragment ]
[ time-range time-range-name ]
```

## 5. ACL80

```
[ sn ] permit hex hex-mask offset
```

## 6. Extended IPv6 ACL

```
[ sn ] permit ipv6-protocol { any | host source-ipv6-address } [ eq port | gt port | lt port | neq port |
range lower upper ] { any | host destination-ipv6-address } [ eq port | gt port | lt port | neq port |
range lower upper ] [ dscp dscp ] [ flow-label flow-label ] [ fragment ] [ match-all tcp-flag |
established ] [ time-range time-range-name ] [ log ]
```

Extended IPv6 ACLs of some important protocols:

Internet Control Message Protocol (ICMP)

```
[ sn ] permit icmp { any | host source-ipv6-address } { any | host destination-ipv6-address }
[ icmp-type ] [ [ icmp-type [ icmp-code ] ] | [ icmp-message ] ] [ dscp dscp ] [ flow-label flow-label ]
[ fragment ] [ time-range time-range-name ] [ log ]
```

Transmission Control Protocol (TCP)

```
[ sn ] permit tcp { any | host source-ipv6-address } [ eq port | gt port | lt port | neq port | range lower
upper ] { any | host destination-ipv6-address } [ eq port | gt port | lt port | neq port | range lower
upper ] [ dscp dscp ] [ flow-label flow-label ] [ fragment ] [ match-all tcp-flag | established ]
[ time-range time-range-name ] [ log ]
```

User Datagram Protocol (UDP)

```
[ sn ] permit udp { any | host source-ipv6-address } [ eq port | gt port | lt port | neq port | range lower
upper ] { any | host destination-ipv6-address } [ eq port | gt port | lt port | neq port | range lower
upper ] [ dscp dscp ] [ flow-label flow-label ] [ fragment ] [ time-range time-range-name ] [ log ]
```

**Parameter  
Description**

Parameter	Description
<i>sn</i>	ACL entry sequence number
<b>permit</b>	If matched, access is permit
<i>source-ipv4-address</i>	Specify the source IP address (host address or network address)
<i>source-ipv4-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-ipv4-address</i>	Specify the destination IP address (host address or network address)
<i>destination-ipv4-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>dscp</b>	Differentiated service code point
<i>dscp</i>	Code point value, ranging from 0 to 63
<b>precedence</b>	Specify the packet priority

<i>precedence</i>	Packet precedence value (0 to 7)
<b>eq</b>	Equal operator
<b>gt</b>	Greater operator
<b>lt</b>	Smaller operator
<b>neq</b>	Unequal operator
<i>port</i>	Layer4 port number
<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>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
<b>host</b> <i>source-mac-address</i>	Source physical address
<b>host</b> <i>destination-mac-address</i>	Destination physical address
<b>cos</b> <i>cos</i>	Match the specified cos field in the outer tag
<b>inner</b> <i>cos</i>	Match the specified cos field in the inner tag
<b>VID</b> <i>vid</i>	Match the specified VLAN ID field in the outer tag
<b>inner</b> <i>vid</i>	Match the specified VLAN ID field in the inner tag
<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
<i>prefix-length</i>	Prefix mask length
<i>source-ipv6-address</i>	Source IPv6 address
<i>destination-ipv6-address</i>	Destination IPv6 address
<b>flow-label</b>	Flow label
<i>flow-label</i>	Flow label value, within the range of 0 to 1048575
<i>ipv6-protocol</i>	For the IPv6, the field can be <code>ipv6   icmp   tcp   udp</code> and number in the range 0 to 255
<b>time-range</b>	Time range of the packet filtering
<i>time-range-name</i>	Time range name of the packet filtering
<b>log</b>	Logs will be periodically output if packets matching the ACEs are found

**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** The following example shows how to create and display an Expert Extended ACL. This expert ACL permits all the TCP packets with the source IP address 192.168.4.12 and the source MAC address 001300498272.

**Examples**

```
Ruijie(config)# expert access-list extended exp-acl
Ruijie(config-exp-nacl)# permit tcp host 192.168.4.12 host 0013.0049.8272 any any
Ruijie(config-exp-nacl)# deny any any any any
Ruijie(config-exp-nacl)# show access-lists
expert access-list extended exp-acl
10 permit tcp host 192.168.4.12 host 0013.0049.8272 any any
20 deny any any any any
```

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
```

This example shows how to use the extended IPv6 ACL. The purpose is to permit the host with the IP address 192.168.4.12 and apply the ACL to interface GigabitEthernet 0/1. The configuration procedure is as below:

```
Ruijie(config)# ipv6 access-list extended v6-acl
Ruijie(config-ipv6-nacl)# 11 permit ipv6 host ::192.168.4.12 any
Ruijie(config-ipv6-nacl)# show access-lists
ipv6 access-list extended v6-acl
11 permit ipv6 host ::192.168.4.12 any
Ruijie(config-ipv6-nacl)# exit
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#ipv6 traffic-filter v6-acl in
```

#### Related Commands

Command	Description
<b>show access-lists</b>	Displays all access lists.
<b>ip access-list</b>	Defines an IP access list.
<b>mac access-list</b>	Defines an extended MAC access list.
<b>expert access-list</b>	Define an extended expert access list.
<b>ipv6 access-list</b>	Defines an extended IPv6 access list.

**Platform** N/A

**Description**

## 1.31 redirect destination interface

Use this command to redirect the traffic matching the access list to the specified interface. Use the **no** form of this command to remove the redirection.

**redirect destination interface** *interface-name* **acl** { *acl-id* | *acl-name* } **in**

**no redirect destination interface** *interface-name* **acl** { *acl-id* | *acl-name* } **in**

#### Parameter Description

Parameter	Description
<i>interface-name</i>	Redirect interface
<i>acl-id</i>	Access list number
<i>acl-name</i>	Access list name

**Defaults** No redirection is configured.

**Command mode** Interface configuration mode

**Usage Guide** Use this command to configure access redirection, namely, to redirect the traffic matching the access list to the specified interface. You can monitor the operation of a specified access list by using this

command.

**Configuration** The following example configures access redirection.

**Examples**

```
Ruijie(config)# interface gigabitEthernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# redirect destination interface
gigabitEthernet 0/18 acl 1 in
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 1.32 remark

Use this command to write a helpful comment (remark) for an entry in the access list. Use the **no** form of this command to remove the remark.

**remark** *comment*

**no remark**

**Parameter  
Description**

Parameter	Description
<i>comment</i>	Comment that describes the access entry.

**Defaults** The access entries have no remarks.

**Command mode** ACL configuration mode.

**Usage Guide** Use this command to write a helpful comment for an access entry.  
Up to 100 characters are allowed in the remark.  
Two identical access entry remarks in one access list is not allowed.  
Removing an access entry may delete the remark for it as well.

**Configuration** The following example writes remarks for the entry in extended IP access list 102.

**Examples**

```
Ruijie(config)# ip access-list extended 102
Ruijie(config-ext-nacl)# remark first_remark
Ruijie(config-ext-nacl)# permit tcp 1.1.1.1 0.0.0.0 2.2.2.2 0.0.0.0
Ruijie(config-ext-nacl)# remark second_remark
Ruijie(config-ext-nacl)# permit tcp 3.3.3.3 0.0.0.0 4.4.4.4 0.0.0.0
Ruijie(config-ext-nacl)# end
Ruijie#
```



Related Commands	Command	Description
	<b>show access-lists</b>	Displays all access lists.
	<b>ip access-list</b>	Defines an IP access list.

**Platform** N/A

**Description**

## 1.33 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-name</i>

**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 Examples**

```
Ruijie# show access-group interface GigabitEthernet 0/17
ip access-list extended 101
Applied On interface GigabitEthernet 0/17 in.
```

Related Commands	Command	Description
	<b>ip access-group</b>	Applies the IP access list to the interface.
	<b>mac access-group</b>	Applies the MAC access list to the interface.
	<b>expert access-group</b>	Applies the expert access list to the interface.
	<b>ipv6 traffic-filter</b>	Applies the IPv6 access list to the interface.

**Platform** N/A

**Description**

## 1.34 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	Parameter	Description
-----------	-----------	-------------

Description	
<i>acl-id</i>	Access list number
<i>acl-name</i>	Name of the IP access list
summary	Access list summary

**Command mode** Global configuration mode

**Usage Guide** Use this command to display the specified access list. If no access list number or name is specified, all the access lists are displayed.

**Configuration** 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 101
permit icmp host 192.168.1.1 any log (1080 matches)
  permit tcp host 1.1.1.1 any established
  deny ip any any (80021 matches)
mac access-list extended mac_acl
expert access-list extended exp_acl
ipv6 access-list extended v6_acl
petmit ipv6 ::192.168.4.12 any (100 matches)
deny any any (9 matches)
```

**Related Commands**

Command	Description
<b>ip access-list</b>	Defines an IP access list.
<b>mac access-list</b>	Defines an extended MAC access list.
<b>expert access-list</b>	Defines an extended expert access list.
<b>ipv6 access-list</b>	Defines an extended IPv6 access list.

**Platform** N/A

**Description**

## 1.35 show expert access-group

Use this command to display the expert access list applied to the interface.

**show expert access-group [ interface *interface-name* ]**

<b>Parameter Description</b>	<b>Parameter</b>	<b>Description</b>
	<i>interface-name</i>	Interface name
<b>Command mode</b>	Privileged EXEC mode	
<b>Usage Guide</b>	Use this command to display the expert access list configured on the interface. If no interface is specified, the expert access lists on all interfaces are displayed.	
<b>Configuration Examples</b>	<pre>Ruijie# show expert access-group interface gigabitethernet 0/17 expert access-group ee in Applied On interface GigabitEthernet 0/17.</pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>expert access-list</b>	Defines an extended expert access list.
<b>Platform Description</b>	N/A	

## 1.36 show ip access-group

Use this command to display the standard and extended IP access lists on the interface.

**show ip access-group [ interface *interface-name* ]**

<b>Parameter Description</b>	<b>Parameter</b>	<b>Description</b>
	<i>interface-name</i>	Interface name
<b>Command mode</b>	Privileged EXEC mode	
<b>Usage Guide</b>	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.	
<b>Configuration Examples</b>	<pre>Ruijie# show ip access-group interface gigabitethernet 0/17 ip access-group aaa in Applied On interface GigabitEthernet 0/17.</pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ip access-list</b>	Defines an IP access list.

**Platform** N/A

**Description**

## 1.37 show ipv6 traffic-filter

Use this command to display the IPv6 access list on the interface.

**show ipv6 traffic-filter** [ **interface** *interface-name* ]

**Parameter  
Description**

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

**Defaults** -

**Command  
mode** Privileged EXEC mode

**Usage Guide** Use this command to display the IPv6 access list configured on the interface. If no interface is specified, the IPv6 access lists on all interfaces are displayed.

**Configuration  
Examples**

```
Ruijie# show ipv6 traffic-filter interface gigabitethernet 0/17
ipv6 access-group v6 in
Applied On interface GigabitEthernet 0/17.
```

**Related  
Commands**

Command	Description
<b>ipv6 access-list</b>	Defines an IPv6 access list.

**Platform** N/A

**Description**

## 1.38 show mac access-group

Use this command to display the MAC access list on the interface.

**show mac access-group** [ **interface** *interface-name* ]

**Parameter  
Description**

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

**Defaults** N/A

**Command** Privileged EXEC mode  
**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 0/17
mac access-group mm in
Applied On interface GigabitEthernet 0/17.
```

Related Commands	Command	Description
		<b>mac access-list</b>

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

## 1.39 show redirect interface

Use this command to display the access redirection configuration.

**show redirect** [ **interface** *interface-name* ]

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

**Defaults** N/A

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

**Usage Guide** Use this command to display the access redirection configuration on the interface. If no interface is specified, the access redirection configuration on all interfaces is displayed.

**Configuration Examples** The following example displays the access redirection configuration on interface GigabitEthernet 0/17.

```
Ruijie #show redirect interface gigabitEthernet 0/17
acl redirect configuration on interface gigabitEthernet 0/17
redirect destination interface gigabitEthernet 0/17 acl 1 in
```

Related Commands	Command	Description
		N/A

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

## 2 QoS Commands

### 2.1 class

Use this command to add reference to an existing class map. Use the **no** form of this command to remove the class from the policy map.

**class** *class-map-name*

**no class** *class-map-name*

Parameter	Parameter	Description
Description	<i>class-map-name</i>	Reference to a class map.

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

**Command Mode** Policy configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example adds reference to the class map named cmap1.

```
Ruijie(config)# class-map cmap1
Ruijie(config-cmap)# match ip dscp 5
Ruijie(config-cmap)# exit
Ruijie(config)# policy-map pmap1
Ruijie(config-pmap)# class cmap1
Ruijie(config-pmap-c)# end
```

Related Commands	Command	Description
	<b>show policy-map</b>	Displays the policy map.

**Platform Description** N/A

### 2.2 class map

Use this command to create a class map and enter class-map configuration mode. Use the **no** or **default** form of this command to remove a class map.

**class-map** *class-map-name*

**no class-map** *class-map-name*

**default class-map** *class-map-name*

Parameter	Parameter	Description
<b>Description</b>	<i>class-map-name</i>	Class map name. The class map name can be a maximum of 31 characters.

**Defaults** None

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example creates a class map named `cm_acl` to match an access list named `me`.

```
Ruijie(config)# mac access-list extended me
Ruijie(config-ext-macl)# permit host 1111.2222.3333 any
Ruijie(config-ext-macl)# exit
Ruijie(config)# class-map cm_acl
Ruijie(config-cmap)# match access-group me
Ruijie(config-cmap)# exit
```

The following example creates a class map named `cm_dscp` to match DHCP 8, 16 and 24.

```
Ruijie(config)# class-map cm_dscp
Ruijie(config-cmap)# match ip dscp 8 16 24
Ruijie(config-cmap)# exit
```

Related Commands	Command	Description
	<b>show class-map</b>	Displays the class map.

**Platform Description** N/A

## 2.3 match

Use this command to define a match criteria in class map configuration mode. Use the **no** form of this command to remove the match criteria.

```
match { access-group { acl-id | acl-name } | ip { dscp dscp-vlaue-list | precedence pre-vlaue-list } }
no match { access-group { acl-id | acl-name } | ip { dscp dscp-vlaue-list | precedence pre-vlaue-list } }
```

Parameter	Parameter	Description
<b>Description</b>	<b>access-group</b> <i>acl-id</i>	Identifies a numbered access list as the match criteria.
	<b>access-group</b> <i>acl-name</i>	Identifies a named access list as the match criteria.
	<b>ip dscp</b> <i>dscp-vlaue-list</i>	Identifies DSCP values as the match criteria. Multiple DSCP can be



	configured. The range is from 0 to 63.
<b>ip precedence</b> <i>pre-value-list</i>	Identifies IP precedence values as the match criteria. Multiple IP precedence can be configured. The range is from 0 to 7.

**Defaults** None

**Command** Class map configuration mode

**Mode**

**Usage Guide** N/A

**Configuration** The following example creates a class map named cmap1 to match DSCP 20, 22, 24 and 30.

**Examples**

```
Ruijie(config)# class-map cmap1
Ruijie(config-cmap)# match ip dscp 20 22 24 30
```

**Related Commands**

Command	Description
<b>show class-map</b>	Displays the class map.

**Platform** N/A

**Description**

## 2.4 mls qos cos

Use this command to configure the CoS value of an interface. Use the **no** form of this command to restore the default setting.

**mls qos cos** *default-cos*

**no mls qos cos**

Parameter	Parameter	Description
<b>Description</b>	<i>default-cos</i>	CoS value of the interface. The range is from 0 to 7.

**Defaults** The default CoS value is 0.

**Command** Interface configuration mode.

**Mode**

**Usage Guide** N/A

**Configuration** The following example configures the default CoS value to 7.

**Examples**

```
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# mls qos cos 7
```

**Related**

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

<b>Commands</b>	<b>show mls qos interface</b>	Displays information of the specified interface.
-----------------	-------------------------------	--

**Platform** N/A

**Description**

## 2.5 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
<b>Description</b>	<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 qo map cos-dscp 8 10 16 18 24 26 32 34

**Examples**

Related	Command	Description
<b>Commands</b>	<b>show mls qos maps cos-dscp</b>	Displays the CoS-DSCP mapping.

**Platform** N/A

**Description**

## 2.6 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 0-7	DSCP 8-15	DSCP 16-23	DSCP 24-31	DSCP 32-39	DSCP 40-47	DSCP 48-55	DSCP 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**

<b>Related</b>	<b>Command</b>	<b>Description</b>
<b>Commands</b>	<b>show mls qos maps</b>	Displays the DSCP-CoS mapping.
	<b>dscp-cos</b>	

**Platform** N/A

**Description**

## 2.7 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**

<b>Parameter</b>	<b>Parameter</b>	<b>Description</b>
<b>Description</b>	<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 Commands	Command	Description
	<code>show mls qos maps ip-pre-dscp</code>	Displays the IP-precedence to DSCP mapping.

**Platform** N/A

**Description**

## 2.8 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 | wfq }**

**no mls qos scheduler**

Parameter Description	Parameter	Description
	<b>sp</b>	Specifies the absolute priority scheduling.
	<b>wrr</b>	Specifies the frame count weighted round-robin scheduling.
	<b>wfq</b>	Specifies the weighted fair queuing.

**Defaults** The default queue scheduling is **wrr**.

**Command Mode** Global configuration mode/Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example specifies the sp scheduling.

```
Ruijie(config)# mls qos scheduler sp

Ruijie(config)# interface gigabitEthernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# mls qos scheduler wrr
```

Related Commands	Command	Description
	<code>show mls qos scheduler</code>	Displays the output queue scheduling.

**Platform** N/A

**Description**

## 2.9 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	Parameter	Description
Description	<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** Interface configuration mode.

**Mode**

**Usage Guide** N/A

**Configuration** The following example configures the CoS trust mode.

**Examples**

```
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# mls qos trust cos
```

Related	Command	Description
Commands	<b>show mls qos interface</b>	Displays the specified interface configuration.

**Platform** N/A

**Description**

## 2.10 police

Use this command to configure traffic policing for a class map in a policy map. Use the **no** form of this command to remove traffic policing for the class map.

**police rate-bps burst-byte [ exceed-action { drop | dscp new-dscp | cos new-cos [ none-tos ] } ]**

**no police**

Parameter	Parameter	Description
Description	<i>rate-bps</i>	Bandwidth limit value per second in KBits. This value range is from 16 to 10000000.
	<i>burst-byte</i>	Burst traffic limit value in KBytes. This value range is from 1 to 8192.
	<b>drop</b>	Drops the packet. This is available only when the packet exceeds the bandwidth limit.
	<b>dscp new-dscp</b>	Modifies the DSCP value of the packet. This is available only when the packet exceeds bandwidth limit. The DSCP value range is from 0 to 63.

<b>cos</b> <i>new-cos</i>	Modifies the CoS value of the packet. This is available only when the packet exceeds bandwidth limit. The CoS value range is from 0 to 7.
<b>none-tos</b>	Modifies the CoS value only.

**Defaults** No traffic policing is configured for the class map by default.

**Command** Policy map class configuration mode

**Mode**

**Usage Guide** N/A

**Configuration Examples** The following example configures traffic policing which modifies the DSCP value of the packet to 16 for class map "cm-acl" in policy map "pmap1".

```
Ruijie(config)# policy-map pmap1
Ruijie(config-pmap)# class cm-acl
Ruijie(config-pmap-c)# police 102400 4096 exceed-action dscp 16
```

Related	Command	Description
<b>Commands</b>	<b>show policy-map</b>	Displays the policy map configuration.

**Platform** N/A

**Description**

## 2.11 policy map

Use the following command to create a policy map and enter policy map configuration mode. Use the **no** or **default** form of this command to remove the specified policy map.

**policy-map** *policy-map-name*

**no policy-map** *policy-map-name*

**default policy-map** *policy-map-name*

Parameter	Parameter	Description
<b>Description</b>	<i>policy-map-name</i>	Policy map name. The policy map name can be a maximum of 31 characters.

**Defaults** No policy map is configured by default.

**Command** Global configuration mode.

**Mode**

**Usage Guide** N/A

**Configuration** The following example creates policy map “po”, and then adds a reference to class map “cmap1”.

**Examples** Sets the rate limit value to 10 Mbps, the burst traffic limit value to 256 Kbps, and discard packets which exceed the limit.

```
Ruijie(config)# policy-map po
Ruijie(config-pmap)# class cmap1
Ruijie(config-pmap-c)# police 10240 256 exceed-action drop
```

Related Commands	Command	Description
	<b>show policy-map</b>	Displays the policy map configuration.

**Platform** N/A

**Description**

## 2.12 priority-queue

Use this command to configure the output queue scheduling policy to SP. Use the **no** or **default** form of this command to restore the default queue scheduling policy.

**priority-queue**

**no priority-queue**

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

**Defaults** The default output queue scheduling policy is WRR.

**Command Mode** Global configuration mode.

**Usage Guide** This command shares the same configuration with the **mls qos scheduler sp**. The **show run** command displays this configuration in the **mls qos scheduler sp** item instead of **priority-queue**.

**Configuration** The following example configures the output queue scheduling policy to SP.

**Examples**

```
Ruijie(config)# priority-queue
```

Related Commands	Command	Description
	<b>show mls qos scheduler</b>	Displays the output queue scheduling policy.

**Platform** N/A

**Description**

## 2.13 priority-queue cos-map

Use this command to configure the mapping between the CoS value and the queue ID. Use the **no** or





<i>bandwidth</i>	
------------------	--

**Defaults** No minimum or maximum of interface bandwidth to a queue is configured by default.

**Command Mode** Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example configures the minimum interface bandwidth of queue 1 to 5 Mbps, and the maximum to 10 Mbps.

```
Ruijie(config)# interface gigabitEthernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# qos queue 1 bandwidth maximum 10240
Ruijie(config-if-GigabitEthernet 0/17)# qos queue 1 bandwidth minimum 5120
```

The following example configures the minimum interface bandwidth of queue 2 to 2 Mbps.

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/17)# qos queue 2 bandwidth minimum 2048
```

Related Commands	Command	Description
	<b>show qos bandwidth</b>	Displays the interface bandwidth of the queue.

**Platform Description** N/A

## 2.15 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* | *mbps* } *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 KBits. This value is from 16 to 1000000.
	<i>mbps</i>	Bandwidth limit value per second in Mbits on G.hn port. This value is from 10 to 1999
	<i>burst-size</i>	Burst traffic limit value in KBytes. This value is from 1 to 32.

**Defaults** Rate limiting is not configured by default.

**Command** Interface configuration mode.  
**Mode**

**Usage Guide** N/A

**Configuration Examples** The following example configures the rate limit value to 10 Mbps, and the burst traffic limit value to 32 Kbps.

```
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# rate-limit input 10240 32
```

Related	Command	Description
Commands	<b>show mls qos rate-limit</b>	Displays the rate limiting configuration of the interface.

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

## 2.16 service-policy

Use this command to apply the policy map to the interface, the virtual group or globally. Use the **no** or **default** form of this command to remove the policy map.

**service-policy input** *policy-map-name*

**no service-policy input** *policy-map-name*

**default service-policy input** *policy-map-name*

Parameter	Parameter	Description
<b>Description</b>	<i>policy-map-name</i>	Policy map name
	<b>input</b>	Applies the policy map to the input direction.

**Defaults** No policy map is configured on the interface or virtual group by default.

**Command** Interface configuration mode, and virtual group configuration mode.  
**Mode**

**Usage Guide** N/A

**Configuration Examples** The following example applies policy map “po” to the input direction of interface GigabitEthernet 0/17.

```
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# service-policy input po
```

Related	Command	Description
Commands	<b>show mls qos interface policers</b>	Displays the policy map configuration on the interface.
	<b>show mls qos virtual-group</b>	Displays the policy map configuration on the virtual group.

<b>policers</b>	
-----------------	--

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

## 2.17 set

Use this command to configure the CoS, DSCP or VID value for the traffic. Use the **no** form of this command to remove the CoS, DSCP or VID value from the traffic.

**set** { **ip dscp** *new-dscp* | **cos** *new-cos* | **vid** *new-vid* }

**no set** { **ip dscp** | **cos** | **vid** }

Parameter	Parameter	Description
<b>Description</b>	<b>ip dscp</b> <i>new-dscp</i>	Configures the DSCP value for the traffic. The range is from 0 to 63.
	<b>cos</b> <i>new-cos</i>	Configures the CoS value for the traffic. The range is from 0 to 7.
	<b>vid</b> <i>new-vid</i>	Configures the VID value for the traffic. The range is from 1 to 4094.

**Defaults** No CoS, DSCP or VID value is configured for the traffic in policy map class mode.

**Command Mode** Policy map class configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example creates policy map “pmap1”, and adds a reference to class map “cmap1”.

```
Ruijie(config)# policy-map pmap1
```

```
Ruijie(config-pmap)# class cmap1
```

The following example modifies the CoS value of the traffic to 3.

```
Ruijie(config-pmap-c)# set cos 3
```

Related Commands	Command	Description
	<b>show policy-map</b>	Displays the policy map configuration on the interface.

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

## 2.18 show class-map

Use this command to display the class map.

**show class-map** [ *class-map-name* ]

Parameter	Parameter	Description
<b>Description</b>	<i>class-map-name</i>	Class map name.

**Defaults** None

**Command Mode** Privileged EXEC mode, global configuration mode, interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays all class maps.

```
Ruijie# show class-map

Class Map cmap1
  Match ip dscp 20 40
Class Map cmap2
  Match access-group 110
```

The fields in the output of this command are described in the following table.

Field	Description
Class Map	Indicates the class map name.
Match	Indicates the matched rule.

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 2.19 show mls qos interface

Use this command to display the QoS configuration of the interface.

**show mls qos interface** [ *interface-name* | **policers** ]

Parameter	Parameter	Description
<b>Description</b>	<i>interface-name</i>	Interface name
	<b>policers</b>	Displays the traffic policing configured on 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 QoS configuration of interface GigabitEthernet 0/17.

```
Examples Ruijie# show mls qos interface gigabitethernet 0/17
Interface: GigabitEthernet 0/17
Ratelimit input: 10240 256
Ratelimit output:
Attached input policy-map: pmap1
Attached output policy-map:
Default trust: dscp
Default cos: 3
```

The fields in the output of this command are described in the following table.

Field	Description
Interface	Indicates the interface name.
Ratelimit input	Indicates the input rate limit value.
Ratelimit output	Indicates the output rate limit value.
Attached input policy-map	Indicates the input policy map.
Attached output policy-map	Indicates the output policy map.
Default trust	Indicates the trust mode of the interface.
Default cos	Indicates the default CoS value.

The following example displays the QoS configuration of all interfaces.

```
Ruijie# show mls qos interface policers
Interface: GigabitEthernet 0/17
Attached input policy-map: pmap1
Interface: GigabitEthernet 0/18
Attached input policy-map: p1
```

Related Commands	Command	Description
	N/A	N/A

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

## 2.20 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
<b>Description</b>	<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** The following example displays the CoS-DSCP mapping.

```

Examples 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.

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

## 2.21 show mls qos queuing

Use this command to display the QoS queuing configuration.

**show mls qos queuing [ interface *interface-name* ]**

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

wfq bandwidth weights:
qid weights
-----
1 3
2 4
3 5
4 6
5 7
6 8
7 9
8 10

Interface: GigabitEthernet 0/17
Wrr queue bandwidth: 1 1 1 1 2 2 2 2
Wfq queue bandwidth: 1 1 2 2 4 4 4 4
    
```

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.
wfq bandwidth weights	Indicates the WFQ queue weight.
cos	Indicates the CoS value.
qid	Indicates the queue ID.
weights	Indicates the weight value

```
Ruijie# show mls qos queueing interface gigabitEthernet 0/17
Interface: GigabitEthernet 0/17
Wrr queue bandwidth: 1 1 1 1 2 2 2 2
Wfq queue bandwidth: 1 1 2 2 4 4 4 4
```

Related Commands	Command	Description
	N/A	N/A

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

## 2.22 show mls qos rate-limit

Use this command to display the rate limiting configuration of the interface.

**show mls qos rate-limit [ interface *interface-name* ]**

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

**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 rate limiting configuration of all interfaces.

```
Ruijie# show mls qos rate-limit
Interface: GigabitEthernet 0/17
rate limit input Kbps = 10240 burst = 256
Interface: GigabitEthernet 0/18
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	Command	Description
Commands	N/A	N/A

Platform N/A  
Description

## 2.23 show mls qos scheduler

Use this command to display the queue scheduling policy.

**show mls qos scheduler** [ interface *interface-name* ]

Parameter	Parameter	Description
Description	interface <i>interface-name</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. The other queue scheduling policies are listed as follows: SP: Strict Priority RR: Round Robin WFQ: Weighted Fair Queue

Related	Command	Description
Commands	N/A	N/A

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

## 2.24 show mls qos virtual-group

Use this command to display the policy map configuration on the virtual group.

**show mls qos virtual-group** [ *virtual-group-number* | **policers** ]

Parameter	Parameter	Description
<b>Description</b>	<i>virtual-group-number</i>	Virtual group number. The range is from 1 to 128.
	<b>policers</b>	Displays the policy map configuration on all virtual groups.

**Defaults** None

**Command Mode** Privileged EXEC mode, global configuration mode, interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays the policy map configuration on all virtual groups.

```
Ruijie# show mls qos virtual-group policers
Virtual-group: 1
Attached input policy-map: pmap1
Virtual-group: 20
Attached output policy-map: pmap2
```

The fields in the output of this command are described in the following table.

Field	Description
Virtual-group	Indicates the virtual group number.
Attached input policy-map	Indicates the policy map applied on the input virtual group.
Attached output policy-map	Indicates the policy map applied on the output virtual group.

Related Commands	Command	Description
	N/A	N/A

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

## 2.25 show policy-map

Use this command to display policy maps.

**show policy-map** [ *policy-map-name* [ **class** *class-map-name* ] ]

Parameter	Parameter	Description
Description	<i>policy-map-name</i>	Policy map name
	<i>class-map-name</i>	Class map name

**Defaults** None

**Command Mode** Privileged EXEC mode, global configuration mode, interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays configuration of policy map “pmap1”.

```
Ruijie# show policy-map pmap1

Policy Map pmap1
  Class cmap1
    set ip dscp 16
  Class cmap2
    police 10240 256 exceed-action dscp 8
  Class cmap3
    police 512000 4096 exceed-action drop
```

The fields in the output of this command are described in the following table.

Field	Description
Policy Map	Indicates the policy map name.
Class	Indicates the class map name.
set	Indicates that the DSCP value is modified in this example.
police	Indicates bandwidth limit configuration and the action policy for the violated packets.

The following example displays the action policy for the traffic of class map “cmap1” in policy map “pmap1”.

```
Ruijie# show policy-map pmap1 class cmap1

Class cmap1
set ip dscp 16
```

Related Commands	Command	Description
	N/A	N/A

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

## 2.26 show policy-map interface

Use this command to display the policy applied to an interface.

**show policy-map interface** *interface-name*

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

**Defaults** None

**Command Mode** Privileged EXEC mode, global configuration mode, interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays the policy configuration of interface GigabitEthernet 0/17.

```
Ruijie# show policy-map interface gigabitEthernet 0/17
GigabitEthernet 0/17 input (tc policy): pm
  Class cm
    current token tbf: NULL
    params: 10240 kbps, 256 limit, 0 extended limit , 0 pir
    conformed 0 packets, 0 bytes; action: drop 0
    exceeded 0 packets, 0 bytes; action: none 0
    violated 0 packets, 0 bytes; action: none 0
    cbucket 0, cbs 0; ebucket 0 ebs 0
```

The fields in the output of this command are described in the following table.

Field	Description
input (tc policy)	Indicates the input policy map name.
Class	Indicates the class map name.
current token tbf	Algorithm of token bucket. NULL indicates single token bucket algorithm.
params	Parameter, including the limits of guaranteed bandwidth, burst traffic and peak bandwidth
conformed	The number of packets lower than the limit of guaranteed bandwidth

exceeded	The number of packets higher than the limit of guaranteed bandwidth while lower than the limit of peak bandwidth
violated	The number of packets higher than the limit of peak bandwidth
cbucket	Number of tokens in bucket C
cbs	Size of bucket C
ebucket	Number of tokens in bucket E
ebs	Size of bucket E

Related Commands	Command	Description
	N/A	N/A

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

## 2.27 show qos bandwidth

Use this command to display the bandwidth configuration.

**show qos bandwidth [ interfaces *interface-name* ]**

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

**Defaults** None

**Command Mode** Privileged EXEC mode, global configuration mode, interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays the bandwidth configuration of interface GigabitEthernet 0/17. (Taking the device supporting the bandwidth configuration of the queue for example.)

```
Ruijie# show qos bandwidth interface gigabitEthernet 0/17
```

```
Interface: GigabitEthernet 0/17
```

```
-----
```

queue-id	minimum-bandwidth	maximum-bandwidth
1	5120	10240
2	0	0

```
-----
```

3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
-----		
Total minimum-bandwidth:		5120
Total maximum-bandwidth:		10240

The fields in the output of this command are described in the following table.

Field	Description
Interface	Indicates the interface name.
queue-id	Indicates the queue ID.
minimum-bandwidth	Indicates the minimum bandwidth configuration. The unit is Kbps.
maximum-bandwidth	Indicates the maximum bandwidth configuration. The unit is Kbps.
Total minimum-bandwidth Total maximum-bandwidth	Indicates the total bandwidth of minimum and maximum

Related Commands	Command	Description
	N/A	N/A

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

## 2.28 show virtual-group

Use this command to display the member port in the virtual group.

**show virtual-group** [ *virtual-group-number* | **summary** ]

Parameter	Parameter	Description
<b>Description</b>	<i>virtual-group-number</i>	Virtual group number. The range is from 1 to 128.
	<b>summary</b>	Displays the member port in all virtual groups.

**Defaults** N/A

**Command Mode** Privileged EXEC mode, global configuration mode, interface configuration mode.

**Usage Guide** N/A

**Configuration** The following example displays the member port in all virtual groups.

**Examples**

```
Ruijie# show virtual-group summary
virtual-group      member
-----
1                  Gi0/17
2                  Gi0/18
```

The fields in the output of this command are described in the following table.

Field	Description
virtual-group	Indicates the virtual group number.
member	Indicates the member port in the virtual group.

**Related Commands**

Command	Description
N/A	N/A

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

## 2.29 virtual-group

Use this command to create a virtual group in global configuration mode.

Use this command to configure add an interface to a virtual group in interface configuration mode.

Use the **no** or **default** form of this command to remove a virtual group in global configuration mode.

Use the **no** or **default** form of this command to remove an interface from a virtual group in interface configuration mode.

**virtual-group** *virtual-group-number*

**no virtual-group** *virtual-group-number*

**default virtual-group** *virtual-group-number*

**Parameter Description**

Parameter	Description
<i>virtual-group-number</i>	Virtual group number. The range is from 1 to 128.

**Defaults** No virtual group is configured, or no interface is added to a virtual group, by default.

**Command Mode** Interface configuration mode, global configuration mode.

**Usage Guide** The member port added to the virtual group must be a physical port or an aggregate port member.

**Configuration** The following example sets the interface gigabitEthernet 0/17 as the member of virtual group 3:

**Examples**

```
Ruijie(config)# interface gigabitEthernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# virtual-group 3
```



Related Commands	Command	Description
		<b>show virtual-group</b>

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

## 2.30 wfq-queue bandwidth

Use this command to configure the WFQ queue weight ratio. Use the **no** or **default** form of this command to restore the default setting.

**wfq-queue bandwidth** *weight1 ... weight8*

**no wfq-queue bandwidth**

**default wfq-queue bandwidth**

Parameter Description	Parameter	Description
		<i>weight1 ... weight8</i>

**Defaults** The default queue weight ratio is 1:1:1:1:1:1:1:1.

**Command Mode** Global configuration mode.

**Usage Guide** If the weight value is 0, the SP scheduling policy is applied.

**Configuration Examples** The following example configures the WFQ queue weight ratio to 1:1:2:4:4:4:6:8.

```
Ruijie(config)# wfq-queue bandwidth 1 1 2 4 4 4 6 8
```

Related Commands	Command	Description
		<b>show mls qos queueing</b>

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

## 2.31 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
<b>Description</b>	<i>weight1...weight8</i>	8 queue weights. The default queue weight ratio is 1:1:1:1:1:1:1:1. The weight range is from 0 to 15.

**Defaults** The default queue weight ratio is 1:1:1:1:1:1:1:1.

**Command Mode** Global configuration mode

**Usage Guide** If the weight value is 0, the SP scheduling policy is applied.

**Configuration Examples** The following example configures the WRR queue weight ratio to 1:1:1:1:2:2:4:8.

```
Ruijie(config)# wrr-queue bandwidth 1 1 1 1 2 2 4 8

Ruijie(config)# interface gigabitEthernet 0/17

Ruijie(config-if-GigabitEthernet 0/17)# wrr-queue bandwidth 1 1 2 2 2 4 4
```

Related Commands	Command	Description
	<b>show mls qos queuing</b>	Displays the QoS queuing configuration.

**Platform Description** N/A



## IP Address & Application Commands

---

1. IP Address and Service Commands
2. ARP Commands
3. IPv6 Commands
4. DHCP Commands
5. DHCPv6 Commands
6. DNS Commands
7. FTP Client Commands
8. Network Connectivity Test Tool Commands
9. TCP Commands
10. IPv4/IPv6 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.

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
```

The following example configures the master and secondary IP addresses as 10.10.10.1/24 and 10.10.20.1/24 respectively.

```
Ruijie(config)# interface vlan 1
Ruijie(config-if-VLAN 1)# ip address 10.10.10.1 255.255.255.0
Ruijie(config-if-VLAN 1)# ip address 10.10.20.1 255.255.255.0 secondary
```

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 Description	Parameter	Description
	<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 directed-broadcast

Use this command to enable the conversion from IP directed broadcast to physical broadcast in the interface configuration mode. Use the **no** form of this command to restore the default setting.

**ip directed-broadcast** [ *access-list-number* ]

**no ip directed-broadcast**

Parameter Description	Parameter	Description
	<i>access-list-number</i>	(Optional) Access list number, in the range from 1 to 199 and from 1300 to 2699. After an access list number has been defined, only the IP directed broadcast packets that match this access list are converted.

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

**Command Mode** Interface configuration mode.

**Usage Guide** IP directed broadcast packet is an IP packet whose destination address is an IP subnet broadcast address. For example, the packet with the destination address 172.16.16.255 is called a directed broadcast packet. However, the node that generates this packet is not a member of the destination subnet.

The device that is not directly connected to the destination subnet receives an IP directed broadcast packet and handles this packet in the same way as forwarding a unicast packet. After the directed broadcast packet reaches a device that is directly connected to this subnet, the device converts the directed broadcast packet into a flooding broadcast packet (typically the broadcast packet whose destination IP address is all "1"), and then sends the packet to all the hosts in the destination subnet in the manner of link layer broadcast.

You can enable conversion from directed broadcast into physical broadcast on a specified interface, so that this interface can forward a direct broadcast packet to a directly connected network. This command affects only the final transmission of directed broadcast packets that have reached the destination subnet instead of normal forwarding of other directed broadcast packets.

You can also define an access list on an interface to control which directed broadcast packets to forward. After an access list is defined, only the packets that conform to the conditions defined in the access list undergo conversion from directed broadcast into physical broadcast.

If the **no ip directed-broadcast** command is configured on an interface, RGOS will discard the directed broadcast packets received from the directly connected network.

**Configuration Examples** The following example enables forwarding of directed broadcast packet on the vlan 1 of a device.

```
Ruijie(config)# interface VLAN 1
Ruijie(config-if-VLAN 1)# ip directed-broadcast
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.4 ip icmp error-interval

Use this command to set the rate to send the ICMP destination unreachable packets triggered by DF in the IP header. Use the **no** form of this command to restore the default setting.

**ip icmp error-interval DF milliseconds [ bucket-size ]**

**no ip icmp error-interval DF milliseconds [ bucket-size ]**

Use this command to set the rate to send other ICMP error packets. Use the **no** form of this command to restore the default setting.

**ip icmp error-interval milliseconds [ bucket-size ]**

**no ip icmp error-interval milliseconds [ bucket-size ]**

Parameter Description	Parameter	Description
	<i>milliseconds</i>	The refresh period of the token bucket, in the range from 0 to 2147483647 in the unit of milliseconds. 0 indicates no limit on the rate to send ICMP error packets. The default is 100.
	<i>bucket-size</i>	The number of tokens in the bucket, in the range is from 1 to 200. The default is 10.

**Defaults** The default rate is 10 packets per 100 millisecond.

**Command Mode** Global configuration mode.

**Usage Guide** To prevent DoS attack, the token bucket algorithm is adopted to limit the rate to send ICMP error packets.

If IP packets need to be fragmented while the DF is set to 1, the device sends ICMP destination unreachable packets numbered 4 to the source IP address for path MTU discovery. Rate limits on ICMP destination unreachable packets and other error packets are needed to prevent path MTU discovery failure.

It is recommended to set the refresh period to an integral multiple of 10 milliseconds. If the refresh period is not an integral multiple of 10 milliseconds, it is adjusted automatically. For example, 1 per 5 milliseconds is adjusted to 2 per 10 milliseconds; 3 per 15 milliseconds is adjusted to 2 per 10 milliseconds.

**Configuration Examples** The following example sets the rate to send the ICMP destination unreachable packets triggered by DF in the IP header to 100 per second.

```
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
```

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

**Platform Description** N/A

## 1.5 ip mask-reply

Use this command to configure the RGOS software to respond the ICMP mask request and send an ICMP response message in the interface configuration mode. Use the **no** form of this command to restore the default setting.

**ip mask-reply**  
**no ip mask-reply**

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

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

**Command mode** Interface configuration mode.

**Usage Guide** Sometimes, a network device needs the subnet mask of a subnet on the Internet. To obtain such information, the network device can send an ICMP mask request message, and the network device that receives this message will send a mask response message.

**Configuration** The following example sets the VLAN 1 interface of a device to respond the ICMP mask



**Examples**

request message.

```
Ruijie(config)# interface VLAN 1
Ruijie(config-if-VLAN 1)# ip mask-reply
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform  
Description**

N/A

## 1.6 ip mtu

Use this command to set the Maximum Transmission Unit (MTU) for an IP packet in the interface configuration mode. Use the **no** form of this command to restore the default setting.

**ip mtu bytes**

**no ip mtu**

**Parameter  
Description**

Parameter	Description
<i>bytes</i>	Maximum transmission unit of IP packet , in the range from 68 to 1500 bytes

**Defaults**

It is the same as the value configured in the interface command **mtu** by default.

**Command Mode**

Interface configuration mode.

**Usage Guide**

If an IP packet is larger than the IP MTU, the RGOS software will split this packet. All the devices in the same physical network segment must have the same IP MTU for the interconnected interface.

If the interface configuration command **mtu** is used to set the maximum transmission unit value of the interface, IP MTU will automatically match with the MTU value of the interface. However, if the IP MTU value is changed, the MTU value of the interface will remain unchanged.

**Configuration**

The following example sets the IP MTU value of the VLAN 1 interface to 512 bytes.

**Examples**

```
Ruijie(config)# interface VLAN 1
Ruijie(config-if-VLAN 1)# ip mtu 512
```

**Related  
Commands**

Command	Description
<b>mtu</b>	Sets the MTU value of an interface.

**Platform  
Description**

N/A

## 1.7 ip redirects

Use this command to allow the RGOS software to send an ICMP redirection message in the interface configuration mode. Use the **no** form of this command to disable this function.

**ip redirects**

**no ip redirects**

Parameter	Parameter	Description
Description	N/A	N/A

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

**Command** Interface configuration mode.

**Mode**

**Usage Guide** When the route is not optimum, it may make the device to receive packets through one interface and send it though the same interface. If the device sends the packet through the interface through which this packet is received, the device will send an ICMP redirection message to the data source, telling the data source that the gateway for the destination address is another device in the subnet. In this way the data source will send subsequent packets along the optimum path.

**Configuration** The following example disables ICMP redirection for the VLAN 1 interface.

**Examples**

```
Ruijie(config)# interface VLAN 1
Ruijie(config-if-VLAN 1)# no ip redirects
```

Related	Command	Description
Commands	N/A	N/A

**Platform** N/A

**Description**

## 1.8 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
Description	N/A	N/A

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

**Command** Global configuration mode.  
**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	Command	Description
Commands	N/A	N/A

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

## 1.9 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** Global configuration mode  
**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

## 1.10 ip unreachable

Use this command to allow the RGOS software to generate ICMP destination unreachable messages. Use the **no** form of this command to disable this function.

**ip unreachable**

**no ip unreachable**

Parameter	Parameter	Description
Description	N/A	N/A

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

**Command Mode** Interface configuration mode.

**Usage Guide** RGOS software will send a ICMP destination unreachable message if it receives unicast message with self-destination-address and can not process the upper protocol of this message.

RGOS software will send ICMP host unreachable message to source data if it can not forward a message due to no routing.

This command influences all ICMP destination unreachable messages.

**Configuration Examples** The following example disables sending ICMP destination unreachable message on VLAN 1.

```
Ruijie(config)# interface VLAN 1
Ruijie(config-if-VLAN 1)# no ip unreachable
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.11 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.

<i>brief</i>	Displays the brief configurations about the IP of the layer-3 interface (including the interface primary ip, secondary ip and interface status)
--------------	---

**Defaults** N/A.

**Command** Privileged EXEC mode.

**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 exmaple displays the output of the **show ip interface brrief command**.

**Examples**

```
Ruijie(config)#show ip interface brief
Interface                               IP-Address (Pri)   IP-Address (Sec)
Status      Protocol
VLAN 1      10.10.10.1/24     no address         down
down
VLAN 1      no address        no address
down      down
VLAN 4094   no address        no address
down      down
```

Ruijie(config)#

Description of fields in the command output is as follows:

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

```

Description of fields in the command output is as follows:

Field	Description
IP interface state is	The network interface is available, and both its interface hardware status and line protocol status are "UP".
IP interface type is	Show the interface type, such as broadcast, point-to-point, etc.
IP interface MTU is	Show the MTU value of the interface.
IP address is	Show the IP address and mask of the interface.
IP address negotiate is	Show whether the IP address is obtained through negotiation.
Forward direct-broadcast is	Show whether the directed broadcast is forwarded.
ICMP mask reply is	Show whether an ICMP mask response message is sent.
Send ICMP redirect is	Show whether an ICMP redirection message is sent.
Send ICMP unreachable is	Show whether an ICMP unreachable message is sent.
DHCP relay is	Show whether the DHCP relay is enabled.
Fast switch is	Show whether the IP fast switching function is enabled.
Route horizontal-split is	Show whether horizontal split is enabled, which will affect the route update behavior of the distance vector protocol.
Help address is	Show the helper IP address.
Proxy ARP is	Show whether the agent ARP is enabled.

ARP packet input number Request packet Reply packet Unknown packet	Show the total number of ARP packets received on the interface, including: ARP request packet ARP reply packet Unknown packet
TTL invalid packet number	Show the TTL invalid packet number
ICMP packet input number Echo request Echo reply Unreachable Source quench Routing redirect	Show the total number of ICMP packets received on the interface, including: Echo request packet Echo reply packet Unreachable packet Source quench packet Routing redirection packet

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

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

## 1.12 show ip packet queue

Use this command to display the statistics of IP packet queues.

**show ip packet queue**


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 statistics of IP packet queues.

 RG-S29 series products do not support the VRF parameter. The following example is for reference purpose. Please take the actual product as the standard.

```
Ruijie# show ip packet queue
Receive 31925 packets(fragment=0):
  IP packet receive queue: length 0, max 1542, overflow 0.
  Receive 13 ICMP echo packets, 25 ICMP reply packets .
Discards:
```

```

Failed to alloc skb: 0.
Receive queue overflow: 0.
Unknow protocol drops: 0.
ICMP rcv drops: 0. for skb check fail.
ICMP rcv drops: 0. for skb is broadcast.
Sent packets:
Success: 15644
Generate 13 and send 8 ICMP reply packets, send 26 ICMP echo packets.
It records 187 us as max time in ICMP reply process.
Failed to alloc ebuf: 0
Dropped by EFMP: 0
NoRoutes: 887
Get vrf fails: 0
Cannot assigned address drops: 0
Failed to encapsulate ethernet head: 0
ICMP error queue: length 0, max 1542, overflow 0.
    
```

Field	Description
IP packet receive queue	Statistics of received packets
Discards	Statistics of discarded packets
Sent packets	Statistics of sent packets
ICMP error queue	Statistics of ICMP error packets

Related Commands	Command	Description
	N/A	N/A

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

### 1.13 show ip packet statistics

Use this command to display the statistics of IP packets.

**show ip packet statistics** [ *interface-name* | **total** ]

Parameter Description	Parameter	Description
	<i>interface-name</i>	Interface name
	<i>total</i>	Displays the total statistics of all interfaces.

**Defaults** N/A.

**Command Mode** Privileged EXEC mode.



**Usage Guide** N/A.

**Configuration** The following example displays the output of this command.

**Examples**

```
Ruijie# 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 0/17
  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
Tunnel 1
  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 21584 packets, 1122848 bytes
  Unicast:21584,Multicast:0,Broadcast:0
```

**Related Commands**

Command	Description
N/A	N/A

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

## 1.14 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
```

Description of fields in the command output is as follows:

Field	Description
Number	Number
Protocol	Protocol
Process name	Process name
Total	Total number

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

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

## 1.15 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      dhcp.elf              RAW       ICMP        0.0.0.0:1     0.0.0.0:0
*
2      vrrp.elf              RAW       ICMP        0.0.0.0:1     0.0.0.0:0
*
3      igmp.elf              RAW       IGMP        0.0.0.0:2     0.0.0.0:0
*
4      vrrp.elf              RAW       VRRP        0.0.0.0:112   0.0.0.0:0
*
5      dhcpc.elf             DGRAM    UDP         0.0.0.0:68    0.0.0.0:0
*
6      rg-snmpd              DGRAM    UDP         0.0.0.0:161   0.0.0.0:0
*
7      wbav2                 DGRAM    UDP         0.0.0.0:2000  0.0.0.0:0
*
8      vrrp_plus.elf        DGRAM    UDP         0.0.0.0:3333  0.0.0.0:0
*
9      mpls.elf              DGRAM    UDP         0.0.0.0:3503  0.0.0.0:0
*
10     rds_other_th         DGRAM    UDP         0.0.0.0:3799  0.0.0.0:0
*
11     rg-snmpd              DGRAM    UDP         0.0.0.0:14800 0.0.0.0:0
*
12     rg-sshd              STREAM   TCP         0.0.0.0:22    0.0.0.0:0
LISTEN
13     rg-telnetd           STREAM   TCP         0.0.0.0:23    0.0.0.0:0
LISTEN
14     wbard                 STREAM   TCP         0.0.0.0:4389  0.0.0.0:0
LISTEN
15     wbard                 STREAM   TCP         0.0.0.0:7165  0.0.0.0:0
```

```
LISTEN
Total: 15
```

Description of fields in the command output is as follows:

Field	Description
Number	Serial number.
Process name	Process name.
Type	Socket type, including the following types: RAW: raw sockets DGRAM: datagram type STREAM: stream type.
Protocol	Protocol.
LocalIP:Port	Local IP address and port.
ForeignIP:Port	Peer IP address and port.
State	State. This field is for only TCP sockets.
Total	The total number of sockets.

Related Commands	Command	Description
	N/A	N/A

Platform N/A  
Description

### 1.16 show ip udp

Use this command to display IPv4 UDP sockets.

**show ip udp [ local-port num | peer-port num ]**

Use this command to display IPv4 UDP socket statistics.

**show ip udp statistics**

Parameter Description	Parameter	Description
	<b>local-port num</b>	Local port number
	<b>peer-port num</b>	Peer 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      0.0.0.0:161           0.0.0.0:0        rg-snmpd
3      0.0.0.0:2000          0.0.0.0:0        wbav2
4      0.0.0.0:3333          0.0.0.0:0        vrrp_plus.elf
5      0.0.0.0:3503          0.0.0.0:0        mpls.elf
6      0.0.0.0:3799          0.0.0.0:0        rds_other_th
7      0.0.0.0:14800         0.0.0.0:0        rg-snmpd
```

Description of fields in the command output is as follows:

Field	Description
Number	Number.
Local Address	Local IP address and port.
Peer Address	Peer IP address and port.
Process name	Process name.

**Related  
Commands**

Command	Description
N/A	N/A

**Platform  
Description**

N/A

## 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*

Parameter	Parameter	Description
<b>Description</b>	<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 Examples** The following example sets an ARP static mapping record for a host in the Ethernet.

```
Ruijie(config)# arp 1.1.1.1 4e54.3800.0002 arpa
```

Related Commands	Command	Description
	<b>clear arp-cache</b>	Clears the ARP cache table

**Platform Description** N/A

### 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	Parameter	Description
Description	<i>num</i>	The number of the IP message to trigger the ARP to set the 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 to set the 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** N/A  
**Description**

## 2.3 arp retry interval

Use this command to set the frequency for sending the arp request message locally, namely, the

time interval between two continuous ARP requests sent for resolving one IP address. Use the **no** form of this command to restore the default setting.

**arp retry interval** *seconds*

**no arp retry interval**

Parameter	Parameter	Description
Description	<i>seconds</i>	Time for retransmitting the ARP request message in the range from 1 to 3600 in the unit of seconds.

**Defaults** The default is 1.

**Command** Global configuration mode.

**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** The following example sets the retry interval of the ARP request as 30 seconds.

**Examples**

```
Ruijie(config)# arp retry interval 30
```

Related	Command	Description
Commands	<b>arp retry times</b>	Number of times for retransmitting an ARP request message.

**Platform** N/A

**Description**

## 2.4 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** Global configuration mode.



**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** The following example sets the local ARP request not to be retried.

**Examples**

```
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	Command	Description
Commands	<b>arp retry interval</b>	Interval for retransmitting an ARP request message

**Platform** N/A

**Description**

## 2.5 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>secondsv</i>	The timeout is in the range from 0 to 2147483 in the unit of seconds.

**Defaults** The default is 3600.

**Command** Global configuration mode

**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** The following example sets the timeout for the dynamic ARP mapping record that is learned dynamically from GigabitEthernet port 0/17 to 120 seconds.

**Examples**

```
Ruijie(config)# arp timeout 120
```

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

<b>Commands</b>	<b>clear arp-cache</b>	Clears the ARP cache list.
	<b>show interfaces</b>	Displays the interface information.

**Platform** N/A

**Description**

## 2.6 arp unresolve

Use this command to set the maximum number of the unresolved ARP entries. Use **no** form of this command to restore the default setting.

**arp unresolve** *number*

**no arp unresolve**

<b>Parameter</b>	<b>Parameter</b>	<b>Description</b>
<b>Description</b>	<i>number</i>	The maximum number of the unresolved ARP entries in the range from 1 to the ARP table size supported by the device.

**Defaults** The default is the ARP table size supported by the device.

**Command** Global configuration mode.

**Mode**

**Usage Guide** If there are a large number of unresolved entries in the ARP cache table and they do not disappear after a period of time, this command can be used to limit the quantity of the unresolved entries.

**Configuration** The following example sets the maximum number of the unresolved items to 500.

**Examples**

```
Ruijie(config)# arp unresolve 500
```

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

**Platform** N/A

**Description**

## 2.7 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** [ *ip* [ *mask* ] ] | **interface** *interface-type interface-number* ]

<b>Parameter</b>	<b>Parameter</b>	<b>Description</b>
<b>Description</b>	<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.
<i>interface interface-type interface-number</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 Examples** The following example deletes all dynamic ARP mapping records.

```
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 SVI1.

```
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 Description** N/A

## 2.8 show arp

Use this command to display the Address Resolution Protocol (ARP) cache table

```
show arp [ interface-type interface-number | [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
Total Numbers of Arp: 7
Protocol Address Age(min) Hardware Type Interface
Internet 192.168.195.68 0 0013.20a5.7a5f arpa VLAN 1
Internet 192.168.195.67 0 001a.a0b5.378d arpa VLAN 1
Internet 192.168.195.65 0 0018.8b7b.713e arpa VLAN 1
Internet 192.168.195.64 0 0018.8b7b.9106 arpa VLAN 1
Internet 192.168.195.63 0 001a.a0b5.3990 arpa VLAN 1
Internet 192.168.195.62 0 001a.a0b5.0b25 arpa VLAN 1
Internet 192.168.195.5 -- 00d0.f822.33b1 arpa VLAN 1
```

Description of fields in the command output is as follows:

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** N/A  
**Description**

## 2.9 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 Examples** The following example displays the output result of the **show arp counter** command:

```
Ruijie#sho arp counter
ARP Limit:                2000
Count of static entries:  0
Count of dynamic entries: 1 (complete: 1 incomplete: 0)
Total:                    1
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A  
Description

## 2.10 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>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 Privileged EXEC mode  
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 Examples** The following example displays the output result of the **show arp detail** command:

```
Ruijie# show arp detail
IP Address MAC Address Type Age(min) Interface Port
20.1.1.1 000f.e200.0001 Static -- -- --
20.1.1.1 000f.e200.0001 Static -- V13 --
20.1.1.1 000f.e200.0001 Static -- V13
193.1.1.70 00e0.fe50.6503 Dynamic 1 V13
192.168.0.39 0012.a990.2241 Local -- V13 --
192.168.0.1 0012.a990.2241 Local -- V13 --
```

The following example displays arp details including InnerVLAN on products supporting QinQ termination:

```
Ruijie# show arp detail
IP Address      MAC Address      Type      Age (min)  Interface  Port
SubVlan  InnerVlan
20.1.1.2        0020.0101.0002  Static    --         V1         --      --
1.1.1.1         00d0.f822.33bb  Local     --         V12        --      --
```

Description of fields in the command output is as follows:

Field	Description
IP Address	IP address corresponding to the hardware address
MAC Address	hardware address corresponding to the IP address
Age (min)	Age of the ARP learning, in minutes
Port	Layer2 port associated with the ARP
Type	ARP type, includes the Static, Dynamic, Trust,Local
Interface	Layer 3 interface associated with the IP addresses
SubVLAN	SubVLAN corresponding to the ARP entries
InnerVLAN	InnerVLAN or CE-VLAN corresponding to the ARP entries
Location	Local: ARP entries are generated or learned on the local device. Remote: ARP entries are synced from a remote gateway.

Related Commands	Command	Description
	N/A	N/A

Platform N/A  
Description

## 2.11 show arp packet statistics

Use this command to display the statistics of ARP packets.

**show arp packet statistics** [ *interface-type interface-number* ]

Parameter Description	Parameter	Description
	<i>interface-type</i> <i>interface-number</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
```

Description of fields in the command output is as follows:

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**

## 2.12 show arp timeout

Use this command to display the aging time of a dynamic ARP entry on the interface.

**show arp timeout**

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



**Defaults** N/A.

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A.

**Configuration Examples** 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 Description** N/A

## 2.13 show ip arp

Use this command to display the Address Resolution Protocol (ARP) cache table.

**show ip arp**

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

**Defaults** N/A.

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A.

**Configuration Examples** The following example displays the output of **show ip arp**:

**Examples**

```
Ruijie#show ip arp
Protocol Address Age(min) Hardware Type Interface
Internet 1.1.1.1 <static> 4e54.3800.0002 arpa
Total number of ARP entries: 1
```

Description of fields in the command output is as follows:

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**

N/A

**Description**

## 3 IPv6 Commands

### 3.1 clear ipv6 neighbors

Use this command to clear the dynamic IPv6 neighbors.

**clear ipv6 neighbors** [ *interface-id* ]

Parameter Description	Parameter	Description
	<i>interface-id</i>	Interface name. Clear the dynamically learned IPv6 neighbors on the specified interface.

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** This command does not clear all the dynamic neighbors on authentication VLAN. Note that the static neighbors will not be cleared.

**Configuration** The following example clears the dynamic IPv6 neighbors.

**Examples** Ruijie# clear ipv6 neighbors

Related Commands	Command	Description
	ipv6 neighbor	Configures the neighbor.
	show ipv6 neighbors	Displays the neighbor information.

**Platform** N/A

**Description**

### 3.2 ipv6 address

Use this command to configure an IPv6 address for a network interface. Use the **no** form of this command to restore the default setting.

**ipv6 address ipv6-address/prefix-length**

**ipv6 address** *ipv6-prefix/prefix-length eui-64*

**ipv6 address** *prefix-name sub-bits/prefix-length [ eui-64 ]*

**no ipv6 address**

**no ipv6 address** *ipv6-address/prefix-length*

**no ipv6 address** *ipv6-prefix/prefix-length eui-64*

**no ipv6 address** *prefix-name sub-bits/prefix-length [ eui-64 ]*

Parameter	Parameter	Description
Description	<i>ipv6-prefix</i>	IPv6 address prefix in the format defined in RFC4291. The address shall be in hex; the fields in the address shall be separated by comma, and each field shall contain 16 bits.
	<i>ipv6-address</i>	IPv6 address in the format defined in RFC4291. The address shall be in hex; the fields in the address shall be separated by comma, and each field shall contain 16 bits.
	<i>prefix-length</i>	Length of the IPv6 prefix, the network address of the IPv6 address. Note: The prefix length range of the IPv6 address of the interface of S86 is 0 to 64 or 128 to 128.
	<i>prefix-name</i>	The general prefix name. Use the specified general prefix to generate the interface address.
	<i>sub-bits</i>	The value of the sub-prefix bit and the host bit generates the interface address combining with the general prefix. The value shall be in the format defined in the RFC4291.
	<i>eui-64</i>	The generated IPv6 address consists of the address prefix and the 64 bit interface ID

**Defaults** N/A

**Command Mode** Interface configuration mode

**Usage Guide** When an IPv6 interface is created and the link status is UP, the system will automatically generate a local IP address for the interface.

The IPv6 address could also be generated using the general prefix. That is, the IPv6 address consists of the general prefix and the sub-prefix and the host bit. The general prefix could be configured using the **ipv6 general-prefix** command or may be learned through the DHCPv6 agent PD (Prefix Discovery) function (please refer to the *DHCPv6 Configuration*). Use the *sub-bits/prefix-length* parameter of this command to configure the sub-prefix and the host bit.

If no deleted address is specified when using **no ipv6 address**, all the manually configured addresses will be deleted.

**no ipv6 address *ipv6-prefix/prefix-length eui-64*** can be used to delete the addresses configured with **ipv6 address *ipv6-prefix/prefix-length eui-64***.

**Configuration Examples**

```
Ruijie(config)# interface VLAN 1
Ruijie(config-if-VLAN 1)# ipv6 address 2001:1::1/64
Ruijie(config-if-VLAN 1)# no ipv6 address 2001:1::1/64
Ruijie(config-if-VLAN 1)# ipv6 address 2002:1::1/64 eui-64
Ruijie(config-if-VLAN 1)# no ipv6 address 2002:1::1/64 eui-64
```

Related Commands	Command	Description
	N/A	N/A

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

### 3.3 ipv6 address autoconfig

Use this command to automatically configure an IPv6 stateless address for a network interface. Use the **no** form of this command to restore the default setting.

**ipv6 address autoconfig [ default ]**  
**no ipv6 address autoconfig**

Parameter	Parameter	Description
<b>Description</b>	<b>default</b>	(Optional) If this keyword is configured, a default routing is generated. Note that only one layer3 interface on the entire device is allowed to use the <b>default</b> keyword

**Defaults** N/A

**Command Mode** Interface configuration mode

**Usage Guide** The stateless automatic address configuration is that when receiving the RA (Route Advertisement) message, the device could use the prefix information of the RA message to automatically generate the EUI-64 interface address.

If the RA message contains the flag of the “other configurations”, the interface will obtain these “other configurations” through the DHCPv6. The “other configurations” usually means the IPv6 address of the DNS server, the IPv6 address of the NTP server, etc.

Use the **no ipv6 address autoconfig** command to delete the IPv6 address.

**Configuration Examples**

```
Ruijie(config)# interface VLAN 1
Ruijie(config-if-VLAN 1)# ipv6 address autoconfig default
Ruijie(config-if-VLAN 1)# no ipv6 address autoconfig
```

Related Commands	Command	Description
	<b>ipv6 address ipv6-prefix/prefix-length [ eui-64 ]</b>	Configures the IPv6 address for the interface manually.

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

### 3.4 ipv6 enable

Use this command to enable the IPv6 function on an interface. Use the **no** form of this command to restore the default setting.

**ipv6 enable**


**no ipv6 enable**

Parameter	Parameter	Description
Description	N/A	N/A

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

**Command Mode** Interface configuration mode

**Usage Guide** The IPv6 function of an interface can be enabled by configuring **ipv6 enable** or by configuring IPv6 address for the interface.

 If an IPv6 address is configured for the interface, the IPv6 function will be enabled automatically on the interface and cannot be disabled with **no ipv6 enable**.

**Configuration Examples** The following example enables the IPv6 function on VLAN.

```
Ruijie(config)# interface VLAN 1
Ruijie(config-if-VLAN 1)# ipv6 enable
```

Related Commands	Command	Description
	<b>show ipv6 interface</b>	Displays the related information of an interface.

**Platform Description** N/A

### 3.5 ipv6 general-prefix

Use this command to configure the IPv6 general prefix in the global configuration mode.

**ipv6 general-prefix** *prefix-name* *ipv6-prefix/prefix-length*

**no ipv6 general-prefix** *prefix-name* *ipv6-prefix/prefix-length*

Parameter	Parameter	Description
Description	<i>prefix-name</i>	The general prefix name.
	<i>pv6-prefix</i>	The network prefix value of the general-prefix following the format defined in RFC4291.
	<i>prefix-length</i>	The length of the general prefix.

**Defaults** N/A

**Command Mode** Global configuration mode.

**Usage Guide** It is convenient to number the network by using the general prefix, which defines a prefix so that many

longer specified prefixes could refer to it. These specified prefixes are updated whenever the general prefix changes. If the network number changes, just modify the general prefix.

A general prefix could contain multiple prefixes.

These longer specified prefixes are usually used for the Ipv6 address configuration on the interface.

**Configuration** The following example configures manually a general prefix as my-prefix.

**Examples**

```
Ruijie(config)# ipv6 general-prefix my-prefix 2001:1111:2222::/48
```

Related	Command	Description
Commands	<b>ipv6 address prefix-name sub-bits/prefix-length</b>	Configures the interface address using the general prefix.
	<b>show ipv6 general-prefix</b>	Displays the general prefix.

**Platform** N/A

**Description**

### 3.6 ipv6 hop-limit

Use this command to configure the default hopcount to send unicast messages in the global configuration mode.

**ipv6 hop-limit** *value*

**no ipv6 hop-limit**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** The default is 64.

**Command Mode** Global configuration mode.

**Usage Guide** This command takes effect for the unicast messages only, not for multicast messages.

**Configuration** The following example sets the default hopcount to 100.

**Examples**

```
Ruijie(config)# ipv6 hop-limit 100
```

Related	Command	Description
Commands	N/A	N/A

**Platform** N/A

**Description**

### 3.7 ipv6 icmp error-interval

Use this command to set the frequency with which ICMPv6-oversize error packets are sent. Use the **no** form of this command to restore the default setting.

**ipv6 icmp error-interval too-big** *milliseconds* [ *bucket-size* ]

**no ipv6 icmp error-interval too-big** *milliseconds* [ *bucket-size* ]

Use this command to set the frequency with which other ICMPv6 error packets are sent. Use the **no** form of this command to restore the default setting.

**ipv6 icmp error-interval** *milliseconds* [ *bucket-size* ]

**no ipv6 icmp error-interval** *milliseconds* [ *bucket-size* ]

Parameter	Parameter	Description
Description	<i>milliseconds</i>	Sets the refresh interval of the token bucket, in the range from 0 to 2147483647 in the unit of seconds. Setting the value to 0 indicates that the frequency with which ICMPv6 error packets are sent is not fixed.
	<i>bucket-size</i>	Sets the number of tokens in the token bucket, in the range from 1 to 200.

**Defaults** The default *milliseconds* is 100 and *bucket-size* is 10.

**Command Mode** Global configuration mode

**Usage Guide** The token bucket algorithm is adopted to set the frequency with which ICMPv6 error packets are sent so as to prevent Denial of Service (DoS) attack, If the forwarded IPv6 packet is greater than the egress IPv6 MTU in size, the router discards the IPv6 packet and sends the ICMPv6-oversize error packet to the source IPv6 address. This kind of ICMPv6 error packet is used for IPv6 path MTU discovery. If there are too many ICMPv6 error packets, the ICMPv6-oversize error packet may not be sent, causing IPv6 path MTU discovery failure. Therefore, it is recommended to set the frequency of ICMPv6-oversize error packet and other ICMPv6 error packet respectively. Note that ICMPv6 redirect packet is not an ICMPv6 error packet and Ruijie sets the frequency of the ICMPv6 redirect packet the same as that of other ICMPv6 error packet. For the timer is accurate to 10 milliseconds, it is recommended to set the refresh interval of the token bucket to an integer multiple of 10 milliseconds. If the refresh interval is not an integer multiple of 10 milliseconds, it is converted automatically. For example, the frequency of 1 per five milliseconds turns out to be 2 per 10 milliseconds; the frequency of 3 per 15 milliseconds is converted to 2 per 10 milliseconds.

**Configuration Examples** The following example sets the frequency with which ICMPv6-oversize error packets are sent to 100 per second.

```
Ruijie(config)# ipv6 icmp error-interval too-big 1000 100
```

The following example sets the frequency with which other ICMPv6 error packets are sent to 10 per



second.

```
Ruijie(config)# ipv6 icmp error-interval 1000 10
```

Related Commands	Command	Description
	N/A	N/A

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

### 3.8 ipv6 mtu

Use this command to configure the MTU of IPv6 packets. Use the **no** form of this command to restore the default setting.

**ipv6 mtu** *bytes*

**no ipv6 mtu**

Parameter Description	Parameter	Description
	<i>bytes</i>	MTU of IPv6 packets, in bytes. The value ranges from 1280 to 1500.

**Defaults** The default configuration is the same as the configuration of the **mtu** command.

**Command Mode** Interface configuration mode

**Usage Guide** If the size of an IPv6 packet exceeds the IPv6 MTU, the RGOS software segments the packet. For all devices in the same physical network segment, the IPv6 MTU of the interconnected interface must be the same.

**Configuration Examples** The following example sets the IPv6 MTU of the VLAN 1 interface to 1400 bytes.

```
Ruijie(config)# interface VLAN 1
Ruijie(config-if-VLAN 1)# ipv6 mtu 1400
```

Related Commands	Command	Description
	<b>mtu</b>	Sets the MTU of an interface.

**Platform** This command cannot be used on Layer 2 devices.  
**Description**

### 3.9 ipv6 nd cache interface-limit

Use this command to set the maximum number of neighbors learned on the interface. Use the **no** form of this command to restore the default setting.

**ipv6 nd cache interface-limit** *value*

**no ipv6 nd cache interface-limit**

Parameter	Parameter	Description
Description	<i>value</i>	Sets the maximum number of neighbors learned on the interface, including the static and dynamic neighbors, in the range from 0 to the number supported by the device. 0 indicates the number is not limited.

**Defaults** The default is 0.

**Command Mode** Interface configuration mode

**Usage Guide** This function can prevent neighbor entries generated by malicious neighbor attacks from consuming memory. *limit* must be no smaller than the number of neighbors learned on the interface. Otherwise, the configuration does not take effect.

**Configuration Examples** The following example sets the number of neighbors learned on the interface to 100.

```
Ruijie(config)# interface VLAN 1
Ruijie(config-if-VLAN 1)# ipv6 nd cache interface-limit 100
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

### 3.10 ipv6 nd dad attempts

Use this command to set the number of the NS packets to be continuously sent for IPv6 address collision check on the interface. Use the **no** form of this command to restore it to the default setting.

**ipv6 nd dad attempts** *value*  
**no ipv6 nd dad attempts** *value*

Parameter	Parameter	Description
Description	<i>value</i>	Number of the NS packets. If it is set to 0, it indicates that the IPv6 address collision check is disabled on the interface. The range is 0 to 600.

**Defaults** The default is 1.

**Command Mode** Interface configuration mode.

**Usage Guide** When the interface is configured with a new IPv6 address, the address collision shall be checked before the address is assigned to the interface, and the address shall be in the "tentative" status. After the address collision check is completed, if no collision is detected, the address can be used normally; if collision is detected and the interface ID of the address is an EUI-64 ID, it indicates that the link-layer address is repeated, and the system will automatically shut down the interface (that is, to prohibit IPv6 operations on the interface). In this case, you shall modify and configure a new address manually, and restart address collision check for the **down/up** interface. Whenever the state of an interface changes from **down** to **up**, the address collision check function of the interface will be enabled.

**Configuration** The following example sets the number of the NS packets to 3.

**Examples**

```
Ruijie(config)# interface VLAN 1
RRuijie(config-if-VLAN 1)# ipv6 nd dad attempts 3
```

Related Commands	Command	Description
	<b>show ipv6 interface</b>	Displays the interface information.

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

### 3.11 ipv6 nd dad retry

Use this command to set the interval for address conflict detection. Use the **no** form of this command to restore the default setting.

**ipv6 nd dad retry** *value*  
**no ipv6 nd dad retry**

Parameter	Parameter	Description
<b>Description</b>	<i>value</i>	Sets the interval for address conflict detection, 60 seconds by default. Setting <i>value</i> to 0 indicates that the function is disabled.

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** Before configuring a new IPv6 address for an interface, enable address conflict detection on the interface. If a conflict address is detected, the device does not receive the IPv6 packet destined to the conflict address. This command is used to perform conflict detection again when the interval expires. If there is no conflict, the address can be used.

**Configuration** The following example sets the interval for address conflict detection to 10s.

**Examples** `Ruijie(config)# ipv6 nd dad retry 10`

Related Commands	Command	Description
	N/A	N/A

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

### 3.12 ipv6 nd managed-config-flag

Use this command to set the “managed address configuration” flag bit of the RA message. Use the **no** form of this command to restore the default setting.

**ipv6 nd managed-config-flag**  
**no ipv6 nd managed-config-flag**

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

**Defaults** N/A

**Command Mode** Interface configuration mode.

**Usage Guide** This flag determines whether the host that receives the RA message obtains an IP address through stateful auto configuration. If the flag is set, the host obtains an IP address through stateful auto configuration, otherwise it does not be used.

**Configuration Examples** The following example sets the “managed address configuration” flag bit of the RA message.

```
Ruijie(config)# interface VLAN 1
Ruijie(config-if-VLAN 1)# ipv6 nd managed-config-flag
```

Related Commands	Command	Description
	<b>show ipv6 interface</b>	Displays the interface information.
	<b>ipv6 nd other-config-flag</b>	Sets the flag for obtaining all information except IP address through stateful auto configuration.

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

### 3.13 ipv6 nd ns-interval

Use this command to set the interval for the interface to retransmitting NS (Neighbor Solicitation). Use

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

**ipv6 nd ns-interval** *milliseconds*

**no ipv6 nd ns-interval**

Parameter	Parameter	Description
<b>Description</b>	<i>milliseconds</i>	Interval for retransmitting NS in the range of 1000 to 429467295 milliseconds

**Defaults** The default value in RA is 0 (unspecified); the interval for retransmitting NS is 1000 milliseconds (1 second).

**Command mode** Interface configuration mode.

**Usage Guide** The configured value will be advertised through RA and will be used by the device itself. It is not recommended to set a too short interval.

**Configuration Examples** The following example sets the interval for the interface to retransmitting NS to 2,000 seconds.

```
Ruijie(config)# interface VLAN 1
Ruijie(config-if-VLAN 1)# ipv6 nd ns-interval 2000
```

Related Commands	Command	Description
	<b>show ipv6 interface</b>	Displays the interface information.

**Platform Description** N/A

### 3.14 ipv6 nd other-config-flag

Use this command to set "other stateful configuration" flag bit of the RA message. Use the **no** form of this command to delete the flag bit.

**ipv6 nd other-config-flag**

**no ipv6 nd other-config-flag**

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

**Defaults** The flag bit is not set by default.

**Command mode** Interface configuration mode.

**Usage Guide** With this flag bit set, the flag bit of the RA message sent by the device is set. After receiving this flag bit, the host uses the dhcpv6 to acquire the information excluding the IPv6 address for the purpose of

automatic configuration. When the **managed address configuration** is set, the default **other stateful configuration** is also set

**Configuration** The following example sets “other stateful configuration” flag bit of the RA message.

**Examples**

```
Ruijie(config)# interface VLAN 1
Ruijie(config-if-VLAN 1)# ipv6 nd other-config-flag
```

Related Commands	Command	Description
	<b>show ipv6 interface</b>	Displays the interface information.

**Platform** N/A

**Description**

### 3.15 ipv6 nd prefix

Use this command to configure the address prefix included in the RA. Use the **no** form of this command to delete the set prefix or restore the default setting.

```
ipv6 nd prefix { ipv6-prefix/prefix-length | default } [ [ valid-lifetime preferred-lifetime ] ] [ at valid-date preferred-date ] [ infinite | preferred-lifetime ] [ no-advertise ] [ [ off-link ] [ no-autoconfig ] ] [ pool pool-name ] ]
```

```
no ipv6 nd prefix { ipv6-prefix/prefix-length | default }
```

Parameter	Parameter	Description
<b>Description</b>	<i>ipv6-prefix</i>	IPv6 network ID following the format defined in RFC4291
	<i>prefix-length</i>	Length of the IPv6 prefix. “/” shall be added in front of the prefix
	<i>valid-lifetime</i>	Valid lifetime of the RA prefix received by the host
	<i>preferred-lifetime</i>	Preferred lifetime of the RA prefix received by the host
	<i>at valid-date preferred-date</i>	Sets the dead line for the valid lifetime and that of the preferred lifetime, in day, month, year, hour, minute.
	<b>infinite</b>	Indicates that the prefix is always valid.
	<b>default</b>	Sets the default prefix.
	<b>no-advertise</b>	The prefix will not be advertised by the device.
	<b>off-link</b>	When the host sends an IPv6 packet, if the prefix of the destination address matches the set prefix, it is considered that the destination is on-link and is directly reachable. If this option is set, it indicates that the prefix is not used for on-link judgment.
	<b>no-autoconfig</b>	Indicates that the RA prefix received by the host cannot be used for auto address configuration.
<b>pool</b> <i>pool-name</i>	Indicates the IPv6 prefix pool	

**Defaults** By default, the advertised prefix is the one set with **ipv6 address** on the interface. The default parameters of the prefix configured in the RA are as follows:

*valid-lifetime*: 2592000s (30 days)

preferred-lifetime: 604800s (7 days),

The prefix is advertised and is used for on-link judgment and auto address configuration.

**Command** Interface configuration mode.

**Mode**

**Usage Guide** This command can be used to configure the parameters of each prefix, including whether to advertise the prefix. By default, the prefix advertised in RA is the one set with **ipv6 address** on the interface. To add other prefixes, use this command.

**ipv6 nd prefix default**

Set the default parameters to be used by the interface. If no parameter is specified for an added prefix, the parameters set with **ipv6 nd prefix default** will be used. Note that after a parameter is specified for the prefix, the default configuration will not be used. That is to say, the configuration of the prefix cannot be modified with **ipv6 nd prefix default**; only the prefix that uses all the default configurations can be modified with this command.

*at valid-date preferred-date*

The valid lifetime of a prefix can be specified in two ways. One way is to specify a fixed time for each prefix in the RA; the other way is to specify the end time (in this mode, the valid lifetime of the prefix sent in RA will be gradually reduced until the end time is 0).

**Configuration** The following example adds a prefix for SVI 1.

**Examples**

```
Ruijie(config)# interface VLAN 1
Ruijie(config-if-VLAN 1)# ipv6 nd prefix 2001::/64 infinite 2592000
```

The following example sets the default prefix parameters for SVI 1 (they cannot be used for auto address configuration):

```
Ruijie(config)# interface VLAN 1
Ruijie(config-if-VLAN 1)# ipv6 nd prefix default no-autoconfig
```

If no parameter is specified, the default parameters will be used, and the prefix cannot be used for auto address configuration.

Related	Command	Description
Commands	<b>show ipv6 interface</b>	Displays the RA information of an interface.

**Platform** N/A

**Description**

### 3.16 ipv6 nd ra-hoplimit

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

**ipv6 nd ra-hoplimit** *value*

**no ipv6 nd ra-hoplimit**

Parameter	Parameter	Description
Description	<i>value</i>	Hopcount

**Defaults** The default is 64.

**Command** Interface configuration mode.

**Mode**

**Usage Guide** This command is used to set the hopcount of the RA message.

**Configuration** The following example sets the hopcount of the RA message.

**Examples**

```
Ruijie(config)# interface VLAN 1
Ruijie(config-if-VLAN 1)# ipv6 nd ra-hoplimit 110
```

Related	Command	Description
Commands	<b>show ipv6 interface</b>	Displays the interface information.
	<b>ipv6 nd ra-lifetime</b>	Sets the lifetime of the device.
	<b>ipv6 nd ra-interval</b>	Sets the interval of sending the RA message.
	<b>ipv6 nd ra-mtu</b>	Sets the MTU of the RA message.

**Platform** N/A

**Description**

### 3.17 ipv6 nd ra-interval

Use this command to set the interval of sending the RA. Use the **no** form of this command to restore the default setting.

```
ipv6 nd ra-interval { seconds | min-max min_value max_value }
no ipv6 nd ra-interval
```

Parameter	Parameter	Description
Description	<i>seconds</i>	Interval of sending the RA message in seconds, 3-1800s.
	<b>min-max</b>	Maximum and minimum interval sending the RA message in seconds
	<i>min_value</i>	Minimum interval sending the RA message in seconds
	<i>max_value</i>	Maximum interval sending the RA message in seconds

**Defaults** 200s. The actual interval of sending the RA message will be fluctuated 20% based on 200s.

**Command** Interface configuration mode.

**Mode**

**Usage Guide** If the device serves as the default device, the set interval shall not be longer than the lifetime of the



device. Besides, to ensure other devices along the link occupies network bandwidth while sending the RA message, the actual interval for sending the RA message will be fluctuated 20% based on the set value.

If the key word **min-max** is specified, the actual interval for sending the packet will be chosen between the range of minimum value and maximum value.

**Configuration** The following example sets the interval of sending the RA.

**Examples**

```
Ruijie(config)# interface VLAN 1
Ruijie(config-if-VLAN 1)# ipv6 nd ra-interval 110
Ruijie(config-if-VLAN 1)# ipv6 nd ra-interval min-max 110 120
```

**Related  
Commands**

Command	Description
<b>show ipv6 interface</b>	Displays the interface information.
<b>ipv6 nd ra-lifetime</b>	Sets the lifetime of the device.
<b>ipv6 nd ra-hoplimit</b>	Sets the hopcount of the RA message.
<b>ipv6 nd ra-mtu</b>	Sets the MTU of the RA message.

**Platform** N/A

**Description**

### 3.18 ipv6 nd ra-lifetime

Use this command to set the device lifetime of the RA sent on the interface. Use the **no** form of this command to restore the default setting.

**ipv6 nd ra-lifetime** *seconds*

**no ipv6 nd ra-lifetime**

**Parameter  
Description**

Parameter	Description
<i>seconds</i>	Default life time of the device on the interface, in the range from 0 to 9000 in the unit of seconds.

**Defaults** The default is 1800.

**Command  
Mode** Interface configuration mode.

**Usage Guide** The router lifetime field is available in each RA. It specifies the time during which the hosts along the link of the interface can select the device as the default device. If the value is set to 0, the device will not serve as the default device any longer. If it is not set to 0, it shall be larger than or equal to the interval of sending the RA (ra-interval)

**Configuration** The following example sets the device lifetime of the RA sent on the interface.

**Examples**

```
Ruijie(config)# interface VLAN 1
```

```
Ruijie(config-if-VLAN 1)# ipv6 nd ra-lifetime 2000
```

Related	Command	Description
Commands	<b>show ipv6 interface</b>	Displays the interface information.
	<b>ipv6 nd ra-interval</b>	Sets the interval of sending the RA.
	<b>ipv6 nd ra-hoplimit</b>	Sets the hopcount of the RA.
	<b>ipv6 nd ra-mtu</b>	Sets the MTU of the RA.

**Platform** N/A

**Description**

### 3.19 ipv6 nd ra-mtu

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

**ipv6 nd ra-mtu** *value*

**no ipv6 nd ra-mtu**

Parameter	Parameter	Description
Description	<i>value</i>	MTU value, in the range from 0 to 4294967295.

**Defaults** IPv6 MTU value of the network interface.

**Command** Interface configuration mode.

**Mode**

**Usage Guide** If it is specified as 0, the RA will not have the MTU option

**Configuration** The following example sets the MTU of the RA message.

**Examples**

```
Ruijie(config)# interface VLAN 1
Ruijie(config-if-VLAN 1)# ipv6 nd ra-mtu 1400
```

Related	Command	Description
Commands	<b>show ipv6 interface</b>	Displays the interface information.
	<b>ipv6 nd ra-lifetime</b>	Sets the lifetime of the device.
	<b>ipv6 nd ra-interval</b>	Sets the interval of sending the RA message.
	<b>ipv6 nd ra-hoplimit</b>	Sets the hopcount of the RA message.

**Platform** N/A

**Description**

### 3.20 ipv6 nd reachable-time

Use this command to set the reachable time after the interface checks the reachability of the neighbor dynamically learned through NDP. Use the **no** form of this command to restore the default setting.

**ipv6 nd reachable-time** *milliseconds*

**no ipv6 nd reachable-time**

Parameter	Parameter	Description
Description	<i>milliseconds</i>	Reachable time for the neighbor in the range from 0 to 3600000 in the unit of milliseconds.

**Defaults** The default value in RA is 0 (unspecified); the reachable time for the neighbor is 30000 milliseconds (30 seconds) when the device discovers the neighbor.

**Command** Interface configuration mode.

**Mode**

**Usage Guide** The device checks the unreachable neighbor through the set time. A shorter time means that the device can check the neighbor failure more quickly, but more network bandwidth and device resource will be occupied. Therefore, it is not recommended to set a too short reachable time. The configured value will be advertised through RA and will be used by the device itself. If the value is set to 0, it indicates that the time is not specified, that is, the default value is used. According to RFC4861, the actual time to reach neighbor is not consistent with the configured value, ranging from 0.5\*configured value to 1.5\*configured value.

**Configuration** The following example sets the reachable time.

**Examples**

```
Ruijie(config)# interface VLAN 1
Ruijie(config-if-VLAN 1)# ipv6 nd reachable-time 1000000
```

Related	Command	Description
Commands	<b>show ipv6 interface</b>	Displays the interface information.

**Platform** N/A

**Description**

### 3.21 ipv6 nd stale-time

Use this command to set the period for the neighbor to maintain the state. Use the **no** form of this command to restore the default setting.

**ipv6 nd stale-time** *seconds*

**no ipv6 nd stale-time**

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

<b>Description</b>	<i>Seconds</i>	Sets the period for the neighbor to maintain the state, in the range from 0 to 86400 in the unit of seconds.				
<b>Defaults</b>	The default is 3600.					
<b>Command Mode</b>	Global configuration mode					
<b>Usage Guide</b>	This command is used to set the period for the neighbor to maintain the state. After the period expires, neighbor unreachability detection is performed. The shorter the period, the faster the neighbor is found unreachable. On the other hand, more network bandwidth and device resources are consumed. Therefore, it is recommended to set a value not too small.					
<b>Configuration Examples</b>	The following example sets the period to 600 seconds for the neighbor to maintain the state.					
<b>Examples</b>	<pre>Ruijie(config)# ipv6 nd stale-time 600</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					

### 3.22 ipv6 nd suppress-ra

Use this command to disable the interface from sending the RA message. Use the **no** form of this command to enable the function.

**ipv6 nd suppress-ra**  
**no ipv6 nd suppress-ra**

<b>Parameter Description</b>	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table>	Parameter	Description	N/A	N/A
Parameter	Description				
N/A	N/A				
<b>Defaults</b>	The <b>ipv6 nd suppress-ra</b> command is enabled by default.				
<b>Command Mode</b>	Interface configuration mode.				
<b>Usage Guide</b>	This command suppresses the sending of the RA message on an interface.				
<b>Configuration Examples</b>	The following example disables the interface from sending the RA message.				
<b>Examples</b>	<pre>Ruijie(config)# interface VLAN 1 Ruijie(config-if-VLAN 1)# ipv6 nd suppress-ra</pre>				
<b>Related</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> </tbody> </table>	Command	Description		
Command	Description				

<b>Commands</b>	<b>show ipv6 interface</b>	Displays the interface information.
-----------------	----------------------------	-------------------------------------

**Platform** N/A

**Description**

### 3.23 ipv6 nd unresolved

Use this command to set the maximum number of the unresolved neighbor table entries. Use the **no** form of this command to restore the default setting.

**ipv6 nd unresolved** *number*

**no ipv6 nd unresolved**

Parameter	Parameter	Description
<b>Description</b>	<i>number</i>	Sets the maximum number of the unresolved neighbor table entries, in the range from 1 to the neighbor table size supported by the device.

**Defaults** The default is 0. The maximum number is the neighbor table size supported by the device.

**Command** Global configuration mode

**Mode**

**Usage Guide** This command is used to prevent unresolved ND table entries generated by malicious scan attacks from consuming table entry resources,

**Configuration** The following example sets the maximum number of the unresolved neighbor table entries to 200.

**Examples** Ruijie(config)# ipv6 nd unresolved 200

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

**Platform** N/A

**Description**

### 3.24 ipv6 neighbor

Use this command to configure a static neighbor. Use the **no** form of this command to delete a static neighbor.

**ipv6 neighbor** *ipv6-address interface-id hardware-address*

**no ipv6 neighbor** *ipv6-address interface-id*

Parameter	Parameter	Description
<b>Description</b>	<i>ipv6-address</i>	The neighbor IPv6 address, in the form as defined in

	RFC 4291.
<i>interface-id</i>	Specifies the network interface where the neighbor is (including Router Port, L3 AP port and SVI interface).
<i>hardware-address</i>	The 48-bit MAC address, a dotted triple of four-digit hexadecimal numbers.

**Defaults** No static neighbor is configured by default.

**Command** Global configuration mode

**Mode**

**Usage Guide** This command can only be configured on the interface enabled with IPv6 protocol, similar to the ARP command.

If the neighbor to be configured has been learned through Neighbor Discovery Protocol (NDP) and stored in the NDP neighbor table, the dynamic neighbor turns to be static. If the static neighbor is valid, it is always reachable. An invalid static neighbor refers to the neighbor whose IPv6 address is not valid (not in the IPv6 network segment configured for the interface or interface address conflict). The packet is not forwarded to the MAC address as specified by the invalid static neighbor. The invalid static neighbor is in inactive state. Use the `show ipv6 neighbor static` command to display the state of the static neighbor.

Use the **clear ipv6 neighbors** command to clear all neighbors learned dynamically through NDP.

**Configuration** The following example configures a static neighbor on SVI 1.

**Examples**

```
Ruijie(config)# ipv6 neighbor 2001::1 vlan 1 00d0.f811.1111
```

Related	Command	Description
Commands	N/A	N/A

**Platform** N/A

**Description**

### 3.25 ipv6 ns-linklocal-src

Use this command to set the local address of the link as the source IP address to send neighbor requests. Use the **no** form of this command to use the global IP address `w` as the source address to send neighbor requests.

**ipv6 ns-linklocal-src**

**no ipv6 ns-linklocal-src**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** The local address of the link is always used as the source address to send neighbor requests.

**Command** Global configuration mode.

**Mode**

**Usage Guide** N/A

**Configuration Examples** The following example sets the local address of the link as the source IP address to send neighbor requests.

```
Ruijie(config)# no ipv6 ns-linklocal-src
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 3.26 ipv6 redirects

Use this command to control whether to send ICMPv6 redirect message when the switch receives and forwards an IPv6 packet through an interface. Use the **no** form of this command to restore the default setting.

**ipv6 redirects**

**no ipv6 redirects**

Parameter Description	Parameter	Description
	N/A	N/A

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

**Command** Interface configuration mode.

**Mode**

**Usage Guide** The transmission rate of any ICMPv6 error message is limited. By default, it is 10pps.

**Configuration Examples** The following example enables ICMPv6 redirection on interface VLAN 1.

```
Ruijie(config)# interface VLAN 1
Ruijie(config-if-VLAN 1)# ipv6 redirects
```

Related Commands	Command	Description
	<b>show ipv6 interface</b>	Displays the interface information.

**Platform** N/A

**Description**

## 3.27 ipv6 source-route

Use this command to forward the IPv6 packet with route header. Use the **no** form of this command to restore the default setting.

**ipv6 source-route**

**no ipv6 source-route**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** The **ipv6 source-route** command is disabled by default.

**Command Mode** Global configuration mode.

**Usage Guide** Because of the potential security of the header of type 0 route, it's easy for the device to suffer from the denial service attack. Therefore, forwarding the IPv6 packet with route header is disabled by default. However, the IPv6 packet of route header with type 0 that destined to the local machine is processed.

**Configuration Examples** The following example forwards the IPv6 packet with route header.

```
Ruijie(config)# no ipv6 source-route
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 3.28 show ipv6 address

Use this command to display the IPv6 addresses.

**show ipv6 address** [ *interface-name* ]

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

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A



**Configuration** The following example displays all IPv6 address configured on the device.

**Examples**

```
Ruijie# show ipv6 address
Global unicast address limit: 1024, Global unicast address count: 2
Tentative address count: 3,Duplicate address count: 0
Preferred address count: 0,Deprecated address count: 0
VLAN 1
  2003:1::23/64                               Tentative
Preferred lifetime: INFINITE, Valid lifetime: INFINITE
  fe80::2d0:f8ff:fe8b:deb2/64                 Tentative
Preferred lifetime: INFINITE, Valid lifetime: INFINITE
  2005:1::1111/64                             Tentative
Preferred lifetime: INFINITE, Valid lifetime: INFINITE
```

The following example displays the IPv6 address configured on the VLAN 1.

```
Ruijie# show ipv6 address VLAN 1
Global unicast address count: 2
Tentative address count: 3,Duplicate address count: 0
Preferred address count: 0,Deprecated address count: 0
  2003:1::23/64                               Tentative
Preferred lifetime: INFINITE, Valid lifetime: INFINITE
  fe80::2d0:f8ff:fe8b:deb2/64                 Tentative
Preferred lifetime: INFINITE, Valid lifetime: INFINITE
  2005:1::1111/64                             Tentative
Preferred lifetime: INFINITE, Valid lifetime: INFINITE
```

Related Commands	Command	Description
	N/A	N/A

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

### 3.29 show ipv6 general-prefix

Use this command to display the information of the general prefix.

**show ipv6 general-prefix**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command** Privileged EXEC mode.

**Mode**

**Usage Guide** Use this command to display the information of the general prefix including the manually configured and learned from the DHCPv6 agent.

**Configuration** The following example displays the information of the general prefix.

**Examples**

```
Ruijie# show ipv6 general-prefix
There is 1 general prefix.
IPv6 general prefix my-prefix, acquired via Manual configuration
 2001:1111:2222::/48
 2001:1111:3333::/48
```

Related Commands	Command	Description
	<b>ipv6 general-prefix</b>	Configures the general prefix.

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

### 3.30 show ipv6 interface

Use this command to display the IPv6 interface information.

**show ipv6 interface** [ *interface-id* ] [ **ra-info** ] [ *brief* [ *interface-id* ] ]

Parameter	Parameter	Description
<b>Description</b>	<i>interface-id</i>	Interface (including Ethernet interface, aggregate port, or SVI)
	<b>ra-info</b>	Displays the RA information of the interface.
	<i>brief</i>	Displays the brief information of the interface (interface status and address information).

**Defaults** N/A

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

**Usage Guide** Use this command to display the address configuration, ND configuration and other information of an IPv6 interface.

**Configuration** The following example displays the information of the IPv6 interface.

**Examples**

```
Ruijie# show ipv6 interface vlan 1
Interface vlan 1 is Up, ifindex: 2001
address(es):
Mac Address: 00:00:00:00:00:01
INET6: fe80::200:ff:fe00:1 , subnet is fe80::/64
Joined group address(es):
```

```

ff01:1::1
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
INET6: 2001::1 , subnet is 2001::/64 [TENTATIVE]
Joined group address(es):
ff01:1::1
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
MTU is 1500 bytes
ICMP error messages limited to one every 10 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds<240--160>
ND device advertisements live for 1800 seconds

```

The following line is included in the above information: 2001::1, subnet is 2001::/64 [TENTATIVE].

The flag bit in the [ ] following the INET6 address is explained as follows:

Flag	Description
ANYCAST	Indicate that the address is an anycast address.
TENTATIVE	Indicate that the DAD is underway. The address is a tentative before the DAD is completed.
DUPLICATED	Indicate that a duplicate address exists.
DEPRECATED	Indicate that the preferred lifetime of the address expires.
NODAD	Indicate that no DAD is implemented for the address.
AUTOIFID	Indicate that the interface ID of the address is automatically generated by the system, which is usually an EUI-64 ID.

The following example displays the RA information of the IPv6 interface.

```

Ruijie# show ipv6 interface vlan 1 ra-info
vlan 1: DOWN
RA timer is stopped
waits: 0, initcount: 3
statistics: RA(out/in/inconsistent): 4/0/0, RS(input): 0
Link-layer address: 00:00:00:00:00:01
Physical MTU: 1500
ND device advertisements live for 1800 seconds
ND device advertisements are sent every 200 seconds<240--160>

```

```

Flags: !M!O, Adv MTU: 1500
ND advertised reachable time is 0 milliseconds
ND advertised retransmit time is 0 milliseconds
ND advertised CurHopLimit is 64
Prefixes: (total: 1)
fec0:1:1:1::/64 (Def,Auto,vltime: 2592000, pltime: 604800, flags: LA)

```

Description of the fields in **ra-info** is as follows:

Field	Description
RA timer is stopped (on)	Indicates whether the RA timer is started.
waits	Indicates that the RS is received but the number of the responses is not available.
initcount	Indicates the number of the RAs when the RA timer is restarted.
RA(out/in/ inconsistent)	out: Indicates the number of the RAs that are sent. In: Indicate the number of the RAs that are received. inconsistent: Indicates the number of the received RAs in which the parameters are different from those contained in the RAs advertised by the device.
RS(input)	Indicates the number of the RSs that are received.
Link-layer address	Link-layer address of the interface.
Physical MTU	Link MTU of the interface.
!M   M	!M indicates the managed-config-flag bit in the RA is not set. M: Conversely
!O   O	!O indicates the other-config-flag bit in the RA is not set. O: Conversely

Description of the fields of the prefix list in **ra-info** is as follows:

Field	Description
total	The number of the prefixes of the interface.
fec0:1:1:1::/64	A specific prefix.
Def	Indicates that the interfaces use the default prefix.
Auto   CFG	Auto: Indicates the prefix is automatically generated after the interface is configured with the corresponding IPv6 address. CFG: Indicates that the prefix is manually configured.
!Adv	Indicates that the prefix will not be advertised.
vltime	Valid lifetime of the prefix, measured in seconds.
pltime	Preferred lifetime of the prefix, measured in seconds.

L   !L	L: Indicates that the on-link in the prefix is set. !L: Indicates that the on-link in the prefix is not set.
A   !A	A: Indicates that the auto-configure in the prefix is set. !A: It indicates that the auto-configure in the prefix is not set.

The following example displays the brief information of the IPv6 interface.

```
Ruijie# show ipv6 interface brief

VLAN 1          [down/down]
    2222::2
    FE80::1614:4BFF:FE5C:ED3A
```

Related Commands	Command	Description
	N/A	N/A

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

### 3.31 show ipv6 neighbors

Use this command to display the IPv6 neighbors.

**show ipv6 neighbors [ verbose ] [ interface-id ] [ ipv6-address ]**  
**show ipv6 neighbors static**

Parameter Description	Parameter	Description
	<b>verbose</b>	Displays the neighbor details.
	<b>static</b>	Displays the validity status of static neighbors.
	<i>interface-id</i>	Displays the neighbors of the specified interface.
	<i>ipv6-address</i>	Displays the neighbors of the specified IPv6 address.

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays the neighbors on the SVI 1 interface:

```
Ruijie# show ipv6 neighbors vlan 1
IPv6 Address Linklayer Addr Interface
fa::1 00d0.0000.0002 vlan 1
fe80::200:ff:fe00:2 00d0.0000.0002 vlan 1
Show the neighbor details:
```

```
Ruijie# show ipv6 neighbors verbose
IPv6 Address Linklayer Addr Interface
2001::1 00d0.f800.0001 vlan 1
  State: Reach/H Age: - asked: 0
fe80::200:ff:fe00:1 00d0.f800.0001 vlan 1
  State: Reach/H Age: - asked: 0
```

Description of fields in the command output is as follows:

Field	Description
IPv6 Address	IPv6 address of the Neighbor
Linklayer Addr	Link address, namely, MAC address. If it is not available, incomplete is displayed.
Interface	Interface the neighbor locates.
State	<p>State of the neighbor: state/H(R)</p> <p>The values of STATE are as below:</p> <p>INCOMP (Incomplete): The address resolution of the neighbor is underway, the NS is sent, but the NA is not received.</p> <p>REACH (Reachable): The switch is connected with the neighbor. In this state, the switch takes no additional action when sending packets to the neighbor.</p> <p>STALE: The reachable time of the neighbor expires. In this state, the switch takes no additional action; it only starts NUD (Neighbor Unreachability Detection) after a packet is sent to the neighbor.</p> <p>DELAY: A packet is sent to the neighbor in STALE state. If the STALE state changes to DELAY, DELAY will be changed to PROBE if no neighbor reachability notification is received within DELAY_FIRST_PROBE_TIME seconds (5s), the NS will be sent to the neighbor to start NUD.</p> <p>PROBE: The NUD is started to check the reachability of the neighbor. The NS packets are sent to the neighbor at the interval of RetransTimer milliseconds until the response from the neighbor is received or the number of the sent NSs hits MAX_UNICAST_SOLICIT(3).</p> <p>?: Unknown state.</p> <p>/R—indicate the neighbor is considered as a device</p> <p>/H: The neighbor is a host.</p>
Age	The reachable time of the neighbor. '-' indicates that the neighbor is always reachable. Note that the reachability of a static neighbor depends on the actual situation. 'expired' indicates that the lifetime of the neighbor expires, and the neighbor is waits for the triggering of NUD.
Asked	The number of the NSs that are sent to the neighbor for the resolution of the link address of the neighbor.

Related

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

<b>Commands</b>	<b>ipv6 neighbor</b>	Configures a neighbor.
-----------------	----------------------	------------------------

**Platform** N/A

**Description**

### 3.32 show ipv6 neighbors statistics

Use the following command to show the statistics of IPv6 neighbors.

**show ipv6 neighbors statistics [ all ]**

Parameter	Parameter	Description
<b>Description</b>	<b>all</b>	Displays the statistics of all IPv6 neighbors.

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A

**Configuration** The following example displays the statistics of the global neighbors.

**Examples**

```
Ruijie# show ipv6 neighbor statistics

Memory: 0 bytes
Entries: 0
  Static: 0,Dynamic: 0,Local: 0
  Incomplete:0, Reachable:0, Stale:0, Delay:0, Probe:0
```

The following example displays the statistics of all IPv6 neighbors.

```
Ruijie# show ipv6 neighbor statistics all

IPv6 neighbor table count: 1
Static neighbor count: 0(0 active, 0 inactive)
Total
Memory: 0 bytes
Entries: 0
  Static: 0,Dynamic: 0,Local: 0
  Incomplete:0, Reachable:0, Stale:0, Delay:0, Probe:0;

Global
Memory: 0 bytes
Entries: 0
  Static: 0,Dynamic: 0,Local: 0
  Incomplete:0, Reachable:0, Stale:0, Delay:0, Probe:0;
```

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

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

### 3.33 show ipv6 packet statistics

Use this command to display the statistics of IPv6 packets.

**show ipv6 packet statistics [ total | interface-name ]**

<b>Parameter Description</b>	<b>Parameter</b>	<b>Description</b>
	<b>total</b>	Displays total statistics of all interfaces.
	<i>interface-name</i>	Interface name

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays the total statistics of the IPv6 packets and the statistics of each interface.

```
Ruijie# show ipv6 pack statistics
Total
  Received 0 packets, 0 bytes
    Unicast:0,Multicast:0
  Discards:0
    HdrErrors:0 (HoplimitExceeded:0,Others:0)
    NoRoutes:0
    Others:0
  Sent 0 packets, 0 bytes
    Unicast:0,Multicast:0
GigabitEthernet 0/17
  Received 0 packets, 0 bytes
    Unicast:0,Multicast:0
  Discards:0
    HdrErrors:0 (HoplimitExceeded:0,Others:0)
    NoRoutes:0
    Others:0
  Sent 0 packets, 0 bytes
    Unicast:0,Multicast:0
```



The following example displays the total statistics of the IPv6 packets.

```
Ruijie# show ipv6 pack statistics total
Total
  Received 0 packets, 0 bytes
    Unicast:0,Multicast:0
  Discards:0
    HdrErrors:0 (HoplimitExceeded:0,Others:0)
    NoRoutes:0
    Others:0
  Sent 0 packets, 0 bytes
    Unicast:0,Multicast:0
```

Related Commands	Command	Description
	N/A	N/A

**Platform** Supported on all platforms.  
**Description**

### 3.34 show ipv6 raw-socket

Use this command to display all IPv6 raw sockets.

```
show ipv6 raw-socket [ num ]
```

Parameter Description	Parameter	Description
	<i>num</i>	Protocol.

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays all IPv6 raw sockets.

```
Ruijie# show ipv6 raw-socket
Number Protocol Process name
1 ICMPv6 vrrp.elf
2 ICMPv6 tcpip.elf
3 VRRP vrrp.elf
Total: 3
```

Field	Description
-------	-------------

Number	Number.
Protocol	Protocol.
Process name	Process number.
Total	Total number of IPv6 raw sockets.

Related	Command	Description
Commands	N/A	N/A

Platform N/A

Description

### 3.35 show ipv6 routers

In the IPv6 network, some neighbor routers send out the advertisement messages. Use this command to display the neighbor routers and the advertisement.

**show ipv6 routers** [ *interface-type interface-number* ]

Parameter	Parameter	Description
Description	<i>interface-type</i>	(Optional) Displays the routing advertisement of the specified interface.
	<i>interface-number</i>	

Defaults N/A

Command Privileged EXEC mode.  
Mode

**Usage Guide** Use this command to display the neighbor routers and the routing advertisement. If no interface is specified, all the routing advertisement of this device will be displayed.

**Configuration** The following example displays the IPv6 router

#### Examples

```
Ruijie# show ipv6 routers
Router FE80::2D0:F8FF:FEC1:C6E1 on VLAN 2, last update 62 sec
Hops 64, Lifetime 1800 sec, ManagedFlag=0, OtherFlag=0, MTU=1500
Preference=MEDIUM
Reachable time 0 msec, Retransmit time 0 msec
Prefix 6001:3::/64 onlink autoconfig
Valid lifetime 2592000 sec, preferred lifetime 604800 sec
Prefix 6001:2::/64 onlink autoconfig
Valid lifetime 2592000 seconds, preferred lifetime 604800 seconds
```

Related	Command	Description
Commands	N/A	N/A

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

### 3.36 show ipv6 sockets

Use this command to display all IPv6 sockets.

**show ipv6 sockets**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A

**Configuration** The following example displays all IPv6 sockets.

**Examples**

```
Ruijie# show ipv6 sockets
Number Process name      Type  Protocol  LocalIP:Port  ForeignIP:Port  State
1    vrrp.elf             RAW   ICMPv6    :::58         :::0            *
2    tcpip.elf            RAW   ICMPv6    :::58         :::0            *
3    vrrp.elf             RAW   VRRP      :::112        :::0            *
4    rg-snmpd             DGRAM UDP        :::161        :::0            *
5    rg-snmpd             DGRAM UDP        :::162        :::0            *
6    dhcp6.elf           DGRAM UDP        :::547        :::0            *
7    rg-sshd              STREAM TCP        ::22         :::0            LISTEN
8    rg-telnetd           STREAM TCP        :::23         :::0            LISTEN
Total: 8
```

Field	Description
Number	Number.
Process name	Process name.
Type	Socket type. RAW indicates the raw socket. DGRAM indicates data packet type. STREAM indicates traffic type.
Protocol	Protocol number
LocalIP:Port	Local IPv6 address and port.
ForeignIP:Port	Peer IPv6 address and port.
State	State (for IPv6 TCP sockets).

Total	Total number of sockets.
-------	--------------------------

Related Commands	Command	Description
	N/A	N/A

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

### 3.37 show ipv6 udp

Use this command to display all IPv6 UDP sockets.

**show ipv6 udp [ local-port num ] [ peer-port num ]**

Use this command to display IPv6 UDP socket statistics.

**show ipv6 udp statistics**

Parameter Description	Parameter	Description
	local-port num	Local port number.
	peer-port num	Peer port number.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays all IPv6 UDP sockets.

```

Examples
Ruijie# show ipv6 udp
Number Local Address Peer Address Process name
1 :::161 :::0 rg-snmpd
2 :::162 :::0 rg-snmpd
3 :::547 :::0 dhcp6.elf
    
```

Filed	Description
Number	Number.
Local Address	Local IPv6 address and port.
Peer Address	Peer IPv6 address and port.
Process name	Process name.

Related Commands	Command	Description
	N/A	N/A

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

## 4 DHCP Commands

### 4.1 address range

Use this command to specify the network segment range of the addresses that can be allocated by CLASS associated with DHCP address pool. Use the **no** form of this command to restore the default setting.

**address range** *low-ip-address high-ip-address*

**no address range**

Parameter	Parameter	Description
Description	<i>low-ip-address</i>	Start address in the network segment range.
	<i>high-ip-address</i>	End address in the network segment range.

**Defaults** By default, the associated CLASS is not configured with the network segment range. The default is the address pool range.

**Command Mode** Address pool CLASS configuration mode.

**Usage Guide** Each CLASS corresponds to one network range which must be from low address to high address, so as to allow the duplication of network segment range between multiple CLASSes. If the CLASS associated with the address pool is specified without configuring the corresponding network segment range, the default network segment range of this CLASS is same as the range of the address pool where this CLASS is.

**Configuration Examples** The following example configures the network segment of class1 associated with address pool mypool0 ranging from 172.16.1.1 to 172.16.1.8.

```
Ruijie(config)# ip dhcp pool mypool0
Ruijie(dhcp-config)# class class1
Ruijie(config-dhcp-pool-class)# address range 172.16.1.1 172.16.1.8
```

Related Commands	Command	Description
	<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.
	<b>class</b>	Configures the CLASS associated with the DHCP address pool and enters the address pool CLASS configuration mode.

**Platform Description** N/A

## 4.2 bootfile

Use this command to define the startup mapping file name of the DHCP client. Use the **no** or **default** form of this command to restore the default setting.

**bootfile** *file-name*

**no bootfile**

**default bootfile**

Parameter	Parameter	Description
Description	<i>file-name</i>	Startup file name.

**Defaults** No startup file name is defined by default.

**Command Mode** DHCP address pool configuration mode

**Usage Guide** Some DHCP clients need to download the operating system and configure the file during the startup. The DHCP server should provide the mapping file name required for the startup, so that DHCP clients can download the file from the corresponding server (such as TFTP). Other servers are defined by the **next-server** command.

**Configuration Examples** The following example defines the device.conf as the startup file name.

```
Ruijie(config)# ip dhcp pool mypool0
Ruijie(dhcp-config)# bootfile device.conf
```

Related Commands	Command	Description
	<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enter the DHCP address pool configuration mode.
	<b>next-server</b>	Configures the next server IP address of the DHCP client startup process.

**Platform Description** N/A

## 4.3 class

Use this command to configure the associated CLASS in the DHCP address pool. Use the **no** form of this command to restore the default setting.

**class** *class-name*

**no class**

Parameter	Parameter	Description
Description	<i>class-name</i>	Class name, which can be the character string or numeric such as myclass or 1.

**Defaults** By default, no CLASS is associated with the address pool.

**Command Mode** DHCP address pool configuration mode

**Usage Guide** Each DHCP address pool performs the address assignment according to the Option82 matching information. We can divide this Option82 information into classes and specify the available network segment range for these classes in the DHCP address pool. These classes are called CLASS. One DHCP address pool can map to multiple CLASSES, and each CLASS can specify different network segment range.

During the address assignment, firstly, ensure the assignable address pool through the network segment where the client is, then according to the Option82 information further ensure the CLASS and assign the IP address from the network segment range corresponding to the CLASS. If one request packet matches multiple CLASSES in the address pool, perform the address assignment according to the sequencing of configuring the CLASS in the address pool. If this CLASS's assigned addresses have been to the upper limit, then continue to assign the address from the next CLASS, and so on. Each CLASS corresponds to one network segment range that must be from low addresses to high addresses and the duplicated network ranges between multiple CLASSES are allowed. If the CLASS corresponding to the address pool is specified and the network segment corresponding to the CLASS is not configured, this CLASS's default network segment range is same as the range of address pool where the CLASS is.

**Configuration Examples** The following example configures the address *mypool0* to associate with class1.

```
Ruijie(config)# ip dhcp pool mypool0
Ruijie(dhcp-config)# class class1
```

**Related Commands**

Command	Description
<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

**Platform Description** N/A

## 4.4 clear ip dhcp binding

Use this command to clear the DHCP binding table in the privileged user mode.

```
clear ip dhcp binding { * | ip-address }
```

**Parameter Description**

Parameter	Description
*	Deletes all DHCP bindings.
<i>ip-address</i>	Deletes the binding of the specified IP addresses.

**Defaults** N/A.



**Command Mode** Privileged EXEC mode.

**Usage Guide** This command can only clear the automatic DHCP binding, but the manual DHCP binding can be deleted by the **no ip dhcp pool** command.

**Configuration Examples** The following example clears the DHCP binding with the IP address 192.168.12.100.

```
Ruijie# clear ip dhcp binding 192.168.12.100
```

Related Commands	Command	Description
	<b>show ip dhcp binding</b>	Displays the address binding of the DHCP server.

**Platform Description** N/A

## 4.5 clear ip dhcp conflict

Use this command to clear the DHCP address conflict record.

**clear ip dhcp conflict** { \* | *ip-address* }

Parameter Description	Parameter	Description
	*	Deletes all DHCP address conflict records.
	<i>ip-address</i>	Deletes the conflict record of the specified IP addresses.

**Defaults** N/A.

**Command Mode** Privileged EXEC mode.

**Usage Guide** The DHCP server uses the ping session to detect the address conflict, while the DHCP client uses the address resolution protocol (ARP) to detect the address conflict. The **clear ip dhcp conflict** command can be used to delete the history conflict record.

**Configuration Examples** The following example clears all address conflict records.

```
Ruijie# clear ip dhcp conflict *
```

Related Commands	Command	Description
	<b>ip dhcp ping packets</b>	Defines the number of the data packets sent by the ping operation for the detection of the address conflict when the DHCP server assigns an IP address.
	<b>show ip dhcp conflict</b>	Displays the address conflict that the DHCP server detects when it assigns an IP address.

**Platform** N/A

**Description**

## 4.6 clear ip dhcp history

Use this command to clear the address assigned by the DHCP server.

**clear ip dhcp history** { \* | *mac-address* }

Parameter	Parameter	Description
<b>Description</b>	*	Clears all addresses assigned by the DHCP server.
	<i>mac-address</i>	Clears the address assigned by the DHCP server corresponding to the specified MAC address.

**Defaults** N/A

**Command** Privileged EXEC mode

**Mode**

**Usage Guide** This command is configured on the DHCP server.

**Configuration** The following example clears all addresses assigned by the DHCP server.

**Examples** Ruijie# clear ip dhcp history \*

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

**Platform** N/A

**Description**

## 4.7 clear ip dhcp relay statistics

Use this command to clear the DHCP relay statistics.

**clear ip dhcp relay statistics**

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

**Defaults** N/A

**Command** Privileged EXEC mode

**Mode**

**Usage Guide** The DHCP relay is configured with the counter to count various packets received or transmitted by

the relay. This command is used to clear the counters.

**Configuration** The following example clears the DHCP relay statistics.

**Examples** Ruijie# clear ip dhcp relay statistics

Related Commands	Command	Description
	N/A	N/A

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

### 4.8 clear ip dhcp server rate

Use this command to clear statistics about the packet processing rate of every module.

**clear ip dhcp server rate**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is used to clear statistics about the packet processing rate of every module, including arp, hot backup, lsm, and socket.

**Configuration** The following example clears statistics about the packet processing rate of every module.

**Examples** Ruijie# clear ip dhcp server rate

Related Commands	Command	Description
	N/A	N/A

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

### 4.9 clear ip dhcp server statistics

Use this command to reset the counter of the DHCP server in the privileged user mode.

**clear ip dhcp server statistics**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** The DHCP server carries out the statistics counter, records the DHCP address pool, automatic binding, manual binding and expired binding. Furthermore, it also carries out the statistics to the number of sent and received DHCP messages. The **clear ip dhcp server statistics** command can be used to delete the history counter record and carry out the statistics starting from scratch.

**Configuration** The following example clears the statistics record of the DHCP server.

**Examples** Ruijie# clear ip dhcp server statistics

Related Commands	Command	Description
	<b>show ip dhcp server statistics</b>	Displays the statistics record of the DHCP server.

**Platform** N/A

**Description**

## 4.10 client-identifier

Use this command to define the unique ID of the DHCP client (indicated in hex, separated by dot) in the DHCP address pool configuration mode. Use the **no** form of this command to restore the default setting.

**client-identifier** *unique-identifier*

**no client-identifier**

Parameter	Parameter	Description
<b>Description</b>	<i>unique-identifier</i>	The DHCP client ID is indicated in hex and separated by dot, for instance, 0100.d0f8.2233.b467.6967.6162.6974.4574.6865.726e.6574.302f.31.

**Defaults** N/A.

**Command Mode** DHCP address pool configuration mode.

**Usage Guide** When some DHCP clients request the DHCP server to assign IP addresses, they use their client IDs rather than their hardware addresses. The client ID consists of media type, MAC addresses and interface name. For instance, the MAC address is 00d0.f822.33b4, the interface name is GigabitEthernet 0/17, and the corresponding client ID is 0100.d0f8.2233.b467.6967.6162.6974.4574.6865.726e.6574.302f.31, where, 01 denotes the type of the Ethernet media. The 67.6967.6162.6974.4574.6865.726e.6574.302f.31 is the hex code of GigabitEthernet0/17. For the

definition of the media code, refer to the Address Resolution Protocol Parameters section in RFC1700. This command is used only when the DHCP is defined by manual binding.

**Configuration** The following example defines the client ID of the Ethernet DHCP client whose MAC address is 00d0.f822.33b4.

**Examples**

```
Ruijie(config)# ip dhcp pool mypool0
Ruijie(dhcp-config)# client-identifier
0100.d0f8.2233.b467.6967.6162.6974.4574.6865.726e.6574.302f.31
```

**Related  
Commands**

Command	Description
<b>hardware-address</b>	Defines the hardware address of DHCP client.
<b>host</b>	Defines the IP address and network mask, which is used to configure the DHCP manual binding.
<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

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

## 4.11 client-name

Use this command to define the name of the DHCP client in the DHCP address pool configuration mode. Use the **no** form of this command to restore the default setting.

**client-name** *client-name*

**no client-name**

**Parameter  
Description**

Parameter	Description
client-name	Name of DHCP client, a set of standards-based ASCII characters. The name should not include the suffix domain name. For instance, you can define the name of the DHCP client as river, not river.i-net.com.cn.

**Defaults** No client name is defined by default.

**Command Mode** DHCP address pool configuration mode.

**Usage Guide** This command can be used to define the name of the DHCP client only when the DHCP is defined by manual binding. This name should not include the suffix domain name.

**Configuration** The following example defines a string river as the name of the client.

**Examples**

```
Ruijie(config)# ip dhcp pool mypool0
Ruijie(dhcp-config)# client-name river
```

Related	Command	Description
Commands	<b>host</b>	Defines the IP address and network mask, which is used to configure the DHCP manual binding.
	<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

**Platform** N/A

**Description**

## 4.12 default-router

Use this command to define the default gateway of the DHCP client in the DHCP address pool configuration mode. Use the **no** form of this command to restore the default setting.

**default-router** *ip-address* [ *ip-address2...ip-address8* ]

**no default-router**

Parameter	Parameter	Description
Description	<i>ip-address</i>	Defines the IP address of the equipment. It is required to configure one IP address at least.
	<i>ip-address2...ip-address8</i>	(Optional) Up to 8 gateways can be configured.

**Defaults** No gateway is defined by default.

**Command Mode** DHCP address pool configuration mode.

**Usage Guide** In general, the DHCP client should get the information of the default gateway from the DHCP server. The DHCP server should specify one gateway address for the client at least, and this address should be of the same network segment as the address assigned to the client.

**Configuration Examples** The following example defines 192.168.12.1 as the default gateway.

```
Ruijie(config)# ip dhcp pool mypool0
Ruijie(dhcp-config)# default-router 192.168.12.1
```

Related	Command	Description
Commands	<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

**Platform** N/A

**Description**

## 4.13 dns-server

Use this command to define the DNS server of the DHCP client in the DHCP address pool configuration mode. Use the **no** form of this command to restore the default setting.

**dns-server** { *ip-address* [ *ip-address2*...*ip-address8* ] | **use-dhcp-client** *interface-type* *interface-number* }

**no dns-server**

Parameter	Parameter	Description
Description	<i>ip-address</i>	Defines the IP address of the DNS server. At least one IP address should be configured.
	<i>ip-address2</i> ... <i>ip-address8</i>	(Optional) Up to 8 DNS servers can be configured.
	<b>use-dhcp-client</b> <i>interface-type</i> <i>interface-number</i>	Uses the DNS server learned by the DHCP client of the RGOS software as the DNS server of the DHCP client.

**Defaults** No DNS server is defined by default.

**Command Mode** DHCP address pool configuration mode.

**Usage Guide** When more than one DNS server is defined, the former will possess higher priority, so the DHCP client will select the next DNS server only when its communication with the former DNS server fails. If the RGOS software also acts as the DHCP client, the DNS server information obtained by the client can be transmitted to the DHCP client.

**Configuration Examples** The following example specifies the DNS server 192.168.12.3 for the DHCP client.

```
Ruijie(config)# ip dhcp pool mypool0
Ruijie(dhcp-config)# dns-server 192.168.12.3
```

Related Commands	Command	Description
	<b>domain-name</b>	Defines the suffix domain name of the DHCP client.
	<b>ip address dhcp</b>	Enables the DHCP client on the interface to obtain the IP address information.
	<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

**Platform Description** N/A

## 4.14 domain-name

Use this command to define the suffix domain name of the DHCP client in the DHCP address pool configuration mode. Use the **no** form of this command to restore the default setting.

**domain-name** *domain-name*

**no domain-name**

Parameter	Parameter	Description
<b>Description</b>	<i>domain-name</i>	Defines the suffix domain name string of the DHCP client.
<b>Defaults</b>	No suffix domain name by default.	
<b>Command Mode</b>	DHCP address pool configuration mode.	
<b>Usage Guide</b>	After the DHCP client obtains specified suffix domain name, it can access a host with the same suffix domain name by the host name directly.	
<b>Configuration Examples</b>	The following example defines the suffix domain name i-net.com.cn for the DHCP client.	
<b>Examples</b>	<pre>Ruijie(config)# ip dhcp pool mypool0 Ruijie(dhcp-config)# domain-name ruijie.com.cn</pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>dns-server</b>	Defines the DNS server of the DHCP client.
	<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enter the DHCP address pool configuration mode.
<b>Platform</b>	N/A	
<b>Description</b>		

## 4.15 hardware-address

Use this command to define the hardware address of the DHCP client in the DHCP address pool configuration mode. Use the **no** form of this command to restore the default setting.

**hardware-address** *hardware-address* [ *type* ]

**no hardware-address**

Parameter	Parameter	Description
<b>Description</b>	<i>hardware-address</i>	Defines the MAC address of the DHCP client.
	<i>type</i>	<p>Indicates the hardware platform protocol of the DHCP client. It uses the string definition or digits definition.</p> <p>String option:</p> <p>Ethernet</p> <p>ieee802</p> <p>Digits option:</p> <p>1 (10M Ethernet)</p> <p>6 (IEEE 802)</p>



**Defaults** No hardware address is defined by default.  
If there is no option when the hardware address is defined, it is the Ethernet by default.

**Command** DHCP address pool configuration mode.

**Mode**

**Usage Guide** This command can be used only when the DHCP is defined by manual binding.

**Configuration** The following example defines the MAC address 00d0.f838.bf3d with the type ethernet.

**Examples**

```
Ruijie(config)# ip dhcp pool mypool0
Ruijie(dhcp-config)# hardware-address 00d0.f838.bf3d
```

**Related  
Commands**

Command	Description
<b>client-identifier</b>	Defines the unique ID of the DHCP client (Indicated by the hexadecimal numeral, separated by dot).
<b>host</b>	Defines the IP address and network mask, which is used to configure the DHCP manual binding.
<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enter the DHCP address pool configuration mode.
<b>default-router</b>	Defines the default route of the DHCP client.

**Platform** N/A

**Description**

## 4.16 host

Use this command to define the IP address and network mask of the DHCP client host in the DHCP address pool configuration mode. Use the **no** form of this command to restore the default setting.

**host** *ip-address* [ *netmask* ]

**no host**

**Parameter  
Description**

Parameter	Description
<i>ip-address</i>	Defines the IP address of DHCP client.
<i>netmask</i>	Defines the network mask of DHCP client.

**Defaults** No IP address or network mask of the host is defined.

**Command** DHCP address pool configuration mode.

**Mode**

**Usage Guide** If the network mask is not defined definitely, the DHCP server will use the natural network mask of this IP address: 255.0.0.0 for class A IP address, 255.255.0 for class B IP address, and 255.255.255.0 for class C IP address.

This command can be used only when the DHCP is defined by manual binding.

**Configuration Examples** The following example sets the client IP address as 192.168.12.91, and the network mask as 255.255.255.240.

```
Ruijie(config)# ip dhcp pool mypool0
Ruijie(dhcp-config)# host 192.168.12.91 255.255.255.240
```

Related Commands	Command	Description
	<b>client-identifier</b>	Defines the unique ID of the DHCP client (Indicated in hex and separated by dot).
	<b>hardware-address</b>	Defines the hardware address of DHCP client.
	<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.
<b>default-router</b>	Define the default route of the DHCP client.	<b>default-router</b>

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

### 4.17 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** form of this command to restore the default setting.

**ip address dhcp**  
**no ip address dhcp**

Parameter Description	Parameter	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 FastEthernet 0 port obtain the IP address automatically.

**Examples**

```
Ruijie(config)# interface VLAN 1
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**

## 4.18 ip dhcp class

Use this command to define a CLASS and enter the global CLASS configuration mode. Use the **no** form of this command to restore the default setting.

**ip dhcp class** *class-name*  
**no ip dhcp class** *class-name*

Parameter	Parameter	Description
<b>Description</b>	<i>class-name</i>	Class name, which can be character string or numeric such as myclass or 1.

**Defaults** By default, the class is not configured.

**Command Mode** Global configuration mode.

**Usage Guide** After executing this command, it enters the global CLASS configuration mode which is shown as "Ruijie (config-dhcp-class)#". In this configuration mode, user can configure the Option82 information that matches the CLASS and the CLASS identification information.

**Configuration** The following example configures a global CLASS.

**Examples**

```
Ruijie(config)# ip dhcp class myclass
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 4.19 ip dhcp excluded-address

Use this command to define some IP addresses and make the DHCP server not assign them to the

DHCP client in the global configuration mode. Use the **no** form of this command to restore the default setting.

**ip dhcp excluded-address** *low-ip-address* [*high-ip-address*]

**no ip dhcp excluded-address** *low-ip-address* [*high-ip-address*]

Parameter	Parameter	Description
Description	<i>low-ip-address</i>	Excludes the IP address, or excludes the start IP address within the range of the IP address.
	<i>high-ip-address</i>	Excludes the end IP address within the range of the IP address.

**Defaults** The DHCP server assigns the IP addresses of the whole address pool by default.

**Command Mode** Global configuration mode.

**Usage Guide** If the excluded IP address is not configured, the DHCP server attempts to assign all IP addresses in the DHCP address pool. This command can reserve some IP addresses for specific hosts to prevent these addresses are assigned to the DHCP client, and define the excluded IP address accurately to reduce the conflict detecting time when the DHCP server assigns the address.

**Configuration Examples** In the following example, the DHCP server will not attempt to assign the IP addresses within 192.168.12.100~150.

```
Ruijie(config)# ip dhcp excluded-address 192.168.12.100 192.168.12.150
```

Related Commands	Command	Description
	<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.
	<b>network (DHCP)</b>	Defines the network number and network mask of the DHCP address pool.

**Platform Description** N/A

## 4.20 ip dhcp force-send-nak

Use this command to configure the forcible NAK packet sending function. Use the **no** or **default** form of this command to restore the default setting.

**ip dhcp force-send-nak**

**no ip dhcp force-send-nak**

**default ip dhcp force-send-nak**

Parameter	Parameter	Description
Description	N/A	N/A

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

**Command Mode** Global configuration mode.

**Usage Guide** The DHCP client checks the previously used IP address every time it is started and sends a DHCPREQUEST packet to continue leasing this IP address. If the address is not available, the DHCP server sends a NAK packet to let the client resend a DHCPDISCOVER packet to apply for a new IP address. If no corresponding lease record can be found on the server, the client keeps sending DHCPDISCOVER packets. The forcible NAK packet sending function is added to shorten the interval at which the client sends DHCPDISCOVER packets.

**Configuration Examples** The following example enables the forcible NAK packet sending function in global configuration mode.

```
Ruijie(config)# ip dhcp force-send-nak
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** N/A

## 4.21 ip dhcp monitor-vrrp-state

Use this command in layer-3 configuration mode to enable the DHCP Server to monitor the status of VRRP interfaces so that the DHCP Server processes only those packets sent from a VRRP interface in the Master state. Use the **no** form of this command to restore the default setting. If it is canceled, the DHCP Server processes packets from VRRP interfaces in the Master or Backup state.

**ip dhcp monitor-vrrp-state**  
**no ip dhcp monitor-vrrp-state**

**Parameter Description**

Parameter	Description
N/A	N/A

**Defaults** The **ip dhcp monitor-vrrp-state** command is disabled by default. .

**Command Mode** Layer-3 interface configuration mode.

**Usage Guide** If a VRRP address is configured for an interface, the DHCP Server processes packets sent from the master interface and discards packets sent from the backup interface. If no VRRP address is configured, the DHCP Server does not monitor the status of VRRP interfaces. All DHCP packets will be processed.

**Configuration** The following example enables the DHCP Server to monitor the status of VRRP interfaces.

**Examples**

```
Ruijie(config)# interface VLAN 1
Ruijie(config-if-VLAN 1) ip dhcp monitor-vrrp-state
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 4.22 ip dhcp ping packets

Use this command to configure the times of pinging the IP address when the DHCP server detects address conflict in the global configuration mode. Use the **no** form of this command to restore the default setting.

**ip dhcp ping packets** [ *number* ]

**no ip dhcp ping packets**

Parameter Description	Parameter	Description
	<i>number</i>	(Optional) Number of packets in the range of 0 to 10, where 0 indicates disabling the ping operation. The Ping operation sends two packets by default.

**Defaults** The Ping operation sends two packets by default.

**Command Mode** Global configuration mode.

**Usage Guide** When the DHCP server attempts to assign the IP address from the DHCP address pool, use the ping operation to check whether this address is occupied by other hosts. Record it if the address is occupied, otherwise, assign it to the DHCP client. The Ping operation will send up to 10 packets, two packets by default.

**Configuration** The following example sets the number of the packets sent by the ping operation as 3.

**Examples**

```
Ruijie(config)# ip dhcp ping packets 3
```

Related Commands	Command	Description
	<b>clear ip dhcp conflict</b>	Clears the DHCP history conflict record.
	<b>ip dhcp ping packet</b>	Configures the timeout time that the DHCP server waits for the Ping response. If all the ping packets are not responded within the specified time, it indicates that this IP address can be assigned. Otherwise, it will record the address conflict.
	<b>show ip dhcp conflict</b>	Displays the DHCP server detects address conflict when it assigns

	an IP address.
--	----------------

**Platform** N/A

**Description**

## 4.23 ip dhcp ping timeout

Use this command to configure the timeout that the DHCP server waits for response when it uses the ping operation to detect the address conflict in the global configuration mode. Use the **no** form of this command to restore the default setting.

**ip dhcp ping timeout** *milli-seconds*

**no ip dhcp ping timeout**

Parameter	Parameter	Description
<b>Description</b>	<i>milli-seconds</i>	Time that the DHCP server waits for ping response in the range 100 to 10000 milliseconds.

**Defaults** The default is 500 seconds.

**Command** Global configuration mode.

**Mode**

**Usage Guide** This command defines the time that the DHCP server waits for a ping response packet.

**Configuration** The following example configures the waiting time of the ping response packet to 600ms.

**Examples**

```
Ruijie(config)# ip dhcp ping timeout 600
```

Related	Command	Description
<b>Commands</b>	<b>clear ip dhcp conflict</b>	Clears the DHCP history conflict record.
	<b>ip dhcp ping packets</b>	Defines the number of the data packets sent by the ping operation for the detection of the address conflict when the DHCP server assigns an IP address.
	<b>show ip dhcp conflict</b>	Displays the address conflict the DHCP server detects when it assigns an IP address.

**Platform** N/A

**Description**

## 4.24 ip dhcp pool

Use this command to define a name of the DHCP address pool and enter the DHCP address pool configuration mode in the global configuration mode. Use the **no** form of this command to restore the default setting.

**ip dhcp pool** *pool-name*  
**no ip dhcp pool** *pool-name*

Parameter	Parameter	Description
Description	<i>pool-name</i>	A string of characters and positive integers, for instance, mypool or 1.

**Defaults** No DHCP address pool is defined by default.

**Command Mode** Global configuration mode.

**Usage Guide** Execute the command to enter the DHCP address pool configuration mode:

```
Ruijie (dhcp-config) #
```

In this configuration mode, configure the IP address range, the DNS server and the default gateway.

**Configuration Examples** The following example defines a DHCP address pool named mypool0.

```
Ruijie(config) # ip dhcp pool mypool0
Ruijie(dhcp-config) #
```

Related Commands	Command	Description
	<b>host</b>	Defines the IP address and network mask, which is used to configure the DHCP manual binding.
	<b>ip dhcp excluded-address</b>	Defines the IP addresses that the DHCP server cannot assign to the clients.
	<b>network (DHCP)</b>	Defines the network number and network mask of the DHCP address pool.

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

## 4.25 ip dhcp relay check server-id

Use this command to enable the **ip dhcp relay check server-id** function. Use the **no** form of this command to restore the default setting.

**ip dhcp relay check server-id**  
**no ip dhcp relay check server-id**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** The **ip dhcp relay check server-id** command is disabled.



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

**Usage Guide** Switch will select the server to be sent according to server-id option when forwarding DHCP REQUEST via this command. Without this command configured, the switch forwards the DHCP REQUEST to all configured DHCP servers.

**Configuration** The following example enables the ip dhcp relay check server-id function.

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp relay check server-id
```

Related	Command	Description
Commands	<b>service dhcp</b>	Enables the DHCP Relay.

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

## 4.26 ip dhcp relay information option82

Use this command to enable the **ip dhcp relay information option82** function. Use the **no** form of this command to restore the default setting.

**ip dhcp relay information option82**

**no ip dhcp relay information option82**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** The **ip dhcp relay information option82** command is disabled.

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

**Usage Guide** This command is exclusive with the **option dot1x** command.

**Configuration** The following example enables the option82 function on the DHCP relay.

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp relay information option82
```

Related	Command	Description
Commands	<b>service dhcp</b>	Enables the DHCP Relay.

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

## 4.27 ip dhcp relay suppression

Use this command to enable the DHCP binding globally. Use the **no** form of this command to disable the DHCP binding globally and enable the **DHCP relay** suppression on the port.

**ip dhcp relay suppression**

**no ip dhcp relay suppression**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** The **ip dhcp relay suppression** command is disabled.

**Command** Interface configuration mode.

**Mode**

**Usage Guide** After executing this command, the system will not relay the DHCP request message on the interface.

**Configuration** The following example enables the relay suppression function on the interface 17.

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# interface VLAN 1
Ruijie(config-if-VLAN 1) ip dhcp relay suppression
```

Related	Command	Description
Commands	<b>service dhcp</b>	Enables the DHCP Relay.

**Platform** N/A

**Description**

## 4.28 ip dhcp use class

Use this command to enable the CLASS to allocate addresses in the global configuration mode. Use the **no** form of this command can be used to disable the CLASS.

**ip dhcp use class**

**no ip dhcp use class**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** Enabled

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

**Mode**

**Usage Guide** N/A

**Configuration** The following example enables the CLASS to allocate addresses.

**Examples**

```
Ruijie(config)# ip dhcp use class
```

Related	Command	Description
Commands	N/A	N/A

**Platform** N/A

**Description**

## 4.29 ip helper-address

Use this command to add an IP address of the DHCP server. Use the **no** form of this command to delete an IP address of the DHCP server.

The server address can be configured globally or on a specific interface. Therefore, this command can run in the global configuration mode or the interface configuration mode to add the DHCP server information.

**ip helper-address** { cycle-mode | A.B.C.D }

**no ip helper-address** { cycle-mode | A.B.C.D }

Parameter	Parameter	Description
Description	cycle-mode	Forwards the DHCP request packets to all DHCP servers.
	A.B.C.D	DHCP server IP address

**Defaults** N/A

**Command Mode** Global configuration mode, interface configuration mode.

**Usage Guide** Up to 20 DHCP server IP addresses can be configured globally or on a layer-3 interface. One DHCP request of this interface will be sent to these servers. You can select one for confirmation.

**Configuration** The following example sets the IP address for the global server to 192.168.1.1

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# ip helper-address 192.168.1.1
```

Related	Command	Description
Commands	service dhcp	Enables the DHCP relay.

**Platform** N/A

**Description**

### 4.30 lease

Use this command to define the lease time of the IP address that the DHCP server assigns to the client in the DHCP address pool configuration mode. Use the **no** form of this command to restore the default setting. A limited lease time ranges from 1 minute to 23 hours and 59 minutes.

**lease** { *days* [ *hours* ] [ *minutes* ] | **infinite** }

**no lease**

Parameter	Parameter	Description
Description	<i>days</i>	Lease time in days
	<i>hours</i>	(Optional) Lease time in hours. It is necessary to define the days before defining the hours.
	<i>minutes</i>	(Optional) Lease time in minutes. It is necessary to define the days and hours before defining the minutes.
	<b>infinite</b>	Infinite lease time.

**Defaults** The lease time for a static address pool is infinite. The lease time for other address pools is 1 day.

**Command Mode** DHCP address pool configuration mode.

**Usage Guide** When the lease is getting near to expire, the DHCP client will send the request of renewal of lease. In general, the DHCP server will allow the renewal of lease of the original IP address.

**Configuration Examples** The following example sets the DHCP lease to 1 hour.

```
Ruijie(config)# ip dhcp pool mypool0
Ruijie(dhcp-config)# lease 0 1
```

The following example sets the DHCP lease to 1 minute.

```
Ruijie(config)# ip dhcp pool mypool0
Ruijie(dhcp-config)# lease 0 0 1
```

Related Commands	Command	Description
	<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

**Platform Description** N/A

### 4.31 lease-threshold

Use this command in DHCP address pool configuration mode to define the DHCP alarm threshold.

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

**lease-threshold** *percentage*

**default lease-threshold**

**no lease-threshold**

Parameter	Parameter	Description
Description	<i>percentage</i>	Usage of the address pool, ranging from 60 to 100 in percentage.

**Defaults** 90

**Command** DHCP address pool configuration mode.

**Mode**

**Usage Guide** If the maximum IP usage of the address pool reaches the threshold, the DHCP Server generates a SYSLOG alarm. The IP usage indicates the ratio of the number of assigned address pools to the total number of assignable address pools. If the number of assigned pools stays above the alarm threshold, an alarm is generated every 5 minutes.

**Configuration** The following example sets the alarm threshold to 80%.

```
Ruijie(config)# ip dhcp pool mypool0
Ruijie(dhcp-config)# lease-threshold 80
```

The following example restores the default alarm threshold.

```
Ruijie(config)# ip dhcp pool mypool0
Ruijie(dhcp-config)# default lease-threshold
```

The following example disables the address pool alarm function.

```
Ruijie(config)# ip dhcp pool mypool0
Ruijie(dhcp-config)# no lease-threshold
```

Related Commands	Command	Description
	<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

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

## 4.32 netbios-name-server

Use this command to configure the WINS name server of the Microsoft DHCP client NETBIOS in the DHCP address pool configuration mode. The **no** form of this command can be used to restore the default setting.

**netbios-name-server** *ip-address* [ *ip-address2...ip-address8* ]

**netbios-name-server**

Parameter	Parameter	Description
Description	<i>ip-address</i>	IP address of the WINS server. It is required to configure one IP address at least.
	<i>ip-address2...ip-address8</i>	(Optional) IP addresses of WINS servers. Up to 8 WINS servers can be configured.

**Defaults** No WINS server is defined by default.

**Command** DHCP address pool configuration mode.

**Mode**

**Usage Guide** When more than one WINS server is defined, the former has higher priority. The DHCP client will select the next WINS server only when its communication with the former WINS server fails.

**Configuration** The following example specifies the WINS server 192.168.12.3 for the DHCP client.

**Examples**

```
Ruijie(config)# ip dhcp pool mypool0
Ruijie(dhcp-config)# netbios-name-server 192.168.12.3
```

Related	Command	Description
Commands	<b>ip address dhcp</b>	Enables the DHCP client on the interface to obtain the IP address.
	<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enter the DHCP address pool configuration mode.
	<b>netbios-node-type</b>	Defines the netbios node type of the client host.

**Platform** N/A

**Description**

## 4.33 netbios-node-type

Use this command to define the node type of the master NetBIOS of the Microsoft DHCP client in the DHCP address configuration mode. Use the **no** form of this command to restore the default setting.

**netbios-node-type** *type*

**no netbios-node-type**

Parameter	Parameter	Description
<b>Description</b>	<i>type</i>	Type of node in two modes: Digit in hexadecimal form in the range of 0 to FF. Only the following numerals are available: 1: b-node. 2: p-node. 4: m-node. 8: h-node. String: b-node: broadcast node p-node: peer-to-peer node m-node: mixed node h-node: hybrid node

**Defaults** No type of the NetBIOS node is defined by default.

**Command** DHCP address pool configuration mode.

**Mode**

**Usage Guide** There are 4 types of the NetBIOS nodes of the Microsoft DHCP client: 1) Broadcast, which carries out the NetBIOS name resolution by the broadcast method, 2) Peer-to-peer, which directly requests the WINS server to carry out the NetBIOS name resolution, 3) Mixed, which requests the name resolution by the broadcast method firstly, and then carry out the name resolution by the WINS server connection, 4) Hybrid, which requests the WINS server to carry out the NetBIOS name resolution firstly, and it will carry out the NetBIOS name resolution by the broadcast method if the response is not received.

By default, the node type for Microsoft operating system is broadcast or hybrid. If the WINS server is not configured, broadcast node is used. Otherwise, hybrid node is used. It is recommended to set the type of the NetBIOS node as Hybrid.

**Configuration** The following example sets the NetBIOS node of Microsoft DHCP client as Hybrid.

**Examples**

```
Ruijie(config)# ip dhcp pool mypool0
Ruijie(dhcp-config)# netbios-node-type h-node
```

Related	Command	Description
<b>Commands</b>	<b>ip dhcp pool</b>	Defines the name of DHCP address pool and enters the DHCP address pool configuration mode.
	<b>netbios-name-server</b>	Configures the WINS name server of the Microsoft DHCP client NETBIOS.

**Platform** N/A

**Description**

## 4.34 network (DHCP)

Use this command to define the network number and network mask of the DHCP address pool in the DHCP address pool configuration mode. Use the **no** form of this command to restore the default setting.

**network** *net-number net-mask*

**no network**

Parameter	Parameter	Description
Description	<i>net-number</i>	Network number of the DHCP address pool
	<i>net-mask</i>	Network mask of the DHCP address pool. If the network mask is not defined, the natural network mask will be used by default.

**Defaults** No network number or network mask is defined by default.

**Command** DHCP address pool configuration mode.

**Mode**

**Usage Guide** This command defines the subnet and subnet mask of a DHCP address pool, and provides the DHCP server with an address space which can be assigned to the clients. Unless excluded addresses are configured, all the addresses of the DHCP address pool can be assigned to the clients. The DHCP server assigns the addresses in the address pool orderly. If the DHCP server found an IP address is in the DHCP binding table or in the network segment, it checks the next until it assigns an effective IP address.

The **show ip dhcp binding** command can be used to view the address assignment, and the **show ip dhcp conflict** command can be used to view the address conflict detection configuration.

**Configuration Examples** The following example defines the network number of the DHCP address pool as 192.168.12.0, and the network mask as 255.255.255.240.

```
Ruijie(config)# ip dhcp pool mypool0
Ruijie(dhcp-config)# network 192.168.12.0 255.255.255.240
```

Related Commands	Command	Description
	<b>ip dhcp excluded-address</b>	Defines the IP addresses that the DHCP server cannot assign to the clients.
	<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

**Platform** N/A

**Description**



## 4.35 next-server

Use this command to define the startup sever list that the DHCP client accesses during startup in the DHCP address configuration mode. Use the **no** form of this command to restore the default setting.

**next-server** *ip-address* [ *ip-address2...ip-address8* ]

**no next-server**

Parameter	Parameter	Description
Description	<i>ip-address</i>	Defines the IP address of the startup server, which is usually the TFTP server. It is required to configure one IP address at least.
	<i>ip-address2...ip-address8</i>	(Optional) Up to 8 startup servers can be configured.

**Defaults** N/A

**Command** DHCP address pool configuration mode.

**Mode**

**Usage Guide** When more than one startup server is defined, the former will possess higher priory. The DHCP client will select the next startup server only when its communication with the former startup server fails.

**Configuration** The following example specifies the startup server 192.168.12.4 for the DHCP client.

**Examples**

```
Ruijie(config)# ip dhcp pool mypool0
Ruijie(dhcp-config)# next-server 192.168.12.4
```

Related Commands	Command	Description
	<b>bootfile</b>	Defines the default startup mapping file name of the DHCP client.
	<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enter the DHCP address pool configuration mode.
	<b>ip help-address</b>	Defines the Helper address on the interface.
	<b>option</b>	Configures the option of the RGOS software DHCP server.

**Platform** N/A

**Description**

## 4.36 option

Use this command to configure the option of the DHCP server in the DHCP address pool configuration mode. Use the **no** form of this command to restore the default setting.

**option** *code* { **ascii** *string* | **hex** *string* | **ip** *ip-address* }

**no option**

Parameter Description	Parameter	Description
	<i>code</i>	Defines the DHCP option codes.
	<i>ascii string</i>	Defines an ASCII string.
	<i>hex string</i>	Defines a hex string.
	<i>ip ip-address</i>	Defines an IP address list.

**Defaults** N/A

**Command Mode** DHCP address pool configuration mode.

**Usage Guide** The DHCP provides a mechanism to transmit the configuration information to the host in the TCP/IP network. The DHCP message has a variable option field that can be defined according to the actual requirement. The DHCP client needs to carry the DHCP message with 32 bytes of option information at least. Furthermore, the fixed data field in the DHCP message is also referred to as an option. For the definition of current DHCP option, refer to RFC 2131.

**Configuration Examples** The following example defines the option code 19, which determines whether the DHCP client can enable the IP packet forwarding. 0 indicates to disable the IP packet forwarding, and 1 indicates to enable the IP packet forwarding. The configuration below enable the IP packet forwarding on the DHCP client.

```
Ruijie(config)# ip dhcp pool mypool0
Ruijie(dhcp-config)# option 19 hex 1
```

The following example defines the option code 33, which provides the DHCP client with the static route information. The DHCP client will install two static routes: 1) the destination network 172.16.12.0 and the gateway 192.168.12.12, 2) the destination network 172.16.16.0 and the gateway 192.168.12.16.

```
Ruijie(config)# ip dhcp pool mypool0
Ruijie(dhcp-config)# option 33 ip 172.16.12.0 192.168.12.12 172.16.16.0
192.168.12.16
```

Related Commands	Command	Description
	<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

**Platform Description** N/A

## 4.37 pool-status

Use this command to enable or disable the DHCP address pool.

**pool-status { enable | disable }**

Parameter	Parameter	Description
Description	<b>enable</b>	Enables the address pool.
	<b>disable</b>	Disables the address pool.

**Defaults** By default, the address pool is enabled after it is configured.

**Command Mode** DHCP address pool configuration mode

**Usage Guide** This command is configured on the DHCP server.

**Configuration** The following example disables the address pool.

**Examples**

```
Ruijie(config)# ip dhcp pool mypool0
Ruijie(dhcp-config)# pool-status disable
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 4.38 relay agent information

Use this command to enter the Option82 matching information configuration mode in the global CLASS configuration mode. Use the **no** form of this command to delete the Option82 matching information of the CLASS.

**relay agent information**

**no relay agent information**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** N/A

**Command Mode** Global CLASS configuration mode

**Usage Guide** After executing this command, it enters the Option82 matching information configuration mode which

is shown as “Ruijie (config-dhcp-class-relayinfo)#”.

In this configuration mode, user can configure the class matching multiple Option82 information.

**Configuration Examples** The following example configures a global CLASS and enters the Option82 matching information configuration mode.

```
Ruijie(config)# ip dhcp class myclass
Ruijie(config-dhcp-class)# relay agent information
Ruijie(config-dhcp-class-relayinfo)#
```

Related Commands	Command	Description
	<b>ip dhcp class</b>	Defines a CLASS and enters the global CLASS configuration mode.

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

### 4.39 relay-information hex

Use this command to enter the Option82 matching information configuration mode. Use the **no** form of this command to delete a piece of matching information.

**relay-information hex** *aabb.ccdd.eeff... [ \* ]*  
**no relay-information hex** *aabb.ccdd.eeff... [ \* ]*

Parameter	Parameter	Description
<b>Description</b>	<i>aabb.ccdd.eeff...[*]</i>	Hexadecimal Option82 matching information. The '*' symbol means partial matching which needs the front part matching only. Without the '*' means needing full matching.

**Defaults** N/A

**Command Mode** Global CLASS configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example configures a global CLASS which can match multiple Option82 information.

```
Ruijie(config)# ip dhcp class myclass
Ruijie(config-dhcp-class)# relay agent information
Ruijie(config-dhcp-class-relayinfo)# relay-information
hex 0102256535
Ruijie(config-dhcp-class-relayinfo)# relay-information
hex 010225654565
Ruijie(config-dhcp-class-relayinfo)# relay-information
hex 060225654565
Ruijie(config-dhcp-class-relayinfo)# relay-information
```

```
hex 060223*
```

Related Commands	Command	Description
	<b>ip dhcp class</b>	Defines a CLASS and enter the global CLASS configuration mode.
	<b>relay agent information</b>	Enters the Option82 matching information configuration mode.

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

### 4.40 remark

Use this command to configure the identification which is used to describe the CLASS in this global CLASS configuration mode. Use the **no** form of this command to delete the identification.

**remark** *class-remark*  
**no remark**

Parameter Description	Parameter	Description
	class-remark	Information used to identify the CLASS, which can be the character strings with space in them.

**Defaults** N/A.

**Command Mode** Global CLASS configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example configures the identification information for a global CLASS.

```
Ruijie(config)# ip dhcp class myclass
Ruijie(config-dhcp-class)# remark used in #1 build
```

Related Commands	Command	Description
	<b>ip dhcp class</b>	Defines a CLASS and enter the global CLASS configuration mode.

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

### 4.41 service dhcp

Use this command to enable the DHCP server and the DHCP relay on the device in global configuration mode. Use the **no** form of this command to restore the default setting.

**service dhcp**  
**no service dhcp**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** The **service dhcp** command is disabled.

**Command Mode** Global configuration mode

**Usage Guide** The DHCP server can assign the IP addresses to the clients automatically, and provide them with the network configuration information such as DNS server and default gateway. The DHCP relay can forward the DHCP requests to other servers, and the returned DHCP responses to the DHCP client, serving as the relay for DHCP packets.

**Configuration Examples** The following example enables the DHCP server and the DHCP relay feature.

```
Ruijie(config)# service dhcp
```

Related Commands	Command	Description
	<b>show ip dhcp server statistics</b>	Displays various statistics information of the DHCP server.
	<b>ip helper-address [ vrf ] A.B.C.D</b>	Adds an IP address of the DHCP server.

**Platform Description** N/A

## 4.42 show dhcp exclude

Use this command to display the excluded address.

**show dhcp exclude**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the excluded address.

```
Ruijie# show dhcp exclude
low                high
-----
```

20.1.1.1	20.1.1.2
30.1.1.1	30.1.1.20

Related Commands	Command	Description
	N/A	N/A

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

### 4.43 show dhcp lease

Use this command to display the lease information of the IP address obtained by the DHCP client.

**show dhcp lease**

Parameter Description	Parameter	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: 192.168.5.71 for peer on Interface: VLAN 1
Temp sub net mask: 255.255.255.0
DHCP Lease server: 192.168.5.70, state: 3 Bound
DHCP transaction id: 168F
Lease: 600 secs, Renewal: 300 secs, Rebind: 525 secs
Temp default-gateway addr: 192.168.5.1
Next timer fires after: 00:04:29
Retry count: 0 Client-ID: redgaint-00d0.f8fb.5740-Gi0/17
```

Related Commands	Command	Description
	N/A	N/A

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

### 4.44 show dhcp manual-bind

Use this command to display the binding address.

**show dhcp manual-bind**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the binding address.

```
Ruijie# show dhcp manual-bind
ip          mask          uid/mac          pool_name      gateway      dns
-----
20.1.1.122  255.0.0.0          0000.0000.0001  static1       1.1.1.1
2.2.2.2
```

ip	IP address
mask	Subnet mask
uid/mac	UID/MAC address
Pool name	Address pool name
gateway	Gateway
dns	DNS server name

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

### 4.45 show dhcp name

Use this command to display all DHCP address pool names.

**show dhcp name**

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



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

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays all DHCP address pool names.

**Examples** Ruijie# show dhcp name

```
DYNAMIC POOL
pool name:net20

MANUAL POOL
pool name:static1
pool name:static2

UNKNOWN POOL
pool name:test
```

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

**Platform** N/A

**Description**

## 4.46 show dhcp pool

Use this command to display the configuration of a specified address pool.

**show dhcp pool** *name*

Parameter	Parameter	Description
<b>Description</b>	<i>name</i>	Specifies the address pool.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the configuration of a specified address pool.

**Examples**

```
Ruijie# show dhcp pool net20
network : 20.0.0.0
netmask : 255.0.0.0
lease-infinite : false
lease-days : 1
lease-hours : 0
lease-minutes : 0
netbios-type : 0
domain-name :
gateway :
dns:
ntp:
option-43:
option-138:
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** N/A

### 4.47 show dhcp state

Use this command to display whether DHCP server is enabled.

**show dhcp state**

**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 whether DHCP server is enabled.

**Examples**

```
Ruijie# show dhcp state
dhcp-server state : true
```

**Related Commands**

Command	Description
N/A	N/A

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

### 4.48 show ip dhcp binding

Use this command to display the binding condition of the DHCP address.

**show ip dhcp binding [ ip-address ]**

Parameter	Parameter	Description
Description	ip-address	(Optional) Only displays the binding condition of the specified IP addresses.

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** If the IP address is not defined, show the binding condition of all addresses. If the IP address is defined, show the binding condition of this IP address

**Configuration Examples** The following is the result of the show ip dhcp binding.

```
Ruijie# show ip dhcp binding
Total number of clients : 4
Expired clients : 3
Running clients : 1

IP address      Hardware address      Lease expiration      Type
20.1.1.1       2000.0000.2011        000 days 23 hours 59 mins Automatic
```

Description of fields in the command output is as follows:

Field	Description
IP address	The IP address to be assigned to the DHCP client.
Client-Identifier /Hardware address	The client identifier or hardware address of the DHCP client.
Lease expiration	The expiration date of the lease. The Infinite indicates it is not limited by the time. The IDLE indicates the address is in the free status currently for it is not renewed or the DHCP client releases it actively.
Type	The type of the address binding. The Automatic indicates an IP address is assigned automatically, and the Manual indicates an IP address is assigned by manual.

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

<b>Commands</b>	<b>clear ip dhcp binding</b>	Clears the DHCP address binding table.
-----------------	------------------------------	--

**Platform** N/A

**Description**

## 4.49 show ip dhcp conflict

Use this command to show the conflict history record of the DHCP sever.

**show ip dhcp conflict**

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

**Defaults** N/A

**Command** Privileged EXEC mode.

**Mode**

**Usage Guide** This command can display the conflict address list detected by the DHCP server.

**Configuration** The following example displays the output result of the **show ip dhcp conflict** command.

**Examples**

```
Ruijie# show ip dhcp conflict
IP address  Detection Method
192.168.12.1 Ping
```

Description of fields in the command output is as follows:

Field	Description
IP address	The IP addresses which cannot be assigned to the DHCP client.
Detection Method	The conflict detection method.

Related	Command	Description
<b>Commands</b>	<b>clear ip dhcp conflict</b>	Clears the DHCP conflict record.

**Platform** N/A

**Description**

## 4.50 show ip dhcp history

Use this command to display the DHCP lease history.

**show ip dhcp history**

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

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

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is configured on the DHCP server.

**Configuration** The following example displays the DHCP lease history.

```

Examples Ruijie# show ip dhcp history
Expired clients          : 3
IP address              Hardware address      Lease expiration      Vlan/Relay
10.1.1.5                2222.abcd.47ac          IDLE                  4097
10.1.1.4                2222.abcd.47ae          IDLE                  4097
10.1.1.3                2222.abcd.47ad          IDLE                  4097
Running clients         : 0
    
```

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

**Platform Description** N/A

### 4.51 show ip dhcp identifier

Use this command to display the DHCP address pool ID and address usage.

**show ip dhcp identifier**

<b>Parameter Description</b>	<b>Parameter</b>	<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 DHCP address pool ID and address usage.

```

Examples Ruijie# show ip dhcp identifier
Pool name  Identifier  Total  Distributed  Remained
-----
    
```

wwp	597455782	65533	0	65533
-----	-----------	-------	---	-------

Field	Description
Pool name	Address pool name.
Identifier	Address pool ID.
Total	Total number of addresses.
Distributed	Number of allocated addresses.
Remained	Number of remained addresses.

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 4.52 show ip dhcp pool

Use this command to display the address statistics of an address pool.

**show ip dhcp pool** [ *poolname* ]

Parameter	Parameter	Description
<b>Description</b>	<i>poolname</i>	(Optional) Address pool whose address statistics are to be displayed.

**Defaults** Privileged EXEC mode.

**Command** N/A

**Mode**

**Usage Guide** Use this command to show the address statistics of an address pool.

**Configuration** The following example displays the output result of the **show ip dhcp pool** *poolname* command.

**Examples**

```
Ruijie# show ip dhcp pool
Pool poolname:
  Address range      192.168.0.1 - 192.168.0.254
  Class range       192.168.0.1 - 192.168.0.254
  Total address     252
  Excluded          2
  Distributed       30
  Conflict          10
  Remained          212
  Usage percentage  84.12698%
  Lease threshold   90%
```

Description of fields in the command output is as follows:

Field	Description
Address range	Address range of the address pool.
Class range	Class address range. By default, the address range for the same address pool is not configured. Otherwise, the class range is displayed.
Total address	Total number of addresses that can be assigned in the address pool.
Excluded	Number of excluded addresses.
Distributed	Number of assigned addresses.
Conflict	Number of conflicting addresses in the address pool.
Remained	Number of remaining addresses that have not been assigned or can be reused.
Usage percentage	Address pool usage.
Lease threshold	Lease threshold.

#### Related Commands

Command	Description
ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

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

## 4.53 show ip dhcp relay-statistics

Use this command to display the statistics of the DHCP relay.

**show ip dhcp relay-statistics**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is used to display the statistics of the DHCP relay.

**Configuration Examples** The following example displays the statistics of the DHCP relay.

```
Ruijie# show ip dhcp relay-statistics
Cycle mode          0
Message             Count
```

```

Discover          0
Offer            0
Request         0
Ack             0
Nak            0
Decline        0
Release        0
Info          0
Bad           0

Direction      Count
Rx client      0
Rx client uni  0
Rx client bro  0
Tx client      0
Tx client uni  0
Tx client bro  0
Rx server      0

```

Related Commands	Command	Description
	N/A	N/A

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

## 4.54 show ip dhcp server statistics

Use this command to display the statistics of the DHCP server.

**show ip dhcp server statistics**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command displays the statistics of the DHCP server.

**Configuration Examples** The following example displays the output result of the **show ip dhcp server statistics** command.

```

Ruijie# show ip dhcp server statistics
Address pools          2

```



```

Lease counter          4
Active Lease Counter   0
Expired Lease Counter  4
Malformed messages    0
Dropped messages      0

Message                Received
BOOTREQUEST           216
DHCPDISCOVER          33
DHCPREQUEST           25
DHCPDECLINE           0
DHCPRELEASE           1
DHCPIFORM             150

Message                Sent
BOOTREPLY              16
DHCPOFFER              9
DHCPACK                7
DHCPNAK                0
DHCPREQTIMES           0
DHCPREQSUCTIMES       0
DISCOVER-PROCESS-ERROR 0
LEASE-IN-PINGSTATE     0
NO-LEASE-RESOURCE     0
SERVERID-NO-MATCH     0
-----
recv                   0
send                   0

```

Description of fields in the command output is as follows:

Field	Description
Address pools	Number of address pools.
Lease count	Number of allocated lease.
Automatic bindings	Number of automatic address bindings.
Manual bindings	Number of manual address bindings.
Expired bindings	Number of expired address bindings.
Malformed messages	Number of malformed messages received by the DHCP.
Message Received or Sent	Number of the messages received and sent by the DHCP server respectively.

Related	Command	Description
Commands	<code>clear ip dhcp server statistics</code>	Clears the DHCP server statistics.

**Platform** N/A

**Description**

## 4.55 show ip dhcp socket

Use this command to display the socket used by the DHCP server.

**show ip dhcp socket**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** N/A

**Command** Privileged EXEC mode

**Mode**

**Usage Guide** N/A

**Configuration** The following example displays the socket used by the DHCP server.

**Examples**

```
Ruijie# show ip dhcp socket
dhcp socket = 47.
```

Related	Command	Description
Commands	N/A	N/A

**Platform** N/A

**Description**

## 5 DHCPv6 Commands

### 5.1 clear ipv6 dhcp client

Use this command to reset the DHCPv6 client.

**clear ipv6 dhcp client** *interface-type interface-number*

Parameter	Parameter	Description
Description	<i>interface-type</i> <i>interface-number</i>	Sets the interface type and the interface number.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is used to reset the DHCPv6 client, which may lead the client to request for the configurations from the server again.

**Configuration** The following example resets DHCP client VLAN 1.

**Examples** Ruijie# clear ipv6 dhcp client vlan 1

Related	Command	Description
Commands	N/A	N/A

**Platform** N/A

**Description**

### 5.2 clear ipv6 dhcp relay statistics

Use this command to clear the packet sending and receiving condition with the DHCPv6 Relay function enabled.

**clear ipv6 dhcp relay statistics**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example clears the packet sending and receiving condition with the DHCPv6 Relay function enabled.

```
Ruijie# clear ipv6 dhcp relay statistics
```

Related Commands	Command	Description
	<b>show ipv6 dhcp relay statistics</b>	Displays the statistical information.

**Platform Description** N/A

### 5.3 ipv6 dhcp client ia

Use this command to enable DHCPv6 client mode and request the IANA address from the DHCPv6 server. Use the **no** form of this command to restore the default setting.

```
ipv6 dhcp client ia [ rapid-commit ]
no ipv6 dhcp client
```

Parameter Description	Parameter	Description
	<b>rapid-commit</b>	Allows the two-message interaction process.

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

**Command Mode** Interface configuration mode

**Usage Guide** This command is used to enable DHCPv6 client mode and request the IANA address from the DHCPv6 server,  
The **rapid-commit** keyword allows the two-message interaction process between the client and the server. After the keyword is configured, the solicit message transmitted by the client contains the rapid-commit option.

**Configuration Examples** The following example enables the request for the IANA address on the interface.

```
Ruijie(config)# interface VLAN 1
Ruijie(config-if-VLAN 1)# ipv6 dhcp client ia
```

Related Commands	Command	Description
	N/A	N/A

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

## 5.4 ipv6 dhcp client pd

Use this command to enable the DHCPv6 client and request for the prefix address information.  
 Use the **no** form of this command to restore the default setting.

**ipv6 dhcp client pd** *prefix-name* [ **rapid-commit** ]  
**no ipv6 dhcp client**

Parameter	Parameter	Description
<b>Description</b>	<i>prefix-name</i>	Defines the IPv6 prefix name.
	<b>rapid-commit</b>	Allows the two-message interaction process.

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

**Command Mode** Interface configuration mode

**Usage Guide** With the DHCPv6 client mode disabled, use this command to enable the DHCPv6 client mode on the interface.  
 With the **ipv6 dhcp client pd** command enabled, the DHCPv6 client sends the prefix request to the DHCPv6 server.  
 The keyword **rapid-commit** allows the client and the server two-message interaction process. With this keyword configured, the solicit message sent by the client includes the **rapid-commit** item.

**Configuration Examples** The following example enables the prefix information request on the interface.

```
Ruijie(config)# interface VLAN 1
Ruijie(config-if-VLAN 1)# ipv6 dhcp client pd pd_name
```

Related Commands	Command	Description
	<b>clear ipv6 dhcp client</b>	Resets the DHCPv6 client function on the interface.
	<b>show ipv6 dhcp interface</b>	Displays the DHCPv6 interface configuration.

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

## 5.5 ipv6 dhcp relay destination

Use this command to enable the DHCPv6 relay service and configure the destination address to which the messages are forwarded.

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

**ipv6 dhcp relay destination***ipv6-address* [ *interface-type interface-number* ]  
**no ipv6 dhcp relay destination***ipv6-address* [ *interface-type interface-number* ]

Parameter	Parameter	Description
Description	<i>ipv6-address</i>	Sets the DHCPv6 relay destination address.
	<i>interface-type</i>	Specifies the forwarding output interface if the forwarding address is the local link address.
	<i>interface-number</i>	

**Defaults** By default, the relay and forward function is disabled, and the forwarding destination address and the output interface are not configured.

**Command Mode** Interface configuration mode

**Usage Guide** With the DHCPv6 relay service enabled on the interface, the DHCPv6 message received on the interface can be forwarded to all configured destination addresses. Those received DHCPv6 messages can be from the client, or from another DHCPv6 relay service.

The forwarding output interface configuration is mandatory if the forwarding address is the local link address or the multicast address. And the forwarding output interface configuration is optional if the forwarding address is global or station unicast or multicast address.

Without the forwarding output interface configured, the interface is selected according to the unicast or multicast routing protocol.

The relay reply message can be forwarded without the relay function enabled on the interface.

**Configuration Examples** The following example sets the relay destination address on the interface.

```
Ruijie(config)# interface VLAN 1
Ruijie(config-if-VLAN 1)# ipv6 dhcp relay destination 2008:1::1
```

Related Commands	Command	Description
	<b>show ipv6 dhcp interface</b>	Displays the DHCPv6 interface information.

**Platform Description** N/A

## 5.6 show ipv6 dhcp

Use this command to display the device DUID.

**show ipv6 dhcp**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** N/A

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

**Usage Guide** The server, client and relay on the same device share a DUID.

**Configuration** The following example displays the device DUID.

**Examples**

```
Ruijie# show ipv6 dhcp
This device's DHCPv6 unique identifier(DUID): 00:03:00:01:00:d0:f8:22:33:b0
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 5.7 show ipv6 dhcp interface

Use this command to display the DHCPv6 interface information.

**show ipv6 dhcp interface** [ *interface-name* ]

Parameter Description	Parameter	Description
	<i>interface-name</i>	Sets the interface name.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** If the *interface-name* is not specified, all DHCPv6 interface information is displayed. If the *interface-name* is specified, the specified interface information is displayed.

**Configuration** The following example displays the DHCPv6 interface information.

**Examples**

```
Ruijie# show ipv6 dhcp interface
VLAN 1 is in server mode
Server pool dhcp-pool
Rapid-Commit: disable
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 5.8 show ipv6 dhcp relay destination

Use this command to display the destination information about DHCPv6 Relay Agent.

**show ipv6 dhcp relay destination**

Parameter	Parameter	Description
description	all	Displays information about all configured destination addresses and relay exits.
	Interface <i>interface-type</i> <i>interface-number</i>	Displays the relay destination address and relay exit configured for a specified interface.

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage guideline** Use this command to show the relay destination address to which DHCPv6 packets sent from a client are forwarded through a specified relay exit (optional) by an interface for which the relay function has been enabled by Relay Agent.

**Examples** The following example displays all the relay destination addresses.

```
Ruijie# show ipv6 dhcp relay destination all
Interface: Vlan1 //interface for which the relay function has been enabled
Destination address(es)                Output Interface
3001::2
FF02::1:2 //specified destination address      Vlan2 //specified
relay exit
```

Related commands	Command	Description
	N/A	N/A

**Platform description** N/A

## 5.9 show ipv6 dhcp relay statistics

Use this command to display the packet sending and receiving condition with the DHCPv6 Relay function enabled.

**show ipv6 dhcp relay statistics**

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



**Defaults** N/A.

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A.

**Configuration Examples** The following example displays the packet sending and receiving condition with the DHCPv6 Relay function enabled.

```
Ruijie# show ipv6 dhcp relay statistics
Packets dropped          : 2
  Error                  : 2
  Excess of rate limit   : 0
Packets received        : 28
  SOLICIT                : 0
  REQUEST                : 0
  CONFIRM                : 0
  RENEW                  : 0
  REBIND                 : 0
  RELEASE                : 0
  DECLINE                : 0
  INFORMATION-REQUEST   : 14
  RELAY-FORWARD          : 0
  RELAY-REPLY            : 14
Packets sent            : 16
  ADVERTISE              : 0
  RECONFIGURE            : 0
  REPLY                  : 8
  RELAY-FORWARD          : 8
  RELAY-REPLY            : 0
```

Related Commands	Command	Description
	<b>clear ipv6 dhcp relay statistics</b>	Clears the statistical information.

**Platform Description** N/A

## 6 DNS Commands

### 6.1 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# clear host *
```

Related Commands	Command	Description
	<b>show hosts</b>	Displays the host name buffer table.

**Platform Description** N/A

### 6.2 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 Examples** 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>	

**Platform** N/A

**Description**

## 6.3 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* [ *telnet-port* ] *ip-address*

**no ip host** *host-name* [ *telnet-port* ] *ip-address*

Parameter Description	Parameter	Description
		<i>host-name</i>
	<i>telnet-port</i>	Telnet port number, ranging from 0 to 65535. The default value is 0.
	<i>ip-address</i>	IP address of the equipment

**Defaults** N/A

**Command Mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example configures IPv4 address 192.168.5.243 for domain name www.test.com.

**Examples** Ruijie(config)# ip host www.test.com 192.168.5.243

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

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

## 6.4 ip name-server

Use this command to configure the IP address of the domain name server. Use the **no** form of this command to delete the configured domain name server.

**ip name-server** { *ip-address* | *ipv6-address* }

**no ip name-server** [ *ip-address* | *ipv6-address* ]

Parameter Description	Parameter	Description
		<i>ip-address</i>
	<i>ipv6-address</i>	The IPv6 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 configures the IPv4 domain name server.

**Examples** Ruijie(config)# ip name-server 192.168.5.134

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

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

## 6.5 ipv6 host

Use this command to configure the mapping of the host name and the IPv6 address by manual. Use the **no** form of the command to remove the host list.

**ipv6 host** *host-name* [ *telnet-port* ] *ipv6-address*

**no ipv6 host** *host-name* [ *telnet-port* ] *ipv6-address*

Parameter Description	Parameter	Description
	<i>host-name</i>	Host name of the equipment
	<i>telnet-port</i>	Telnet port number, ranging from 0 to 65535. The default value is 0.
	<i>ipv6-address</i>	IPv6 address of the equipment

**Defaults** N/A

**Command Mode** Global configuration mode.

**Usage Guide** To delete the host list, use the **no ipv6 host** *host-name* *ipv6-address* command.

**Configuration Examples** The following example configures the IPv6 address for the domain name.

```
Ruijie(config)# ipv6 host switch 2001:0DB8:700:20:1::12
```

Related Commands	Command	Description
	<b>show hosts</b>	Displays the DNS related configuration information.

**Platform** N/A

**Description**

## 6.6 show hosts

Use this command to display DNS configuration.

**show hosts** [ *hostname* ]

Parameter Description	Parameter	Description
	<i>hostname</i>	Displays the specified domain name information,

**Defaults** All domain name information is displayed by default.

**Command** Privileged EXEC mode.

**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
```

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: 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**

## 7 FTP CLIENT Commands

### 7.1 copy flash

Use this command to upload the file from the server to the device through FTP Client.

**copy flash:** *[ local-directory/ ]local-file*

**ftp://username:password@dest-address** *[ /remote-directory ]/remote-file*

Parameter Description	Parameter	Description
	<i>username</i>	The username for logging into FTP Server. It is limited to 40 bytes and must not contain ":", "@", "/" and space, neither can it be omitted.
	<i>password</i>	The password for logging into FTP Server. It is limited to 32 bytes and must not contain ":", "@", "/" and space, neither can it be omitted.
	<i>dest-address</i>	IP address of the target FTP Server.
	<i>remote-directory</i>	File directory of FTP Server. It is optional and limited to 255 bytes. No space or Chinese character is supported. If left blank, it implies the current directory of FTP server.
	<i>remote-file</i>	Filename on the remote server. It is limited to 255 bytes and doesn't support space or Chinese character.
	<i>local-directory</i>	Directory of local folder (optional). If this directory is specified, this directory must have been created beforehand. This command doesn't support automatic directory creation. If left blank, it implies the current directory on the local device. It is limited to 255 bytes and doesn't support space or Chinese characters.
	<i>local-file</i>	Filename on the local device. It is limited to 255 bytes and doesn't support space or Chinese character.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example uploads the file named "local-file" in directory "home" of local device to directory "root" on the FTP Server whose user name is user, password is pass and IP address is 192.168.23.69, and changes the filename to "remote-file".

```
Ruijie# copy flash:home/local-file
ftp://user:pass@192.168.23.69/root/remote-file
```

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

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

## 7.2 copy ftp

Use this command to download the file from the server to the device through FTP Client.

**copy ftp://username:password@dest-address[ /remote-directory ]/remote-file**

**flash:[ local-directory/ ]local-file]**

<b>Parameter Description</b>	Parameter	Description
	<i>username</i>	The username for logging into FTP Server. It is limited to 40 bytes and must not contain ":", "@", "/" and space, neither can it be omitted.
	<i>password</i>	The password for logging into FTP Server. It is limited to 32 bytes and must not contain ":", "@", "/" and space, neither can it be omitted.
	<i>dest-address</i>	IP address of the target FTP Server.
	<i>remote-directory</i>	File directory of FTP Server. It is optional and limited to 255 bytes. No space or Chinese character is supported. If left blank, it implies the current directory of FTP server.
	<i>remote-file</i>	Filename on the remote server. It is limited to 255 bytes and doesn't support space or Chinese character.
	<i>local-directory</i>	Directory of local folder (optional). If this directory is specified, this directory must have been created beforehand. This command doesn't support automatic directory creation. If left blank, it implies the current directory on the local device. It is limited to 255 bytes and doesn't support space or Chinese characters.
	<i>local-file</i>	Filename on the local device. It is limited to 255 bytes and doesn't support space or Chinese character.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example uses username of "user" and password of "pass" to download a file named "remote-file" from the directory "root" on FTP Server with IP address 192.168.23.69 to directory



"home" on the local device, and changes the name to "local-file".

```
Ruijie# copy ftp://user:pass@192.168.23.69/root/remote-file
flash:home/local-file
```

Related Commands	Command	Description
		copy tftp

Platform N/A  
 Description

### 7.3 ftp-client ascii

Use this command to use ASCII mode for FTP transfer.

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

**ftp-client ascii**

**no ftp-client ascii**

**default ftp-client ascii**

Parameter Description	Parameter	Description
		N/A

**Defaults** The default FTP transfer mode is binary.

**Command Mode** Global configuration mode

**Usage Guide** The **default** command is used to restore the FTP client setting. Specifically, data connection is in PASV mode and file transfer BINARY. The client source IP address is not bound.

**Configuration Examples** The following example configures ASCII FTP transfer.

```
Ruijie (config)# ftp-client ascii
```

The following example configures binary FTP transfer.

```
Ruijie(config)# no ftp-client ascii
```

The following example restores the default setting of the FTP Client.

```
Ruijie(config)# default ftp-client ascii
```

Related Commands	Command	Description
		N/A

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

## 7.4 ftp-client port

Use this command to configure PORT mode used for FTP data connection. Use the **no** or **default** form of this command to restore the default setting.

**ftp-client port**  
**no ftp-client port**  
**default ftp-client port**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** The default is PASV mode for FTP data connection.

**Command Mode** Global configuration mode.

**Usage Guide** This command is used to configure the connection mode to PORT mode, in which the server will actively connect with the client.  
 The **default** command is used to restore the FTP client setting. Specifically, data connection is in PASV mode and file transfer BINARY. The client source IP address is not bound.

**Configuration** The following example configures PORT mode used for FTP data connection

**Examples** Ruijie (config)# ftp-client port

The following example configures PASV mode for FTP data connection.

Ruijie(config)# no ftp-client port

Related Commands	Command	Description
	N/A	N/A

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

## 7.5 ftp-client source-address

Use this command to bind FTP Client with the source IP address of client and use this IP address to

communicate with server. Use the **no** form of this command to disable source IP address binding. Use the **no** or **default** form of this command to restore the default setting.

**ftp-client source** { *ip-address* | *ipv6-address* }  
**no ftp-client source**  
**default ftp-client source**

Parameter Description	Parameter	Description
	<i>ip-address</i>	Specifies the IPv4 address of a local interface.
	<i>ipv6-address</i>	Specifies the IPv6 address of a local interface.

**Defaults** By default, the IP address is not bound with the client locally. Instead, it is selected by the route.

**Command Mode** Global configuration mode

**Usage Guide** The **default** command is used to restore the FTP client setting. Specifically, data connection is in PASV mode and file transfer BINARY. The client source IP address is not bound.

**Configuration Examples** The following example binds FTP Client with source IP address 192.168.23.236.

```
Ruijie(config)# ftp-client source 192.168.23.236
```

The following example binds FTP Client with source IP address 2003:0:0:0::2.

```
Ruijie(config)# ftp-client source 2003:0:0:0::2
```

The following example disables source IP address binding.

```
Ruijie(config)# no ftp-client source
```

The following example restores the default setting of the FTP Client.

```
Ruijie(config)# default ftp-client source
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 8 Network Connectivity Test Tool Commands

### 8.1 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 [next-hop next-hop]] }
```

Parameter Description	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
	<i>next-hop</i>	Specifies the next hop IPv4 address


**Defaults** Five packets with 100Byte in length are sent to the specified IP address within specified time (2s by default).

**Command Mode** Privileged EXEC mode.

**Usage Guide** 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.

**Configuratio** The following example tests the connectivity of a network to locate the network connectivity problem.

n Examples

 (RG-S29 series products do not support the VRF parameter. The following example is for reference purpose. Please take the actual device as the standard.)

```
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=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 Commands	Command	Description
	N/A	N/A

Platform N/A

Description

## 8.2 ping ipv6

Use this command to test the connectivity of a network to locate the network connectivity problem. The command format is as follows:

**ping [ ipv6 ] { address [ length length ] [ ntimes times ] [ timeout seconds ] [ data data ] [ source source ] [ detail ] [ out-interface interface [next-hop next-hop] ] }**

Parameter Description	Parameter	Description
	<i>ip-address</i>	Specifies an IPv6 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 IPv6 address or the source interface. The loopback interface address (for example: 127.0.0.1) is not allowed to

	be the source address.
<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
<i>next-hop</i>	Specifies the next hop IPv6 address

**Defaults** Five packets with 100Byte in length are sent to the specified IP address within specified time 2 seconds by default

**Command Mode** Privileged EXEC mode.

**Usage Guide** If the device can be pinged, the response information is displayed, and the statistics is listed at the end. If the response data does not match the request data, a ‘Request receive error.’ message is displayed and the statistics is listed in the end. For the extension functions of ping ipv6, 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 Examples** The following example tests the connectivity of a network to locate the network connectivity problem.

```
Ruijie# ping ipv6 2000::1
Sending 5, 100-byte ICMP Echoes to 2000::1, 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 example below shows the extension ping ipv6.

```
Ruijie# ping ipv6 2000::1 length 1500 ntimes 100 timeout 3 data ffff source 192::10:
Sending 100, 1500-byte ICMP Echoes to 2000::1, 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
```

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

**Platform Description** N/A

### 8.3 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 ] [ ttl minimum maximum ] [out-interface interface [next-hop next-hop] ] }

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
	<i>next-hop</i>	Specifies the next hop IPv4 address

**Defaults** By default, *seconds* is 3 seconds, *number* is 3, *minimum* and *maximum* are 1 and 255.

**Command** Privileged EXEC mode: enables extended functions.

**Mode** User EXEC mode: enables basic functions.

**Usage Guide** Use the **traceroute** 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 three examples of the application about traceroute, 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# traceroute 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# traceroute 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. When this function is enabled based on 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** N/A  
**Description**

### 8.4 traceroute ipv6

Use this command to display all gateways passed by the test packets from the source address to the destination address.

**traceroute** [ **ipv6** ] { **address** [ **probe number** ] [ **source source** ] [ **timeout seconds** ] [ **tll minimum maximum** ] [ **out-interface** interface [ **next-hop next-hop** ] }

**Parameter Description**

Parameter	Description
<i>address</i>	Specifies an IPv6 address.
<i>number</i>	Specifies the number of probe packets to be sent.
<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.
<i>minimum maximum</i>	Specifies the minimum and maximum TTL values.
<i>interface</i>	Specifies the outbound interface
<i>next-hop</i>	Specifies the next hop IPv6 address

**Defaults** By default, *seconds* is 3 seconds, *number* is 3, *minimum* and *maximum* are 1 and 255.

**Command** Privileged EXEC mode: enables extended functions.

**Mode** User EXEC mode: enables basic functions.

**Usage Guide** Use the **traceroute ipv6** 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 traceroute ipv6, 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# traceroute ipv6 3004::1
< press Ctrl+C to break >
Tracing the route to 3004::1
 1  3000::1      0 msec  0 msec  0 msec
 2  3001::1      4 msec  4 msec  4 msec
 3  3002::1      8 msec  8 msec  4 msec
 4  3004::1      4 msec  28 msec 12 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 3004::1 (gateways 1~4) and the spent time are displayed. Such information is helpful for network analysis.

2. When some gateways in the network fail:

```
Ruijie# traceroute ipv6 3004::1
< press Ctrl+C to break >
Tracing the route to 3004::1
 1  3000::1      0 msec  0 msec  0 msec
 2  3001::1      4 msec  4 msec  4 msec
 3  3002::1      8 msec  8 msec  4 msec
 4  * * *
 5  3004::1      4 msec  28 msec 12 msec
```

The above result clearly shown that the gateways passed by the packets sent to the host with an IP address of 3004::1 (gateways 1~5) and the spent time are displayed, and gateway 4 fails.

**Related Commands**

Command	Description
N/A	N/A

**Platform Description**

N/A

## 9 TCP Commands

### 9.1 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** N/A

## 9.2 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. This command applies to both IPv4 and IPv6 TCP.

**Configuration Examples** The following example sets the upper limit of the MSS value to 1300 bytes.

```
Ruijie(config)# ip tcp mss 1300
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 9.3 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
<b>show tcp pmtu</b>	Shows the PMTU value for the TCP connection.

**Platform Description** N/A

## 9.4 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** N/A

## 9.5 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**

## 9.6 show ipv6 tcp connect

Use this command to display the current IPv6 TCP connection information.

**show ipv6 tcp connect** [ **local-ipv6** X:X:X:X::X ] [ **local-port** num ] [ **peer-ipv6** X:X:X:X::X ] [ **peer-port** num ]

Use this command to display the current IPv6 TCP connection statistics.

**show ipv6 tcp connect statistics**

**Parameter Description**

Parameter	Description
<b>local-ipv6</b> X:X:X:X::X	Local IPv6 address
<b>local-port</b> num	Local port
<b>peer-ipv6</b> X:X:X:X::X	Peer IPv6 address
<b>peer-port</b> num	Peer port
<b>statistics</b>	Displays IPv6 TCP connection statistics

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the current IPv6 TCP connection information.

**Examples**

```
Ruijie# show ipv6 tcp connect
Number Local Address      Foreign Address          State      Process name
1      :::22                   :::0                     LISTEN    rg-sshd
2      :::23                   :::0                     LISTEN    rg-telnetd
3      1000::1:23             1000::2:64201           ESTABLISHED rg-telnetd
```

The following example displays the current IPv6 TCP connection statistics.



```
Ruijie#show ipv6 tcp connect statistics
State      Count
-----
ESTABLISHED 1
SYN_SENT   0
SYN_RECV   0
FIN_WAIT1  0
FIN_WAIT2  0
TIME_WAIT  0
CLOSED     0
CLOSE_WAIT 0
LAST_ACK   0
LISTEN     1
CLOSING    0
Total: 2
```

Related Commands	Command	Description
	N/A	N/A

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

### 9.7 show ipv6 tcp pmtu

Use this command to display information about IPv6 TCP PMTU.

**show ipv6 tcp pmtu** [ **local-ipv6** X:X:X:X::X ] [ **local-port** num ] [ **peer-ipv6** X:X:X:X::X ] [ **peer-port** num ]

Parameter Description	Parameter	Description
		<b>local-ipv6</b> X:X:X:X::X
	<b>local-port</b> num	Local port
	<b>peer-ipv6</b> X:X:X:X::X	Peer IPv6 address
	<b>peer-port</b> num	Peer port

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example information about IPv6 TCP PMTU.

**Examples**

```
Ruijie# show ipv6 tcp pmtu
Number Local Address Foreign Address PMTU
1 1000::1:23 1000::2.13560
```

Field	Description
Number	Number
Local Address	Local address and port number. The number after the last colon is the port number.
Foreign Address	Remote address and port number. The number after the last colon is the port number.
PMTU	Path MTU.

**Related Commands**

Command	Description
N/A	N/A

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

## 9.8 show ipv6 tcp port

Use this command to display the current IPv6 TCP port status.

**show ipv6 tcp port [ num ]**

**Parameter Description**

Parameter	Description
<i>num</i>	Port number

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the current IPv6 TCP port status.

**Examples**

```
Ruijie# show ipv6 tcp port
TCP connections on port 23:
Number Local Address Foreign Address State
1 1000::1:23 1000::2:64571 ESTABLISHED
Total: 1
```

```
TCP connections on port 2650:
Number Local Address Foreign Address State
Total: 0
```

Field	Description
Number	Number
Local Address	Local address and port number.
Foreign Address	Remote address and port number.
State	<p>Current status of the TCP connection. There are eleven possible states:</p> <p>CLOSED: The connection has been closed.</p> <p>LISTEN: Listening state</p> <p>SYNSENT: In the three-way handshake phase when the SYN packet has been sent out.</p> <p>SYNRCVD: In the three-way handshake phase when the SYN packet has been received.</p> <p>ESTABLISHED: The connection has been established.</p> <p>FINWAIT1: The local end has sent the FIN packet.</p> <p>FINWAIT2: The FIN packet sent by the local end has been acknowledged.</p> <p>CLOSEWAIT: The local end has received the FIN packet from the peer end.</p> <p>LASTACK: The local end has received the FIN packet from the peer end, and then sent its own FIN packet.</p> <p>CLOSING: The local end has sent the FIN packet from the peer end, and received the FIN packet from the peer end before the ACK packet for the peer end to respond with this FIN packet is received.</p> <p>TIMEWAIT: The FIN packet sent by the local end has been acknowledged, and the local end has also acknowledged the FIN packet.</p>

**Related Commands**

Command	Description
N/A	N/A

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

## 9.9 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
```

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	Current status of the TCP connection. There are eleven possible states: CLOSED: The connection has been closed. LISTEN: Listening state SYNSENT: In the three-way handshake phase when the SYN packet has been sent out. SYNRCVD: In the three-way handshake phase when the SYN packet has been received. ESTABLISHED: The connection has been established. FINWAIT1: The local end has sent the FIN packet. FINWAIT2: The FIN packet sent by the local end has been

	<p>acknowledged.</p> <p>CLOSEWAIT: The local end has received the FIN packet from the peer end.</p> <p>LASTACK: The local end has received the FIN packet from the peer end, and then sent its own FIN packet.</p> <p>CLOSING: The local end has sent the FIN packet from the peer end, and received the FIN packet from the peer end before the ACK packet for the peer end to respond with this FIN packet is received.</p> <p>TIMEWAIT: The FIN packet sent by the local end has been acknowledged, and the local end has also acknowledged the FIN packet.</p>
Process name	Process name.

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
```

Related Commands	Command	Description
		N/A

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

### 9.10 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
```

**Related Commands**

Command	Description
N/A	N/A

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

## 9.11 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.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<code>ip tcp path-mtu-discovery</code>	Enables the TCP PMTU discovery function.

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

## 9.12 show tcp port

Use this command to display information about the current TCP port.

**show tcp port** [ *num* ]

<b>Parameter Description</b>	<b>Parameter</b>	<b>Description</b>
	<i>num</i>	Port number

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the current IPv4 TCP port status.

```
Ruijie# show 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
```

Description of fields in the command output is as follows:

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**

### 9.13 show tcp statistics

Use this command to show TCP statistics on received packets, three way handshake and time-wait.  
**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 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
```

Description of fields in the command output is as follows:

Field	Description
TCP Packets	Normal packets and error packets
Three way handshake	Three way handshake information, including session request count, server-client connection count, three way handshake failure count caused by Web authentication limit, TCP socket failure count caused by memory shortage, sub-session failure count, packet retransmission count and session failure count caused by retransmission timeout.
Time-wait	Session in TIMEWAIT state

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 10 IPv4/IPv6 REF Commands

### 10.1 clear ipv6 ref packet statistics

Use this command to clear IPv6 REF packet statistics.

**clear ipv6 ref packet statistics**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example clears IPv6 REF packet statistics.

**Examples** Ruijie# clear ipv6 ref packet statistics

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

### 10.2 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 Examples** The following example displays the information about all adjacent nodes in the adjacent node table.

```
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   forward  1    0  192.168.50.78  VLAN 1 00 25 64 C5 9D 6A 00 D0
F8 98 76 54 08 00
7  resolved   forward  1    0  192.168.50.200 VLAN 1 00 04 5F 87 69 66 00 D0
F8 98 76 54 08 00
6  unresolved glean    1    0  0.0.0.0        VLAN 1
4  unresolved local    3    0  0.0.0.0        Local 1
```

Description of fields in the command output is as follows:

Field	Description
id	Adjacent node ID
state	Adjacent node state: Unresolved Resolved
type	Adjacent node type Local: local adjacency Forward: forward adjacency Discard: discard adjacency Glean: glean adjacency Mcast: multicast adjacency
rfct	Reference count of the adjacent node
chg	Whether the adjacent node is on the changing link.
ip	IP address of the adjacent node
interface	Interface
linklayer	Layer 2 head

Related Commands	Command	Description
	<b>show ip ref route</b>	Displays all route information in the current REF module.

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

### 10.3 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 Description	Parameter	Description
	<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 Examples** The following example displays the IPv4 REF exact route from 192.168.217.74 to 192.168.13.1.

```
Ruijie# show ip ref exact-route 192.168.217.74 192.168.13.1
192.168.217.74 --> 192.168.13.1:
id state type rfct chg ip interface linklayer(header
data)
9 resolved forward 1 0 192.168.17.1 VLAN 1 00 25 64 C5 9D 6A 00 D0 F8
98 76 54 08 00
```

Description of fields in the command output is as follows:

Field	Description
id	Adjacency ID
state	Adjacency state: Unresolved Resolved
type	Adjacency type Local: local adjacency Forward: forward adjacency Discard: discard adjacency Glean: glean adjacency Mcast: multicast adjacency

rfct	Reference count of the adjacency
chg	Whether the adjacency is on the changing link.
ip	Adjacency IP address
interface	Interface
linklayer	Layer 2 head

Related Commands	Command	Description
	<b>show ip ref route</b>	Displays all routing information in the current REF module.

**Platform** N/A

**Description**

## 10.4 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**

## 10.5 show ip ref resolve-list

Use this command to display the IPv4 REF resolution information.

**show ip ref resolve-list**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays IPv4 REF resolution information.

#### Examples

```
Ruijie# show ip ref resolve-list
IP                res_state flags interface
1.1.1.1          unres    1     VLAN 1
```

Field	Description
IP	IP address

res_state	unres: unresolved res: resolved
flags	0: related to adjacency 1: unrelated to adjacency
interface	Interface

Related Commands	Command	Description
	N/A	N/A

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

## 10.6 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 VLAN 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 VLAN 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 VLAN 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

## 10.7 show ipv6 ref adjacency

Use this command to display the information about the IPv6 adjacent node.

**show ipv6 ref adjacency** [ **glean** | **local** | *ipv6-address* | **interface** *interface\_type* *interface\_number* | **discard** | **statistics** ]

Parameter	Parameter	Description
<b>Description</b>	<b>glean</b>	Aggregate adjacent node, which is used for a direct route
	<b>local</b>	Local adjacent node, which is used by the local host
	<i>ipv6-address</i>	Next-hop IP address
	<i>interface_type</i>	Interface type
	<i>interface_number</i>	Interface number
	<b>discard</b>	Displays discarded adjacent nodes.
	<b>statistics</b>	Statistics

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command can be used to display the information about the adjacent node table in the privileged EXEC mode and global configuration mode.

**Configuration** The following example displays the information about the IPv6 adjacent node.

**Examples**

```
Ruijie# show ipv6 ref adjacency
id   state      type   rfct chg ip   interface      linklayer(header
data)
1    unresolved  glean  1    0   ::   VLAN 1
2    unresolved  local  2    0   ::1  Local 1
```

Description of fields in the command output is as follows:

Field	Description
id	Adjacent node ID
state	Adjacent node state: Unresolved Resolved
type	Adjacent node type Local: local adjacency Forward: forward adjacency Discard: discard adjacency Glean: glean adjacency Mcast: multicast adjacency
rfct	Reference count of the adjacent node
chg	Whether the adjacent node is on the changing link.
ip	IP address of the adjacent node
interface	Interface
linklayer	Layer 2 head

For distributed routers, id is divided into two fields, namely, gid and lid, standing for global adjacent node ID and local adjacent node ID respectively.

Related	Command	Description
Commands	N/A	N/A

**Platform** N/A

**Description**

## 10.8 show ipv6 ref exact-route

This command is used to display the IPv6 REF exact route.

**show ipv6 ref exact-route** *source-ipv6-address destination-ipv6-address*

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

<b>Description</b>	<i>source-ipv6-address</i>	Source IP address of the packet
	<i>destination-ipv6-address</i>	Destination IP address of the packet

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the IPv4 REF exact route from 2001:db8:1::1 to 3001:db8:2::2.

```
Ruijie# show ipv6 exact-route 2001:db8:1::1 3001:db8:2::2
2001:db8:1::1 --> 3001:db8:2::2:
ID state      type      rfct chg ip interface      linklayer(header data)
3  unresolve  glean    1    0  :: VLAN 1
```

Description of fields in the command output is as follows:

Field	Description
id	Adjacent node ID
state	Adjacent node state: Unresolved Resolved
type	Adjacent node type Local: local adjacency Forward: forward adjacency Discard: discard adjacency Glean: glean adjacency Mcast: multicast adjacency
rfct	Reference count of the adjacent node
chg	Whether the adjacent node is on the changing link.
ip	IP address of the adjacent node
interface	Interface
linklayer	Layer 2 head

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 10.9 show ipv6 ref packet statistics

Use this command to display IPv6 REF packet statistics.

**show ipv6 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 IPv6 REF packet statistics.

**Examples** Ruijie# show ipv6 ref packet statistics

```

ref packet statistic:
  bad head      : 0
  lookup fib fail : 0
  local adj     : 0
  glean adj     : 0
  forward       : 0
  redirect      : 0
  hop-limit expiration : 0
  no ipv6 unicast-routing : 0

```

Field	Description
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**

## 10.10 show ipv6 ref resolve-list

This command is used to display the IPv6 REF resolution information.

**show ipv6 ref resolve-list**

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 IPv6 REF resolution information.

```
Ruijie#show ipv6 ref resolve-list
IP          res_state flags interface
1000::1    unres     1     VLAN 1
```

Field	Description
IP	IPv6 address
res_state	unres: unresolved res: resolved
flags	0: related to adjacency 1: unrelated to adjacency
interface	Interface

Related Commands	Command	Description
	N/A	N/A

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

## 10.11 show ipv6 ref route

Use this command to display all the routing information in the IPv6 REF table.

**show ipv6 ref route [ default | statistics | *prefix/len* ]**

Parameter Description	Parameter	Description
	<b>default</b>	Specifies the default route.
	<b>statistics</b>	Statistics
	<i>prefix/len</i>	Displays the route with the specified prefix (X:X:X:X:<0-128>).

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is used to display all routing information in the IPv6 REF table.

**Configuration** The following example displays all the routing information in the REF IPv6 table.

**Examples**

```
Ruijie#show ipv6 ref route
Codes: * - default route
prefix/len          weight path_id next_hop interface
2001:da8:ffe:2::/64      1      3      ::      VLAN 1
2001:da8:ffe:2::3/128   1      2      :::1    Local 1
fe80::/10             1      6      ::      Null 0
fe80::21a:a9ff:fe3b:fa41/128 1      2      :::1    Local 1
```

Field	Description
prefix/len	IPv6 prefix and prefix length.
path-id	Adjacent identity
next-hop	Address of next hop
weight	Routing weight
interface	Interface

Related Commands	Command	Description
	N/A	N/A



## IP Routing Configuration Commands

---

1. RIP Commands(beta)
2. RIPng Commands(beta)
3. NSM Commands(beta)
4. Keys(beta)
5. Routing Policies(beta)

# 1 RIP Commands(beta)

## 1.1 auto-summary

Use this command to enable automatic summary of RIP routes. Use the **no** form of this command to disable this function

**auto-summary**  
**no auto-summary**

**Parameter Description**

Parameter	Description
N/A	N/A

**Defaults**

Automatic summary of RIP routes is enabled by default

**Command Mode**

Routing progress configuration mode


**Usage Guide**

Automatic RIP route summary means the subnet routes will be automatically summarized into the routes of the classified network when they traverse through the subnet. Automatic route summary is enabled by default for RIPv1 and RIPv2.

Automatic RIP route summary improves the flexibility and effectiveness of the network. If the summarized route exists, the sub-routes contained in the summarized route cannot be seen in the routing table, reducing the size of the routing table significantly.

Advertising the summarized route is more efficient than advertising individual routes in light of the following factors:

- The summarized route is always processed preferentially when you query the RIP database.
- Any sub-route is ignored when you query the RIP database, reducing the processing time.
- If you want to learn the specific sub-routes instead of the summarized route, disable the automatic route summary function. Only when RIPv2 is configured, the automatic route summary function can be disabled. For the RIPv1, the automatic route summary function is always enabled.

 The range of the supernet route is wider than that of the classful network. Therefore, this command takes no effect on the supernet route.

**Configuration**

The following example disables automatic route summary of RIPv2.

**Examples**

```
Ruijie (config)# router rip
Ruijie (config-router)# version 2
Ruijie (config-router)# no auto-summary
```

**Related**

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



<b>Commands</b>	
<b>version</b>	Defines the RIP software versions: v1 or v2. Both v1 and v2 are supported by default.

**Platform** N/A

**Description**

## 1.2 default-information originate

Use this command to generate a default route in the RIP process. Use the **no** form of this command to delete the generated default route.

**default-information originate** [ **always** | **metric** *metric-value* | **route-map** *route-map-name* ] \*

**no default-information originate** [ **always** | **metric** *metric-value* | **route-map** *route-map-name* ] \*

Parameter Description	Parameter	Description
	<b>always</b>	(Optional) Enables RIP to generate the default route, no matter whether the default route exists or not.
	<b>metric</b> <i>metric-value</i>	(Optional) Sets the original metric value of the default route with the value ranging from 1 to 15.
	<b>route-map</b> <i>map-name</i>	(Optional) Indicates the name of the associated route-map. Route-map is not associated by default.

**Defaults** No default route is generated by default.  
The default metric value is 1.

**Command**


**Mode** Routing process configuration mode


**Usage Guide** By default, RIP will not advertise the default route if the default route exists in the routing table of the router. In this case, use the **default-information originate** command to notify the neighbor of the default route.

With the parameter **always** configured, no matter whether the default route exists in the RIP routing process or not, the default route will be advertised to the neighbor but is not shown in the local routing table. You can use the **show ip rip database** command to view the RIP routing information database to confirm whether the default route is generated.

Use the parameter **route-map** to control more about the default route advertised to RIP. For example, use the **set metric** command to set the metric value of the default route.

The route-map set metric rule takes precedence over the parameter metric value configuration of the default route. If the parameter metric is not configured, the default metric value is used by the default route.

 If the default route can be generated in the RIP process by using this command, RIP will not learn the default route advertised from the neighbor.

-  For the default route generated by using the `ip default-network` command, the `default-information originate` command is required to add the default route to RIP.

**Configuration** The following example generates a default route to the RIP routing table.

**Examples**

```
Ruijie(config-router)# default-information originate always
```

**Related Commands**

Command	Description
<code>ip rip default-information</code>	Notifies the default route through an interface.
<code>redistribute</code>	Redistributes the routes from other protocols to RIP.

**Platform** N/A

**Description**

## 1.3 default-metric

Use this command to define the default RIP metric value. Use the **no** form of this command to restore the default setting.

**default-metric** *metric-value*

**no default-metric**

**Parameter Description**

Parameter	Description
<i>metric-value</i>	Indicates the default metric value with the range from 1 to 16. If the metric value is greater than or equal to 16, the RGNOS regards the route unreachable.

**Defaults** The default is 1.

**Command**

**Mode** Routing process configuration mode

**Usage Guide**

This command needs to work with the command **redistribute**. When the routes are redistributed to the RIP routing process from a routing protocol process, the route metric value cannot be converted due to the incompatibility of the metric calculation mechanisms for different protocols. During the conversion, therefore, it is required to redefine the metric values of redistributed routes in the RIP routing domain. If there is no clear definition of the metric value in redistributing a routing protocol process, the RIP uses the metric value defined with **default-metric**. If the metric value is defined, this value overwrites the metric value defined with `default-metric`. If this command is not configured, the default value of `default-metric` is 1.

**Configuration Examples** The following example enables the RIP routing protocol to redistribute the routes learned by the static routing protocol, whose initial RIP metric value is set to 3.

```
Ruijie (config)# router rip
```

```
Ruijie (config-router)# default-metric 3
Ruijie (config-router)# redistribute static
```

**Related  
Commands**

Command	Description
<b>redistribute</b>	Redistributes the routes from one routing domain to another routing domain.

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

## 1.4 distance

Use this command to set the management distance of the RIP route. Use the **no** form of this command to restore the default setting.

**distance** *distance* [ *ip-address wildcard* ]

**no distance** [ *distance ip-address wildcard* ]

**Parameter  
Description**

Parameter	Description
<i>distance</i>	Sets the management distance of a RIP route, an integer in the range from 1 to 255.
<i>ip-address</i>	Indicates the prefix of the source IP address of the route.
<i>wildcard</i>	Defines the comparison bit of the IP address, where 0 means accurate matching and 1 means no comparison.

**Defaults** The default is 120.**Command****Mode** Routing process configuration mode**Usage Guide**

Use this command to set the management distance of the RIP route.

You can use this command to create several management distances with source address prefixes.

When the source address of the RIP route is within the range specified by the prefixes, the corresponding management distance is applied; otherwise, the route uses the management distance configured by the RIP.

**Configuration** The following example sets the management distance of the RIP route to 160, and specifies the**Examples** management distance of the route learned from 192.168.2.1 as 123.

```
Ruijie(config)# router rip
Ruijie(config-router)# distance 160
Ruijie(config-router)# distance 123 192.168.12.1 0.0.0.0
```

**Related  
Commands**

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

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

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

### 1.5 distribute-list in

Use this command to control route update for route filtering. Use the **no** form of this command to restore the default setting.

**distribute-list** { [ *access-list-number* | *name* ] | [ **prefix** *prefix-list-name* ] [ **gateway** *prefix-list-name* ] }  
**in** [ *interface-type* *interface-number* ]

**no distribute-list** { [ *access-list-number* | *name* ] | [ **prefix** *prefix-list-name* ] [ **gateway** *prefix-list-name* ] } **in** [ *interface-type* *interface-number* ]

**Parameter Description**

Parameter	Description
<i>access-list-number</i>   <i>name</i>	Specifies the ACL. Only the routes that are allowed by the ACL can be accepted.
<b>prefix</b> <i>prefix-list-name</i>	Uses the prefix list to filter the routes.
<b>gateway</b> <i>prefix-list-name</i>	Uses the prefix list to filter the source of the routes.
<i>interface-type</i> <i>interface-number</i>	(Optional) Applies the distribution list only to a specified interface.

**Defaults** The distribution list is not defined by default.

**Command Mode** Routing process configuration mode

**Usage Guide** To deny receiving some specified routes, you can process all the received route update packets by configuring the route distribute control list.  
 Without any interface specified, the system will process the route update packets received on all the interfaces.

**Configuration Examples** The following example enables RIP to control the routes received from the GigabitEthernet 0/17, only permitting the routes starting with 172.16.0.0/16.

```
Ruijie (config)# router rip
Ruijie (config-router)# network 200.168.23.0
Ruijie (config-router)# distribute-list 10 in GigabitEthernet 0/17
Ruijie (config-router)# no auto-summary
Ruijie (config-router)# access-list 10 permit 172.16.0.0 0.0.255.255
```

**Related Commands**

Command	Description
<b>access-list</b>	Defines the ACL rule.
<b>prefix-list</b>	Defines the prefix list.

**Platform** N/A

**Description**

## 1.6 distribute-list out

Use this command to control route update advertisement for filtering routes. Use the **no** form of this command to restore the default setting.

**distribute-list** { [ *access-list-number* | *name* ] | **prefix** *prefix-list-name* } **out** [ *interface-type* | *interface-number* | **connected** | **rip** | **static** ]

**no distribute-list** { [ *access-list-number* | *name* ] | **prefix** *prefix-list-name* } **out** [ *interface* | **connected** | **rip** | **static** ]

**Parameter Description**

Parameter	Description
<i>access-list-number</i>   <i>name</i>	Specifies the ACL.
<b>prefix</b> <i>prefix-list-name</i>	Uses the prefix list to filter routes.
<i>interface</i>	(Optional) Applies route update advertisement control to a specified interface in the distribution list.
<b>connected</b>	(Optional) Applies route update advertisement control to only connected routes in this distribution list.
<b>rip</b>	(Optional) Applies route update advertisement control to only RIP routes in this distribution list.
<b>static</b>	(Optional) Applies route update advertisement control to only static routes in this distribution list.

**Defaults** No route update advertisement is configured by default.

**Command**

**Mode** Routing process configuration mode

**Usage Guide** If this command relates to none of optional parameters, route update advertisement control applies to all interfaces. If this command relates to interface options, route update advertisement control applies to only the specified interface. If this command relates to other route process parameters, route update advertisement control applies to only the specific route process.

**Configuration** The following example advertises only the 192.168.12.0/24 route.

**Examples**

```
Ruijie (config)# router rip
Ruijie (config-router)# network 200.4.4.0
Ruijie (config-router)# network 192.168.12.0
Ruijie (config-router)# distribute-list 10 out
Ruijie (config-router)# version 2
Ruijie (config-router)#access-list 10 permit 192.168.12.0 0.0.0.255
```

**Related**

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

Commands	
<b>access-list</b>	Defines the ACL rule.
<b>prefix-list</b>	Defines the prefix list.
<b>redistribute</b>	Configures route redistribution.

Platform N/A

Description

Platform N/A

Description

## 1.7 enable mib-binding

Use this command to bind a MIB with a specified RIP instance. Use the **no** form of this command to restore the default setting.

**enable mib-binding**

**no enable mib-binding**

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command

Mode Routing process configuration mode.

**Usage Guide** As RIP MIB does not have RIP instance information, you can only operate only one RIP instance using SNMP.

**Configuration** The following example operates the RIP instance.

**Examples**

```
Ruijie(config)# router rip
Ruijie(config-router)# enable mib-binding
```

Related Commands	Command	Description
	<b>show ip rip</b>	Displays the global configuration of RIP.

Platform N/A

Description

## 1.8 graceful-restart

Use this command to configure the RIP graceful restart (GR) function for a device. Use the **no** form of this command to restore the default configuration.

**graceful-restart [ grace-period *grace-period* ]**

**no graceful-restart [ grace-period ]**

Parameter Description	Parameter	Description
	<b>grace-period</b>	(Optional) Configures the grace period.
	<i>grace-period</i>	(Optional) Indicates the user-defined GR period. The default value is the smaller value between twice the update time and 60 seconds. The range is from 1 to 1,800. The unit is second.

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

### Command

**Mode** Routing process configuration mode

**Usage Guide** The GR function is configured on the RIP instances. Different parameters can be configured for different RIP instances.

The GR period refers to the time from the startup to the end of RIP GR. During this period, the forwarding table remains unchanged and the RIP route is restored to the state before protocol restart. When the GR period expires, RIP exits the GR state and performs normal RIP operation.

The **graceful-restart grace-period** command enables users to modify GR period. Note: Make sure that GR is completed before the RIP route is validate and after an RIP route update cycle elapses. If an improper value is configured, non-stop data forwarding cannot be ensured during the GR process. For example, if the GR period is longer than the time when the neighbor's route is unavailable and GR is not completed before the route is validated, then the neighbor is not re-informed of the route and forwarding of the neighbor's route is terminated when it is validated, which results in data forwarding interruption. Therefore, unless otherwise specified, it is not recommended to adjust the GR period. If the period needs to changed, determine that the grace period is longer than the route update cycle and shorter than the time when the route is unavailable in combination with the configuration of the **timers basic** command.

 During the RIP GR period, the network must be stable.

**Configuration Examples** The following example enables the RIP GR function and configures the GR period parameters of the GR function.

```
Ruijie(config)# router rip
Ruijie(config-router)# graceful-restart grace-period 90
```

### Related Commands

Command	Description
<b>timers basic</b>	Configures RIP timers.

**Platform Description** N/A

## 1.9 ip rip authentication key-chain

Use this command to enable RIP authentication and specify the keychain used for RIP authentication.

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

**ip rip authentication key-chain** *name-of-keychain*

**no ip rip authentication key-chain**

Parameter Description	Parameter	Description
	<i>name-of-keychain</i>	Indicates the name of the keychain, which specifies the keychain used for RIP authentication.

**Defaults** The keychain is not associated by default.

### Command

**Mode** Interface configuration mode

**Usage Guide** If the keychain is specified in the interface configuration, use the key chain global configuration command to define the keychain. Otherwise, RIP data packet authentication fails. RIPv2 instead of RIPv1 supports authentication of the RIP data packet.

**Configuration Examples** The following example enables RIP authentication on the vlan 1 with the associated keychain ripchain.

```
Ruijie(config)#interface vlan 1
Ruijie(config-if-VLAN 1)#ip rip authentication key-chain ripchain
```

Meanwhile, use the **key chain** command to define this keychain in global configuration mode.

```
Ruijie(config)#key chain ripchain
Ruijie(config-keychain)#key 1
Ruijie(config-keychain-key)#key-string Hello
```

Related Commands	Command	Description
	<b>ip rip authentication mode</b>	Defines the RIP authentication mode.
	<b>ip rip authentication text-password</b>	Enables RIP authentication, and sets the password string of RIP plaintext authentication. RIP data packet authentication is supported only by RIPv2.
	<b>ip rip receive version</b>	Defines the version of RIP packets received on the interface.
	<b>ip rip send version</b>	Defines the version of RIP packets sent on the interface.
	<b>key chain</b>	Defines the keychain and enters keychain configuration mode.



**Platform** N/A

**Description**

## 1.10 ip rip authentication mode

Use this command to define the RIP authentication mode. Use the **no** form of this command to restore the default setting.

**ip rip authentication mode { text | md5 }**

**no ip rip authentication mode**

Parameter Description	Parameter	Description
	<b>text</b>	Configures RIP authentication as plaintext authentication.
	<b>md5</b>	Configures RIP authentication as MD5 authentication.

**Defaults** It is plaintext authentication by default.

**Command**

**Mode** Interface configuration mode

**Usage Guide** During the RIP authentication configuration process, the RIP authentication modes of all devices requiring exchange of RIP routing information must be the same. Otherwise, RIP packet exchange will fail.

If the plaintext authentication mode is adopted, but the password string of the plaintext authentication or the associated keychain is not configured, no authentication occurs. In the same way, if the MD5 authentication mode is adopted, but the associated keychain is not configured, no authentication occurs.

RIPv2 instead of RIPv1 supports authentication of the RIP data packet.

**Configuration** The following example configures the RIP authentication mode on the vlan 1 as MD5.

**Examples**

```
Ruijie (config)#interface vlan 1
Ruijie (config-if-VLAN 1)# ip rip authentication mode md5
```

Related Commands	Command	Description
	<b>ip rip authentication key-chain</b>	Enables the RIP authentication mode and specifies the keychain used for RIP authentication. Only RIPv2 supports authentication of the RIP data packet.
	<b>ip rip authentication text-password</b>	Enables the RIP authentication mode, and sets the password string of RIP plaintext authentication. Only RIPv2 supports authentication of the RIP data packet.
	<b>key chain</b>	Defines the keychain and enters the keychain configuration mode

**Platform** N/A

**Description**

## 1.11 ip rip authentication text-password

Use this command to enable RIP authentication and set the password string of RIP plaintext authentication. Use the **no** form of this command to restore the default setting.

**ip rip authentication text-password** [ 0 | 7 ] *password-string*

**no ip rip authentication text-password**

Parameter Description	Parameter	Description
	0	Specifies that the key is displayed as plaintext.
	7	Specifies that the key is displayed as cipher text.
	<i>password-string</i>	Indicates the password string of the plaintext authentication, in the length of 1-16 bytes.

**Defaults** No password string of RIP plaintext authentication is configured by default.

**Command**

**Mode** Interface configuration mode

**Usage Guide** This command works only in plaintext authentication mode.

To enable the RIP plaintext authentication function, use this command to configure the corresponding password string, or use the associated key chain to obtain the password string. The latter takes the precedence over the former one.

RIPv1 does not support RIP authentication but RIPv2 does.

**Configuration Examples** The following example enables the RIP plaintext authentication on vlan 1 and sets the password string to hello.

```
Ruijie(config)#interface vlan 1
Ruijie(config-if-VLAN 1)# ip rip authentication text-password hello
```

Related Commands	Command	Description
	<b>ip rip authentication mode</b>	Defines the RIP authentication mode.
	<b>ip rip authentication key-chain</b>	Enables the RIP authentication mode and specifies the keychain used for RIP authentication. Only RIPv2 supports authentication.

**Platform** N/A

**Description**

## 1.12 ip rip default-information

Use this command to advertise the default route through a RIP interface. Use the **no** form of this command to restore the default setting.

**ip rip default-information** { **only** | **originate** } [ **metric** *metric-value* ]

**no ip rip default-information**


Parameter Description	Parameter	Description
	<b>only</b>	Notifies the default route rather than other routes.
	<b>originate</b>	Notifies the default route and other routes.
	<b>metric</b> <i>metric-value</i>	Specifies the metric value of the default route, in the range from 1 to 15.

**Defaults** No default route is configured by default. The default metric value is 1.

### Command

**Mode** Interface configuration mode

**Usage Guide** After you configure this command on a specified interface, a default route is generated and notified through the interface. If the **ip rip default-information** command of the interface and the **default-information originate** command of the RIP process are configured at the same time, only the default route of the interface is advertised.

 RIP will no longer learn the default route notified by the neighbor if any interface is configured with the **ip rip default-information** command.

**Configuration** The following example creates a default route which is notified on vlan 1 only.

### Examples

```
Ruijie(config)#interface vlan 1
Ruijie(config-if-VLAN 1)#ip rip default-information only
```

Related Commands	Command	Description
	<b>default-information originate</b>	Generates a default route in the RIP process.

**Platform** N/A

### Description

## 1.13 ip rip receive enable

Use this command to enable RIP to receive the RIP data package on a specified interface. Use the **no** form of this command to restore the default setting.

**ip rip receive enable**

**no ip rip receive enable**

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

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

**Defaults** RIP packages can be received through the interface by default.

**Command**

**Mode** Interface configuration mode

**Usage Guide** To prevent an interface from receiving RIP packets, use the **no** form of this command in interface configuration mode. This command works on interfaces configured with this command. You can use the **default** form of this command to enable the interface to receive the RIP data package.

**Configuration** The following example prohibits receiving RIP data packages on vlan 1.

**Examples**

```
Ruijie (config)# interface vlan 1
Ruijie (config-if-VLAN 1)# no ip rip receive enable
```

<b>Related Commands</b>	Command	Description
	<b>ip rip send enable</b>	Enables or disables the interface to send RIP data packages.
	<b>passive-interface</b>	Configures a passive RIP interface.

**Platform** N/A

**Description**

## 1.14 ip rip receive version

Use this command to define the version of RIP packets received on an interface. Use the **no** form of this command to restore the default setting.

**ip rip receive version** [ 1 | 2 ]

**no ip rip receive version**

<b>Parameter Description</b>	Parameter	Description
	<b>1</b>	(Optional) Receives only RIPv1 packets.
	<b>2</b>	(Optional) Receives only RIPv2 packets.

**Defaults** The default behavior depends on the configuration with the version command.

**Command**

**Mode** Interface configuration mode

**Usage Guide** This command overwrites the default configuration of the **version** command. It affects only RIP packet receiving through the interface and allows RIPv1 and RIPv2 packets to be received on the interface at the same time. If the command is configured without parameters, data package receiving

depends on the configuration of the version.

**Configuration** The following example enables receiving both RIPv1 and RIPv2 data packages.

**Examples**

```
Ruijie(config)# interface vlan 1
Ruijie(config-if-VLAN 1)# ip rip receive version 1 2
```

**Related  
Commands**

Command	Description
<b>version</b>	Defines the default version of the RIP packets received/sent on the interface.

**Platform** N/A

**Description**

## 1.15 ip rip send enable

Use this command to enable RIP to send a RIP data package on a specified interface. Use the **no** form of this command to restore the default setting.

**ip rip send enable**

**no ip rip send enable**

**Parameter  
Description**

Parameter	Description
N/A	N/A

**Defaults** RIP packages can be sent through the interface by default.

**Command**

**Mode** Interface configuration mode

**Usage Guide** To prevent an interface from sending RIP packets, use the **no** form of this command in interface configuration mode. This command works on interfaces configured with this command. You can use the **default** form of this command to enable the interface to send the RIP data package.

**Configuration** The following example prohibits sending RIP data packages on vlan 1.

**Examples**

```
Ruijie(config)# interface vlan 1
Ruijie(config-if-VLAN 1)# no ip rip send enable
```

**Related  
Commands**

Command	Description
<b>ip rip receive enable</b>	Enables or disables receiving RIP packets on the interface.
<b>passive-interface</b>	Configures a passive RIP interface.

**Platform** N/A

**Description**

## 1.16 ip rip send supernet-routes

Use this command to enable RIP to send the supernet route on a specified interface. Use the **no** form of this command to disable this function.

**ip rip send supernet-routes**

**no ip rip send supernet-routes**


Parameter Description	Parameter	Description
	N/A	N/A

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

**Command**

**Mode** Interface configuration mode

**Usage Guide** When the RIPv1 router monitors a RIPv2 router response packet and if the supernet routing information is monitored, incorrect route information is learned because the RIPv1 ignores the subnet mask of the routing information. In this case, you are advised to use the no form of this command on the RIPv2 router to disable advertising the supernet route on the corresponding interface. This command works only on interfaces configured with this command.

 This command is only valid upon sending the RIPv2 packets on the interface and it is used to control sending the supernet route.

**Configuration** The following example disables sending RIP supernet routes on the vlan 1 interface.

```
Ruijie(config)# interface vlan 1
Ruijie(config-if-VLAN 1)# no ip rip send supernet-routes
```

Related Commands	Command	Description
	<b>version</b>	Defines the RIP version
	<b>ip rip send enable</b>	Enables or disables sending the RIP package on the interface.

**Platform** N/A

**Description**

## 1.17 ip rip send version

Use this command to define the version of the RIP packets sent on the interface. Use the **no** form of this command to restore the default setting.

**ip rip send version [ 1 | 2 ]**

**no ip rip send version**

Parameter Description	Parameter	Description
	1	(Optional) Receives only RIPv1 packets.
	2	(Optional) Receives only RIPv2 packets.

**Defaults** The default behavior depends on the configuration with the version command.

**Command**

**Mode** Interface configuration mode

**Usage Guide** This command overwrites the default configuration of the **version** command. It affects only RIP packet sending through the interface and allows RIPv1 and RIPv2 packages sent on the interface at the same time. If the command is configured without parameters, package receiving depends on the configuration of the version.

**Configuration** The following example enables sending both RIPv1 and RIPv2 packages on the VLAN 1 interface.

**Examples**

```
Ruijie (config)# interface vlan 1
Ruijie (config-if-VLAN 1)# ip rip send version 1 2
```

**Related Commands**

Command	Description
<b>version</b>	Defines the default version of the RIP packets received/sent on the interfaces.

**Platform** N/A

**Description**

## 1.18 ip rip split-horizon

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

**ip rip split-horizon [ poisoned-reverse ]**

**no ip rip split-horizon [ poisoned-reverse ]**

Parameter Description	Parameter	Description
	<b>poisoned-reverse</b>	(Optional) Enables split horizon with poisoned reverse.

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

**Command**

**Mode** Interface configuration mode

**Usage Guide** When multiple devices are connected to the IP broadcast network and run a distance vector routing

protocol, the split horizon mechanism is required to prevent loop. The split horizon prevents the device from advertising routing information from the interface that learns that information, which optimizes routing information exchange between multiple devices.

For non-broadcast multi-path access networks (such as frame relay and X.25), split horizon may cause some devices to be unable to learn all routing information. Split horizon may need to be disabled in this case. If an interface is configured the secondary IP address, attentions shall be paid also for split horizon.

If the **poisoned-reverse** parameter is configured, split horizon with poisoned reverse is enabled. In this case, devices still advertise the route information through the interface from which the route information is learned. However, the metric value of the route information is set to unreachable.

The RIP routing protocol is a distance vector routing protocol, and the split horizon issue shall be cautioned in practical applications. If it is unsure whether split horizon is enabled on the interface, use the show ip rip command to judge. This function makes no influence on the neighbor defined with the **neighbor** command.

**Configuration** The following example disables the RIP split horizon function on the interface vlan 1.

**Examples**

```
Ruijie (config)# interface vlan 1
Ruijie (config-if-VLAN 1)# no ip rip split-horizon
```

**Related Commands**

Command	Description
<b>neighbor (RIP)</b>	Defines the IP address of the neighbor of RIP.
<b>validate-update-source</b>	Enables the source address authentication of the RIP route update message.

**Platform** N/A

**Description**

## 1.19 ip rip summary-address

Use this command to configure port-level convergence through an interface. Use the **no** form of this command to disable this function.

**ip rip summary-address** *ip-address ip-network-mask*

**no ip rip summary-address** *ip-address ip-network-mask*

**Parameter Description**

Parameter	Description
<i>ip-address</i>	Indicates the IP addresses to be converged.
<i>ip-network-mask</i>	Indicates the subnet mask of the specified IP address for route convergence.


**Defaults** The RIP routes are automatically converged to the classful network edge by default.

**Command**

**Mode** Interface configuration mode



**Usage Guide** The **ip rip summary-address** command converges an IP address or a subnet on a specified port. RIP routes are automatically converged to the classful network edge. The classful subnet can be configured through only port convergence.

 The summary range configured by this command cannot be a super class network, that is, the configured mask length is greater than or equal to the natural mask length of the network.

**Configuration Examples** The following example disables the automatic route convergence function of RIPv2. Interface convergence is configured so that vlan 1 advertises the converged route 172.16.0.0/16.

```
Ruijie (config)# interface vlan 1
Ruijie (config-if-VLAN 1)# ip rip summary-address 172.16.0.0 255.255.0.0
Ruijie (config-if-VLAN 1)# ip address 172.16.1.1 255.255.255.0
Ruijie (config)# router rip
Ruijie (config-router)# network 172.16.0.0
Ruijie (config-router)# version 2
Ruijie (config-router)# no auto-summary
```

**Related Commands**

Command	Description
<b>auto-summary</b>	Enables the automatic convergence of RIP routes.

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

## 1.20 ip rip triggered

Use this command to enable triggered RIP based on links. Use the **no** form of this command to restore the default setting.

**ip rip triggered** [ **retransmit-count** *count* | **retransmit-timer** *timer* ]  
**no ip rip triggered** [ **retransmit-count** | **retransmit-timer** ]

**Parameter Description**

Parameter	Description
<b>retransmit-count</b> <i>count</i>	Configures the maximum number of times Update Request and Update Response packets are retransmitted. The range is from 1 to 3600. The default is 36.
<b>retransmit-timer</b> <i>timer</i>	Configures the interval at which the Update Request and Update Response packets are retransmitted. The range is from 1 to 3,600, in seconds. The default is 5.

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

**Command** Interface configuration mode


**Mode**


**Usage Guide** Triggered RIP (TRIP) is the extension of RIP on the wide area network (WAN), mainly used for demand-based links.


With the TRIP function enabled, RIP no longer sends route updates periodically and sends route updates to the WAN interface only if:


- Update Request packets are received.
- RIP routing information is changed.
- Interface state is changed.
- The router is started.


As periodical RIP update is disabled, the confirmation and retransmission mechanism is required to ensure that update packets are sent and received successfully over the WAN. The **retransmit-timer** and **retransmit-count** commands can be used to specify the retransmission interval and maximum retransmission times for request and update packets.


 The function can be enabled in the case of the following conditions: a) The interface has only one neighbor. b) There are multiple neighbors but they interact information using unicast packets. You are advised to enable the function for link layer protocols such as PPP, frame relay, and X.25.

 You are advised to enable split horizon with poison reverse on the interface enabled with the function; otherwise invalid routing information might be left.

 Make sure that the function is enabled on all routers on the same link; otherwise the function will be invalid and the routing information cannot be exchanged correctly.

 The function cannot be enabled at the same time with BFD and RIP functions.

 To enable the function, make sure that the RIP configuration is the same on both ends of the link, such as RIP authentication and the RIP version supported by the interface.

 If this function is enabled on this interface, the source address of packets on this interface will be checked no matter whether the source IP address verification function (validate-update-source) is enabled.

**Configuration Examples** The following example enables TRIP and sets the retransmission interval and the maximum number of retransmission times to 10 seconds and 18 respectively for Update Request and Update Response packets.

```
Ruijie(config)# interface vlan 1
Ruijie(config-if-VLAN 1)# ip rip triggered
Ruijie(config-if-VLAN 1)# ip rip triggered retransmit-timer 10
Ruijie(config-if-VLAN 1)# ip rip triggered retransmit-count 18
```

**Related Commands**

Command	Description
<b>show ip rip database</b>	Displays the summarized routing information of the RIP database.

<b>show ip rip interface</b>	Displays the RIP interface information.
<b>ip rip split-horizon</b>	Configures RIP split horizon.

**Platform** N/A

**Description**

## 1.21 ip rip v2-broadcast

Use this command to send RIPv2 packets in broadcast rather than multicast mode. Use the **no** form of this command to restore the default setting.

**ip rip v2-broadcast**

**no ip rip v2-broadcast**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** By default, RIPv2 packets are sent in multicast mode on the interface.

**Command**

**Mode** Interface configuration mode

**Usage Guide** If the links or neighbors do not support multicast, configure RIPv2 packets to be sent in broadcast mode.

**Configuration Examples** # The following example sends RIPv2 packets in broadcast mode instead of multicast mode on the Layer 3 Ethernet interface.

```
Ruijie(config)# interface vlan 1
Ruijie(config-if-VLAN 1)# ip rip v2-broadcast
```

Related Commands	Command	Description
	<b>show ip rip interface</b>	Displays the RIP interface information.

**Platform** N/A

**Description**

## 1.22 neighbor

Use this command to define the IP address of a RIP neighbor. Use the **no** form of this command to restore the default setting.

**neighbor ip-address**

**no neighbor ip-address**

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

<i>ip-address</i>	Indicates the IP address of the neighbor. The IP address must be that of the network connected to the local device.
-------------------	---

**Defaults** The neighbor is not defined by default.

**Command**

**Mode** Routing process configuration mode

**Usage Guide** By default, RIPv1 uses the IP broadcast address (255.255.255.255) to advertise routing information, and RIPv2 uses the multicast address 224.0.0.9 to do so. If you do not want to allow all the devices on the broadcast network or non-broadcast multi-path access network to receive routing information, use the **passive-interface** command to configure related interfaces as passive interfaces and then define only some neighbors who can receive the routing information. This command has no impact on the receiving of RIP information. The passive interface is configured. No request packet is sent after the interface is enabled.

**Configuration** The following RIP advertises routing information to neighbor IP address 192.168.1.2 only.

```
Ruijie(config)# router rip
Ruijie(config-router)# passive-interface default
Ruijie(config-router)# neighbor 192.168.1.2
```

**Related Commands**

Command	Description
<b>passive-interface</b>	Configures the interface as a passive interface.

**Platform** N/A

**Description**

## 1.23 network

Use this command to define the list of networks to be advertised in the RIP routing process. Use the **no** form of this command to delete the defined network.

**network** *network-number* [ *wildcard* ]

**no network** *network-number* [ *wildcard* ]

**Parameter Description**

Parameter	Description
<i>network-number</i>	Indicates the network number of the directly-connected network. The network number is a natural one. All interfaces whose IP addresses belong to that natural network can send/receive RIP packages.
<i>wildcard</i>	Defines the IP address comparing bit: 0 refers to accurate matching, and 1 refers to no comparison.

**Defaults** N/A

**Command**

**Mode** Routing process configuration mode

**Usage Guide** The *network-number* and *wildcard* parameters can be configured simultaneously to enable the IP address of the interface within the IP address range to join RIP running. Without the *wildcard* parameter, RGOS make the interface IP address within the classful address range join the RIP running. Only when the IP address of an interface is in the network list defined by RIP, RIP route update packets can be received and sent on the interface.

**Configuration Examples** The following example defines two network numbers associated with RIP and allows the interface IP address between 192.168.12.0/24 and 172.16.0.0/24 to join RIP running.

```
Ruijie (config)# router rip
Ruijie (config-router)# network 192.168.12.0
Ruijie(config-router)# network 172.16.0.0 0.0.0.255
```

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 1.24 offset-list

Use this command to increase the metric value of received or sent RIP routes. Use the **no** form of this command to restore the default setting.

**offset-list** { *access-list-number* | *name* } { **in** | **out** } *offset* [ *interface-type interface-number* ]

**no offset-list** { *access-list-number* | *name* } { **in** | **out** } *offset* [ *interface-type interface-number* ]

**Parameter Description**

Parameter	Description
<i>access-list-number</i>   <i>name</i>	Specifies the ACL.
<b>in</b>	Modifies the metric of the received routes using the ACL.
<b>out</b>	Modifies the metric of the sent routes using the ACL.
<i>offset</i>	Indicates the offset of changed metric values. The value is in the range from 0 to 16.
<i>interface-type</i>	Applies the ACL to a specified interface.
<i>interface-number</i>	Specifies the interface number.

**Defaults** No offset is specified by default.

**Command**

**Mode** Routing process configuration mode

**Usage Guide** If a RIP route matches against both the offset-list of the specified interface and the global offset-list, it will increase the metric value of the offset-list of the specified interface.

**Configuration** The following example increases the metric of the RIP routes by 7 in the range specified by ACL 7.

**Examples**

```
Ruijie (config-router)# offset-list 7 out 7
```

The following example increases the metric of the RIP routes by 7 in the range specified by ACL 7 and learned by vlan 1.

```
Ruijie (config-router)# offset-list 8 in 7 vlan 1
```

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 1.25 output-delay

Use this command to modify the delay to send RIP update packets. Use the **no** form of this command to restore the default setting.

**output-delay** *delay*

**no output-delay**

**Parameter Description**

Parameter	Description
<i>delay</i>	Sets the delay to send RIP update packets, in the range from 8 to 50 in the unit of milliseconds.

**Defaults** No sending delay is configured by default.

**Command**

**Mode** Routing process configuration mode

**Usage Guide** In normal cases, the size of a RIP update packet is 512 bytes including 25 routes. If the number of updated routes is greater than 25, update packets will be sent through multiple routes. Note that the update packets should be sent as fast as possible.

However, when a high-speed device sends a large number of packets to a low-speed device, the low-speed device may not process all the packets timely, resulting in packet loss. In this case, you can use this command to increase the delay to send packets on the high-speed device so that the low-speed device can process all the update packets.

**Configuration** The following example sets the delay to send RIP update packets to 30 milliseconds.

**Examples**

```
Ruijie(config)# router rip
```

```
Ruijie(config-router)# output-delay 30
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A  
Description

## 1.26 passive-interface

Use this command to disable the function of sending update packets on an interface. Use the **no** form of this command to restore the default setting.

**passive-interface** { **default** | *interface-type interface-num* }

**no passive-interface** { **default** | *interface-type interface-num* }

Parameter Description	Parameter	Description
	<b>default</b>	
<i>interface-type interface-num</i>		Indicates the interface type and number.

**Defaults** Interfaces are set to the non passive interfaces by default.

**Command**

**Mode** Routing process configuration mode

**Usage Guide** The **passive-interface default** command sets all interfaces to the passive interfaces. You can use **no passive-interface** *interface-type interface-num* command to set specified interfaces as non-passive interfaces.

After you set an interface to the passive interface, RIP route update packets will no longer be sent but can be received through the interface. In this case, route update packets can be sent to a specified neighbor through the interfaces by using the **neighbor** command. You can use the **ip rip send enable** and **ip rip receive enable** commands to control whether route update packets can be sent or received through the interface.

**Configuration Examples** The following example sets all interfaces to the passive interfaces and then sets vlan 1 to the non-passive interface.

```
Ruijie(config-router)# passive-interface default
Ruijie(config-router)# no passive-interface vlan 1
```

Related Commands	Command	Description
	<b>ip rip receive enable</b>	
<b>ip rip send enable</b>		Enables or disables sending RIP packets on the interface.

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

## 1.27 redistribute

Use this command to redistribute external routes in route configuration mode. Use the **no** form of this command to restore the default setting.


**redistribute** { **connected** | **static** } [ **metric** *metric-value* | **route-map** *route-map-name* ] \*  
**no redistribute** { **connected** | **static** } [ **metric** | **route-map** *route-map-name* ] \*

Parameter Description	Parameter	Description
	<b>connected</b>	Is redistributed from a connected route.
	<b>static</b>	Is redistributed from static routes.
	<b>metric</b> <i>metric-value</i>	Sets the metric value of the redistributed route and specifies the metric value by using the metric-value parameter. The value is in the range from 1 to 16.
	<b>route-map</b> <i>route-map-name</i>	Sets the redistribution filtering rule.

**Defaults** By default, external routes are not redistributed to RIP. The metric of the redistributed routes is 1 by default.  
 The route-map is not associated.

**Command Mode** Routing process configuration mode

**Usage Guide** This command is executed to redistribute external routes to RIP. It is unnecessary to convert the metric of one routing protocol into that of another routing protocol for route redistribution, since different routing protocols use different metric measurement methods. However, a symbolic metric value must be set for route redistribution. Otherwise, route redistribution will fail.  
 The rule of configuring the no form of the redistribute command is as follows:  
 1. If the no form of this command specifies certain parameters, the parameters must be restored to the default configuration.  
 2. If the **no** form of this command does not specify any parameter, the command must be deleted.

 The redistribute command cannot redistribute the default route of other protocol to the RIP process. To this end, use the **default-information originate** command.

**Configuration Examples** The following example redistributes static routes to RIP.

**Examples**

```
Ruijie(config-router)# redistribute static
```

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



<b>default-metric</b> <i>metric</i>	Sets the default metric of the route to be redistributed.
<b>default-information originate</b>	Generates the default route in the RIP process.

**Platform** N/A

**Description**

## 1.28 router rip

Use this command to create the RIP routing process and enter the routing process configuration mode. Use the **no** form of this command to restore the default setting.

**router rip**

**no router rip**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** No RIP process is running by default.

**Command**

**Mode** Global configuration mode

**Usage Guide** One RIP routing process must be defined with one network number. If a dynamic routing protocol runs on asynchronous lines, configure the **async default routing** command on the asynchronous interface.

**Configuration Examples** The following example creates the RIP routing process and enters the routing process configuration mode.

```
Ruijie (config)# router rip
Ruijie(config-router)#
```

Related Commands	Command	Description
	<b>network (RIP)</b>	Defines the network number of the RIP process.

**Platform** N/A

**Description**

## 1.29 show ip rip

Use this command to display the RIP process information.

**show ip rip**

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

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

**Defaults** N/A

**Command**

**Mode** All CLI user modes except user EXEC mode

**Usage Guide** It is used to display the three timers, routing distribution status, routing re-distribution status, interface RIP version, RIP interface and network range, metric, and distance of the RIP process quickly.

**Configuration Examples** The following example displays the basic information of the RIP process such as the update time and management distance.

```
Ruijie(config)#show ip rip
Routing Protocol is "rip"
  Sending updates every 30 seconds
  Invalid after 180 seconds, flushed after 120 seconds
  Outgoing update filter list for all interface is:
    distribute-list 10 out
  Incoming update filter list for all interface is: not set
  Redistribution default metric is 3
  Redistributing: static
  Default-information originate always
  Default version control: send version 2, receive version 2
  Routing for Networks:
    172.16.0.0 255.255.255.0
    192.168.12.0 255.255.255.0
    200.4.4.0 255.255.255.0
    192.168.1.2
  Distance: 160 (default is 120)
  Address          Distance List
  192.168.12.1/32      123
  Graceful-restart enabled
  Restart grace period 90 secs
Ruijie(config)#
```

Description of fields in the command output is as follows:

Field	Description
Sending updates	Packet update time
Invalid	Invalid time
flushed	Refresh time
Outgoing update filter list for all interface	Filter all sent routes
Incoming update filter list for all interface	Filter all received routes
Default redistribution metric	Redistribution metric by default

Redistributing	Redistribution protocol
Default version control	RIP version of instance by default
Routing for Networks	Routing segment advertised by RIP
Distance	Management distance of instance
Graceful-restart	Whether GR is enabled
Restart grace period	GR time
Current Restart remaining time	Remaining GR time

**Related  
Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

### 1.30 show ip rip database

Use this command to display the route summary information in the RIP routing database.

**show ip rip database** [ *network-number network-mask* | **count** ]

**Parameter  
Description**

Parameter	Description
<i>network-number</i>	(Optional) Indicates the ID of the subnet on which route information is to be displayed.
<i>network-mask</i>	Indicates the subnet mask. It must be specified if the network number is specified.
<b>count</b>	(Optional) Displays the abstract of the route statistics in the RIP database.

**Defaults** N/A

**Command**

**Mode** All CLI user modes except user EXEC mode

**Usage Guide** Only when the related sub-routes are converged, the converged address entries appear in the RIP routing database. When the last sub-route information in the converged address entries becomes invalid, the converged address information will be deleted from the database.

**Configuration Examples** The following example displays all converged address entries in the RIP routing database.

```
Ruijie# show ip rip database
192.168.1.0/24    auto-summary
192.168.1.0/30    directly connected, Loopback 3
192.168.1.8/30    directly connected, VLAN 1
192.168.121.0/24  auto-summary
```

```
192.168.121.0/24    redistributed
[1] via 192.168.2.22, VLAN 2
192.168.122.0/24    auto-summary
192.168.122.0/24
```

The following example displays the converged address entries related with 192.168.121.0/24 in the RIP routing database.

```
Ruijie# show ip rip database 192.168.121.0 255.255.255.0
192.168.121.0/24    redistributed
[1] via 192.168.2.22, VLAN 1
```

The following example displays the statistical information summary of various routes in the RIP routing database.

```
Ruijie# show ip rip database count
           All      Valid  Invalid
database      5        5       0
auto-summary  5         5       0

connected     1         1       0
rip           4         4       0
```

Description of fields in the command output is as follows:

Field	Description
auto-summary	Summarized routes
directly connected	Directed-connected routes
redistributed	Redistributed routes
database	RIP route database
All	Count of all routes
Valid	Count of valid routes
Invalid	Count of invalid routes

**Related Commands**

Command	Description
<b>show ip rip</b>	Displays the information of the currently-running routing protocol process.

**Platform** N/A

**Description**

### 1.31 show ip rip external

Use this command to display the information of the external routes redistributed by the RIP protocol.

```
show ip rip external [ connected | static ]
```

**Parameter**

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

Description	
<b>connected</b>	Displays redistributed directly-connected routes.
<b>static</b>	Displays redistributed static routes.

**Defaults** N/A

**Command**

**Mode** All CLI user modes except user EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays direct routes redistributed by the RIP process.

```
Ruijie# show ip rip external
Protocol connected route:
[connected] 192.100.3.0/24 metric=0
    nhop=0.0.0.0, if=2
[connected] 192.101.1.0/24 metric=0
    nhop=0.0.0.0, if=3
Protocol static route:
[static] 10.1.1.1/32 metric=0
    nhop=0.0.0.0, if=4096
[static] 10.1.2.1/32 metric=0
    nhop=0.0.0.0, if=4096
```

Description of fields in the command output is as follows:

Field	Description
Protocol connected route	Type of redistributed route
connected	Redistributed route
metric	Redistributed route metric
nhop	Next hop of redistributed route
if	Outbound interface of redistributed route

Related Commands	Command	Description
	<b>show ip rip</b>	Displays the information of the currently running routing protocol process.
	<b>ip vrf</b>	Creates a VRF.

**Platform** N/A

**Description**

## 1.32 show ip rip interface

Use this command to display the RIP interface information.

**show ip rip interface** [ *interface-type interface-number* ]

Parameter Description	Parameter	Description
	<i>interface-type interface-number</i>	(Optional) Displays the specified interface type and interface number.

**Defaults** N/A

**Command**

**Mode** All CLI user modes except user EXEC mode

**Usage Guide** This command is used to display the information about RIP interfaces. If no RIP interface exists, no information is displayed.

**Configuration Examples** The following example displays the RIP interface information.

```
Ruijie# show ip rip interface
GigabitEthernet 0/17 is up, line protocol is up
Routing Protocol: RIP
Receive RIPv2 packets only
Send RIPv2 packets only
Recv RIP packet total: 0
Send RIP packet total: 3
Passive interface: Disabled
Split Horizon with Poisoned Reverse: Enabled
Triggered RIP Enabled:
Retransmit-timer: 5, Retransmit-count: 36
V2 Broadcast: Disabled
Multicast registe: Registered
Interface Summary Rip:
Not Configured
Authentication mode: Text
Authentication key-chain: ripk1
Authentication text-password: ruijie
Default-information: only, metric 5
IP interface address:
192.168.64.100/24, next update due in 14 seconds
2.2.1.1/24, next update due in 24 seconds
    neighbor 2.2.1.6, next update due in 3 seconds
    neighbor 2.2.1.77, next update due in 13 seconds
        2.2.2.57/24, next update due in 16 seconds
```

Description of fields in the command output is as follows:

Field	Description
Receive RIPv1 and RIPv2 packets	Packet types that the interface can receive
Send RIPv1 packets only	Packet types that the interface can send

Receive RIP packet	Whether the interface can receive packets
Send RIP packet	Whether the interface can send packets
Passive interface	Whether the passive port is enabled
Send RIP supernet routes	Whether the interface can send supernet routes
Recv RIP packet total	Total number of packets received on the interface
Send RIP packet total	Total number of packets sent by the interface
Split Horizon with Poisoned Reverse	Whether split horizon poison is enabled
Triggered RIP	Whether the Triggered function is enabled
Retransmit-timer	Retransmission time
Retransmit-count	Retransmission count
V2 Broadcast	V2 broadcast packet
Multicast register	Whether multicast is registered
Interface Summary Rip	Whether summary is enabled on the interface
Authentication mode	Authentication mode
Authentication key-chain	Key chain used for authentication
Authentication text-password	Authentication string
Default-information	Default metric, route and other information
IP interface address	IP address of the interface

**Related  
Commands**

Command	Description
<b>show ip rip</b>	Displays the information of the currently running routing protocol process.

**Platform** N/A

**Description**

### 1.33 show ip rip peer

Use this command to show the RIP peer information. RIP records a summary for the RIP routing information source learnt (source addresses of RIP route update packets) for the convenience of user monitoring. This routing information source is called RIP neighbor information.

**show ip rip peer** [ *ip-address* ]

**Parameter  
Description**

Parameter	Description
<i>ip-address</i>	(Optional) Displays the IP address of a specified RIP neighbor.

**Defaults** N/A

**Command**

**Mode** All CLI user modes except user EXEC mode

**Usage Guide** This command is used to display the RIP neighbor information. If no RIP neighbor exists, no information will be displayed.

**Configuration Examples** The following example displays the RIP neighbor information.

```
Ruijie# show ip rip peer
Peer 192.168.3.2:
  Local address: 192.168.3.1
  Input interface: GigabitEthernet 0/17
  Peer version: RIPv1
  Received bad packets: 3
  Received bad routes: 0
```

Description of fields in the command output is as follows:

Field	Description
Peer	Neighbor IP address
Local address	Local address
Input interface	Connected interface
Peer version	RIP version of neighbor
Received bad packets	Wrong packets received from neighbor
Received bad routes	Wrong routes

**Related Commands**

Command	Description
<b>show ip rip</b>	Displays the information of the routing protocol process that is running.

**Platform** N/A

**Description**

### 1.34 timers basic

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

**timers basic** *update invalid flush*

**no timers basic**

**Parameter Description**

Parameter	Description
<i>update</i>	Indicates the route update time in seconds. The update keyword defines the period at which the device sends route update packets. Each time an update packet is received, the "Invalid" and "Flush" clocks are reset. By default, a route update packet is sent every 30 seconds.



<i>invalid</i>	Indicates the route invalid time in seconds, starting from the last valid update packet. The "invalid" defines the period when the route in the routing table becomes invalid due to no update. The invalid period of route shall be at least three times the route update period. If no update packet is received within the route invalid period, the related route becomes invalid and enters into the "invalid" state. If an update packet is received within the period, the clock resets. By default, the Invalid time is 180 seconds.
<i>flush</i>	Indicates the route flushing time in seconds, starting when a RIP route enters into the invalid status. When the flush time is due, the routes in the invalid status will be cleared out of the routing table. The default Flush time is 120 seconds.


**Defaults** By default, the update time is 30 seconds, the invalid time is 180 seconds, and the flushing time is 120 seconds.

**Command**

**Mode** Routing process configuration mode

**Usage Guide** Adjusting the above clocks may speed up routing protocol convergence and fault recovery. Devices connected to the same network must have consistent RIP clock values. Adjustment of RIP clocks is not recommended unless otherwise specified.

To check the current RIP clock parameters, use the **show ip rip** command.

 If you set the clock to a small value on low-speed links, some risks will be caused because numerous update packets may use up the bandwidth. In general, the clocks can be configured with smaller values on Ethernet or the lines of above 2 Mbit/s to reduce the convergence time of routes.

**Configuration Examples** The following example enables the RIP update packets that are sent every 10 seconds. If no update packet is received within 30 seconds, related routes become invalid and enter the invalid status.

When another 90s elapses, they will be cleared.

```
Ruijie (config)# router rip
Ruijie (config-router)# timers basic 10 30 90
```

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

### 1.35 validate-update-source

Use this command to validate the source address of the received RIP route update packet. Use the

**no** form of the command to disable this function.

**validate-update-source**

**no validate-update-source**

Parameter Description	Parameter	Description
	N/A	N/A

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

#### Command

**Mode** Routing process configuration mode

**Usage Guide** You can validate the source address of the RIP route update packet. The validation aims to ensure that the RIP routing process receives only the route update packets from the same IP subnet neighbor.

Disabling split horizon on the interface causes the RIP routing process to enable update message source address validation, no matter whether it has been configured with the **validate-update-source** command in routing process configuration mode.

In addition, for the ip unnumbered interface, the RIP routing process does not implement update message source address validation, no matter whether it has been configured with the command **validate-update-source**.

**Configuration** The following example disables verification of the source IP address of the update packet.

#### Examples

```
Ruijie (config)# router rip
Ruijie (config-router)# no validate-update-source
```

#### Related Commands

Command	Description
<b>ip split-horizon</b>	Enables split horizon.
<b>ip unnumbered</b>	Defines the IP unnumbered interface.
<b>neighbor (RIP)</b>	Defines the IP address of a RIP neighbor.

**Platform** N/A

**Description**

## 1.36 version

Use this command to define the RIP version of a device. Use the **no** form of this command to restore the default setting.

**version { 1 | 2 }**

**no version**

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

<b>1</b>	Defines the RIP version 1.
<b>2</b>	Defines the RIP version 2.

**Defaults** The route update packets of RIPv1 and are received by default, but only the RIPv1 route update packets are sent.

**Command**

**Mode** Routing process configuration mode

**Usage Guide** This command defines the RIP version running on the device. It is possible to redefine the messages of which RIP version are processed on every interface by using the **ip rip receive version** and **ip rip send version** commands.

**Configuration** The following example configures the RIP version as version 2.

**Examples**

```
Ruijie (config)# router rip
Ruijie (config-router)# version 2
```

**Related  
Commands**

Command	Description
<b>ip rip receive version</b>	Defines the version of RIP packets received on the interface.
<b>ip rip send version</b>	Defines the version of RIP packets sent on the interface.
<b>show ip rip</b>	Displays RIP information.

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

## 2 RIPng Commands(beta)

### 2.1 clear ipv6 rip

Use this command to clear the RIPng routes.

**clear ipv6 rip**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** None

**Command mode** Privileged EXEC mode

**Usage Guide** Running this command removes all RIPng routes and this operation may have great impact on the RIPng protocol. This command should be used with caution.

**Configuration Examples** The following example clears the RIPng routes:

```
Ruijie# clear ipv6 rip
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

### 2.2 default-metric

Use this command to configure the default metric for RIPng. Use the **no** form of this command to restore the default value.

**default-metric metric**

**no default-metric**

Parameter Description	Parameter	Description
	<i>metric</i>	Sets the default metric value. The valid range is from 1 to 16. The route is unreachable if the metric value is larger than or equal to 16.

**Defaults** The default value is 1.

**Command** Routing process configuration mode.

**mode**

**Usage Guide** This command shall be used with the **redistribute** command. When redistributing the route from one route process to RIPng, due to the incompatibility of metric calculation mechanisms of different routing protocols, it fails to translate the routing metric values. To this end, the RIPng metric value shall be defined when translating the metric values. If there is no defined metric value, use the **default-metric** command to define one; and the defined metric value will overwrite the value of the **default-metric** command. By default, the **default-metric** value is 1.

**Configuration Examples** The following example shows how to set the RIPng metric value as 3 when redistributing static process 100:

```
Ruijie(config-router)# default-metric 3
```

**Related Commands**

Command	Description
<b>redistribute</b>	Redistributes the route from one route domain to another route domain.

**Platform** N/A

**Description****2.3 distance**

Use this command to set the administrative distance of RIPng. Use the **no** form of this command to restore the default value.

**distance** *distance*

**no distance**

**Parameter Description**

Parameter	Description
<i>distance</i>	Sets the RIPng administrative distance. The range is from 1 to 254.

**Defaults** The default distance is 120

**Command mode** Routing process configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example shows how to set the RIPng administrative distance as 160:

```
Ruijie(config)# ipv6 router rip
Ruijie(config-router)# distance 160
```

**Related Commands**

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

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

**Platform** N/A

**Description**

## 2.4 distribute-list

Use this command to filter the in/out route in the prefix list. Use the **no** form of this command to remove route filtering.

**distribute-list prefix-list** *prefix-list-name* { **in** | **out** } [ *interface-type interface-name* ]

**no distribute-list prefix-list** *prefix-list-name* { **in** | **out** } [ *interface-type interface-name* ]

Parameter	Parameter	Description
<b>Description</b>	<b>prefix-list</b> <i>prefix-list-name</i>	Name of the prefix list which is used to filter the route.
	<b>in</b>   <b>out</b>	Filters the in or out route in the distribute list.
	<i>interface-type</i> <i>interface-name</i>	(Optional) Applies the distribute list to the specified interface.

**Defaults** By default, no distribute list is defined.

**Command mode** Routing process configuration mode.

**Usage Guide** This command is used to configure the route distribution control list to filter all update routes for the purpose of refusing to receive or send the specified routes. If the interface is not specified, the update routes on all interfaces are filtered.

**Configuration Examples** The following example shows how to filter the received update route on the interface vlan 1 (only those update routes within the **prefix-list allowpre** prefix list range can be received)

```
Ruijie(config)# ipv6 router rip
Ruijie(config-router)# distribute-list prefix-list allowpre in vlan 1
```

Related Commands	Command	Description
	<b>redistribute</b>	Sets route redistribution.

**Platform** N/A

**Description**

## 2.5 graceful-restart

Use this command to configure the graceful restart (GR) function for the RIPng process.

**graceful-restart** [ **grace-period** *grace-period* ]

Use the **no** form of this command restore the default configurations.

**no graceful-restart [ grace-period ]****Parameter  
Description**

Parameter	Description
<b>grace-period</b>	Displays the configured grace period.
<i>grace-period</i>	Indicates the configured GR period, ranging from 1 to 1800 seconds. The default value is the smaller between twice of the update time and 60s.

**Defaults** The GR function is enabled by default.

**Command Mode** Routing process configuration mode

**Default Level** 14

**Usage Guide** The GR function is configured based on RIPng instances. Different parameters can be configured for different RIPng instances as required.

The GR period indicates the maximum duration from RIPng restart to RIPng GR completion. In this time period, the forwarding table before restart is used and the RIPng route is restored to the status before restart. After the GR period expires, the RIPng process exits the GR status and the common RIPng operation is performed.

The **graceful-restart grace-period** command allows a user to modify the GR period in explicit mode. Note that GR is completed and the RIPng route is updated once before the RIPng route becomes invalid. If the GR period is improperly set, continuous data forwarding in the GR process cannot be ensured. A typical case is as follows:

If the GR period is greater than the invalid time of the neighbor route, GR is not completed before the route becomes invalid and the route is not advertised to the neighbor again. The neighbor route stops forwarding data after the route becomes invalid, resulting in data forwarding interruption. Therefore, unless otherwise specified, it is not recommended to adjust the GR period. If the GR period needs to be configured, check configuration of the **timers** command to ensure that the GR period value is greater than the route update time and smaller than the route invalid time.

When GR is performed for the RIPng process, ensure that the network environment is stable.

**Configuration Examples** The following example enables the GR function for the RIPng process and configures the GR period.

```
Ruijie(config)# ipv6 router rip
Ruijie(config-router)# graceful-restart grace-period 90
```

**Verification** Run the **show ipv6 rip** command to check whether the GR function is configured and query the configured grace period.

**Prompts** N/A

**Common Errors** N/A

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

## 2.6 ipv6 rip default-information

Use this command to generate a default IPv6 route to the RIPng. Use the **no** form of this command to remove the default route.

**ipv6 rip default-information** { **only** | **originate** } [ **metric** *metric-value* ]  
**no ipv6 rip default-information**

**Parameter**  
**Description**

Parameter	Description
<b>only</b>	Advertises the IPv6 default route only.
<b>originate</b>	Advertises both of the IPv6 default route and other routes.
1. <b>metric</b> <b><i>metric-value</i></b>	Sets the metric value for the default route. The valid range is from 1 to 15. The default metric is 1.

**Defaults** By default, no default route is configured.

**Command mode** Interface configuration mode

**Usage Guide** With this command configured on an interface, the interface advertises an IPv6 default route and the route itself is not to join the device route forwarding table and the RIPng route database. To avoid the route loop, once this command has been configured on the interface, RIPng refuses to receive the default route update message advertised from the neighbor.

**Configuration Examples** The following example shows how to create a default route to the RIPng routing process on the interface vlan 1 and enable this interface to advertise the default route only:1

```
Ruijie(config)# interface vlan 1
Ruijie(config-if-VLAN 1)# ipv6 rip default-information only
```

**Related Commands**

Command	Description
<b>show ipv6 rip</b>	Displays the RIPng process and statistics.
<b>show ipv6 rip database</b>	Displays the RIPng route.

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

## 2.7 ipv6 rip enable

Use this command to enable the RIPng on the interface. Use the **no** form of this command to disable RIPng on the interface.

**ipv6 rip enable**



**no ipv6 rip enable**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** It is disabled by default.

**Command mode** Interface configuration mode.

**Usage Guide** This command is used to add the RIPng interface. Before this command is configured, if the RIPng is not enabled, use this command to enable the RIPng automatically.

**Configuration** The following example shows how to enable the RIPng on the interface vlan 1:

**Examples**

```
Ruijie(config)# interface vlan 1
Ruijie(config-if-VLAN 1)# ipv6 rip enable
```

Related Commands	Command	Description
	N/A	N/A

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

## 2.8 ipv6 rip metric-offset

Use this command to set the interface metric value. Use the **no** form of this command to remove the metric configurations.

**ipv6 rip metric-offset** *value*

**no ipv6 rip metric-offset**

Parameter Description	Parameter	Description
	<i>value</i>	Sets the interface metric value on the interface. The valid range is from 1 to 16.

**Defaults** The default value is 1.

**Command mode** Interface configuration mode.

**Usage Guide** Before the route is added to the routing list, the interface metric value shall be upon the route metric. To this end, the interface metric value influences the route usage.

**Configuration** The following example shows how to set the metric value of the interface vlan 1 as 5:

**Examples**

```
Ruijie(config)# interface vlan 1
Ruijie(config-if-vlan 1)# ipv6 rip metric-offset 5
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform**

N/A

**Description**

## 2.9 ipv6 router rip

Use this command to create the RIPng process and enter routing process configuration mode. Use the **no** form of this command to remove the RIPng process.

**ipv6 router rip**

**no ipv6 router rip**

**Parameter  
Description**

Parameter	Description
N/A	N/A

**Defaults**

No RIPng process is configured by default.

**Command  
mode**

Global configuration mode.

**Usage Guide**

N/A.

**Configuration Examples** The following example shows how to create the RIPng process and enter routing process configuration mode:

```
Ruijie(config)# ipv6 router rip
S2300(config-router)#
```

**Related  
Commands**

Command	Description
<b>ipv6 rip enable</b>	Enables the RIPng on the specified interface.

**Platform**

N/A

**Description**

## 2.10 passive-interface

Use this command to disable the interface to send update packets. Use the **no** form of this command

to enable the interface to send update packets.

**passive-interface** { **default** | *interface-type interface-num* }

**no passive-interface** { **default** | *interface-type interface-num* }

**Parameter  
Description**

Parameter	Description
<b>default</b>	Enables the passive mode on all interfaces.
<i>interface-type interface-num</i>	Interface type and interface number.

**Defaults** No passive interface is configured by default.

**Command mode** Routing process configuration mode.

**Usage Guide** You can use the **passive-interface default** command to enable the passive mode on all interfaces. Then, use the **no passive-interface interface-type interface-num** command to remove the specified interface from the passive mode.

**Configuration Examples** The following example shows how to enable the passive mode on all interfaces and remove interface vlan 1 from the passive mode:

```
Ruijie(config-router)# passive-interface default
Ruijie(config-router)# no passive-interface vlan 1
```

**Related  
Commands**

Command	Description
N/A	N/A

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

## 2.11 redistribute

Use this command to redistribute the route of other routing protocols to RIPng. Use the **no** form of this command to remove the redistribution configuration.

**redistribute** { **connected** | **static** } [ **metric** *metric-value* | **route-map** *route-map-name* ] \*

**no redistribute** { **connected** | **static** } [ **metric** | **route-map** *route-map-name* ] \*

**Parameter  
Description**

Parameter	Description
<b>connected</b>	Redistributes the connected routes to RIPng.
<b>static</b>	Redistributes the static routes to RIPng.
<b>metric</b> <i>metric-value</i>	(Optional) Sets the metric value for the route redistributed to RIPng.
<b>route-map</b> <i>route-map-name</i>	(Optional) Sets the redistribution route filtering.

**Defaults** By default, the routes of other routing protocols are not redistributed.  
 If the **default-metric** command is not configured, the default metric value is 1;  
 By default, the **route-map** is not configured;  
 By default, all sub-type routes in the specified routing process are redistributed.

**Command mode** Routing process configuration mode.

**Usage Guide** This command is used to redistribute the external routes to RIPng.  
 It is unnecessary to transform the metric of one routing protocol into another routing protocol in the process of the route redistribution, for the metric calculation methods of the different routing protocols are different.  
 The instance, from where the routing information is redistributed to the RIPng, must be specified in the process of configuring the multi-instance protocol redistribution.

**Configuration Examples** The following example shows how to redistribute the static route, use the route map *mymap* to filter and set the metric value as 8:

```
Ruijie(config)# ipv6 router rip
Ruijie(config-router)# redistribute static route-map mymap metric 8
```

**Related Commands**

Command	Description
<b>default-metric</b>	Defines the default RIPng metric value when redistributing other routing protocols.
<b>distribute-list</b>	Filters the RIPng routing update packets.

**Platform** N/A

**Description**

## 2.12 show ipv6 rip

Use this command to show the parameters and each statistical information of the RIPng routing protocol process.

**show ipv6 rip**

**Parameter Description**

Parameter	Description
N/A	N/A

**Defaults** N/A

**Command mode** All CLI user modes except user EXEC mode

**Usage Guide** N/A

```

Configuration Ruijie# show ipv6 rip
Examples Routing Protocol is "RIPng"
Sending updates every 10 seconds with +/-50%, next due in 8 seconds
Timeout after 30 seconds, garbage collect after 60 seconds
Outgoing update filter list for all interface is:
distribute-list prefix aa out
Incoming update filter list for all interface is: not set
Default redistribution metric is 1
Default distance is 120
Redistribution:
Redistributing protocol connected route-map rm
Redistributing protocol static
Redistributing protocol ospf 1
Default version control: send version 1, receive version 1
Interface          Send  Recv
VLAN 1             1    1
Loopback 1         1    1
Routing Information Sources:
None

```

Description of fields in the command output is as follows:

Field	Description
Sending update	Interval for sending updates
Timeout	Expiration time
garbage	Recovery time
Outgoing update filter list	Configured sending filtering table
Incoming update filter	Configured receiving filtering table
Default redistribution metric	Default redistribution metric
distance	Management distance
Redistribution	Redistribution routing protocol
Default version control	Default transceiver version
Interface	RIPng interface
Routing Information Sources:	Routing information

**Related  
Commands**

Command	Description
<b>show ipv6 rip</b>	Displays the parameters and each statistical information of the RIPng process.

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

## 2.13 show ipv6 rip database

Use this command to display the RIPng route entries.

**show ipv6 rip database**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command mode** All CLI user modes except user EXEC mode

**Usage Guide** N/A

**Configuration** Ruijie# show ipv6 rip database

### Examples

```
Codes: R - RIPng,C - Connected,S - Static,O - OSPF,B - BGP
sub-codes:n - normal,s - static,d - default,r - redistribute,
i - interface, a/s - aggregated/suppressed
S(r) 2001:db8:1::/64, metric 1, tag 0
Loopback 0/::
S(r) 2001:db8:2::/64, metric 1, tag 0
Loopback 0/::
C(r) 2001:db8:3::/64, metric 1, tag 0
VLAN 1/::
S(r) 2001:db8:4::/64, metric 1, tag 0
Null 0/::
C(i) 2001:db8:5::/64, metric 1, tag 0
Loopback 1/::
S(r) 2001:db8:6::/64, metric 1, tag 0
Null 0/::
```

Description of fields in the command output is as follows:

Field	Description
codes	Route type and corresponding abbreviation
2001:db8:1::	Route prefix
metric 1	Route metric
tag 0	Route label value
VLAN 1/::	Routing interface

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 2.14 split-horizon

Use the **split-horizon** command to enable the RIPng split-horizon function in routing process configuration mode. Use the **no** form of this command to disable this function. Use the **split-horizon poisoned-reverse** command to enable the RIPng poisoned reverse horizontal split function in routing process configuration mode. Use the **no** form of this command to disable this function.

**split-horizon [ poisoned-reverse ]**

**no split-horizon [ poisoned-reverse ]**

**Parameter Description**

Parameter	Description
<b>poisoned-reverse</b>	(Optional) Enables the poisoned-reverse horizontal split.

**Defaults** RIPng split horizon is enabled by default.

**Command mode** Routing process configuration mode.

**Usage Guide** In the process of packet updating, split-horizon function prevents some routing information from being advertised through the interface learning those routing information. The poisoned reverse horizontal split function advertises some routing information to the interface learning those routing information, and the metric value is set as 16. The RIPng routing protocol belongs to the distance vector routing protocol, so the horizontal split shall be noticed in the actual application. You can use the **show ipv6 rip** command to determine whether the RIPng split-horizon function is enabled or not.

**Configuration** The following example shows how to disable the RIPng horizontal split:

**Examples**

```
Ruijie(config)# ipv6 router rip
Ruijie(config-router)# no split-horizon
```

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 2.15 timers

Use this command to adjust the RIPng timer. Use the **no** form of this command to restore the default settings.

**timers update invalid flush**

**no timers**

Parameter Description	Parameter	Description
	<i>update</i>	Sets the routing update time, in seconds. The update parameter defines the period of sending the routing update packets by the device. The invalid and flush parameter reset once the update packets are received.
	<i>invalid</i>	Sets the routing invalid time, in seconds, starting from receiving the last valid update packet. The invalid parameter defines the invalid time for the un-updated routing in the routing list. The routing invalid time shall be three times larger than the routing update time. The routing will be invalid if no update packets are received within the routing invalid time, and it will reset if the update packets are received within the invalid time.
	<i>flush</i>	Sets the routing flush time, in seconds, starting from RIPng entering to invalid state. The invalid routing will be removed from the routing list if the flush time expires.

**Defaults** The default update time is 30 seconds; the default invalid time is 180 seconds; and the default flush time is 120 seconds.

**Command mode** Routing process configuration mode.

**Usage Guide** Adjusting the above time may speed up the RIPng convergence time and the troubleshooting time. The RIPng time must be consistent for the devices connecting to the same network. You are not recommended to adjust the RIP time, except for the specific requirement.

Use the **show ipv6 rip** command to view the current RIPng time parameter setting.

In the low-speed link, with the short time configured, large amount of the update packets consumes a lot of bandwidth. Generally, the short time can be configured in the Ethernet or 2Mbps-higher line to shorten the convergence time of the network routing.

**Configuration Examples** The following example shows how to send the RIP update packets every 10 seconds. The routing will be invalid if no update packets are received within 30 seconds, and the routing will be removed after being invalid for 90 seconds.

```
Ruijie(config)# ipv6 router rip
Ruijie(config-router)# timers 10 30 90
```

**Related Commands**

Command	Description
<b>show ipv6 rip</b>	Displays the parameters and the statistical information of the RIPng process.
<b>show ipv6 rip database</b>	Displays the RIPng routes.



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

# 3 NSM Commands(beta)

## 3.1 clear ip route

Use this command to clear the route cache.

**clear ip route** { \* | *network* [ *netmask* ] }

	Parameter	Description
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.

```
Ruijie# clear ip route 192.168.12.0
```

Related Commands	Command	Description
	N/A	N/A

### Platform

**Description** N/A

## 3.2 ip default-gateway

Use this command to configure the default gateway IP address. Use the **no** or **default** form of this command to restore the default setting.

**ip default-gateway** *ipv4-address*

**no ip default-gateway**

**default ip default-gateway**

Parameter	Parameter	Description
Description	<i>ipv4-address</i>	IPv4 address of the default gateway

**Defaults** No gateway IP address is configured by default.

**Command****Mode** Global configuration mode**Usage Guide** When the device does not know the destination address of a packet, the device will forward the packet to the default gateway.**Examples**

The following example sets the IP address of default gateway to 192.168.1.1.

```
Ruijie(config)# ip default-gateway 192.168.1.1
```

**Related Commands**

Command	Description
N/A	N/A

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

### 3.3 ip default-network

Use this command to configure the default network globally. Use the **no** or **default** form of this command to restore the default setting.

**ip default-network** *network***no ip default-network** *network***default ip default-network** *network***Parameter Description**

Parameter	Description
<i>network</i>	Default network

**Defaults** The default is 0.0.0.0/0.**Command****Mode** Global configuration mode**Usage Guide** The goal of this command is to generate the default route. The default network must be reachable in the routing table, but not the directly connected network.

The default network always starts with an asterisk ("\*"), indicating that it is the candidate of the default route. If there is connected route and the route without the next hop in the default network, the default route must be a static route.

The following example sets 192.168.100.0 as the default network. Since the static route to the network is configured, the device will automatically generate a default route.

```
Ruijie(config)# ip route 192.168.100.0 255.255.255.0 vlan 1
Ruijie(config)# ip default-network 192.168.100.0
```

**Examples**

The following example sets 200.200.200.0 as the default network. The route becomes the default one only when it is available in the routing table.

```
Ruijie(config)# ip default-network 200.200.200.0
```

Related Commands	Command	Description
	<b>show ip route</b>	Displays the routing table.

### 3.4 ip route

Use this command to configure a static route. Use the **no** or **default** form of this command to restore the default setting.

**ip route** *network mask* { *ipv4-address* [ **global** ] | *interface* [ *ipv4-address* [ **global** ] ] } [ *distance* | **description** *description-text* | [ **disabled** | **enabled** ] | [ **permanent** ] | **tag** *tag* | **weight** *number* ] \*

**no ip route** *network net-mask* { *ip-address* | *interface* [ *ip-address* ] } [ *distance* ]

**default ip route** *network net-mask* { *ip-address* | *interface* [ *ip-address* ] } [ *distance* ]

Parameter	Description
<i>network</i>	Network address of the destination
<i>net-mask</i>	Mask of the destination
<i>ipv4-address</i>	The next hop IP address of the static route
<b>global</b>	(Optional) Indicates next hop address is global
<i>interface</i>	(Optional) The next hop egress of the static route
<i>distance</i>	(Optional) The administrative distance of the static route
<b>description</b> <i>description-text</i>	(Optional) Indicates the description of the static route. By default, no description is configured. <i>description-text</i> is a string of 1 to 60 characters.
<b>disabled</b>   <b>enabled</b>	(Optional) Indicates the enable flag of the static route. The flag is enabled by default.
<b>permanent</b>	(Optional) Indicates the permanent route ID
<b>tag</b> <i>tag</i>	(Optional) Indicates the tag of the static route
<b>weight</b> <i>number</i>	(Optional) Indicates the weight of the static route. The weight is 1 by default.

**Defaults** No static route is configured by default.

**Command Mode** Global configuration mode

**Usage Guide** The default administrative distance of the static route is 1. Setting the administrative distance allows the learnt dynamic route to overwrite the static route. Setting the administrative distance of the static route can enable route backup, which is called floating route in this case. For example, the administrative distance of the RIP is 120. You can set its administrative distance to 125. Then the data can switch over the static route when the route running RIP fails.

The default weight of the static route is 1. To view the static route of non default weight, execute the **show ip route weight** command. The parameter weight is used to enable WCMP. When there are

load-balanced routes to the destination, the device assigns data flows by their weights. The higher the weight of a route is, the more data flow the route carries. WCMP limit is generally 32 for routers. When the sum of the weights of load balanced routes is beyond this weight limit, the excessive ones will not take effect.

Enablement/disablement shows the state of the static route. Disablement means the static route is not used for forwarding. The forwarding table used the permanent route until administrator deletes it. When you configure the static route on an Ethernet interface, do not set the next hop as an interface, for example, `ip route 0.0.0.0 0.0.0.0 vlan 1`. In this case, the switch may consider that all unknown destination networks are directly connected to the vlan 1. So it sends an ARP request to every destination host, which occupies many CPU and memory resources. It is not recommended to set the static route to an Ethernet interface.

The following example adds a static route to the destination network of 172.16.100.0/24 whose next hop is 192.168.12.1 and administrative distance is 155.

```
Ruijie(config)# ip route 172.16.199.0 255.255.255.0 192.168.12.1 155
```

### Examples

If the static route has not a specific interface, data flows may be sent through other interface in case of interface failure. The following example configures data flows to be sent through vlan 1 to the destination network of 172.16.100.0/24.

```
Ruijie(config)# ip route 172.16.199.0 255.255.255.0 vlan 1 192.168.12.1
```

### Related

**Commands**      N/A

## 3.5 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.

### Usage Guide

After the IP routing function is disabled, the device functions as a common host. The device can send and receive packets but cannot forward packets. All route-related configurations will be deleted except the static route configuration. A large number of static routes may be configured. If a user runs the **no ip routing** command, the configuration of a large number of static routes may be lost. To

prevent this situation, the static route configuration will be hidden temporarily when the **no ip routing** command is run. If the **ip routing** command is run again, the static route configuration can be restored.

Note that if the process or whole system restarts when the **no ip routing** command is run, the static route configuration will not be reserved.

**Examples** The following example disables IP routing.

```
Ruijie(config)# no ip routing
```

**Related**

**Commands** N/A

**Platform**

**Description** N/A

### 3.6 ip static route-limit

Use this command to set the upper threshold of the static route. Use the **no** or **default** form of this command to restore the default setting.

**ip static route-limit** *number*

**no ip static route-limit** *number*

**default ip static route-limit**

Parameter	Parameter	Description
<b>Description</b>	<i>number</i>	Upper threshold of static routes in the range from 1 to 10000

**Defaults** The default is 1024.

**Command Mode**

Global configuration mode

**Usage Guide** The goal is to control the number of static routes. You can view the upper threshold of the configured non-default static routes with the **show running-config** command.

**Examples** The following example sets the upper threshold of the static routes to 900 and then restores the setting to the default value.

```
Ruijie(config)# ip static route-limit 900
```

**Related**

**Commands** N/A

**Platform**

N/A

Description

### 3.7 ipv6 default-gateway

Use this command to configure the default gateway IPv6 address on 2-layer devices. Use the **no** or **default** form of this command to restore the default setting.

**ipv6 default-gateway** *ipv6-address*  
**no ipv6 default-gateway**  
**default ipv6 default-gateway**

Parameter Description	Parameter	Description
	<i>ipv6-address</i>	Sets the default gateway IPv6 address.

**Defaults** No gateway IPv6 address is configured by default.

**Command Mode** Global configuration mode

**Usage Guide** When the device does not know the destination address of a packet, the device will forward the packet to the default gateway. Use the command **show ipv6 redirects** to display default gateway configuration.

**Examples** The following example sets the default gateway IPv6 address to 10::1.

```
Ruijie(config)# ipv6 default-gateway 10::1
```

**Platform Description** N/A

### 3.8 ipv6 route

Use this command to configure an ipv6 static route. Use the **no** or **default** form of this command to restore the default setting.

**ipv6 route** *ipv6-prefix / prefix-length* { *ipv6-address* | *interface* [ *ipv6-address* ] } [ *distance* | **description** *description-text* | **tag** *tag* | **weight** *number* ] \*  
**no ipv6 route** *ipv6-prefix / prefix-length* { *ipv6-address* | *interface* [ *ipv6-address* ] } [ *distance* ]

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

<b>Description</b>	<i>prefix-length</i>	Mask length of the destination
	<i>ipv6-address</i>	The next hop IP address of the static route
	<i>interface</i>	(Optional) The next hop egress of the static route
	<i>distance</i>	(Optional) The administrative distance of the static route. The default is 1.
	<b>description</b> <i>description-text</i>	(Optional) Indicates the description of the static route. By default, no description is configured. <i>description-text</i> is a string of 1 to 60 characters.
	<b>tag</b> <i>tag</i>	(Optional) Indicates the tag value of the static route. The default is 0.
	<b>weight</b> <i>number</i>	(Optional) Indicates the weight of the static route, which must be specified when you configure equal-cost routes. The weight ranges from 1 to 8. When the weights of all equal-cost routes of a route are summed up, the sum cannot exceed the maximum number of equal-cost routes that can be configured for the route. Weighting of equal-cost routes of a route indicates the traffic ratio of these routes. The weight is 1 by default.

**Defaults** No IPv6 static route is configured by default.

**Command Mode** Global configuration mode

**Usage Guide** N/A

The following example adds a static route to the destination network of 2001::/64 whose next hop is 2002::2 and administrative distance are 115.

```
Ruijie(config)# ipv6 route 2001::/64 2002::2 115
```

### Examples

If the static route has not a specific interface, data flows may be sent through other interface in case of interface failure. The following example configures that data flows are sent through vlan 1 to the destination network of 2001::/64.

```
Ruijie(config)# ipv6 route 2001::/64 vlan 1 2002::2
```

Related	Command	Description
<b>Commands</b>	<b>show ipv6 route</b>	Displays IPv6 routing table.

**Platform Description** N/A



### 3.9 ipv6 static route-limit

Use this command to set the upper threshold of the static route. Use the **no** or **default** form of this command to restore the default setting.

**ipv6 static route-limit** *number*

**no ipv6 static route-limit** *number*

**default ipv6 static route-limit**

Parameter	Parameter	Description
Description	<i>number</i>	Upper threshold of static routes in the range from 1 to 10000.

**Defaults** The default is 1000.

**Command Mode** Global configuration mode

**Usage Guide** The goal is to control the number of static routes. You can view the upper threshold of the configured non-default static routes with the show running config command.

**Examples** The following example sets the upper threshold of the ipv6 static routes to 900 and then restores the setting to the default value.

```
Ruijie(config)# ipv6 static route-limit 900
Ruijie(config)# no ipv6 static route-limit
```

Related Commands	Command	Description
	<b>ipv6 route</b>	Configures the IPv6 static route.
	<b>show ipv6 route</b>	Displays the IPv6 routing table.

**Platform Description** N/A

### 3.10 ipv6 unicast-routing

Use this command to enable the IPv6 route function of the RGOS. Use the **no** or **default** form of this command to disable this function.

**ipv6 unicast-routing**

**no ipv6 unicast-routing**

**default ipv6 unicast-routing**

**Parameter Description** N/A

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

**Command**

**Mode** Global configuration mode

**Usage Guide** This function can be disabled if the device is just used as the bridge-connection device or the VOIP gateway device.

**Examples** The example disables the IPv6 route function of RGOS.

```
Ruijie(config)# no ipv6 unicast-routing
```

Related Commands	Command	Description
	<b>ipv6 route</b>	Configure the IPv6 static route.
	<b>show ipv6 route</b>	Displays the IPv6 routing table.

**Platform**

**Description** N/A

### 3.11 show ip redirects

Use this command to display the IPv4 default gateway IP address.

**show ip redirects**

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

**Defaults** N/A

**Command**

**Mode** All CLI user modes except user EXEC mode

**Usage Guide** Use this command to display the default gateway IP address. This command is supported with the **no ip routing** command executed.

The following example displays the default gateway.

```
Ruijie# show ip redirects
Default Gateway: 192.168.195.1
```

**Examples**

Field	Description
Default Gateway	IP address of the default gateway.

Related Commands	Command	Description
	N/A	N/A

#### Platform

Description N/A

## 3.12 show ip route

Use the commands to display the configuration of the IP routing table.

```
show ip route [ network [ mask [ longer-prefix ] ] | count [ [ ecmp | normal ] [ network [ mask ] ] ] /
protocol | weight ]
```

Parameter	Description
<i>network</i>	(Optional) The route information to the network.
<i>mask</i>	(Optional) 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, it displays one route.)
<b>ecmp</b>	Displays only equivalent routes.
<b>normal</b>	Displays normal routes, instead of equivalent routes and fast reroutes.
<i>protocol</i>	(Optional) The route information of specific protocol.
<b>weight</b>	(Optional) Displays the route information of non default weight.

**Defaults** All routes are displayed by default.

#### Command

**Mode** All CLI user modes except user EXEC mode

#### Usage Guide

This command can display route information flexibly.

This command shows all routes. To show different attributes of routes, specify normal or ecmp.

- The following example displays the configuration of the IP routing table.

#### Examples

```
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, * - candidate default

Gateway of last resort is no set
S    20.0.0.0/8 is directly connected, VLAN 1
S    22.0.0.0/8 [1/0] via 20.0.0.1
```

```
R 40.0.0.0/8 [120/20] via 192.1.1.2, 00:00:23, VLAN 1
C 192.1.1.0/24 is directly connected, VLAN 1
C 192.1.1.254/32 is local host.
```

Description of fields in the command output is as follows:

Field	Description
S	Source routing protocol, which may be: C: directly connected route S: static route R: RIP route
20.0.0.0/8	Network address and mask of the destination network
[1/0]	Administrative distance/metric
Via 20.0.0.1	Next-hop IP address
00:00:06	Lifetime of protocol route
VLAN 1	Next-hop forwarding interface

2. The following example displays the routing information of destination 30.0.0.0.

```
Ruijie# show ip route 30.0.0.0
Routing entry for 30.0.0.0/8
Distance 120, metric 20
Routing Descriptor Blocks:
192.1.1.1, 00:01:11 ago, via VLAN 1, generated by RIP
```

Description of fields in the command output is as follows:

Field	Description
distance	Route management distance
metric	Route metric
Routing Descriptor Blocks	Display the next-hop IP address, routing source, update time, interface, source routing protocol, type, BGP community attribute, etc.
00:01:11 ago	Protocol routing lifetime

3. The following example displays the number of routes.

```
Ruijie# show ip route count
----- route info -----
the num of active route: 9
```

Description of fields in the command output is as follows:

Field	Description
the num of active route	Number of valid routes

```
Ruijie# show ip route weight
```

```
-----[distance/metric/weight]-----
S   23.0.0.0/8 [1/0/2] via 192.1.1.20
S   172.0.0.0/16 [1/0/4] via 192.0.0.1
```

Description of fields in the command output is as follows:

Field	Description
S	Source routing protocol
distance	Route management distance
metric	Route metric
weight	Route weight

Related Commands	Command	Description
	N/A	N/A

#### Platform

Description N/A

### 3.13 show ip route summary

Use this command to display the statistical information about routing table.

**show ip route summary [ all ]**

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

#### Command

Mode All CLI user modes except user EXEC mode

#### Usage

N/A

#### Guideline

- 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
```

#### Examples

```
IP routing table count: 0
```

```
Total
```

```
Memory: 756 bytes
```

```
Entries: 7, based on route prefixes
```

	NORMAL	ECMP	FRR	TOTAL
Connected	6	0	0	6
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	7	0	0	7

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: 756 bytes
Entries: 7, based on route prefixes

          NORMAL    ECMP    FRR    TOTAL
Connected 6         0         0         6
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     7         0         0         7

Global
Memory: 756 bytes
Entries: 7, based on route prefixes

          NORMAL    ECMP    FRR    TOTAL
Connected 6         0         0         6
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     7         0         0         7
```

Description of fields in the command output is as follows:

Field	Description
-------	-------------

NORMAL	Type of the table entries. Value: NORMAL: common routes (not ECMP or FRR); ECMP: equivalent route; FRR: fast reroute; TOTAL: total
Memory	Memory occupied by the table.
Entries	Number of entries (based on prefix, not next-hop)
Connected	Protocol type. Value: Connected: direct connection; Static: static; RIP: RIP; OSPF: OSPF; ISIS: ISIS; BGP: BGP; TOTAL: total

Related	Command	Description
Commands	N/A	N/A

**Platform**

Description N/A

### 3.14 show ipv6 redirects

Use this command to display the IPv6 default gateway IP address.

**show ipv6 redirects**

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

**Command****Mode**

All CLI user modes except user EXEC mode

**Usage Guide**

N/A

The following example displays the default gateway IPv6 address.

```
Ruijie# show ipv6 redirects
Default Gateway: 10::1
```

**Examples**

Field	Description
Default Gateway	IPv6 address of the default gateway

Related	Command	Description
Commands	N/A	N/A

**Platform**

Description N/A

### 3.15 show ipv6 route

Use the command to display the configuration of the IPv6 routing table.

**show ipv6 route** [ [ *ipv6-prefix / prefix-length* [ **longer-prefixes** ] | **local** | *protocol* | **weight** ] ]

Parameter	Description
<i>ipv6-prefix/prefix-length</i>	(Optional) A prefix for route's IPv6 address.
<b>longer-prefixes</b>	(Optional) Displays the route with an IPv6 address prefix mostly matched.
<b>local</b>	(Optional) Displays IPv6 local route.
<i>protocol</i>	(Optional) The route information of specific protocol.
<b>weight</b>	(Optional) Displays the non-default-weight routes only.

**Defaults** All routes are displayed by default.

**Command**

**Mode** All CLI user modes except user EXEC mode

**Usage Guide** Use this command to display route information.

The following example displays the output of this command.

```

Ruijie(config)# show ipv6 route
IPv6 routing table - Default - 7 entries
Codes: C - Connected, L - Local, S - Static
       R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area
C      10::/64 via Loopback 1, directly connected
L      10::1/128 via Loopback 1, local host
S      20::/64 [20/0] via 10::4, Loopback 1C
C      FE80::/10 via Null 0, directly connected
C      FE80::/64 via Loopback 1, directly connected
L      FE80::2D0:F8FF:FE22:33AB/128 via Loopback 1, local host

```

**Examples**



Description of fields in the command output is as follows:

Field	Description
C	Source routing protocol, which may be: C: directly connected route S: static route R: RIP route
20::/64	Network address and mask of the destination network
[20/0]	Administrative distance/metric

Related Commands	Command	Description
	<code>ipv6 route</code>	Configures the IPv6 static route.

#### Platform

Description N/A

## 3.16 show ipv6 route summary

Use this command to display the statistics of the IPv6 routing table.

**show ipv6 route summary [ all ]**

Parameter	Parameter	Description
Description		

#### Command

**Mode** All CLI user modes except user EXEC mode

**Usage Guide** N/A

The following example displays statistics of IPv6 routing table.

**Examples**

```
Ruijie#show ipv6 route summary
IPv6 routing table name is - Default(0) global scope - 0 entries
IPv6 routing table default maximum-paths is 1
Local          2
Connected     3
Static         0
RIP            0
-----
```

```
Total          5
```

The following example displays the statistics of all IPv6 routing tables.

```
Ruijie# show ipv6 route summary all
```

```
IPv6 routing table count: 1
```

```
Total
```

```
Memory: 0 bytes
```

```
Entries: 0
```

```
Local:0,Connected:0,Static:0,RIP:0,OSPF:0,ISIS:0,BGP:0
```

```
Global
```

```
Memory: 0 bytes
```

```
Entries: 0
```

```
Local:0,Connected:0,Static:0,RIP:0,OSPF:0,ISIS:0,BGP:0
```

Description of fields in the command output is as follows:

Field	Description
Memory	The memory size occupied by the current routing table.
Entries	The entries in the current routing table (based on the entry prefix instead of the next hop entry.)
Connected	Describes the protocol type of the entry. The field can be: Connected: Connected route entry. Static: Static route entry. RIP: RIP route entry. OSPF: OSPF route entry. ISIS: ISIS route entry. BGP: BGP route entry. TOTAL: Total number of all protocol entries.
IPv6 routing table count	The number of the routing tables.
Global	The name of the current routing table. The field can be: Global : Global (The default VRF) TOTAL: All VRF routing table summaries.

**Related  
Commands**

Command	Description
N/A	N/A

**Platform  
Description**

N/A

# 4 Keys Commands(beta)

## 4.1 accept-lifetime

Use this command in the encryption key configuration mode to specify the lifetime of an encryption key in its receiving direction. Use the no form of this command to restore the default value.

**accept-lifetime** *start-time* {infinite | *end-time* | **duration** *seconds*}

**no accept-lifetime**

Parameter description	Parameter	Description
	<i>start-time</i>	Start time of the lifetime. The syntax is as follows: <i>hh:mm:ss month date year</i> <i>hh:mm:ss date month year</i> <ul style="list-style-type: none"> <li>● hh—hour</li> <li>● mm—minute</li> <li>● ss—second</li> <li>● month—month</li> <li>● date—day</li> <li>● year—year</li> </ul> The default start time is Jun 1, 1993, which is also the earliest start time available.
	<b>infinite</b>	Indicates that the encryption key is valid for ever.
	<i>end-time</i>	<i>End time of the encryption key. It must be later than the start time.</i>
	<b>duration</b> <i>seconds</i>	Duration of the encryption key after the start time. The value ranges from 1 to 2147483646.

**Default** infinite

**Command mode** Encryption key configuration mode

**Usage guideline** Use this command to specify the lifetime of an encryption key in its receiving direction.

**Examples** The following example configures the lifetime of key 1.

```
Ruijie(config)#key chain kc

Ruijie(config-keychain)#key 1

Ruijie(config-keychain-key)#key-string Hello
Ruijie(config-keychain-key)#accept-lifetime 16:30:00 Oct 1 2010 duration 43200
```

Related command	Command	Description
	-	-

Platform description

-

## 4.2 key

Use this command to define an encryption key and enter the encryption key chain configuration mode.

Use the no form of this command to delete it.

**key** *key-id*

**no key** *key-id*

Parameter description	Parameter	Description
	<i>key-id</i>	Key ID, ranging from 0 to 2147483647.

**Default** No encryption key is configured.

**Command mode** Encryption key chain configuration mode.

**Usage guideline** Use this command to define an encryption key.

**Examples** The following example configures encryption key chain ripkeys and key 1.

```
Ruijie(config)# key chain ripkeys
Ruijie(config-keychain)# key 1
```

Related command	Command	Description
	-	-

Platform description

-

## 4.3 key chain

Use this command to define a key chain and enter the key chain configuration mode. Use the no form of this command to delete it.


**key chain** *key-chain-name*

**no key chain** *key-chain-name*

Parameter description	Parameter	Description
	<i>key-chain-name</i>	Key chain name.

**Default** No key chain is configured.

**Command mode** Global configuration mode.

**Usage guideline**  For a key chain to take effect, you need to configure at least one key.

**Examples** The following example configures key chain ripkeys and enters the key chain configuration mode.

```
Ruijie(config)# key chain ripkeys
```

Related command	Command	Description
	-	-

**Platform description** -

## 4.4 key-string

Use this command to specify a key string. Use the no form of this command to delete it.

**key-string** [0|7] *text*

**no key-string**

Parameter description	Parameter	Description
	<b>0</b>	Use plaintext.
	<b>7</b>	Use encryption.
	<i>text</i>	Authentication string.

**Default** No key string is configured.

**Command mode** Encryption key configuration mode.

**Usage guideline** Use this command to specify a key string.

**Examples** The following example configures key chain ripkeys, key 1 and the key string abc:

```
Ruijie(config)# key chain ripkeys
Ruijie(config-keychain)# key 1
Ruijie(config-keychain-key)#key-string abc
```

Related command	Command	Description
	-	-

**Platform** -

**description**

## 4.5 send-lifetime

Use this command in the encryption key configuration mode to specify the lifetime of an encryption key in its send direction. Use the no form of this command to restore the default value.

**send-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}

**no send-lifetime**

Parameter	Parameter	Description
<b>description</b>	<i>start-time</i>	Start time of the lifetime.
	<b>infinite</b>	Indicates that the encryption key is valid for ever.
	<i>end-time</i>	<i>End time of the encryption key. It must be later than the start time.</i>
	<b>duration</b> <i>seconds</i>	Duration of the encryption key after the start time. The value ranges from 1 to 2147483646.

**Default** infinite

**Command mode** Encryption key configuration mode

**Usage guideline** Use this command to specify the lifetime of an encryption key in its send direction.

**Examples** The following example configures the lifetime from 0:00 on September 9, 2000 to 0:00 on October 12, 2011

```
Ruijie(config)# key chain ripkeys
Ruijie(config-keychain)# key 1
Ruijie(config-keychain-key)# send-lifetime 00:00:00 Sep 9 2000 00:00:00 Dec 12 2011
```

Related command	Command	Description
	-	-

**Platform description** -

## 4.6 show key chain

Use this command to display the key chain configuration.

**show key chain** [*key-chain-name*]

Parameter	Parameter	Description
<b>description</b>	<i>key-chain-name</i>	(Optional) Display the configuration of the specified key chain.

**Default** The configuration information of all key chains is displayed.

**Command mode** Privileged EXEC mode, global configuration mode, interface configuration mode, routing protocol configuration mode, and key chain configuration mode.

**Usage guideline** If no key chain is specified, the configuration information of all key chains is displayed.

**Examples**

```
Ruijie# show key chain
route-map AAA, permit, sequence 10
Match clauses:
ip address 2
Set clauses:
metric 10
Ruijie(config)#show key chain
key chain kc
  key 1 -- text "ruijie"
    accept-lifetime (12:11:00 May 2 2001) - (infinite)
    send-lifetime (always valid) - (always valid) [valid now]
```

Description of fields in the command output is as follows:

Field	Description
key chain	Key chain name.
key	Key ID.
accept-lifetime	Lifetime in the accept direction.
send-lifetime	Lifetime in the send direction.

**Related command**

Command	Description
-	-

**Platform description**

-

# 5 Routing Policies Commands(beta)

## 5.1 ip prefix-list

Use this command to create a prefix list or add an entry to the prefix list. Use the **no** form of this command to remove the prefix list or an entry.

**ip prefix-list** *prefix-list-name* [ **seq** *seq-number* ] { **deny** | **permit** } *ip-prefix* [**ge** *minimum-prefix-length*][ **le** *maximum-prefix-length*]

**no ip prefix-list** *prefix-list-name* [ **seq** *seq-number* ] { **deny** | **permit** } *ip-prefix* [**ge** *minimum-prefix-length*][ **le** *maximum-prefix-length*]

Parameter	Description
<i>prefix-list-name</i>	Name of the prefix list
<i>seq-number</i>	Sequence number of an entry in the range of 1 to 2147483647. When you execute this command to add an entry without a sequence number, the system allocates a default sequence number for the entry. The default sequence number of the first entry is 5. Every subsequential entry without a sequence number uses the time of 5 larger than the previous sequence number as the default sequence number.
<b>deny</b>	Denies the route matching the prefix list.
<b>permit</b>	Permits the route matching the prefix list.
<i>ip-prefix</i>	Network address and mask. Network address can be any valid IP address and the mask length is in the range of 0 to 32.
<i>minimum-prefix-length</i>	(Optional) Minimum length of the prefix (the starting length) Note: "ge" indicates the operation of "larger than" and "equivalent to".
<i>maximum-prefix-length</i>	(Optional) Maximum length of the prefix (the ending length) Note: "le" indicates the operation of "less than" and "equivalent to".

### Parameter description

### Default

**configuration** None

### Command mode

Global configuration mode.

### Usage guidelines

The ip prefix-list command configures the prefix list, with the permit or deny keyword to determine the action in case of matching.



You can execute this command to define an exact match, or use “ge” or “le” to define a range match for a prefix for flexible configuration. “ge” indicates the range of minimum-prefix-length to 32; “le” indicates the range of the mask length of the IP prefix to maximum-prefix-length; “ge” and “le” indicates the range of minimum-prefix-length to maximum-prefix-length, namely, mask length of IP prefix < minimum-prefix-length < maximum-prefix-length <=32.

The following example filters the static routes the RIP redistributes by the destination IP address following the rule defined in the associated IP prefix list, for example, redistribute the routes whose destination IP address is in the range 201.1.1.0/24.

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# ip prefix-list pre1 permit 201.1.1.0/24
Ruijie(config)# router rip
Ruijie(config-router)# distribute-list prefix pre1 out static
Ruijie(config-router)# end
```

## 5.2 ip prefix-list description

Use this command to add the description of a prefix list. Use the **no** form of this command to delete the description.

**ip prefix-list** *prefix-list-name* **description** *description-text*

	Parameter	Description
<b>Parameter description</b>	<i>prefix-list-name</i>	Name of the prefix list
	<i>description-text</i>	Description of the prefix list

**Default**

**configuration** No description is added for a prefix list, by default.

**Command**

**mode** Global configuration mode

The example below adds the description for the prefix list:

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# ip prefix-list pre description Deny
```

## 5.3 ip prefix-list sequence-number

Use this command to enable sort function for a prefix list. Use the **no** form of this command to disable the sort function.

**ip prefix-list** **sequence-number**

**Parameter description** Disabled

**Default**

**configuration** No sequence number is added for a prefix list, by default.

**Command**

**mode** Global configuration mode

The example below adds a sequence number for the prefix list:

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# ip prefix-list pre description deny
```

**Related****commands**

Command	Description
<b>ip prefix-list</b>	Configures the prefix list.

**Platform**

**description** N/A

## 5.4 ipv6 prefix-list

Use this command to create an IPv6 prefix list or add an entry in the prefix list. Use the **no** form of this command to delete an IPv6 prefix list or an entry in the prefix list.

**ipv6 prefix-list** *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ipv6-prefix* [**ge** *minimum-prefix-length*][**le** *maximum-prefix-length*]

**no ipv6 prefix-list** *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ipv6-prefix* [**ge** *minimum-prefix-length*][**le** *maximum-prefix-length*]

**Parameter description**

Parameter	Description
<i>prefix-list-name</i>	Name of the prefix list
<i>seq-number</i>	Sequence number of an entry in the prefix list. Its range is 1 to 4294967294. If the sequence number is not specified in this command, the system will allocate a default one for the entry. The default sequence number of the first entry is 5, and that of each subsequent one is the product of adding 5 to the sequence number of the proceeding entry.
<b>permit</b>	Permits the access to the matching result.
<b>deny</b>	Denies the access to the matching result.
<i>ipv6-prefix</i>	Network address and its mask. The network address can be any valid IP address. The mask can be 0 to 32 characters.
<i>minimum-prefix-length</i>	(Optional) Minimum length of the prefix (the starting length) Note: "ge" indicates the operation of "larger than" and "equivalent to".
<i>maximum-prefix-length</i>	(Optional) Maximum length of the prefix (the ending length) Note: "le" indicates the operation of "less than" and "equivalent to".

**Default**

**configuration** No prefix list is created.

**Command**

**mode** Global configuration mode

The ipv6 prefix-list command configures the prefix list, with the permit or deny keyword to determine the action in case of matching.

**Usage guideline**

You can execute this command to define an exact match, or use “ge” or “le” to define a range match for a prefix for flexible configuration. “ge” indicates the range of minimum-prefix-length to 128; “le” indicates the range of the mask length of the IP prefix to maximum-prefix-length; “ge” and “le” indicates the range of minimum-prefix-length to maximum-prefix-length, namely, ipv6-prefix mask length < minimum-prefix-length < maximum-prefix-length <= 128

The following example filters the static routes the RIP redistributes by the destination IP address following the rule defined in the associated IP prefix list, for example, redistribute the routes whose destination IP address is in the range 2222::/64.

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# ipv6 prefix-list pre1 permit 2222::64/64
Ruijie(config)# ipv6 router rip
Ruijie(config-router)# distribute-list prefix pre out
Ruijie(config-router)# end
```

## 5.5 ipv6 prefix-list description

Use this command to add the description of an IPv6 prefix list. Use the **no** form of this command to delete the description.

**ipv6 prefix-list** *prefix-lis-name* **description** *description-text*

**no ipv6 prefix-list** *prefix-lis-name* **description** *description-text*

Parameter	Description
<i>prefix-lis-name</i>	Name of the ipv6 prefix list
<i>description-text</i>	Description of the ipv6 prefix list

**Default**

**configuration** No description is added for an IPv6 prefix list, by default.

**Command**

**mode** Global configuration mode

The example below adds the description for the prefix list:

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# ipv6 prefix-list pre description Deny
```

Related	Command	Description
commands	<b>ipv6 prefix-list</b>	Configures the IPv6 prefix list.

## 5.6 ipv6 prefix-list sequence-number

Use this command to enable the sorting function for an IPv6 prefix list. Use the **no** form of this command to remove the settings.

**ipv6 prefix-list sequence-number**

**no ipv6 prefix-list sequence-number**

**Parameter description** Disabled.

**Default configuration** No sequence number is added for a prefix list, by default.

**Command mode** Global configuration mode

The example below adds a sequence number for the prefix list:

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# ipv6 prefix-list pre description Deny
```

Related	Command	Description
commands	<b>ipv6 prefix-list</b>	Configures the IPv6 prefix list.

## 5.7 match interface

Use **match interface** command to redistribute the routes whose next hop is the specified interface.

Use the **no** form of this command to remove the setting.

**match interface** *interface-type interface-number* [*...interface-type interface-number*]

**no match interface** [*interface-type interface-number* [*...interface-type interface-number*]]

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

**Default configuration** None.

**Command** Route map configuration mode.

**mode**

This command can be followed by multiple interfaces.

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the static routes in the RIP routing domain. The mutual route redistribution can be implemented between all the IP routing protocols.

**Usage guidelines**

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

The route map can be configured very flexibly for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.

The following example redistributes the static route with the next hop of vlan 1 in the RIP routing protocol.

**Examples**

```
Ruijie(config)#router rip
Ruijie(config-router)#redistribute static route-map redrip
Ruijie(config-router)#network 192.168.12.0 0.0.0.255
Ruijie(config-router)#
Ruijie(config-router)#route-map redrip permit 10
Ruijie(config-route-map)#match interface vlan 1
```

**Related commands**

Command	Description
<b>match ip address</b>	Matches the address in the access list.
<b>match ip next-hop</b>	Matches the next-hop IP address in the access list.
<b>match ip route-source</b>	Matches the source IP address in the access list.
<b>match metric</b>	Matches the metric.
<b>match tag</b>	Matches the tag.
<b>set metric</b>	Sets the metric.
<b>set tag</b>	Sets the tag.

## 5.8 match ip address

Use **match ip address** command to redistribute the routes matching the IP address permitted by the ACL or the prefix list. Use the **no** form of this command to remove the setting.

**match ip address** {*access-list-number* [*access-list-number* | *access-list-name*] [*access-list-name* [*access-list-number*|*access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name*]]}

**no match ip address** [*access-list-number* [*access-list-number* | *access-list-name*] [*access-list-name* [*access-list-number*|*access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name*]]]

	Parameter	Description
<b>Parameter description</b>	<i>access-list-number</i>	Number of the access list
	<i>access-list-name</i>	Name of the access list
	<b>prefix-list</b> <i>prefix-list-name</i>	Specifies the prefix list to match.

**Default configuration** None.

**Command mode** Route map configuration mode.

Multiple access list numbers or names may follow match ip address.

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the static routes in the RIP routing domain. The mutual route redistribution can be implemented between all the IP routing protocols.

**Usage guidelines**

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

The route map can be configured very flexibly for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.

The following example enables the RIP routing protocol to redistribute static routes that match access list 10 and the default metric being 40.

**Examples**

```
Ruijie(config)#router rip
Ruijie(config-router)#redistribute static route-map redrip
Ruijie(config-router)#network 192.168.12.0 0.0.0.255
Ruijie(config-router)#
Ruijie(config-router)#route-map redrip permit 10
Ruijie(config-route-map)#match ip address 10
Ruijie(config-route-map)#set metric 40
Ruijie(config-route-map)#
```

**Related commands**

Command	Description
<b>access-list</b>	Sets the access list.
<b>match interface</b>	Matches the next-hop interface of the route.
<b>match ip next-hop</b>	Matches the next-hop address in the access list.
<b>match ip route-source</b>	Matches the route source address in the access list.
<b>match metric</b>	Matches the metric.
<b>match tag</b>	Matches the tag.

<b>set metric</b>	Sets the metric.
<b>set tag</b>	Sets the tag.

## 5.9 match ip next-hop

Use **match ip next-hop** command to redistribute the routes whose next-hop IP address matches the access list or the prefix list. Use the **no** form of this command to remove the setting.

**match ip next-hop** {*access-list-number* [*access-list-number* | *access-list-name*] | *access-list-name* [*access-list-number*|*access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name*]}

**no match ip next-hop** [*access-list-number* [*access-list-number* | *access-list-name*] | *access-list-name* [*access-list-number*|*access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name*]]

Parameter	Description
<i>access-list-number</i>	Number of the access list
<i>access-list-name</i>	Name of the access list
<b>prefix-list</b> <i>prefix-list-name</i>	Specifies the prefix list to match.

### Default

**configuration** None.

### Command

**mode** Route map configuration mode.

Multiple access list numbers or names may follow match ip next-hop.

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the static routes in the RIP routing domain. The mutual route redistribution can be implemented between all the IP routing protocols.

### Usage

#### guidelines

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

In the example below, the RIP routing protocol redistributes the static routes. As long as the next hop address of the static route matches the access list 10 or 20, the RIP allows for redistribution.

### Examples

```
Ruijie(config)# router rip
Ruijie(config-router)# redistribute static route-map redrip
Ruijie(config-router)# network 192.168.12.0 0.0.0.255
Ruijie(config-router)# exit
Ruijie(config)# access-list 10 permit host 192.168.10.1
Ruijie(config)# access-list 20 permit host 172.16.20.1
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# match ip next-hop 10 20
```

	Command	Description
Related commands	<b>access-list</b>	Sets the access list.
	<b>match ip address</b>	Matches the IP address in the access list.
	<b>match interface</b>	Matches the next-hop interface of the route.
	<b>match ip route-source</b>	Matches the route source address in the access list.
	<b>match metric</b>	Matches the metric.
	<b>match tag</b>	Matches the tag.
	<b>set metric</b>	Sets the metric.
	<b>set tag</b>	Sets the tag.

## 5.10 match ip route-source

Use **match ip route-source** command to redistribute the routes whose source IP address matches the access list. Use the **no** form of this command to remove the setting.

**match ip route-source** {*access-list-number* [*access-list-number* | *access-list-name*] | *access-list-name* [*access-list-number*|*access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name*]}

**no match ip route-source** [*access-list-number* [*access-list-number* | *access-list-name*] | *access-list-name* [*access-list-number*|*access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name*]]

	Parameter	Description
Parameter description	<i>access-list-number</i>	Number of the access list
	<i>access-list-name</i>	Name of the access list
	<b>prefix-list</b> <i>prefix-list-name</i>	Specifies the prefix list to match.

**Default configuration** None.

**Command mode** Route map configuration mode.

Multiple access list numbers may follow match ip route-source.

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the static routes in the RIP routing domain. The mutual route redistribution can be implemented between all the IP routing protocols.

### Usage guidelines

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

**Examples** In the example below, the RIP routing protocol redistributes the static routes. As long as the source IP address of the static route matches the access list 5, the RIP allows for redistribution.

```
Ruijie(config)# access-list 5 permit 192.168.100.1 0.0.0.255
```



```
Ruijie(config)#router rip
Ruijie(config-router)#redistribute static route-map redrip
Ruijie(config-router)#network 192.168.12.0 0.0.0.255
Ruijie(config-router)#
Ruijie(config-router)#route-map redrip permit 10
Ruijie(config-route-map)# match ip route-source 5
Ruijie(config-route-map)#
```

#### Related commands

Command	Description
<b>access-list</b>	Sets the access list.
<b>match ip address</b>	Matches the IP address in the access list.
<b>match interface</b>	Matches the next-hop interface of the route.
<b>match ip next-hop</b>	Matches the next-hop IP address in the access list.
<b>match metric</b>	Matches the metric.
<b>match tag</b>	Matches the tag.
<b>set metric</b>	Sets the metric.
<b>set tag</b>	Sets the tag.

## 5.11 match ipv6 address

Use this command to redistribute the network routes permitted in the IPv6 access list or the IPv6 prefix list. Use the **no** form of this command to delete the setting.

**match ipv6 address** { *access-list-name*] | **prefix-list** *prefix-list-name* }

**no match ipv6 address**

#### Parameter description

Parameter	Description
<i>access-list-name</i>	Name of the access list.
<b>prefix-list</b> <i>prefix-list-name</i>	Specifies the IPv6 prefix list to match.

#### Default

**configuration** None

#### Command

**mode** Route map configuration mode

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the static routes in the RIP routing domain. The mutual route redistribution can be implemented between all the IP routing protocols.

#### Usage guideline

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

The route map can be configured very flexibly to be used for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.

The following example enables the RIP routing protocol to redistribute static routes that match access list v6acl, with the default metric being 30.

**Examples**

```
Ruijie(config)#ipv6 access-list v6acl
Ruijie(config-ipv6-acl)#10 permit ipv6 host 2620::64 any
Ruijie(config-ipv6-acl)#exit
Ruijie(config)#ipv6 router rip
Ruijie(config-router)#redistribute static route-map redrip
Ruijie(config-router)#route-map redrip permit 10
Ruijie(config-route-map)#match ipv6 address v6acl
Ruijie(config-route-map)#set metric 30
```

**Related commands**

Command	Description
<b>ipv6 access-list</b>	Sets the IPv6 access list.
<b>match interface</b>	Matches the next-hop interface of the route.
<b>match ipv6 next-hop</b>	Matches the next-hop address in the IPv6 access list.
<b>match ipv6 route-source</b>	Matches the route source address in the IPv6 access list.
<b>match metric</b>	Matches the route metric.
<b>match tag</b>	Matches the route tag.
<b>set metric</b>	Sets the metric for route redistribution.
<b>set tag</b>	Sets the tag for route redistribution.

## 5.12 match ipv6 next-hop

Use this command to redistribute the network routes whose next-hop IP address matches the IPv6 access list or the IPv6 prefix list. Use the **no** form of this command to delete the setting.

**match ipv6 next-hop** { *access-list-name* | **prefix-list** *prefix-list-name* }

**no match ipv6 next hop**

**Parameter description**

Parameter	Description
<i>access-list-name</i>	Name of the IPv6 access list.
<b>prefix-list</b> <i>prefix-list-name</i>	Specifies the IPv6 prefix list to match.

**Default**

**configuration** None

**Command**

**mode** Route map configuration mode

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the static routes in the RIP routing domain. The mutual route redistribution can be implemented between all the IP routing protocols.

**Usage**

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

**guideline**

One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

The route map can be configured very flexibly to be used for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.

The following example enables the RIP routing protocol to redistribute static routes that only match access list v6acl, with the default metric being 40.

**Examples**

```
Ruijie(config)#ipv6 access-list v6acl
Ruijie(config-ipv6-acl)#10 permit ipv6 host 2620::64 any
Ruijie(config-ipv6-acl)#exit
Ruijie(config)#ipv6 router rip
Ruijie(config-router)#redistribute static route-map redrip
Ruijie(config-router)#route-map redrip permit 10
Ruijie(config-route-map)#match ipv6 address v6acl
Ruijie(config-route-map)#set metric 40
```

**Related commands**

Command	Description
<b>ipv6 access-list</b>	Sets the IPv6 access list.
<b>match interface</b>	Matches the next-hop interface of the route.
<b>match ipv6 address</b>	Matches the IP address in the IPv6 access list.
<b>match ipv6 route-source</b>	Matches the route source address in the IPv6 access list.
<b>match metric</b>	Matches the route metric.
<b>match tag</b>	Matches the route tag.
<b>set metric</b>	Sets the metric for route redistribution.
<b>set tag</b>	Sets the tag for route redistribution.

## 5.13 match ipv6 route-source

Use this command to redistribute the network routes whose next-hop IP address matches the IPv6 access list or the IPv6 prefix list. Use the **no** form of this command to delete the setting.

```
match ipv6 route-source { access-list-name | prefix-list prefix-list-name }
no match ipv6 route-source
```

Parameter	Description
<i>access-list-name</i>	Name of the IPv6 access list.
<b>prefix-list</b> <i>prefix-list-name</i>	Specifies the IPv6 prefix list to match.

**Default configuration** None

**Command mode** Route map configuration mode

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the static routes in the RIP routing domain. The mutual route redistribution can be implemented between all the IP routing protocols.

**Usage guideline** In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.  
In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

The route map can be configured very flexibly to be used for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.

The following example enables the RIP routing protocol to redistribute static routes that only match access list v6acl, with the default metric being 50.

```
Examples
Ruijie(config)#ipv6 access-list v6acl
Ruijie(config-ipv6-acl)#10 permit ipv6 host 5200::64 any
Ruijie(config-ipv6-acl)#exit
Ruijie(config)#ipv6 router rip
Ruijie(config-router)#redistribute static route-map redrip
Ruijie(config-router)#route-map redrip permit 10
Ruijie(config-route-map)#match ipv6 address v6acl
Ruijie(config-route-map)#set metric 50
```

Command	Description
<b>ipv6 access-list</b>	Sets the IPv6 access list.
<b>match interface</b>	Matches the next-hop interface of the route.
<b>match ipv6 address</b>	Matches the IP address in the IPv6 access list.

<b>match ipv6 next-hop</b>	Matches the next hop in the IPv6 access list.
<b>match metric</b>	Matches the route metric.
<b>match tag</b>	Matches the route tag.
<b>set metric</b>	Sets the metric for route redistribution.
<b>set tag</b>	Sets the tag for route redistribution.

## 5.14 match metric

Use **match metric** command to redistribute the routes of the specified metric. Use the **no** form of this command to remove the setting.

**match metric** *metric*

**no match metric** *metric*

Parameter	Parameter	Description
<b>description</b>	<i>metric</i>	Route metric, in the range of 0 to 4294967295

### Default

**configuration** None.

### Command

**mode** Route map configuration mode.

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the static routes in the RIP routing domain. The mutual route redistribution can be implemented between all the IP routing protocols.

### Usage

#### guidelines

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

In the example below, the RIP routing protocol redistributes the static routes of metric 10.

### Examples

```
Ruijie(config)#router rip
Ruijie(config-router)#redistribute static route-map redrip
Ruijie(config-router)#network 192.168.12.0 0.0.0.255
Ruijie(config-route-map)#match metric 10
Ruijie(config-route-map)#
```

Related	Command	Description
<b>commands</b>	<b>access-list</b>	Sets the access list.
	<b>match ip address</b>	Matches the IP address.
	<b>match interface</b>	Matches the interface.

<b>match ip next-hop</b>	Matches the next-hop IP address.
<b>match ip route-source</b>	Matches the source IP address.
<b>match tag</b>	Matches the tag.
<b>set metric</b>	Sets the metric.
<b>set tag</b>	Sets the tag.

## 5.15 match tag

Use this command to redistribute the network routes with the specified tag. Use the **no** form of this command to delete the setting.

**match tag** *tag* [...*tag*]

**no match tag** [*tag* [...*tag*]]

Parameter	Parameter	Description
<b>description</b>	<i>tag</i>	Route tag

**Default configuration** None

**Command mode** Route map configuration mode

Multiple tags may follow the match tag command.

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the static routes in the RIP routing domain. The mutual route redistribution can be implemented between all the IP routing protocols.

**Usage guideline**

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

In the example below, the RIP routing protocol redistributes only the static routes with tag 50 and 80.

**Examples**

```
Ruijie(config)# router rip
Ruijie(config-router)# redistribute static route-map redrip
Ruijie(config-router)# network 192.168.12.0
Ruijie(config-router)# exit
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# match tag 50 80
```

Related commands	Command	Description
	<b>access-list</b>	Sets the access list.

<b>match ip address</b>	Matches the IP address.
<b>match interface</b>	Matches the next-hop IP interface.
<b>match ip route-source</b>	Matches the source IP address.
<b>match metric</b>	Matches the metric.
<b>match ip next-hop</b>	Matches the next-hop IP address.
<b>set metric</b>	Sets the metric.
<b>set tag</b>	Sets the tag.

## 5.16 memory-lack exit-policy

Use this command to configure a policy to preferentially exit a routing protocol when the memory reaches the lower limit. Use the **no** form of this command to restore the default policy, namely, exit the routing protocol which occupies the largest memory.

**memory-lack exit-policy { pim-sm | rip }**

**no memory-lack exit-policy**

Parameter description	Parameter	Description
	<b>pim-sm</b>	Preferentially exits PIM-SM if the memory is insufficient.
	<b>rip</b>	Preferentially exits RIP if the memory is insufficient.

**Default** By default, the routing protocol which occupies the largest memory exits preferentially.

**Command mode** Global configuration mode

**Usage guideline** When the memory reaches the lower limit, you can disable a routing protocol to release the memory to ensure the normal running of other protocols.

When the system runs out of memory, disable a routing protocol which has the minimal impact on the system to ensure the operation of main services.

Configuring the policy to preferentially exit the routing protocols which are disabled cannot help the system release memory.

This command ensures the operation of main services to some extent when the memory is insufficient. If the memory is further consumed, all routing protocols will exit and stop running.

**Examples** Ruijie(config)#memory-lack exit-policy rip

Related command	Command	Description
	-	-

**Platform description** -

## 5.17 route-map

Use **route-map** to enter the route map configuration mode and define a route map. Use the **no** form of this command to remove the setting.

**route-map** *route-map-name* [**permit** | **deny**] [*sequence-number*]

**no route-map** *route-map-name* [{**permit** | **deny**}*sequence-number*]

Parameter	Description
<i>route-map-name</i>	Name of the route map. The redistribute command references the route map according to its name. Multiple routing policies can be defined in a route map, and each policy corresponds to one sequence number.
<b>permit</b>	(Optional) If the permit keyword is defined and the rule defined by match is met, The set command controls the redistributed routes. For policy-based routing, the set command controls the packet forwarding, and exits the route map operation.  If the permit keyword is defined but the rule defined by match is not met, the system performs the routing policy of the second route map till the set command is executed finally.
<b>deny</b>	(Optional) If the deny keyword is defined and the rule defined by match is met, no operation will be performed. Neither route redistribution nor policy-based routing is supported in the route map. The system exits the route map operation.  If the deny keyword is defined but the rule defined by match is not met, the system performs the routing policy of the second route map till the set command is executed finally.
<i>sequence-number</i>	Sequence number of the route map. The policy with a lower sequence number is preferred, so it's noted when setting the sequence number.

### Parameter description

### Default

**configuration** None.

### Command

**mode** Global configuration mode.

At present, the RGOS software primarily uses the route map for route redistribution and policy-based routing.

1. Route redistribution control

### Usage guidelines

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the static routes in the RIP routing domain. The mutual route redistribution can be implemented between all the IP routing protocols.

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more match or set commands can be executed to configure a route map. If the match



command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

When configuring route maps, pay attention to the following when using the sequence number of a route map:

When you create the first route map policy, if *sequence-number* is not specified, it is 10 by default;

If only one route map policy exists and *sequence-number* is not specified, no new route map policy will be created, and the existing route map policy will be accessed for configuration;

If more than one route map policy is available, the sequence number of each policy shall be specified; otherwise an error message will be displayed.

## 2. policy-based routing

Policy-based routing refers to a routing mechanism based on user defined policies. Compared with traditional destination IP address-based routing, policy-based routing offers a flexibility for routing based on source IP address, length and port of IP packets. Policy-based routing can apply to the IP packets received on an interface or the IP packets sent from the local device.

Policy-based routing utilizes route map to define routing and forwarding policy. The match command defines packet filtering rule and the set command defines the action for the packets matching the filtering rules. The match command used includes match ip address; the set command includes set ip [default] nexthop.

The following example enables the RIP routing protocol to redistribute the static routes with the hop count of 4. In the RIP route domain, the default metric is 40 and the tag is 40.

### Examples

```
Ruijie(config)#router rip
Ruijie(config-router)# redistribute static route-map redrip
Ruijie(config-router)# network 192.168.12.0 0.0.0.255
Ruijie(config-router)#route-map redrip permit 10
Ruijie(config-route-map)# match metric 4
Ruijie(config-route-map)# set metric 40
Ruijie(config-route-map)# set tag 40
```

### Related commands

Command	Description
<b>redistribute</b>	Redistribute the routes.

## 5.18 set ip default next-hop

Use this command to specify the default next-hop IP address for the packets that match the rule in the route map configuration mode. Use the **no** form of this command to remove the setting.

**set ip default next-hop** *ip-address* [ *weight* ] [ ...*ip-address* [ *weight* ] ]

**no set ip default next-hop** [ *ip-address* [ *weight* ] [ ...*ip-address* [ *weight* ] ] ]

### Parameter description

Parameter	Description
<i>ip-address</i>	IP address of the next hop.
<i>weight</i>	Weight of the next hop.

**Default****configuration** None**Command****mode** Route map configuration mode

This command supports two operation modes: WCMP load balancing mode and non-WCMP load balancing mode. In the former mode, the system implements WCMP load balancing according to the weight inputted.

Up to 32 IP addresses may follow the **set ip default next-hop** command.

If a weight follows ip address, up to 4 next hop IP addresses can be configured.

Note: If a weight follows any next-hop, the operation mode of this command will be automatically switched to the WCMP load balancing mode. In this mode, the weight of those next hop IP addresses whose weight is not configured is 1 by default.

Differences between set ip next-hop and set ip default next-hop: After the set ip next-hop command is configured, the policy-based routing takes precedence over the routing table; while after the set ip default next-hop command is configured, the routing table takes precedence over the policy-based routing.

**Usage guideline**

Use this command to customize a default route for a specified user. If the software fails to find the forwarding route, the packet will be forwarded to the nexthop set with this command.

To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded through the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

A route-map policy may contain multiple set operations.

The following example forwards the packets from two different nodes through different routes.

For the messages received on the synchronous interface 1 from 1.1.1.1, if the software cannot find the forwarding route, they are forwarded to device 6.6.6.6. For the messages received from 2.2.2.2, if the software cannot find the forwarding route, they are forwarded to device 7.7.7.7. The other messages will be discarded if the software cannot find the forwarding route.

**Examples**

```
Ruijie(config)#access-list 1 permit 1.1.1.1 0.0.0.0
Ruijie(config)#access-list 2 permit 2.2.2.2 0.0.0.0
Ruijie(config)#route-map equal-access permit 10
Ruijie(config-route-map)#match ip address 1
Ruijie(config-route-map)#set ip default next-hop 6.6.6.6
Ruijie(config)#route-map equal-access permit 20
Ruijie(config-route-map)#match ip address 2
Ruijie(config-route-map)#set ip default next-hop 7.7.7.7
Ruijie(config)#route-map equal-access permit 30
```

	Command	Description
Related commands	<b>route-map</b>	Defines a route map.
	<b>match ip address</b>	Matches the IP address.
	<b>set ip next-hop</b>	Sets the next hop of the packets.

**Platform description** N/A

## 5.19 set ip next-hop

Use this command to specify the next-hop IP address for the packets that meet the matching rule. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

**set ip next-hop** *ip-address* [ *weight* ] [ ...*ip-address* [ *weight* ] ]

**no set ip next-hop** [ *ip-address* [ *weight* ] [ ...*ip-address* [ *weight* ] ] ]

	Parameter	Description
Parameter description	<i>ip-address</i>	Next-hop IP address.
	<i>weight</i>	Weight of this next hop.

**Default configuration** None

**Command mode** Route map configuration mode

This command supports two operation modes: WCMP load balancing mode and non-WCMP load balancing mode. In the former mode, the system implements WCMP load balancing according to the weight entered by the user.

Multiple IP addresses may follow set ip next-hop and the number of addresses should be less than 32.



If weight follows any next-hop, the operation mode of this command will be automatically switched to the WCMP load balancing mode. In the WCMP load balancing mode, for the nexthop address without configuring the corresponding weight, the weight is 1 by default.

**Usage guideline**

If weight follows ip address, up to 4 next hop addresses can be configured.

This command can be used to set different routes for the traffic that meets different match rule. If multiple IP addresses are configured, they can be used in turn.

Policy-based routing is a packet forwarding mechanism more flexible than the routing based on the target network. After the policy-based routing is used, the device will decide how to process the packets that need be routed according to the route map, which decides the next-hop device of the packets.

To use the policy-based routing, you must specify the route map for it and create the route map. A route

map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

A route-map policy may contain multiple set operations.

When the interface receives the packets from 10.0.0.0/8, they will be sent to 192.168.100.1; when the interface receives the packets from 172.16.0.0/16, they will be sent to 172.16.100.1; all other packets will be discarded.

### Examples

```
Ruijie(config)#access-list 10 permit 10.0.0.0 0.255.255.255
Ruijie(config)#access-list 20 permit 172.16.0.0 0.0.255.255
Ruijie(config)#route-map load-balance permit 10
Ruijie(config-route-map)#match ip address 10
Ruijie(config-route-map)#set ip next-hop 192.168.100.1
Ruijie(config)#route-map load-balance permit 20
Ruijie(config-route-map)#match ip address 20
Ruijie(config-route-map)#set ip next-hop 172.16.100.1
```

### Related commands

Command	Description
<b>route-map</b>	Defines the route map.
<b>match ip address</b>	Matches the IP address.
<b>set ip default next-hop</b>	Sets the default next hop.

## 5.20 set ipv6 default next-hop

Use this command to specify the default next-hop IPv6 address for the IPv6 packets that match the rule in the route map configuration mode. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

**set ipv6 default next-hop** *global-ipv6-address* [ *weight* ] [ *global-ipv6-address* [ *weight* ] ]

**no set ipv6 default next-hop** *global-ipv6-address* [ *weight* ] [ *global-ipv6-address* [ *weight* ] ]

### Parameter description

Parameter	Description
<i>global-ipv6-address</i>	Next-hop IPv6 address for packet forwarding. The next-hop router must be a neighbor router.
<i>weight</i>	Weight in the load balancing mode, ranging from 1 to 8. A larger value means larger packet traffic to be shared by the next hop.

### Default

**configuration** None

**Command** Route map configuration mode

**mode**

With the policy-based routing applied to the interface, for the IPv6 packets matching the corresponding rules, if the usual route (that is the non default route) with the destination of this packet is not in the routing table, this packet will be forwarded to the next hop specified by the set ipv6 default next-hop command. Otherwise it is forwarded through the usual route. Noted that the match rule should be the IPv6 corresponded.

Packets select the egress from the policy-based routing and routing table in following priority.


- set ipv6 next-hop;
- usual route (the non default route)


**Usage**

set ipv6 default next-hop

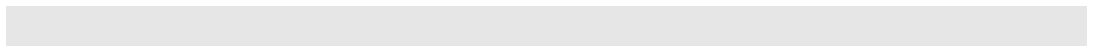
**guideline**

default route.

 For the switches, this function does not take effect if the mask length is beyond 64.

 If this command and the set ipv6 next-hop verify-availability are both configured ,the next hop set by the set ipv6 next-hop verify-availability command will take effect preferentially.

**Examples**



**Related commands**

Command	Description
match ipv6 address	Sets the matching rule of policy-based routing.
set ipv6 next-hop	Sets the next hop of the policy-based routing.

**Platform**

description N/A

### 5.21 set ipv6 next-hop

Use this command to specify the next-hop IPv6 address for the packets that meet the matching rule.

Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

**set ipv6 next-hop** *global-ipv6-address* [*weight*] [...*global-ipv6-address* [*weight*]]

**no set ip next-hop** *global-ipv6-address* [*weight*] [...*global-ipv6-address* [*weight*]]

**Parameter description**

Parameter	Description
<i>global-ipv6-address</i>	IPv6 address of the next hop. The next hop router should be the neighbor router.
<i>weight</i>	Weight of the next hop in the load balancing mode, in the range of 1 to 8.

**Default****configuration** None**Command****mode** Route map configuration mode

This command supports two operation modes: WCMP load balancing mode and non-WCMP load balancing mode. In the former mode, the system implements WCMP load balancing according to the weight entered by the user.

Multiple IP addresses may follow set ip next-hop and the number of addresses should be less than 32.

If weight follows ip address, up to 4 next hop addresses can be configured.



If weight follows any next-hop, the operation mode of this command will be automatically switched to the WCMP load balancing mode. In the WCMP load balancing mode, for the nexthop address without configuring the corresponding weight, the weight is 1 by default.

**Usage****guideline**

When the packets select the egress from the policy-based routing and routing table, the priorities are as follows.

set ipv6 next-hop;

usual route (the non default route)

set ipv6 default next-hop

Default route.

**Related commands**

Command	Description
<b>match ipv6 address</b>	Sets the matching rule of policy-based routing.
<b>set ipv6 next-hop</b>	Sets the next hop of the policy-based routing.

**Platform****description** N/A

## 5.22 set metric

Use **set metric** to set the metric for the routes to be redistributed. Use the **no** form of this command to remove the setting.

**set metric** [+ *metric-value* | - *metric-value* | *metric-value*]

**no set metric**

**Parameter description**

Parameter	Description
+	Increases based on the metric of the original route
-	Decreases based on the metric of the original route
<i>metric-value</i>	Metric for the route to be redistributed

**Default**

**configuration** The default metric for route redistribution varies with the routing protocol.

**Command**

**mode** Route map configuration mode

You should set the metric according to the actual network topology, because the routing depends on the metric of routes. Attentions should be paid to the upper and lower limits of the routing protocols when you execute the `set metric`, `+ metric` or `- metric` commands. When the RIP protocol redistributes the routes of other protocols, the range of the metric after increase or decrease is 1 to 16.

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the static routes in the RIP routing domain. The mutual route redistribution can be implemented between all the IP routing protocols.

**Usage****guideline**

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more `match` or `set` commands can be executed to configure a route map. If the `match` command is not used, all the routes will be matched. If the `set` command is not used, no operation will be performed.

The following example enables the RIP routing protocol to redistribute the static routes and sets the default metric to 40.

**Examples**

```
Ruijie(config)# router rip
Ruijie(config-router)# redistribute static route-map redrip
Ruijie(config-router)# network 192.168.12.0 0.0.0.255
Ruijie(config-router)# exit
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# set metric 40
```

**Related****commands**

Command	Description
<b>match interface</b>	Matches the interface.
<b>match ip address</b>	Matches the IP address.
<b>match ip next-hop</b>	Matches the next-hop IP address.
<b>match ip route-source</b>	Matches the source IP address.
<b>match metric</b>	Matches the metric.
<b>match tag</b>	Matches the tag.
<b>set tag</b>	Sets the tag.

## 5.23 set next-hop

Use this command to specify the next-hop IP address for the routes that match the rule. Use the **no** form of this command to remove the setting. This command is only used to configure routing policies.

**set next-hop** *ip-address*

**no set next-hop**

Parameter	Parameter	Description
description	<i>ip-address</i>	IP address of the next hop.

**Default configuration** None

**Command mode** Route map configuration mode

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the static routes in the RIP routing domain. The mutual route redistribution can be implemented between all the IP routing protocols.

**Usage guideline** In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

The following example enables the RIP routing protocol to redistribute the static route and sets the next-hop to 192.168.1.2.

**Examples**

```
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# match ip address 1
Ruijie(config-route-map)# set next-hop 192.168.1.2
```

Command	Description
<b>match interface</b>	Matches the interface.
<b>match ip address</b>	Matches the IP address.
<b>match ip next-hop</b>	Matches the next-hop IP address.
<b>match ip route-source</b>	Matches the source IP address.
<b>match metric</b>	Matches the metric.
<b>match tag</b>	Matches the tag.
<b>set tag</b>	Sets the tag.

## 5.24 set tag

Use this command to set the tag for the routes to be redistributed. Use the **no** form of this command to remove the setting.

**set tag tag**

**no set tag**

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



<b>description</b>	<i>tag</i>	Tag of the route to be redistributed
--------------------	------------	--------------------------------------

**Default**

**configuration** The original routing tag remains unchanged.

**Command**

**mode** Route map configuration mode

**Usage guideline** This command can only be used for route redistribution. If this command is not configured, the default route tag is used.

The following example enables the RIP routing protocol to redistribute the static route and sets the tag as 100.

**Examples**

```
Ruijie(config)# router rip
Ruijie(config-router)# redistribute static route-map redrip
Ruijie(config-router)# network 192.168.12.0 0.0.0.255
Ruijie(config-router)# exit
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# set tag 100
```

**Related commands**

Command	Description
<b>match interface</b>	Matches the interface.
<b>match ip address</b>	Matches the IP address.
<b>match ip next-hop</b>	Matches the next-hop IP address.
<b>match ip route-source</b>	Matches the source IP address.
<b>match metric</b>	Matches the metric.
<b>match tag</b>	Matches the tag.
<b>set metric</b>	Sets the metric.

## 5.25 show ip prefix-list

Use **show ip prefix-list** to display the prefix list or the entries.

**show ip prefix-list** [*prefix-name*]

Parameter	Parameter	Description
<b>description</b>	<i>prefix-name</i>	Name of the prefix list.

**Default**

**configuration** The configuration information of all the prefix lists is displayed by default.

**Command mode** Privileged EXEC mode, global configuration mode, interface configuration mode, routing protocol configuration mode, route map configuration mode.

**Usage guidelines** If no prefix list is specified, the configurations of all the prefix lists are displayed, otherwise only the configuration of the specified prefix list is displayed.

**Examples**

```
Ruijie# show ip prefix-list
seq pre: 2 entries
seq 5 permit 192.168.564.0/24
seq 10 permit 192.2.2.0/24
```

## 5.26 show ip protocols

Use this command to display information about the status of the currently running IPv4 routing protocol.

**show ip protocols [ rip ]**

Parameter Description	Parameter	Description
	rip	Displays information about the status of the RIP protocol.
	-	Displays information about the status of all running routing protocols.

**Command Mode** Privileged EXEC mode, global configuration mode, interface configuration mode, routing protocol configuration mode, and routing map configuration mode

**Default Level** 14

**Usage Guide** Information about the status of only the currently running routing protocol is displayed, and the information about a routing protocol that is not running is not displayed.

**Examples**

```
Ruijie(config)#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds
  Invalid after 180 seconds, flushed after 120 seconds
  Outgoing update filter list for all interface is: not set
  Incoming update filter list for all interface is: not set
  Redistribution default metric is 1
  Redistributing: static
  Default version control: send version 1, receive any version
  Routing for Networks:
    192.168.12.0 255.255.255.0
  Distance: 120 (default is 120)
  Graceful-restart enabled
    Restart grace period 60 secs
```

## 5.27 show ipv6 prefix-list

Use this command to display the information about the IPv6 prefix list or its entries.

**show ipv6 prefix-list** [*prefix-name*]

Parameter	Parameter	Description
<b>description</b>	<i>prefix-name</i>	Name of the IPv6 prefix list.

**Default configuration** The configuration information of all the IPv6 prefix lists is displayed.

**Command mode** Privileged EXEC mode, global configuration mode, interface configuration mode, route protocol configuration mode, route map configuration mode

**Usage guideline** If no prefix list is specified, the configurations of all the prefix lists are displayed, otherwise only the configuration of the specified prefix list is displayed.

### Examples

```
Ruijie# show ipv6 prefix-list
ipv6 prefix-list p6: 2 entries
    seq 5 permit 13::/20
    seq 10 permit 14::/20
```

## 5.28 show route-map

Use the command to display the configuration of the route map.

**show route-map** [*route-map-name*]

Parameter	Parameter	Description
<b>description</b>	<i>route-map-name</i>	(Optional) Name of the specified the route map.

**Default configuration** The configuration information of all the route maps is displayed.

**Command mode** Privileged EXEC mode, global configuration mode, interface configuration mode, routing protocol configuration mode, route map configuration mode.

**Usage guidelines** If no route map is specified, the configurations of all the route maps will be displayed, otherwise only the configuration of the specified route map is displayed.

### Examples

```
Ruijie# show route-map
route-map AAA, permit, sequence 10
Match clauses:
ip address 2
```

```
Set clauses:  
metric 10
```

Field	Description
route-map	Name of the route map.
Permit	The route map contains the permit keyword.
sequence 10	Sequence number of the route map.
Match clauses	Set the matching rule. Whether to perform the set operation depends on the permit or deny keyword in the route map.
Set clauses	Set the operation when the rule is matched.



## Multicast Commands

---

1. IPv4 Multicast Routing Commands(beta)
2. IGMP Snooping Commands

# 1 IPv4 Multicast Routing Commands(beta)

## 1.1 msf ipmc-overflow override

Use this command to enable the overflow overriding mechanism. Use the **no** or **default** form of this command to disable the overflow overriding mechanism.

**msf ipmc-overflow override**  
**no msf ipmc-overflow override**  
**default msf ipmc-overflow override**

Parameter	Parameter	Description
Description	-	-

**Default** Disabled.

**Command Mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example enables the overflow overriding mechanism.

```
Ruijie(config)# msf ipmc-overflow override
```

## 1.2 msf nsf

Use this command to configure the parameter for the continuous multicast forwarding. Use the **no** or **default** form of this command to restore the default setting.

**msf nsf { convergence-time *time* | leak *interval* }**  
**no msf nsf { convergence-time | leak }**  
**default msf nsf { convergence-time | leak }**

Parameter	Parameter	Description
Description	<b>convergence-time <i>time</i></b>	Maximum time for the multicast protocol convergence, in the valid range of the 0-3600s.
	<b>leak <i>interval</i></b>	Packet multicast leak time, in the valid range of 0-3600s

**Default** **convergence-time *time* :140s;**  
**leak interval: 150s**

**Command Mode** Global configuration mode.

**Usage Guide** N/A

The following example sets the maximum time for the protocol convergence.

```
Ruijie(config)# msf nsf convergence-time 300
```

### Examples

The following example sets the packets leak time:

```
Ruijie(config)# msf nsf leak 200
```

## 1.3 show msf msc

Use this command to show IPv4 multi-layer multicast forwarding table.

```
show msf msc [ source-address ] [ group-address ] [ vlan-id ]
```

### Parameter Description

Parameter	Description
<i>source-address</i>	Specified source IP address of the multi-layer multicast forwarding table.
<i>group-address</i>	Specified group address of the multi-layer multicast forwarding table.
<i>vlan-id</i>	The Vlan id where the incoming interface of the multi-layer multicast forwarding table is. 4096 indicates a routed port.

### Default

### Command

#### Mode

Privileged EXEC mode/Global configuration mode/Interface EXEC mode

The three parameters in this command are optional.

If no source address and group address are specified, all msc entries are displayed.

- If only the source address is specified as s1, all msc entries with source address 1 are displayed.
- If the source address is specified as s1 and the group address as g1, all corresponding msc entries are displayed.
- If the source address is specified as s1, the group address as g1 and the vlan id as v1, all corresponding msc entries are displayed.
- Each parameter shall be input in order. Only when the parameter in front has been configured, the following one could be set.

### Usage Guide

The following example shows the IPv4 layer-3 multicast forwarding entries with source IP address 192.168.195.25.

### Examples

```
Ruijie# show msf msc 192.168.195.25
Multicast Switching Cache Table
```

```
(192.168.195.23, 233.3.3.3, 1), SYNC, MTU:0, 1 OIFs
VLAN 1(0): 1 OPORTs, REQ: DONE
OPORT 6, IGMP-SNP, REQ: DONE
```

The fields in the execution of the **show mrf mfc** command are described in the following table.

Field	Description
192.168.195.23	Source address of the entry.
233.3.3.3	Group address of the entry.
1	Vlan id where the incoming interface of the entry is.
SYNC	The entry has been synchronized to the hardware.
MTU	MTU value
OIFs	Layer-3 outgoing interface number.
VLAN1(0)	The vlan where the layer-3 outgoing interface oif is.
1 OPORTs	The number of layer-2 port in the layer-3 outgoing oif.
REQ: DONE	This oif configuration on the hardware has done.
OPORT 6	The layer-2 port in the oif with index 6.
IGMP-SNP	This port is created by the IGMP SNOOPING protocol. This value can also be the PIM-SNP, which means this port is created by the PIM SNOOPING protocol. And the ROUTER means this port is created by the layer-3 protocol.
REQ: DONE	The port configuration on the hardware has done.

### 1.4 show msf nsf

Use this command to show the configuration of continuous multicast forwarding.

**show msf nsf**

Parameter	Parameter	Description
Description	-	-

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

The following example shows the configuration of continuous multicast forwarding.

```
Ruijie# show msf nsf
Multicast HA Parameters
-----+-----
protocol convergence timeout 120 secs
flow leak interval 20 secs
```

Related Commands	Command	Description
	<b>msf nsf</b>	Configure the multicast NSF parameter.



## 2 IGMP Snooping Commands

### 2.1 clear ip igmp snooping gda-table

Use this command to clear the Group Destination Address (GDA) table.

**clear ip igmp snooping gda-table**

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command 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 Description	N/A	

### 2.2 clear ip igmp snooping statistics

Use this command to clear IGMP Snooping statistics.

**clear ip igmp snooping statistics**

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command 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**

## 2.3 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**

## 2.4 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>	Profile number, in the range from 1 to 1024
<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 permitted.</li> <li>● If the <b>permit</b> command is used without any profile specified, all profiles in the profile are denied.</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>		

## 2.5 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 this command to enable IGMP snooping and enter the IVGL-SVGL mode.

**ip igmp snooping ivgl-svgl**

Use the **no** or **default** command to restore the default setting.

**no ip igmp snooping**

**no ip igmp snooping ivgl**

**no ip igmp snooping svgl**

**no ip igmp snooping ivgl-svgl**

**default ip igmp snooping**

**default ip igmp snooping ivgl**

**default ip igmp snooping svgl**

**default ip igmp snooping ivgl-svgl**

<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. As shown in Figure-3:
  - **IVGL-SVGL mode:** also known as promiscuous mode. In this mode, the IVGL mode and the SVGL mode can co-exist. Use IGMP Profile to divide a set of multicast address range to the SVGL, within which the member port of the multicast forwarding entry can be forwarded across VLANs and without which the member ports are forwarded in the same VLAN.



SVGL mode and IVGL-SVGL mode conflict with the IP multicast function.



PIM Snooping must depend on either IVGL or IVGL-SVGL 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
```

The following example enables IGMP Snooping and enters the IVGL-SVGL mode.

```
Ruijie(config)# ip igmp snooping ivgl-svgl
Ruijie(config)# ip igmp snooping svgl profile 1
```

**Platform Description** N/A

## 2.6 ip igmp snooping disable

Use this command to disable layer-2 multicast on a layer-2 interface.

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

**ip igmp snooping disable**

**no ip igmp snooping disable**

**default ip igmp snooping disable**

Parameter Description	Parameter	Description
	N/A	N/A

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

**Command Mode** Interface configuration mode

**Usage Guide** When this command is run on a layer-2 interface, it will not process the IGMP packet, namely, it cannot generate layer-2 multicast entry to forward the multicast traffic on layer-2 and this port cannot be configured as a static member port.

**Configuration** The following example disables layer-2 multicast on a layer-2 interface.

**Examples**

```
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# ip igmp snooping disable
```

**Platform** N/A

**Description**

## 2.7 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>	Aging time from 1 to 3,600 in the unit of seconds

**Defaults** The default is 300 seconds.

**Command** Global configuration mode

**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**

## 2.8 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

## 2.9 ip igmp snooping port-fast-leave enable

Use this command to enable port-fast-leave.

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

**ip igmp snooping port-fast-leave enable**

**no ip igmp snooping port-fast-leave enable**

**default ip igmp snooping port-fast-leave enable**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** By default, this function is disabled.

**Command Mode** Global configuration mode

**Usage Guide** With this command configured, the system will delete the multicast groups on related interfaces as it receives IGMP leave packet. Then, as it receives query packets from a specific multicast group, it can not forward this packet to the related interface. The IGMPv2 leave packet without source addresses and the IGMPv3 report message with types included are not included in the leave packet. This fast leave function applies to scenarios in which one interface is connected to only one host. This function saves bandwidth and resources.

**Configuration** The following example enables the fast leave function.

**Examples**

```
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# ip igmp snooping port-fast-leave enable
```

**Platform** N/A

**Description**

## 2.10 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** *vid filter profile-number*  
**no ip igmp snooping vlan** *vid filter*  
**default ip igmp snooping vlan** *vid filter*

Parameter Description	Parameter	Description
	<b>vlan</b> <i>vid</i>	VLAN ID. By default, the specified version is supported on all VLANs.
	<i>profile-number</i>	Profile number from 1 to 1024

**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.

**Configuration Examples** The following example specifies profile 1 for interface GigabitEthernet 0/17.

```
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# ip igmp snooping filter 1
```

**Platform Description** N/A

## 2.11 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 Description	Parameter	Description
	<i>seconds</i>	Aging time. The unit is second. The value ranges from 1 to 65,535.

**Defaults** The default is 260 seconds.

**Command Mode** Global configuration mode

**Usage Guide** The aging time of a dynamic port is set by the system when the port receives an IGMP packet from the host for joining a certain IP multicast group.  
 When such an IGMP packet is received, the system resets the aging timer for the port. The duration of this timer is determined by **host-aging-time**. If the timer expires, the system determines that there is



no host in this port for receiving multicast packets. The multicast device removes the port from the IGMP Snooping group. After the **ip igmp snooping host-aging-time** command is executed, the aging time will be determined by **host-aging-time**. This command takes effect only after the system receives the next IGMP packet. This command does not change the current aging time.

**Configuration** The following example sets the aging time to 30 seconds.

**Examples** Ruijie(config)# ip igmp snooping host-aging-time 30

Related	Command	Description
Commands	N/A	N/A

**Platform** N/A

**Description**

## 2.12 ip igmp snooping l2-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 l2-entry-limit** *number*

**no ip igmp snooping l2-entry-limit**

**default ip igmp snooping l2-entry-limit**

Parameter	Parameter	Description
Description	<i>number</i>	Number of multicast groups. The value ranges from 0 to 6144.

**Defaults** The default is 6144.

**Command Mode** Global configuration mode

**Usage Guide** 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 2000.

**Examples** Ruijie(config)# ip igmp snooping l2-entry-limit 2000

Related Commands	Command	Description
	<b>show ip igmp snooping</b>	Displays the maximum number of multicast groups.

**Platform Description** N/A

## 2.13 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**

<b>Parameter Description</b>	Parameter	Description
	<i>number</i>	The maximum group number from 0 to 6144.
<b>Defaults</b>	No maximum group number is configured by default.	
<b>Command Mode</b>	Interface configuration mode	
<b>Usage Guide</b>	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.	
<b>Configuration Examples</b>	The following example configures the maximum number of multicast groups to 100 on the megabit interface 0/17:	
	<pre>Ruijie(config)# interface gigabitethernet 0/17 Ruijie(config-if-GigabitEthernet 0/17)# ip igmp snooping max-group 100</pre>	
<b>Platform Description</b>	N/A	

## 2.14 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**

<b>Parameter Description</b>	Parameter	Description
	<i>vlan vid</i>	VLAN ID. 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.

**Configuration** The following example enables the dynamic routing interface learning function on VLAN 1.

**Examples**

```
Ruijie(config)# no ip igmp snooping mrouter learn pim-dvmrp
Ruijie(config)# ip igmp snooping vlan 1 mrouter learn pim-dvmrp
```

**Platform** N/A

**Description**

## 2.15 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>	Profile number (1-1024)

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

**Command**

**Mode** Global configuration mode

**Usage Guide** 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.

**Configuration** The following example associates the profile 2 to the GigabitEthernet 0/17 and associates multicast preview with profile 1.

**Examples**

```
Ruijie(config)# ip igmp snooping preview 1
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# ip igmp snooping filter 2
```

**Platform** N/A

**Description**

## 2.16 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	Parameter	Description
Description	<i>seconds</i>	Preview interval from 1 to 300 in the unit of seconds

**Defaults** The default is 60 seconds.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration** The following example sets the multicast preview interval as 100 seconds on the 100M port of 0/1:

**Examples**

```
Ruijie(config)# ip igmp snooping preview 1
Ruijie(config)# ip igmp snooping preview interval 100
```

**Platform** N/A

**Description**

## 2.17 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>	VLAN ID. 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 Description** N/A

## 2.18 ip igmp snooping querier address

Use this command to specify a source IP address for IGMP querier.

Use **no** or **default** form of this command to remove the source IP address configured.

**ip igmp snooping [ vlan *vid* ] querier address *ip-address***

**no ip igmp snooping [ vlan *vid* ] querier address**

**default ip igmp snooping [ vlan *vid* ] querier address**

Parameter Description	Parameter	Description
	<b>vlan <i>vid</i></b>	VLAN ID. By default, the specified version is supported on all VLANs.
	<b><i>ip-address</i></b>	Source IP address of the IGMP querier.

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** After enabling IGMP querier, you must configure a source IP address for the IGMP querier to activate this function.

If the IGMP querier source IP has been specified in VLAN, the source IP configured in the relevant VLAN will be used first.

**Configuration** The following example specifies the source IP of the IGMP querier as 1.1.1.1 on the device.

**Examples** 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**

**Description**

## 2.19 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 vid</b>	VLAN ID. 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**

## 2.20 ip igmp snooping querier query-interval

Use this command to specify the interval for IGMP querier to send query packets.

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

**ip igmp snooping querier query-interval** *seconds*

**no ip igmp snooping querier query-interval**

**default ip igmp snooping [ vlan *vid* ] querier query-interval**

Parameter Description	Parameter	Description
	<i>seconds</i>	Query interval from 1 to 18,000 in the unit of seconds
	<b>vlan</b> <i>vid</i>	VLAN ID. By default, the specified version is supported on all VLANs.

**Defaults** The default is 60 seconds.

**Command Mode** Global configuration mode

**Usage Guide** If the query interval has been configured in the corresponding VLAN, the value specified in VLAN will be used first.

**Configuration Examples** The following example configures the query interval on the device.

```
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 Description** N/A

## 2.21 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</b> <i>vid</i>	VLAN ID. By default, the specified version is supported on all VLANs.

**Defaults** The default is 125 seconds.

<b>Command</b>	Global configuration mode
<b>Mode</b>	
<b>Usage Guide</b>	<p>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.</p> <p>If expiration timer has been configured in the corresponding VLAN, the value specified in VLAN will be used first.</p>
<b>Configuration</b>	The following example configures the non-querier expiration timer on the device.
<b>Examples</b>	<pre>Ruijie(config)# ip igmp snooping querier timer expiry 60</pre> <p>The following example configures the non-querier expiration timer in VLAN 3.</p> <pre>Ruijie(config)# ip igmp snooping vlan 3 querier timer expiry 60</pre>
<b>Platform</b>	N/A
<b>Description</b>	

## 2.22 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	Parameter	Description
<b>Description</b>	<b>vlan <i>vid</i></b>	VLAN ID. 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** The following example configures IGMP querier version on the device.

**Examples**

```
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**

## 2.23 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>	The aging time of the routing interface that the switch learns dynamically, in the range from 1 to 65.535

**Defaults** The default is 10 seconds.

**Command Mode** Global configuration mode

**Usage Guide** 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.

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.

**Configuration Examples** The following examples sets the aging time of the routing interface that the switch learns dynamically to 100 seconds.

```
Ruijie(config)# ip igmp snooping query-max-response-time 100
```

**Platform** N/A

**Description**

## 2.24 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 Description** N/A

**2.25 ip igmp snooping suppression svgl vlan enable**

Use this command to enable primary VLAN suppression of SVGL of IGMP snooping.

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

**ip igmp snooping suppression svgl vlan enable**

**no ip igmp snooping suppression svgl vlan enable**

**default ip igmp snooping suppression svgl vlan enable**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** By default, this function is enabled.

**Command Mode** Global configuration mode

**Usage Guide** With this function enabled, IGMP snooping will forward the first report from a specific VLAN or group only, suppress follow-up reports and restrict network traffic. This function only applies to IGMPv2 report and IGMPv2 report.

**Configuration** The following example enables primary VLAN suppression of SVGL of IGMP snooping.

**Examples** `Ruijie(config)# ip igmp snooping suppression svgl vlan enable`

**Platform** N/A

**Description**

## 2.26 ip igmp snooping suppression sip

Use this command to customize the function of IGMP Snooping suppressing the source IP of packets. Use the **no** or **default** of this command to restore default settings.

**ip igmp snooping suppression vlan *vid* sip address**

**no ip igmp snooping suppression vlan *vid* sip**

**default ip igmp snooping suppression vlan *vid* sip**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** By default, the source IP address of IGMP snooping suppression is 0.0.0.0.

**Command Mode** Global configuration mode

**Usage Guide** With the IGMP snooping suppression enabled, the device can globally customize the source IP address of the report packet as well as the source address based on VLAN. The suppression can only be applied to an IGMPv1 and IGMPv2 report packet, not an IGMPv3 report packet.

**Configuration** The following example customizes the source IP address of report packet.

**Examples** `Ruijie(config)# ip igmp snooping suppression vlan 1 sip 1.1.1.1`

**Platform** N/A

**Description**

## 2.27 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>	Profile number, in the range of 1-1,024

<b>Defaults</b>	No profile is associated.
<b>Command Mode</b>	Global configuration mode
<b>Usage Guide</b>	When the IGMP Snooping works in the SVGL and IVGL-SVGL mode, a profile shall be associated to specify the multicast group address range applied in the SVGL or IVGL-SVGL mode.
<b>Configuration Examples</b>	The following example specifies the profile 2 applied in SVGL mode.
<b>Examples</b>	<pre>Ruijie(config)# ip igmp snooping svgl profile 2</pre>
<b>Platform</b>	N/A
<b>Description</b>	

## 2.28 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 settings.

**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>	VLAN ID or range of VLAN ID

<b>Defaults</b>	By default, all VLANs except shared VLANs serve as its sub VLANs.
<b>Command Mode</b>	Global configuration mode
<b>Usage Guide</b>	This command only takes effect in SVGL and IVGL-SVGL mode.
<b>Configuration Examples</b>	The following example specifies VLAN 3 as the shared VLAN and VLAN 2, VLAN 5 to 7 as the sub VLANs.
<b>Examples</b>	<pre>Ruijie(config)# ip igmp snooping svgl vlan 3 Ruijie(config)# ip igmp snooping svgl subvlan 2,5-7</pre>
<b>Platform</b>	N/A
<b>Description</b>	

## 2.29 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>	VLAN ID

**Defaults** By default , the shared VLAN is VLAN 1.

**Command Mode** Global configuration mode

**Usage Guide** This command only works in the SVGL and IVGL-SVGL mode.

**Configuration Examples** The following example specifies the vlan2 as the shared VLAN.

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**

## 2.30 ip igmp snooping tunnel

Use this command to enable 802.1Q tunneling (QinQ) support for IGMP Snooping.

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

**ip igmp snooping tunnel**

**no ip igmp snooping tunnel**

**default ip igmp snooping tunnel**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** This function is disabled.

**Command** Global configuration mode

**Mode**

**Usage Guide** After IGMP Snooping is enabled and dot1q-tunnel port is configured on the device, IGMP packets received from dot1q-tunnel port will be handled in two ways:

- First: QinQ transmits IGMP packets transparently. Create multicast entries in the VLAN to which the IGMP packets belong, and forward IGMP packets in the VLAN.
- For example: It is assumed that IGMP Snooping has been enabled on the device; Port A is a dot1q-tunnel port; the default VLAN of Port A is VLAN 1, and packets from VLAN 1 and VLAN 10 are allowed by Port A. When multicast requests of VLAN 10 are sent to port A, IGMP Snooping will create the multicast entry of VLAN 10 and forward the multicast requests to the router port of VLAN 10.
- Second: Create multicast entries in the default VLAN to which the dot1q-tunnel ports belong, and forward multicast packets in the default VLAN of dot1q-tunnel port after inserting the VLAN Tag of the default VLAN of dot1q-tunnel port.
- For example: It is assumed that IGMP Snooping has been enabled on the device; Port A is a dot1q-tunnel port; the default VLAN of port A is VLAN 1, and packets from VLAN 1 and VLAN 10 are allowed Port A. When multicast requests of VLAN 10 are sent to Port A, IGMP Snooping will create the multicast entry of VLAN 1 and insert the VLAN Tag of VLAN 1 into multicast requests before forwarding the multicast requests to the router port of VLAN 1.  
By default, the second way is used.

**Configuration** The following example enables QinQ support for IGMP Snooping.

**Examples** Ruijie(config)# ip igmp snooping tunnel

**Platform** N/A

**Description**

## 2.31 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>	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.

 The PIM Snooping in the specified VLAN works only when IGMP Snooping is configured. To disable PIM Snooping, you must disable IGMP Snooping in the VLAN first, or disabling will fail and be prompted.

**Configuration Examples** The following example enters IVGL mode and disables the IGMP Snooping in the VLAN 2.

```
Ruijie(config)# ip igmp snooping ivgl
Ruijie(config)# no ip igmp snooping vlan 2
```

**Platform Description** N/A

## 2.32 ip igmp snooping vlan mrouter interface

Use this command to configure a static routing interface.  
 Use the **no** form of this command to delete a static routing interface.  
 Use the **default** form of this command to restore the default setting.  
**ip igmp snooping vlan vid mrouter interface interface-type interface-number**  
**no ip igmp snooping vlan vid mrouter interface interface-type interface-number**  
**default ip igmp snooping vlan vid mrouter interface interface-type interface-number**

Parameter Description	Parameter	Description
	<i>vid</i>	VLAN ID in the range from 1 to 4,094
	<i>interface-type</i> <i>interface-number</i>	Interface ID

**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 0/17
```

**Platform** N/A

**Description**

## 2.33 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** *ip-address* **interface** *interface-type* *interface-number*

**no ip igmp snooping vlan** *vid* **static** *ip-address* **interface** *interface-type* *interface-number*

**default ip igmp snooping vlan** *vid* **static** *ip-address* **interface** *interface-type* *interface-number*

**Parameter  
Description**

Parameter	Description
<i>vid</i>	VLAN ID in the range from 1 to 4,094
<i>ip-address</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** The following example configures a static member interface for the multicast group 224.1.1.1.

**Examples**

```
Ruijie(config)# ip igmp snooping vlan 1 static 224.1.1.1 interface  
gigabitethernet 0/17
```

**Platform** N/A

**Description**

## 2.34 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
<b>Defaults</b>	The forwarding of the multicast streams in the range specified by the profile is denied.	
<b>Command Mode</b>	Profile configuration mode	
<b>Usage Guide</b>	<p>A profile is used to filter a group of multicast packets, so as to assist other features.</p> <p>Configuration steps:</p> <ol style="list-style-type: none"> <li>1. Use the <b>ip igmp profile</b> command to create a profile and enter profile configuration mode.</li> <li>2. Use the <b>range</b> command to define a range for the profile.</li> <li>3. Use the <b>permit</b> command to permit the multicast forwarding for the profile.</li> </ol>	
<b>Configuration Examples</b>	<p>The following example permits the forwarding of the multicast streams from 224.2.2.2 to 224.2.2.244 of profile 1.</p> <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 Description</b>	N/A	

## 2.35 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
<b>Defaults</b>	No range is defined for a profile by default.	
<b>Command Mode</b>	Profile configuration mode	
<b>Usage Guide</b>	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 is an example of allowing 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 224.2.2.2 224.2.2.244224.2.2.2
Ruijie(config-profile)# permit
```

**Platform** N/A

**Description**

## 2.36 show ip igmp profile

Use this command to display the profile information.

**show ip igmp profile**  
**show ip igmp profile** *profile-number*

Parameter Description	Parameter	Description
	<i>profile-number</i>	Displays configuration information of the designated profile.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command to display the profile information.

**Configuration Examples** The following example displays the profile information.

```
Ruijie# show ip igmp profile
Profile 1
Permit
range 224.0.1.0, 239.255.255.255
```

## 2.37 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
	<code>vlan vid</code>	VLAN ID. By default, IGMP Snooping information of all VLANs are displayed.
	<code>interface-type</code> <code>interface-number</code>	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: 65536
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: 65536
Global IGMPv2 Fast-Leave :Disable
Global multicast router learning mode :Enable
Query Max Response Time: 10 (Seconds)
Dynamic Mroute Aging Time : 300(Seconds)
Dynamic Host Aging Time : 260(Seconds)

vlan 1
-----
IGMP Snooping state: Enable
Multicast router learning mode: pim-dvmrp
IGMP Fast-Leave: Disable
```

```
IGMP VLAN querier: Disable
IGMP VLAN Mode: STATIC
```

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



## Network Management & Monitoring Commands

---

1. SNMP Commands
2. RMON Commands(beta)
3. NTP Commands
4. SNTP Commands(beta)
5. SPAN Commands

# 1 SNMP Commands

## 1.1 no snmp-server

Use this command to disable the SNMP agent function.

**no snmp-server**

Parameter 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 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 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 Description	Parameter	Description
	N/A	N/A

**Defaults** Sending link traps on the interface is enabled by default. If the interface link status changes, SNMP link traps will be sent.

**Command mode** Interface configuration mode

**Usage Guide** This command can be configured on the Ethernet interface, aggregate ports and SVI interfaces.

**Configuration** The following example disables the interface to send link traps.

**Examples**

```
Ruijie(config)# interface gigabitEthernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# no snmp trap link-status
```

The following example enables the interface to send link traps.

```
Ruijie(config)# interface gigabitEthernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# snmp trap link-status
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 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 Description	Parameter	Description
	<i>text</i>	SNMP chassis ID: numerals or characters.

**Defaults** The default is 60FF60.

**Command mode** Global configuration mode.



**Usage Guide** The SNMP chassis ID is generally the serial number of the device to facilitate identification. The SNMP chassis ID can be displayed through the **show snmp** command.

**Configuration** 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* ] [ **ipv6** *ipv6-aclname* ] [ *aclnum* ] [ *aclname* ]  
**no snmp-server community** [ 0 | 7 ] *string*

**Parameter Description**

Parameter	Description
0	Indicates that the community string is in plaintext.
7	Indicates that the community string is in ciphertext.
<i>string</i>	Community string, which is the communication password between the NMS and the SNMP agent
<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>ipv6-aclname</i>	IPv6 access list name, which specifies the IPv6 addresses that are permitted to access the MIB.
<i>ipaddr</i>	Specifies the IP address of the NMS to access the MIB.

**Defaults** All communities are read only by default.

**Command mode** Global configuration mode.

**Usage Guide** This command is an essential command to enable the SNMP agent function, such as specifying the community attribute and IP addresses of NMS to access the MIB.  
To disable the SNMP agent function, use the **no snmp-server** command.

**Configuration Examples** The following example defines a SNMP community access string named public, which can be read-only.

```
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>	
<b>no snmp-server</b>		Disables the SNMP agent function.

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

## 1.7 snmp-server enable traps

Use this command to enable the SNMP agent to send the SNMP trap message to NMS. Use the **no** form of this command to disable the SNMP agent to send the SNMP trap message to NMS.

**snmp-server enable traps** [ *notification-type* ]

**no snmp-server enable traps**

Parameter Description	Parameter	Description
	<i>notification-type</i>	Specifies the type of trap messages. authentication: Allow authentication notifications. bridge: Bridge trap message. entity: Entity Trap message. mac-notification: MAC trap message. snmp: SNMP trap message. vrrp: VRRP 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**

## 1.8 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 Examples** The following example configures the number of SNMP requests processed per second to 200.

```
Ruijie(config)# snmp-server flow-control pps 200
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.9 snmp-server group

Use this command to configure a new SNMP group. Use the **no** form of this command to remove a specified SNMP group.

```
snmp-server group groupname { v1 | v2c | v3 { auth | noauth | priv } } [ read readview ] [ write writeview ] [ access { [ ipv6 ipv6-aclname ] aclnum | aclname } ]  
no snmp-server group groupname { v1 | v2c | v3 { auth | noauth | priv } }
```

Parameter Description	Parameter	Description
	<b>v1</b>   <b>v2c</b>   <b>v3</b>	Specifies the SNMP version
	<b>auth</b>	Specifies authentication of a packet without encrypting it. This applies to SNMPv3 only.
	<b>noauth</b>	Specifies no authentication a packet. This applies to SNMPv3 only.
	<b>priv</b>	Specifies authentication of a packet with encryption. This applies to SNMPv3 only.
	<i>readview</i>	Specifies a read-only view for the SNMP group. This view enables you to view only the contents of the agent.
	<i>writeview</i>	Specifies a write view for the SNMP group. This view enables you to enter data and configure the contents of the agent.

<i>aclnum</i>	Access list number, which specifies the IPv4 addresses that are permitted to access the MIB.
<i>aclname</i>	Name of the access list, which specifies the IPv4 addresses that are permitted to access the MIB.
<i>ipv6-aclname</i>	Name of the IPv6 access list, which specifies the IPv6 addresses that are permitted to access the MIB.

**Defaults** No SNMP groups are configured by default.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration** The following example configures a new SNMP group.

**Examples**

```
Ruijie(config)# snmp-server group mib2user v3 priv read mib2
```

Related Commands	Command	Description
		<b>show snmp group</b>

**Platform** N/A

**Description**

### 1.10 snmp-server host

Use this command to specify the SNMP host (NMS) to send the trap message. Use the **no** form of this command to remove the specified SNMP host.

**snmp-server host** { *host-addr* | **ipv6** *ipv6-addr* } [ **traps** | **informs** ] [ **version** { **1** | **2c** | **3** [ **auth** | **noauth** | **priv** ] ] *community-string* [ **udp-port** *port-number* ] [ *notification-type* ]  
**no snmp-server host** { *host-addr* | **ipv6** *ipv6-addr* } [ **traps** | **informs** ] [ **version** { **1** | **2c** | **3** { **auth** | **noauth** | **priv** } ] *community-string* [ **udp-port** *port-number* ]

Parameter Description	Parameter	Description
		<i>host-addr</i>
	<i>ipv6-addr</i>	SNMP host address(ipv6)
	<b>trap</b>   <b>informs</b>	Enables the host to send the SNMP notification as traps or informs.
	<b>version</b>	SNMP version: v1, v2c or v3
	<b>auth</b>   <b>noauth</b>   <b>priv</b>	Security level of SNMPv3 users
	<i>community-string</i>	Community string or username (SNMPv3 version)
	<i>port-number</i>	Port of the SNMP host in the range from 0 to 65535.
	<i>notification-type</i>	The type of the SNMP trap message, such as <b>snmp</b> .

	If no type of the SNMP trap message is specified, all types of the SNMP trap message will be included.
--	--

**Defaults** No SNMP host is specified by default.

**Command mode** Global configuration mode.

**Usage Guide** This command must be used together with the **snmp-server enable traps** command to send the SNMP trap messages to NMS.

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** The following example specifies an SNMP host to receive the SNMP event trap:

**Examples** 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**

## 1.11 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-time</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** The following example configures the resend times of inform requests to 5.

**Examples**

```
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**

## 1.12 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**

## 1.13 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 Examples** N/A

Related Commands	Command	Description
	<b>snmp-server queue-length</b>	Specifies the length of the message queue for each SNMP trap host.

**Platform Description** N/A

## 1.14 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** Global configuration mode.



**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**

## 1.15 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** Global configuration mode.

**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**

## 1.16 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-id*

**no snmp-server trap-source**

### Parameter Description

Parameter	Description
<i>interface-id</i>	Specifies the source interface of the SNMP trap messages.

### 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 0/17 as the source address of the SNMP trap message:

```
Ruijie(config)# snmp-server trap-source gigabitethernet 0/17
```

### Related Commands

Command	Description
<b>snmp-server enable traps</b>	Enables the SNMP agent to send the SNMP trap message to NMS.
<b>snmp-server host</b>	Specifies the NMS host to send the SNMP trap message.

### Platform

N/A

### Description

## 1.17 snmp-server trap-timeout

Use this command to define the retransmission timeout time of the SNMP trap message. Use the **no** form of this command to restore the default value.

**snmp-server trap-timeout** *seconds*

**no snmp-server trap-timeout**

### Parameter Description

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

<i>seconds</i>	Timeout (in milliseconds) of retransmit the SNMP trap message. The range is from 1 to 1,000.
----------------	--

**Defaults** The default is 300 milliseconds.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration** The following example specifies the timeout period as 600 milliseconds.

**Examples**

```
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**

## 1.18 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.

**Defaults** The default is 161.

**Command** Global configuration mode.

**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**

## 1.19 snmp-server user

Use this command to configure a new user to an SNMP group. Use the **no** form of this command to remove a user from an SNMP group.

```
snmp-server user username groupname { v1 | v2c | v3 [ encrypted ] [ auth { md5 | sha }
auth-password ] [ priv des56 priv-password ] } [ access { [ ipv6 ipv6-aclname ] aclnum | aclname } ]
no snmp-server user username groupname { v1 | v2c | v3 }
```

**Parameter  
Description**

Parameter	Description
<i>username</i>	Name of the user on the host that connects to the agent.
<i>groupname</i>	Name of the group to which the user belongs.
<b>v1</b>   <b>v2c</b>   <b>v3</b>	Specifies the SNMP version. But only SNMPv3 supports the following security parameters.
<b>encrypted</b>	Specifies whether the password appears in cipher text. 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. <code>des56</code> 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.
<i>aclnumber</i>	Access list number, which specifies the IPv4 addresses that are permitted to access the MIB.
<i>aclname</i>	Name of the access list, which specifies the IPv4 addresses that are permitted to access the MIB.
<i>ipv6-aclname</i>	Name of the IPv6 access list, which specifies the IPv6 addresses that are permitted to access the MIB.

**Defaults** N/A

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration** The following example configures an SNMPv3 user with MD5 authentication and DES encryption:

**Examples**

```
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**

## 1.20 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 Description** N/A

## 2 RMON Commands(beta)

### 2.1 rmon alarm

Use this command to monitor a MIB variable. Use the **no** form of this command to remove the alarm entry.

**rmon alarm** *number variable interval {absolute | delta } rising-threshold value [event-number] falling-threshold value [event-number] [owner ownername]*

**no rmon alarm** *number*

#### Parameter description

Parameter	Description
<i>number</i>	Alarm number. The value ranges from 1-65,535.
<i>variable</i>	Alarm variable. The value is a character string consisting of 1 to 255 characters in OID dotted format (the format is entry.integer.instance or a leaf node named .instance, for example. 1.3.6.1.2.1.2.1.10.1).
<i>interval</i>	Sampling interval. The value ranges from 1 to 2,147,483,647 in the unit of second.
<b>absolute</b>	Absolute sampling. In this mode, when the sampling time arrives, the system directly invokes the variable value.
<b>delta</b>	Delta sampling. In this mode, when the sampling time arrives, the system invokes the delta value of the variable within the sampling interval.
<b>rising-threshold value</b>	Rising threshold and the corresponding event number when the threshold is reached. The threshold ranges from -2,147,483,648 to +2,147,483,647.
<i>event-number</i>	The event number ranges from 1 to 65,535.
<b>falling-threshold value</b>	Falling threshold and the corresponding event number when the threshold is reached. The threshold ranges from -2,147,483,648 to +2,147,483,647
<b>owner ownername</b>	Owner of an entry. The value is a character string consisting of 1 to 63 characters that are case sensitive.

**Default** N/A.

**Command mode** Global configuration mode.

#### Usage guidelines

The RGOS allows you to modify the configured history information of the Ethernet network, including variable, absolute/delta, owner, rising-threshold/falling-threshold, and the corresponding events. However, the modification does not take effect immediately until the system triggers the monitoring event at the next time.

#### Examples

The example below monitors the MIB variable instance ifInNUcastPkts.6.

```
Ruijie(config)# rmon alarm 10 1.3.6.1.2.1.2.2.1.12.6 30 delta
```

```
rising-threshold 20 1 falling-threshold 10 1 owner zhangsan
```

### Related commands

Command	Description
<b>rmon event</b> <i>number</i> [ <b>log</b> ] [ <b>trap</b> <i>community</i> ] <b>description</b> <i>string</i> [ <b>owner</b> <i>ownername</i> ]	Adds an event definition.

## 2.2 rmon collection history

Use this command to enable history statistics on the Ethernet interface. Use the **no** form of this command to remove the history entry.

**rmon collection history** *index* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]

**no rmon collection history** *index*

### Parameter description

Parameter	Description
<i>index</i>	Index of a history entry. The value ranges from 1 to 65,535.
<b>owner</b> <i>ownername</i>	Owner of an entry. The value is a character string consisting of 1 to 63 characters that are case sensitive.
<b>buckets</b> <i>bucket-number</i>	Capacity of a history entry (that is, the maximum number of history entries). The value ranges from 1 to 65,535. The default value is 10.
<b>interval</b> <i>seconds</i>	Statistics period. The unit is second. The value ranges from 1 to 3,600. The default value is 1,800 seconds.

### Default

N/A.

### Command mode

Interface configuration mode.

### Usage guidelines

The configured history control entry parameters cannot be modified. And the history entry cannot be removed from the interface where the entry configured.

### Examples

The example below enables log statistics on interface GigabitEthernet 0/17.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#interface gigabitEthernet 0/17
Ruijie(config-GigabitEthernet0/17)#rmon collection history 1 owner UserA
buckets 5 interval 60
```

### Related commands

Command	Description
<b>rmon collection stats</b> <i>index</i> [ <b>owner</b> <i>ownername</i> ]	Adds a statistical entry on the Ethernet interface.



## 2.3 rmon collection stats

Use this command to monitor an Ethernet interface. Use the **no** form of this command to remove the configuration.

**rmon collection stats** *index* [**owner** *ownername* ]

**no rmon collection stats** *index*

Parameter description	Parameter	Description
	<i>index</i>	Index of the statistic table. The value ranges from 1 to 65,535.
	<b>owner</b> <i>ownername</i>	Owner of an entry. The value is a character string consisting of 1 to 63 characters that are case sensitive and do not contain spaces.

**Default** N/A.

**Command mode** Interface configuration mode.

**Usage guidelines** The configured history control entry parameters cannot be modified. And the history entry cannot be removed from the interface where the entry configured.

The example below enables monitoring the statistics of interface GigabitEthernet 0/17.

### Examples

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#interface gigabitEthernet 0/17
Ruijie(config-GigabitEthernet0/17)# rmon collection stats 1 owner UserA
```

Related commands	Command	Description
	<b>rmon collection history</b> <i>index</i> [ <b>owner</b> <i>ownername</i> ] [ <b>buckets</b> <i>bucket-number</i> ] [ <b>interval</b> <i>seconds</i> ]	Adds a history control entry.

## 2.4 rmon event

Use this command to define an event. Use the **no** form of this command to remove the event entry.

**rmon event** *number* [**log** ] [**trap** *community* ] [*description-string* ] [**description** *description-string* ] [**owner** *ownername* ]

**no rmon event** *number*

Parameter description	Parameter	Description
	<i>number</i>	Event number. The value ranges from 1 to 65,535.
	<b>log</b>	(Optional) Log event. When a log event is triggered, the system records a log.

<b>trap</b> <i>community</i>	(Optional) Trap event. When a trap event is triggered, the system sends trap with the group named "community".
<b>description</b> <i>description-string</i>	(Optional) Description of the event. The value is a character string consisting of 1 to 127 characters.
<b>owner</b> <i>ownername</i>	(Optional) Owner of an entry. The value is a character string consisting of 1 to 63 characters that are case sensitive.

**Default** N/A.

**Command mode** Global configuration mode.

**Usage guidelines** The RGOS allows you to modify the configured history information of the Ethernet network, including variable, absolute/delta, owner, rising-threshold/falling-threshold, and the corresponding events. However, the modification does not take effect immediately until the system triggers the monitoring event at the next time.

The example below defines the event actions: log event and send trap message.

**Examples**

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#rmon event 1 log trap public description "ifInNUcastPkts
is abnormal" owner UserA
```

**Related commands**

Command	Description
<b>rmon alarm</b> <i>number variable interval {absolute   delta } rising-threshold value [event-number] falling-threshold value [event-number] [owner ownername]</i>	Adds an alarm entry.

## 2.5 show rmon

**Default** Use this command to display the RMON configuration.

**show rmo**

**Default** N/A.

**Command mode** Privileged EXEC mode.

**Usage guidelines** N/A.

The example below displays the RMON configuration.

**Examples**

```
Ruijie#show rmon
ether statistic table:
    index = 1
```

```
interface = GigabitEthernet 0/17
owner = admin
status = 0
dropEvents = 61
octets = 170647461
pkts = 580375
broadcastPkts = 2135
multiPkts = 3615
crcAlignErrors = 0
underSizePkts = 0
overSizePkts = 0
fragments = 0
jabbers = 0
collisions = 0
packets64Octets = 3254668
packets65To127Octets = 1833370
packets128To255Octets = 2098146
packets256To511Octets = 126716
packets512To1023Octets = 363621
packets1024To1518Octets = 1077865

rmon history control table:
    index = 1
    interface = GigabitEthernet 0/17
    bucketsRequested = 5
    bucketsGranted = 5
    interval = 60
    owner = UserA
    stats = 1

rmon history table:
    index = 1
    sampleIndex = 2485
    intervalStart = 7d:22h:56m:38s
    dropEvents = 0
    octets = 5840
    pkts = 27
    broadcastPkts = 0
    multiPkts = 0
    crcAlignErrors = 0
    underSizePkts = 0
    overSizePkts = 0
    fragments = 0
    jabbers = 0
```

```

        collisions = 0
        utilization = 0
rmon alarm table:
        index: 1
        interval: 60
        oid = 1.3.6.1.2.1.2.2.1.12.6
        sampleType: 2
        alarmValue: 0
        startupAlarm: 3
        risingThreshold: 20
        fallingThreshold: 10
        risingEventIndex: 1
        fallingEventIndex: 1
        owner: UserA
        status: 1

rmon event table:
        index = 1
        description = ifInNUcastPkts is abnormal
        type = 4
        community = public
        lastTimeSent = 0d:0h:0m:0s
        owner =UserA
        status = 1

rmon log table:
        eventIndex = 1
        index = 1
        logTime = 6 d:19 h:21 m:48 s
        logDescription = ifInNUcastPkts is abnormal
    
```

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

## 2.6 show rmon alarm

**Default** Use this command to display the RMON alarm table.

**show rmon alarm**

**Default** N/A.

**Command mode** Privileged EXEC mode.

**Usage guidelines** N/A.

The example below displays the RMON alarm table.

**Examples**

```
Ruijie#show rmon alarm
rmon alarm table:
      index: 1
      interval: 60
      oid = 1.3.6.1.2.1.2.2.1.12.6
      sampleType: 2
      alarmValue: 0
      startupAlarm: 3
      risingThreshold: 20
      fallingThreshold: 10
      risingEventIndex: 1
      fallingEventIndex: 1
      owner: UserA
      status: 1
```

**Related commands**

Command	Description
<b>rmon alarm</b> <i>number variable interval {absolute   delta }</i> <b>rising-threshold</b> <i>value</i> <i>[event-number]</i> <b>falling-threshold</b> <i>value</i> <i>[event-number]</i> <b>owner</b> <i>ownername</i>	Adds an alarm entry.

## 2.7 show rmon event

Use this command to display the event configuration.

**show rmon event**

**Default** N/A.

**Command mode** Privileged EXEC mode.

**Usage guidelines** N/A.

The example below displays the event configuration.

**Examples**

```
Ruijie#show rmon event
rmon event table:
      index = 1
      description = ifInNUcastPkts is abnormal
      type = 4
```

```

community = public
lastTimeSent = 0d:0h:0m:0s
owner =UserA
status = 1

rmon log table:
eventIndex = 1
index = 1
logTime = 6d:19h:21m:48s
logDescription = ifInNUcastPkts is abnormal
    
```

**Related commands**

Command	Description
<b>rmon event</b> <i>number</i> [ <b>log</b> ] [ <b>trap</b> <i>community</i> ] [ <b>description</b> <i>description-string</i> ] [ <b>owner</b> <i>ownername</i> ]	Adds an event entry.

## 2.8 show rmon history

Use this command to display the history information.

**show rmon history**

**Default** N/A.

**Command mode** Privileged EXEC mode.

**Usage guidelines** N/A.

The example below displays the history information.

```

Ruijie#show rmon history
rmon history control table:
index = 1
interface = GigabitEthernet 0/17
bucketsRequested = 5
bucketsGranted = 5
interval = 60
owner = UserA
stats = 1

rmon history table:
index = 1
sampleIndex = 2485
intervalStart = 7d:22h:56m:38s
dropEvents = 0
octets = 5840
    
```

**Examples**

```

pkts = 27
broadcastPkts = 0
multiPkts = 0
crcAlignErrors = 0
underSizePkts = 0
overSizePkts = 0
fragments = 0
jabbers = 0
collisions = 0
utilization = 0
    
```

**Related commands**

Command	Description
<b>rmon collection history</b> <i>index</i> [owner <i>ownername</i> ] [ <b>buckets</b> <i>bucket-number</i> ] [ <b>interval</b> <i>seconds</i> ]	Adds a history control entry.

## 2.9 show rmon statistics

Use this command to display the RMON statistics.

**show rmon statistics**

**Default**

N/A.

**Command mode**

Privileged EXEC mode.

**Usage guidelines**

N/A.

The example below displays the RMON statistics.

**Examples**

```

Ruijie#show rmon statistics
ether statistic table:
    index = 1
    interface = GigabitEthernet 0/17
    owner = admin
    status = 0
    dropEvents = 61
    octets = 170647461
    pkts = 580375
    broadcastPkts = 2135
    multiPkts = 3615
    crcAlignErrors = 0
    underSizePkts = 0
    overSizePkts = 0
    
```

```
fragments = 0
jabbers = 0
collisions = 0
packets64Octets = 3254668
packets65To127Octets = 1833370
packets128To255Octets = 2098146
packets256To511Octets = 126716
packets512To1023Octets = 363621
packets1024To1518Octets = 1077865
```

**Related  
commands**

Command	Description
<code>rmon collection stats index [owner ownerstring]</code>	Adds a statistical entry.



## 3 NTP Commands

### 3.1 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

### 3.2 ntp access-group

Use this command to configure an access group to control NTP access. Use the **no** form of this command to remove the peer access group.

**ntp access-group** { **peer** | **serve** | **serve-only** | **query-only** } *access-list-number* | *access-list-name*  
**no ntp access-group** { **peer** | **serve** | **serve-only** | **query-only** } *access-list-number* | *access-list-name*


Parameter Description	Parameter	Description
	peer	Allows the device to receive time requests and NTP control queries to synchronize itself to the servers specified in the access list.

<b>serve</b>	Allows the device to receive time requests and NTP control queries from the servers specified in the access list but not to synchronize itself to the specified servers.
<b>serve-only</b>	Allows the device to receive only time requests from the servers specified in the access list.
<b>query-only</b>	Allows the device to receive only NTP control queries from servers specified in the access list.
<i>access-list-number</i>	Access control list number, ranging from 1 to 99 and 1300 to 1999.
<i>access-list-name</i>	Access control list name.

**Defaults** No access rule to control NTP access is configured by default, namely, NTP access is granted to all devices.

**Command mode** Global configuration mode.

**Usage Guide** Use this command to configure an access group to control NTP access, providing a minimal security measures (more secure way is to use the NTP authentication mechanism).  
 The NTP service enables the access group options to be scanned in the following order, from least restrictive to most restrictive: **peer, serve, serve-only, query-only**.  
 If you do not configure any access groups, NTP access is granted to all devices. However, once you configure the access rule, NTP access is granted only to the devices specified in the access list.

 NTP control query is not supported in the current system. Although it matches with the order in accordance with the above rules, the related requests about the control and query are not supported.

**Configuration Examples** The following example shows how to allow the device to only receive time requests from the device of 192.168.1.1.

```
Ruijie(config)# access-list 1 permit host 192.168.1.1
Ruijie(config)# ntp access-group serve-only 1
```

Related Commands	Command	Description
	<b>ip access-list</b>	Creates an IP access control list.

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

### 3.3 ntp authenticate

Use this command to enable NTP authentication. Use the **no** form of this command to disable NTP

authentication.

**ntp authenticate**

**no ntp authenticate**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** Disabled.

**Command mode** Global configuration mode.

**Usage Guide** If NTP authentication is disabled, the synchronization communication is not encrypted. To enable encrypted communication on the server, enable the NTP authentication and configure other keys globally.

NTP authentication is implemented through the trusted key specified by the **ntp authentication-key** and **ntp trusted-key** commands.

**Configuration Examples** After an authentication key is configured and specified as the global trusted key, enable NTP authentication.

```
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

### 3.4 ntp authentication-key

Use this command to configure an NTP authentication key. Use the **no** form of this command to remove the NTP authentication key.

**ntp authentication-key** *key-id* **md5** *key-string* [*enc-type*]

**no ntp authentication-key** *key-id*

Parameter Description	Parameter	Description
	<i>key-id</i>	Key ID, ranging from 1 to 4294967295.
	<i>key-string</i>	Key string

<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>
	<b>ntp trusted-key</b>	Configures an NTP trusted key.
	<b>ntp server</b>	Specifies an NTP server.

**Platform** N/A

**Description**

### 3.5 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

**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-GigabitEthernet 0/17)#no ntp disable
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

### 3.6 ntp master

Use this command to configure the device to act as an authoritative NTP server, synchronizing time to other devices. Use the **no** form of this command to remove the device as an authoritative NTP server.

**ntp master** [ *stratum* ]

**no ntp master**


**Parameter  
Description**


Parameter	Description
<i>stratum</i>	Stratum level. The range is from 1 to 15. The default is 8.

**Defaults** N/A

**Command  
mode** Global configuration mode.

**Usage Guide** In general, the local device synchronizes time from the external time source directly or indirectly. However, if the time synchronization fails due to network connection trouble, you can use this command to configure the local device to act as an authoritative NTP server to synchronize time to other devices. Once configured, the device will not perform time synchronization with the time source which is of a higher stratum.

 Configuring the device to act as an authoritative NTP server (in particular, specify a lower stratum level), may be likely to overwrite the effective time. If multiple devices in the same network are configured with this command, the time synchronization may be instable due to the time difference between the devices.

 Before configuring this command, you need to manually correct the system clock to avoid too much bias if the device has never performed time synchronization with the external clock

source.

**Configuration Examples** The following example configures the device to act as an authoritative NTP server, and sets the stratum level to 12:

```
Ruijie(config)# ntp master 12
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** N/A

### 3.7 ntp server

Use this command to specify a NTP server for the NTP client. Use the **no** form of this command to delete the specified NTP server.

```
ntp server { ip-addr | domain | ip domain | ipv6 domain } [ version version ] [ source interface-id ]
[ 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 or IPv6 format.
<i>domain</i>	Sets the domain name of the NTP server, supporting IPv4 and IPv6.
<i>version</i>	(Optional) Specifies the NTP version (1-3). The default is NTPv3.
<i>interface-id</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`

For IPv6: `Ruijie(config)# ntp server 10::2`

**Related  
Commands**

Command	Description
<code>no ntp</code>	Disables NTP.

**Platform** N/A

**Description**

### 3.8 ntp trusted-key

Use this command to set a global trusted key. Use the **no** form of this command to remove the global trusted key.

**ntp trusted-key** *key-id*

**no ntp trusted-key** *key-id*

**Parameter  
Description**

Parameter	Description
<i>key-id</i>	Global trusted key ID, ranging from 1 to 4294967295.

**Defaults** N/A

**Command  
mode** Global configuration mode.

**Usage Guide** The NTP communication parties must use the same trusted key. The key is identified by ID and is not transmitted to improve security.

**Configuration** The following example configures an authentication key and sets it as a trusted key.

**Examples** `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
---------	-------------

<b>ntp authenticate</b>	Enables NTP authentication.
<b>ntp authentication-key</b>	Configures an NTP authentication key.
<b>ntp server</b>	Configures an NTP server.

**Platform** N/A

**Description**

### 3.9 ntp update-calendar

Use this command to enable the NTP client to periodically update the device clock with the time synchronized from the external source clock. Use the **no** form of this command to remove this function.

**ntp update-calendar**  
**no ntp update-calendar**

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

**Defaults** By default, update the calendar periodically is not configured.

**Command mode** Global configuration mode.

**Usage Guide** By default, the NTP update-calendar is not configured. After configuration, the NTP client updates the calendar at the same time when the time synchronization of external time source is successful. It is recommended to enable this function for keeping the accurate calendar.

**Configuration** The following example configures the NTP update calendar periodically.

**Examples**

```
Ruijie(config)# ntp update-calendar
```

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

**Platform** N/A

**Description**

### 3.10 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
-----
-----
10:::2             None       None       FALSE   3
192.168.210.222   None       None       FALSE   3
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

### 3.11 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

## 4 SNTP Commands(beta)

### 4.1 show sntp

Use this command to display the SNTP configuration.

**show sntp**

Parameter Description	Parameter	Description
	N/A	N/A

#### Defaults

**Command mode** Privileged EXEC mode, global configuration mode, interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays the SNTP configuration.

```
Ruijie# show sntp
SNTP state           : Enable
SNTP server          : 192.168.4.12
SNTP sync interval   : 60
Time zone            : +8
```

Related Commands	Command	Description
	<b>sntp enable</b>	Enables SNTP.

**Platform** N/A

**Description**

### 4.2 sntp enable

Use this command to enable the SNTP function. Use the **no** form of this command to restore the default value.

**sntp enable**

**no sntp enable**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** SNTP is disabled by default.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration** The following example enables SNTP.

**Examples** Ruijie(config)# **sntp enable**

**Related Commands**

Command	Description
<b>show sntp</b>	Displays the SNTP configuration.

**Platform Description** N/A

### 4.3 sntp interval

Use this command to set the interval for the SNTP client to synchronize its clock with the NTP/SNTP server. Use the **no** form of this command to restore the default synchronization interval.

**sntp interval** *seconds*

**no sntp interval**

**Parameter Description**

Parameter	Description
<i>seconds</i>	Synchronization interval. The unit is second, and the range is from 60 to 65,535.

**Defaults** The default synchronization interval is 1,800 seconds.

**Command mode** Global configuration mode.

**Usage Guide** To make the synchronization interval configuration effective, run the **sntp enable** command.

**Configuration** The following example configures the synchronization interval to 3,600 seconds.

**Examples** Ruijie(config)# **sntp interval 3600**

**Related Commands**

Command	Description
<b>sntp enable</b>	Enables SNTP.
<b>show sntp</b>	Displays the SNTP configuration.

**Platform** N/A

**Description**

## 4.4 sntp server

Use this command to specify an SNTP server. Use the **no** form of this command to remove the SNTP server.

**sntp server** { *ip-address* | *domain* } [ **source** *source-ip-address* ]

**no sntp server**

Parameter Description	Parameter	Description
	<i>ip-address</i>	IP address of the SNTP server.
	<i>domain</i>	Specifies the domain name of the SNTP server.
	<i>source-ip-address</i>	(Optional) Indicates the specified source IP address.

**Defaults** No SNTP server is configured by default.

**Command mode** Global configuration mode.

**Usage Guide** As SNTP is fully compatible with NTP, the SNTP server can be used as an NTP server in Internet.

**Configuration** The following example specifies an SNTP server in Internet.

**Examples**

```
Ruijie(config)# sntp server 192.168.4.12
```

Related Commands	Command	Description
	<b>show sntp</b>	Displays the SNTP configuration.
	<b>sntp enable</b>	Enables SNTP.

**Platform** N/A

**Description**

## 5 SPAN Commands

### 5.1 monitor session

Use this command to configure the SPAN session and specify the source port (monitored port).

**monitor session** *session-num* **source interface** *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** *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** *session-num* [ **source interface** *interface-id* | **destination interface** *interface-id* ]

Use this command to remove the specified SPAN session, or remove the source port or destination port of the SPAN session.

**default monitor session** *session-num* { **source interface** *interface-id* | **destination interface** *interface-id* }

#### Parameter Description

Parameter	Description
<i>session-num</i>	SPAN session number
<i>interface-id</i>	Interface name
<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.

**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.

Configuring an access list for the source port indicates that only the traffic permitted by the access list is monitored.

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 0/17
Ruijie(config)# monitor session 1 destination interface gigabitEthernet 0/18
```

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 0/17
Ruijie(config)# no monitor session 1 destination interface gigabitEthernet
0/18
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform**

N/A

**Description**

## 5.2 show monitor

Use this command to display the SPAN configurations.

**show monitor** [ **session** *session-num* ]

**Parameter  
Description**

Parameter	Description
<i>session-num</i>	Displays the specified SPAN session.

**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 0/17      frame-type Both
dest-intf:
```

```
GigabitEthernet 0/18
```

The following example displays SPAN session 1.

```
Ruijie#show monitor session 1
sess-num: 1
span-type: LOCAL_SPAN
src-intf:
GigabitEthernet 0/17      frame-type Both
dest-intf:
GigabitEthernet 0/18
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform  
Description**

N/A





## Reliability Configuration Commands

---

1. REUP Commands(beta)
2. RLDP Commands
3. IP Event Dampening Commands(beta)

# 1 REUP Commands(beta)

## 1.1 link state group

Use this command to add the port into the specified link state track group. The **no** form of this command is used to delete a port from the specified link state track group.

**link state group** *num* { **upstream** | **downstream** }

**no link state group**

Parameter Description	Parameter	Description
	<i>num</i>	ID of the link state track group.
	<b>upstream</b>	Configures the port to be an upstream port in the link state track group.
	<b>downstream</b>	Configures the port to be a downstream port in the link state track group.

**Defaults** The port is not added into any link state track group.

**Command Mode** Interface configuration mode.

**Usage Guide** First create a link state track group and then add a port into the specified link state track group.

**Configuration Examples** The following example shows how to add the port GigabitEthernet 0/17 into the link state track group:

```
Ruijie(config)# link state track 1
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# link state group 1 upstream
```

Related Commands	Command	Description
	<b>link state track</b>	Enables a link state track group.

**Platform Description** N/A.

## 1.2 link state track

Use this command to enable the link state track group. The **no** form of this command is used to disable a link state track group

**link state track** [ *num* [ **up-delay** *delay-time* ] ]

**no link state track** [ *num* ]

**Parameter  
Description**

Parameter	Description
<i>num</i>	Interface ID of the link aggregation group.
<b>up-delay</b> <i>delay-time</i>	Downlink delay for link tracking in seconds. The value ranges from 0 to 300. The default value is 0.

**Defaults** N/A.

**Command  
Mode** Global configuration mode.

**Usage Guide** First create a link state track group and then add a port into the specified link state track group.

**Configuration** The following example shows how to create a link state track group:

**Examples** Ruijie(config)# link state track 1

**Related  
Commands**

Command	Description
<b>link state group</b>	Adds the port to the specified link state track group.

**Platform  
Description** N/A.

### 1.3 mac-address-table move update max-update-rate

Use this command to configure the maximum number of MAC address update packets sent per second.

**mac-address-table move update max-update-rate** *pkts-per-second*

**no mac-address-table move update max-update-rate**

**Parameter  
Description**

Parameter	Description
<i>pkts-per-second</i>	The maximum number of MAC address update packets sent per second. It ranges from 0 to 32000, and the default value is 150.

**Defaults** A maximum of 150 MAC address update packets are sent per second.

**Command  
Mode** Global configuration mode.

**Usage Guide** When a link is switched, REUP sends a certain number of MAC address update packets to an uplink

device in every second to recover downlink data transmission of the uplink device.

**Configuration Examples** The following example shows how to configure the maximum number of MAC address update packets sent per second:

```
Ruijie(config)# mac-address-table move update max-update-rate 20
```

**Related Commands**

Command	Description
N/A.	N/A.

**Platform Description** N/A.

## 1.4 mac-address-table move update receive

Use this command to enable REUP to receive the mac-address-table update messages.

**mac-address-table move update receive**

**no mac-address-table move update receive**

**Parameter Description**

Parameter	Description
N/A.	N/A.

**Defaults** Disabled.

**Command Mode** Global configuration mode.

**Usage Guide** The dual link backup switchover will lead to the loss of downstream data flow, for the MAC address for the uplink switch has not been updated in time. Therefore, it is necessary to update the MAC address table of the uplink switch, to reduce the loss of L2 data flow. You need to enable the switch of receiving the MAC address update messages on the uplink switch.

**Configuration Examples** Ruijie(config)# mac-address-table move update receive

**Related Commands**

Command	Description
<b>mac-address-table move update transit</b>	Enables REUP to transmit the mac-address-table update messages.

**Platform Description** N/A.

## 1.5 mac-address-table move update receive vlan

Use this command to configure the VLANs processing MAC address update packets.

**mac-address-table move update receive vlan** *vlan-range*

**no mac-address-table move update receive vlan** *vlan-range*

Parameter Description	Parameter	Description
	<i>vlan-range</i>	Range of the VLANs processing MAC address update packets.

**Defaults** All VLANs process MAC address update packets.

**Command Mode** Global configuration mode.

**Usage Guide** This command can be used to disable some VLANs from processing MAC address update packets. VLANs disabled from processing MAC address update packets can still recover downlink data transmission of the uplink device using MAC address update packets, but the capability to provide convergence on link failure will be degraded.

**Configuration Examples** The following example configures VLANs processing MAC address update packets:

```
Ruijie(config)# no mac-address-table move update receive vlan 20
```

Related Commands	Command	Description
	<b>mac-address-table move update receive</b>	Enables REUP to receive MAC address update packets.

**Platform** N/A.

**Description**

## 1.6 mac-address-table move update transit

Use this command to enable REUP to transmit the mac-address-table update messages.

**mac-address-table move update transit**

**no mac-address-table move update transit**

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

**Defaults** Disabled.

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

**Usage Guide** In order to reduce the link switchover and the loss of the downstream data flow, it is necessary to enable the switch of receiving the MAC address update messages on the uplink switch.

**Configuration Examples** Ruijie(config)# mac-address-table move update transit

Related Commands	Command	Description
	<b>mac-address-table move update transit vlan</b>	Enables REUP to transmit the mac-address-table update messages.

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

## 1.7 mac-address-table move update transit vlan

Use this command to enable REUP to transmit the mac-address update messages.

**mac-address-table move update transit vlan** *vid*

**no mac-address-table move update transit vlan**

Parameter Description	Parameter	Description
	<i>vid</i>	ID of the VLAN transmitting MAC address update packets.

**Defaults** Transmit the MAC-address update messages in the default VLAN on the port.

**Command** Interface configuration mode.  
**Mode**

**Usage Guide** When a link is switched, the VLAN enabled to transmit MAC address update packets will send MAC address update packets to its uplink device.

**Configuration Examples** The following example configures VLANs transmitting MAC address update packets:

**Examples** Ruijie(config)# mac-address-table move update transit

Related Commands	Command	Description
	<b>mac-address-table move update transit</b>	Enables REUP to receive the mac-address-table update messages.

**Platform** N/A.

## Description

## 1.8 mac-address-table update group

Use this command to set the mac-address-table update group.

**mac-address-table update group** [ *group-num* ]

**no mac-address-table update group**

**Parameter  
Description**

Parameter	Description
<i>group-num</i>	The mac-address-table update group ID.

**Defaults**

By default, no mac-address-table update group is configured.

**Command**

Interface configuration mode.

**Mode**

**Usage Guide**

In order to reduce the flood due to the MAC address update and the influence on the normal data transmission of the switch, Ruijie products add a configuration of MAC address update group. Only if all the interfaces are added to a MAC address update group, the downstream data transmission be restored rapidly.

**Configuration**

```
Ruijie(config-if-GigabitEthernet 0/17)# mac-address-table update group 2
```

**Examples**

**Related  
Commands**

Command	Description
<b>show mac-address-table update group detail</b>	Displays the mac-address-table update group information.

**Platform**

N/A.

**Description**

## 1.9 show interfaces switchport backup

Use this command to display the dual link backup information on the interfaces.

**show interfaces** [ *interface-id* ] **switchport backup** [ **detail** ]

**Parameter  
Description**

Parameter	Description
<i>interface-id</i>	The interface id of the dual link backup.
<b>detail</b>	Displays the detailed information about the dual link backup.

**Defaults** Show the dual link backup information on all interfaces.

**Command** Privileged EXEC mode.

**Mode**

**Usage Guide** N/A.

**Configuration** Ruijie # show interfaces switchport backup detail

**Examples** Switch Backup Interface Pairs:

```
Active Interface      Backup Interface      State
-----
Gi0/17                Gi0/18                Active Up/Backup Standby
Interface Pair : Gi0/17, Gi0/18
Preemption Mode : Off
Preemption Delay : 35 seconds
Bandwidth : Gi0/17(1000 Mbits), Gi0/18(1000 Mbits)
```

**Related  
Commands**

Command	Description
N/A.	N/A.

**Platform** N/A.

**Description**

## 1.10 show link state group

Use this command to display the information of a link state track group.

**show link state group**

**Parameter  
Description**

Parameter	Description
N/A.	N/A.

**Defaults** N/A.

**Command** Privileged EXEC mode.

**Mode**

**Usage Guide** N/A.

**Configuration** The following example displays the link state track group:

**Examples** Ruijie(config)#show interfaces switchport backup detail  
Ruijie(config)#show link state group



```

Link State Group:1 Status: Enabled, Down
Up-delay (default 0s): 0(s)
Upstream Interfaces :Gi0/17(Down)
Downstream Interfaces :

Link State Group:2 Status: Disabled, Down
Up-delay (default 0s): 0(s)
Upstream Interfaces :
Downstream Interfaces :

(Up):Interface up (Down):Interface Down (Dis):Interface disabled
    
```

**Related Commands**

Command	Description
N/A.	N/A.

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

### 1.11 show mac-address-table move update

Use this command to display the statistics about the MAC address updates tranceived on the interface.

**show mac-address-table move update**

**Parameter Description**

Parameter	Description
N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A.

**Configuration Examples**

```

Ruijie(config)#show mac-address-table move update
Mac address table move update status:
Transit:enable
Receive:enable
Max-update-rate:20
Receive vlan:1-19,21-4094
    
```

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

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

## 1.12 show mac-address-table update group

Use this command to display the mac-address-table update group information.

**show mac-address-table update group [ detail ]**

Parameter Description	Parameter	Description
	<b>detail</b>	

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A.

**Configuration Examples**

```
Ruijie # configure terminal
Ruijie (config)# mac-address-table move update receive
Ruijie (config)# interface range gigabitEthernet 0/17-18
Ruijie (config-if-range)# mac-address-table update group
Ruijie (config-if-range)# end
Ruijie # show mac-address-table update group detail
Mac-address-table Update Group:1
Received mac-address-table update message count:7
Group member  Receive Count  Last Receive  Switch-ID  Receive Time
-----
GigabitEthernet 0/17  0                0000.0000.0000
GigabitEthernet 0/18  0                0000.0000.0000
```

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

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

## 1.13 switchport backup interface

Use this command to configure the REUP dual link backup interface.

**switchport backup interface** *interface-id*

**no switchport backup**

Parameter Description	Parameter	Description
	<i>interface-id</i>	Interface ID of the backup link.

**Defaults** N/A.

**Command Mode** Interface configuration mode.

**Usage Guide** Enter the primary interface configuration mode, the *interface-id* in the parameter is for the backup interface. When the active link fails, the backup link transmission is restored rapidly

**Configuration Examples** The following example shows how to set the dual link backup, with GigabitEthernet 0/17 and

GigabitEthernet 0/18 as primary interface and backup interface:

```
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# switchport backup interface
gigabitethernet 0/18
```

Related Commands	Command	Description
	<b>show interface switchport backup</b>	Displays the dual link backup configuration on the switch.

**Platform** N/A.

**Description**

## 1.14 switchport backup interface preemption

Use this command to configure the REUP link preemption function.

**switchport backup interface** *interface-id* **preemption mode** { **forced** | **bandwidth** | **off** }

**switchport backup interface** *interface-id* **preemption delay** *delay-time*

**no switchport backup interface** *interface-id* **preemption delay**

**no switchport backup interface** *interface-id* **preemption mode**

Parameter Description	Parameter	Description
	<i>interface-id</i>	The interface id of the backup link.

<i>delay-time</i>	The preemption delay time.
-------------------	----------------------------

**Defaults** The default preemption delay time is 35s.

**Command** Interface configuration mode.

**Mode**

**Usage Guide** The preemption mode includes **forced**, **bandwidth** and **off**. In the **bandwidth** preemption mode, the interface with high bandwidth has priority over other interfaces to transmit the data. In the **forced** preemption mode, the primary has priority over backup interfaces to transmit the data. No preemption event occurs in the **off** preemption mode. By default, the preemption mode is off.

The preemption delay refers to the delay time of the link switchover after the restoration of the link failure.

**Configuration Examples** The following example shows how to set the dual link backup, with GigabitEthernet 0/17 and GigabitEthernet 0/18 as the primary interface and backup interface, set the bandwidth preemption mode and 40s preemption delay:

```
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(GigabitEthernet 0/17)# switchport backup interface gigabitethernet
0/18 preemption mode bandwidth
Ruijie(GigabitEthernet 0/17)# switchport backup interface gigabitethernet
0/18 preemption delay 40
```

**Related Commands**

Command	Description
<b>show interface switchport backup</b>	Displays the dual link backup configuration.

**Platform** N/A.

**Description**

## 1.15 switchport backup interface prefer

Use this command to configure VLAN load balancing on a link. The **no** form of this command is used to delete the configured VLAN load strategy.

**switchport backup interface** *interface-id* **prefer instance** *instance-range*

**no switchport backup interface** *interface-id* **prefer**

**Parameter Description**

Parameter	Description
<i>interface-id</i>	Interface ID of the backup link.
<i>instance-range</i>	Instance range of loading on the backup interface.

**Defaults** No VLAN load on the backup interface.

**Command** Interface configuration mode.  
**Mode**

**Usage Guide** MSTP instance mapping can be used to modify the mapping between an instance and a VLAN.

**Configuration** The following example configures VLAN load balancing on dual links.

**Examples**

```
Ruijie(GigabitEthernet 0/17)# switchport backup interface gigabitEthernet  
0/18 prefer instance 1
```

**Related  
Commands**

Command	Description
<b>show interface switchport backup</b>	Displays the configuration of dual-link backup on the switch.
<b>spanning-tree mst configuration</b>	Configures MSTP instances.

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

## 2 RLDP Commands

### 2.1 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 of this command to restore the default value.

**rldp detect-interval** *interval*

**no rldp detect-interval**

Parameter Description	Parameter	Description
	<i>interval</i>	Detection interval in the range 2 to 15 seconds

**Defaults** 3 seconds.

**Command** Global configuration mode.

**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** The following example shows how to set the detection interval as 5s:

**Examples** Ruijie(config)# rldp detect-interval 5

Related Commands	Command	Description
	<b>rldp detect-max</b>	Sets the maximum number of detections.

**Platform** N/A.

**Description**

### 2.2 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 of this command to restore it to the default value.

**rldp detect-max** *num*

**no rldp detect-max**

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

<i>num</i>	Maximum number of detections in the range 2 to 10
------------	---

**Defaults** 2.

**Command** Global configuration mode.

**Mode**

**Usage Guide** This command is used together with the detection interval to specify the maximum number of detections.

**Configuration** The following example shows how to set the maximum number of detections as 5:

**Examples** Ruijie(config)# rldp detect-max 5

**Related  
Commands**

Command	Description
<b>rldp detect-interval</b>	Sets the detection interval.

**Platform** N/A.

**Description**

## 2.3 rldp enable

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

**rldp enable**

**no rldp enable**

**Parameter  
Description**

Parameter	Description
N/A.	N/A.

**Defaults** Disabled.

**Command** Global configuration mode.

**Mode**

**Usage Guide** You can enable RLDP on the interface only when the global RLDP is enabled.

**Configuration** The following example shows how to enable RLDP:

**Examples** Ruijie(config)# rldp enable

**Related  
Commands**

Command	Description
<b>rldp port</b>	Enables the RLDP function on the port.

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

## 2.4 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.	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
	<b>rldp port</b>	Enables the RLDP function on the port.

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

## 2.5 rldp port

Use this command to enable RLDP on the port and specify detection type and troubleshooting method. Use the **no** form of this command to disable the function.

**rldp port { unidirection-detect | bidirection-detect | loop-detect } { warning | shutdown-svi | shutdown-port | block }**  
**no 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-svi</b>	Shut downs the SVI the port belongs to.
	<b>shutdown-port</b>	Shut downs the port.
	<b>block</b>	Indicates the failure treatment is disabling learning and forwarding of a 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 0/17, specify the detection type as loop detection, and troubleshooting method as block.

```
Ruijie(config)# interface gigabitethernet 0/17
Ruijie(config-if-GigabitEthernet 0/17)# rldp port loop-detect block
```

Related Commands	Command	Description
	<b>rldp enable</b>	Enables RLDP globally.

**Platform Description** N/A.

## 2.6 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**

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

**Defaults** N/A.

**Command** Privileged EXEC mode.

**Mode****Usage Guide** N/A.**Configuration** The example below demonstrates how to use this command:**Examples** Ruijie# rldp reset**Related  
Commands**

Command	Description
rldp enable	Enables RLDP globally.

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

## 2.7 show rldp

Use this command to display the RLDP information.

**show rldp** [ **interface** *interface-id* ]**Parameter  
Description**

Parameter	Description
<i>interface-id</i>	Interface ID

**Defaults** N/A.**Command** Privileged EXEC mode.**Mode****Usage Guide** N/A.**Configuration** N/A.**Examples****Related  
Commands**

Command	Description
N/A.	N/A.

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

## 3 IP Event Dampening Commands(beta)

### 3.1 dampening

Use this command to enable the IP event dampening function on the interface. Use the **no** or **default** form of this command to disable this function.

**dampening** [ *half-life-period* [ *reuse-threshold* *suppress-threshold* *max-suppress* [ **restart** [ *restart-penalty* ] ] ] ] ]

**no dampening**

**default dampening**

Parameter Description	Parameter	Description
	<i>half-life-period</i>	Configures the half-life period of suppression penalty. The range is from 1 to 30. The unit is seconds. The default value is 5 seconds.
	<i>reuse-threshold</i>	Configures the penalty threshold to unsuppress the interface. The range is from 1 to 20,000. The default value is 1,000.
	<i>suppress-threshold</i>	Configures the penalty threshold to suppress the interface. The range is from 1 to 20,000. The default value is 2,000.
	<i>max-suppress</i>	Configures the maximum suppress time. The range is from 1 to 255. The default value is 4 times of the <i>half-life-period</i> .
	<b>restart-penalty</b>	Configures the initial penalty value on the interface. The range is from 1 to 20,000. The default value is 2,000.

**Defaults** IP event dampening is disabled by default.

**Command mode** Interface configuration mode.

**Usage Guide** This function will influence the modules of the directly-connected/host route, static route, dynamic route and VRRP. If one interface meets the configuration condition of this command, which is in the suppression status, the above influenced modules consider the status of this interface as DOWN, so as to delete the corresponding route and not transceive the data packets on this interface.

Re-configuring the dampening command on the interface that has been configured this command makes all dampening information on this interface cleared. However, the interface flapping times will be remained unless use the clear counters command to clear the statistical information of the interface.

**Configuration Examples** The following example configures the IP event dampening function.

```
Ruijie(config)#interface vlan 1
Ruijie(config-if-VLAN 1)# dampening 30 1500 10000 100
```

Related Commands	Command	Description
	<b>clear counters</b>	Clears the interface counters.
	<b>show dampening interface</b>	Displays the statistics of the dampening interface.
	<b>show interface dampening</b>	Displays details of the dampening interface.

**Platform** When a Layer-3 port on a switch is converted to a Layer-2 port (for example, from a routed port to a switch port), the IP Event Dampening configuration on the port will be deleted.

**Description**

## 3.2 show dampening interface

Use this command to show the statistics of the dampening interface.

**show dampening interface**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command mode** Privileged EXEC mode/ global configuration mode/ interface configuration mode

**Usage Guide** N/A

**Configuration** The following example displays the statistics of the dampening interface.

### Examples

```
Ruijie# show dampening interface
3 interfaces are configured with dampening.
No interface is being suppressed.
```

Related Commands	Command	Description
	<b>dampening</b>	Enables the IP event dampening function on the interface.
	<b>clear counters</b>	Clears the interface counters.
	<b>show interface dampening</b>	Displays details of IP event dampening configuration.

**Platform** N/A

**Description**

### 3.3 show interface dampening

Use this command to display the details of IP event dampening configuration.

**show interface** [ *interface-Id* ] **dampening**

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** If the interface-id is specified, only the dampening information of this specified interface is displayed.

**Configuration** The following example shows the details of IP event dampening configuration.

```
Ruijie# show interface gigabitethernet 0/17 dampening
GigabitEthernet 0/17
  Flaps Penalty Supp   ReuseTm HalfL   ReuseV  SuppV  MaxSTm  MaxP  Restart
  0    0    FALSE  0      30      1500   10000  100   15119  0
```

Domain	Description
Flaps	Interface flapping times.
Penalty	The current penalty value on the interface.
Supp	Suppressed or not.
ReuseTm	Time to unsuppress the interface, in seconds.
HalfL	Half-life period, in seconds.
ReuseV	Unsuppressed threshold.
SuppV	Start suppression threshold.
MaxSTm	Maximum suppression time.
MaxP	Maximum penalty value.
Restart	The initial penalty value on the interface.

Related Commands	Command	Description
	<b>dampening</b>	Enables the IP event dampening function.
	<b>clear counters</b>	Clears the interface counters.
	<b>show dampening interface</b>	Displays statistics of the dampening interface.

**Platform** N/A

**Description**



## Security Configuration Commands

---

- 1 AAA Commands(beta)
- 2 RADIUS Commands(beta)
- 3 TACACS+ Commands(beta)
- 4 Global IP-MAC Binding Commands(beta)
- 5 Password-Policy Commands
- 6 Port Security Commands(beta)
- 7 Storm Control Commands
- 8 SSH Commands
- 9 CPU Protection Commands
- 10 DHCP Snooping Commands(beta)
- 11 DHCPv6 Snooping Commands(beta)
- 12 ARP-CHECK Commands(beta)
- 13 DAI Commands(beta)
- 14 IP Source Guard Commands(beta)
- 15 DoS Protection Commands
- 16 PPPoE Intermediate Agent Commands(beta)

# 1 AAA Commands(beta)

## 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 Examples** The following example enables NAS command accounting.

```
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 exec network start-stop group radius



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 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 Description** 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.

**Platform Description** N/A

## 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
Description	<i>interval</i>	Interval of sending the accounting update message, in the unit of minutes. The value ranges from 1 to 525600. The shortest interval is 1 minute.

**Defaults** The default is 5 minutes.

**Command Mode** Global configuration mode

**Usage Guide** If the AAA security service is not enabled, the accounting update function cannot be used. This command is used to set the accounting interval if the AAA security service has been enabled.

**Configuration Examples** The following example sets the interval of accounting update to 1 minute.

```
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 Description** N/A

## 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	Parameter	Description
Description	<b>default</b>	When this parameter is used, the following defined authentication method list is used as the default method for Enable authentication.
	<i>method</i>	It must be one of the keywords: <b>local</b> , <b>none</b> and <b>group</b> . One method list can contain up to four methods.
	<b>local</b>	Uses the local user name database for authentication.
	<b>none</b>	Does not perform authentication.
	<b>group</b>	Uses the server group for authentication. At present, the RADIUS and TACACS+ server groups are supported.
	<b>enable</b>	Enables AAA Enable authentication.

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** If the AAA Enable authentication service is enabled on the device, users must use AAA for Enable authentication negotiation. You must use the **aaa authentication enable** command to configure a default or optional method list for Enable authentication.

The next method can be used for authentication only when the current method does not work.

The Enable authentication function automatically takes effect after configuring the Enable authentication method list.

**Configuration Examples** The following example defines an AAA Enable authentication method list. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
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 Description** N/A

## 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	Parameter	Description
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> and <b>subs</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>subs</b>	Uses the subs database for authentication.

**Defaults** N/A

**Command Mode** Global configuration 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 Description** N/A

## 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	Parameter	Description
Description	<i>level</i>	Command level to be authorized in the range from 0 to 15
	<b>default</b>	When this parameter is used, the following defined method list is used as the default method for command authorization.
	<i>list-name</i>	Name of the user authorization method list, which could be any character strings
	<i>method</i>	It must be one of the keywords: <b>none</b> and <b>group</b> . One method list can contain up to four methods.
	<b>none</b>	Do not perform authorization.
	<b>group</b>	Uses the server group for authorization. At present, the TACACS+ server group is supported.

**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** N/A

## Description

## 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	Parameter	Description
Description	N/A	N/A

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

**Command** Global configuration mode

**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	Command	Description
Commands	<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	Parameter	Description
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 server group is supported.
--------------	--

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

**Command Mode** Global configuration mode

**Usage Guide** RGOS supports authorization of users logged in the NAS CLI and assignment of CLI authority level (0-15). The **aaa authorization exec** function is effective on condition that Login authentication function has been enabled. It cannot enter the CLI if it fails to enable the **aaa authorization exec**. You must apply the exec authorization method to the terminal line; otherwise the configured method is ineffective.

**Configuration Examples** The following example uses the RADIUS server to authorize Exec.

```
Ruijie(config)# aaa authorization exec default group radius
```

Related Commands	Command	Description
	<b>aaa new-model</b>	Enables the AAA security service.
	<b>authorization exec</b>	Applies the command authorization to the terminal line.
	<b>username</b>	Defines a local user database.

**Platform** N/A

**Description**

## 1.11 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 Description	Parameter	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



	server group is supported.
--	----------------------------

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

**Command Mode** Global configuration 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 Commands	Command	Description
	<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
<b>Description</b>	<i>max-attempts</i>	In the range from 1 to 2,147,483,647

**Defaults** The default is 3.

**Command** Global configuration mode

**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****Description**

Parameter	Description
<i>lockout-time</i>	In the range from 1 to 43,200 in the unit of minutes

**Defaults** The default is 15 minutes.

**Command** Global configuration mode

**Mode**

**Usage Guide** Use this command to configure the length of lockout-time when the login user has attempted for more than the limited times.

**Configuration** The following example sets the lockout-time period to 5 minutes.

**Examples**

```
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	Parameter	Description
Description	N/A	N/A

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

**Command** Global configuration mode

**Mode**

**Usage Guide** Use this command to enable the system to print the syslog informing aaa authentication success.

**Configuration** The following example disables the system to print the syslog informing aaa authentication success.

**Examples**

```
Ruijie(config)# no aaa log enable
```

Related	Command	Description
Commands	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**

Parameter	Parameter	Description
Description	<i>num</i>	The number of syslog entries printed per second. The range is from 0 to 65,535. 0 indicates the printing rate is not limited.

**Defaults** The default is 5.

**Command Mode** Global configuration mode

**Usage Guide** Too much printing may flood the screen or even reduce device performance. In this case, use this command to adjust the printing rate.

**Configuration Examples** The following example sets the rate of printing the syslog informing AAA authentication success to 10.

```
Ruijie(config)# aaa log rate-limit 10
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** 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**

Parameter Description	Parameter	Description
	N/A	N/A

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

**Command Mode** Global configuration mode

**Usage Guide** Use this command to enable AAA. If AAA is not enabled, none of the AAA commands can be configured.

**Configuration Examples** The following example enables the AAA security service.

```
Ruijie(config)# aaa new-model
```

Related	Command	Description
Commands	<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
Description	<b>all</b>	Indicates all locked users.
	<b>user-name word</b>	Indicates the ID of the locked User.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command to clear all the user lists or a specified user list.

**Configuration** The following example clears the lockout user list.

**Examples**

```
Ruijie# clear aaa local user lockout all
```

Related	Command	Description
Commands	<b>show running-config</b>	Displays the current configuration of the switch.
	<b>show aaa lockout</b>	Displays the lockout configuration parameter of current login.

**Platform** N/A

**Description**

## 1.18 show aaa accounting update

Use this command to display the accounting update information.

```
show aaa accounting update
```

Parameter	Parameter	Description						
Description	N/A	N/A						
Defaults	N/A							
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode							
Usage Guide	Use this command to display the accounting update interval and whether the accounting update is enabled.							
Configuration	The following example displays the accounting update information.							
Examples	<pre>Ruijie# show aaa accounting update</pre>							
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>aaa new-model</td> <td>Enables the AAA security service.</td> </tr> <tr> <td>aaa domain enable</td> <td>Enables the domain-name-based AAA service.</td> </tr> </tbody> </table>	Command	Description	aaa new-model	Enables the AAA security service.	aaa domain enable	Enables the domain-name-based AAA service.	
Command	Description							
aaa new-model	Enables the AAA security service.							
aaa domain enable	Enables the domain-name-based AAA service.							
Platform Description	N/A							

## 1.19 show aaa group

Use this command to display all the server groups configured for AAA.

**show aaa group**

Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	N/A	
Configuration	The following command displays all the server groups.	
Examples	<pre>Ruijie# show aaa group Type      Reference Name -----</pre>	

```
radius 1 radius
tacacs+ 1 tacacs+
radius 1 dot1x_group
radius 1 login_group
radius 1 enable_group
```

Related	Command	Description
Commands	<b>aaa group server</b>	Configures the AAA server group.

**Platform** N/A

**Description**

## 1.20 show aaa lockout

Use this command to display the lockout configuration.

**show aaa lockout**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** N/A

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

**Usage Guide** Use this command to display the lockout configuration.

**Configuration** The following example displays the lockout configuration.

**Examples**

```
Ruijie# show aaa lockout
Lock tries: 3
Lock timeout: 15 minutes
```

Related	Command	Description
Commands	N/A	N/A

**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
Description	N/A	N/A

**Defaults** N/A

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

**Usage Guide** Use this command to display all AAA method lists.

**Configuration** The following example displays the AAA method list.

### Examples

```
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
Authorization method-list
aaa authorization network default group radius
```

Related Commands	Command	Description
	<b>aaa authentication</b>	Defines a user authentication method list
	<b>aaa authorization</b>	Defines a user authorization method list
	<b>aaa accounting</b>	Defines a user accounting method list

**Platform Description** N/A

## 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
Description	<b>all</b>	Displays all AAA user information.
	<b>lockout</b>	Displays the locked AAA user information.
	<b>by-id</b> <i>session-id</i>	Displays the information of the AAA user that with a specified session ID.
	<b>by-name</b> <i>user-name</i>	Displays the information of the AAA user with a specified user name.

**Defaults** N/A

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

**Usage Guide** Use this command to display AAA user information.

**Configuration Examples** The following example displays AAA user information.

```
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 RADIUS Commands(beta)

### 2.1 aaa group server radius

Use this command to enter AAA server group configuration mode.

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

**aaa group server radius** *name*

**no aaa group server radius** *name*

Parameter Description	Parameter	Description
	<i>name</i>	Server group name. Keywords "radius" and "tacacs +" are excluded as they are the default RADIUS and TACACS+ server group names.

**Defaults** N/A

**Command** Global configuration mode

**Mode**

**Usage Guide** This command is used to configure a RADIUS AAA server group.

**Configuration** The following example configures a RADIUS AAA server group named ss.

**Examples**

```
Ruijie(config)# aaa group server radius ss
Ruijie(config-gs-radius)# end
Ruijie# show aaa group
Type      Reference Name
-----
radius    1          radius
tacacs+   1          tacacs+
radius    1          ss
```

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 2.2 ip radius source-interface

Use this command to specify the source IP address for the RADIUS packet.

Use the **no** form of this command to delete the source IP address for the RADIUS packet.

**ip radius source-interface** *interface-name*

**no radius source-interface** *interface-name*

Parameter Description	Parameter	Description
	<i>interface-name</i>	Interface that the source IP address of the RADIUS packet belongs to.

**Defaults** The source IP address of the RADIUS packet is set by the network layer.

**Command mode** Global configuration mode

**Usage Guide** In order to reduce the NAS information to be maintained on the RADIUS server, use this command to set the source IP address of the RADIUS packet. This command uses the first IP address of the specified interface as the source IP address of the RADIUS packet. This command is used in the layer 3 devices.

**Configuration Examples** The following example specifies that the RADIUS packet obtains an IP address from the GigabitEthernet 0/1 interface and uses it as the source IP address of the RADIUS packet.

```
Ruijie(config)# ip radius source-interface GigabitEthernet 0/1
```

Related Commands	Command	Description
	<b>radius-server host</b>	Defines the RADIUS server.
	<b>ip address</b>	Configures the IP address of the interface.

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

## 2.3 radius set qos cos

Use this command to set the QoS value sent by the RADIUS server as the CoS value of the interface.

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

**radius set qos cos**

**no radius set qos cos**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** Set the QoS value sent by the RADIUS server as the DSCP value.

**Command Mode** Global configuration mode.

**Usage Guide** This command is used to set the QoS value sent by the RADIUS server as the CoS value, and the DSCP value by default.

**Configuration Examples** The following example sets the QoS value sent by the RADIUS server as the CoS value of the interface:

```
Ruijie(config)# radius set qos cos
```

Related Commands	Command	Description
	<b>radius vendor-specific extend</b>	Extends RADIUS as not to differentiate the IDs of private vendors.

**Platform Description** N/A

## 2.4 radius support cui

Use this command to enable RADIUS to support the cui function.

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

**radius support cui**

**no radius support cui**

Parameter Description	Parameter	Description
	N/A	N/A

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

**Command Mode** Global configuration mode

**Usage Guide** This command is used to enable RADIUS to support the cui function.

**Configuration** The following example enables RADIUS to support the cui function.

**Examples**

```
Ruijie(config)# radius support cui
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 2.5 radius vendor-specific attribute support

Use this command to configure whether RADIUS accounting request packets carry the private attribute of a specified vendor.

Use the **no** form of this command to configure that RADIUS accounting request packets do not carry the private attribute of a specified vendor.

**radius vendor-specific attribute support { cisco | huawei | ms}**

**no radius vendor-specific attribute support { cisco | huawei | ms}**

**Parameter  
Description**

Parameter	Description
<b>cisco</b>	Indicates the private attribute of Cisco.
<b>huawei</b>	Indicates the private attribute of Huawei.
<b>ms</b>	Indicates the private attribute of Microsoft.

**Defaults** By default, RADIUS accounting request packets carry the private attribute of a specified vendor.

**Command  
Mode** Global configuration mode

**Usage Guide** This command is used to configure whether RADIUS accounting request packets carry the private attribute of a specified vendor as required.

**Configuration  
Examples** 1. The following example configures that RADIUS accounting request packets carry the private attribute of Huawei.

```
Ruijie(config)# radius vendor-specific attribute support huawei
```

2. The following example configures that RADIUS accounting request packets do not carry the private attribute of Huawei.

```
Ruijie(config)# no radius vendor-specific attribute support huawei
```

Related Commands	Command	Description
	N/A	N/A

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

## 2.6 radius vendor-specific extend

Use this command to extend RADIUS not to differentiate the IDs of private vendors.

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

**radius vendor-specific extend**

**no radius vendor-specific extend**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** Only the private vendor IDs of Ruijie are recognized.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to identify the attributes of all vendor IDs by type.

**Configuration Examples** The following example extends RADIUS so as not to differentiate the IDs of private vendors:

```
Ruijie(config)# radius vendor-specific extend
```

Related Commands	Command	Description
	<b>radius attribute</b>	Configures vendor type.
<b>radius set qos cos</b>	Sets the QoS value sent by the RADIUS server as the cos value of the interface.	

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

## 2.7 radius-server account attribute

Use this command to enable account-request packets to contain a specified RADIUS attribute.

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

**radius-server account attribute *type* package**

**no radius-server account attribute *type* package**

**default radius-server account attribute *type* package**

Use this command to disable account-request packets to contain a specified RADIUS attribute.

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

**radius-server account attribute *type* unpackage**

**no radius-server account attribute *type* unpackage**

**default radius-server account attribute *type* unpackage**

<b>Parameter Description</b>	Parameter	Description
	<i>type</i>	RADIUS attribute in the range from 1 to 255
<b>Defaults</b>	RFC-compliant	
<b>Command Mode</b>	Global configuration mode	
<b>Usage Guide</b>	Use this command to enable or disable account-request packets to contain a specified RADIUS attribute.	
<b>Configuration Examples</b>	The following example disables account-request packets to contain attribute NAS-PORT-ID.	
	<pre>Ruijie(config)# radius-server account attribute 87 unpackage</pre>	
<b>Platform Description</b>	N/A	

## 2.8 radius-server account update retransmit

Use this command to configure accounting update packet retransmission for the second generation Web authentication user.

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

**radius-server account update retransmit**

**no radius-server account update retransmit**



<b>Parameter Description</b>	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table>	Parameter	Description	N/A	N/A
Parameter	Description				
N/A	N/A				
<b>Defaults</b>	This function is disabled by default.				
<b>Command Mode</b>	Global configuration mode				
<b>Usage Guide</b>	This command is used to configure accounting update packet retransmission for the second generation Web authentication user exclusively.				
<b>Configuration Examples</b>	<p>The following example configures accounting update packet retransmission for the second generation Web authentication user.</p> <pre>Ruijie(config)#radius-server account update retransmit</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				

## 2.9 radius-server account vendor

Use this command to enable account-request packets to contain vendor-specific RADIUS attributes.

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

**radius-server account vendor** *vendor\_name* **package**

**no radius-server account vendor** *vendor\_name* **package**

**default radius-server account vendor** *vendor\_name* **package**

<b>Parameter Description</b>	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>vendor_name</i></td> <td><b>cmcc/ microsoft/cisco</b></td> </tr> </tbody> </table>	Parameter	Description	<i>vendor_name</i>	<b>cmcc/ microsoft/cisco</b>
Parameter	Description				
<i>vendor_name</i>	<b>cmcc/ microsoft/cisco</b>				
<b>Defaults</b>	Account-request packets do not contain vendor- specific RADIUS attributes by default.				
<b>Command Mode</b>	Global configuration mode				
<b>Usage Guide</b>	Use this command to enable account-request packets to contain vendor-specific RADIUS attributes.				

<b>Configuration</b>	The following example enables account-request packets to contain "cmcc".
<b>Examples</b>	<pre>Ruijie(config)# radius-server account vendor cmcc package</pre>
<b>Platform</b>	N/A
<b>Description</b>	

## 2.10 radius-server attribute class

Use this command to analyze the flow control value of the RADIUS CLASS attributes.

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

**radius-server attribute class user-flow-control { format-16bytes | format-32bytes }**  
**no radius-server attribute class**

<b>Parameter Description</b>	Parameter	Description
	<b>user-flow-control</b>	Analyzes flow control value in the CLASS attribute.
	<b>format-16bytes</b>	Sets the format of flow control value to 16 bytes.
	<b>format-32bytes</b>	Sets the format of flow control value to 32 bytes.

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

**Command Mode** Global configuration mode

**Usage Guide** This command is required if the server pushes the flow control through the CLASS attribute.

**Configuration Examples** The following example analyzes the flow control value of the CLASS attribute and sets the format to 32 bytes.

```
Ruijie(config)#radius-server attribute class user-flow-control
format-32bytes
```

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

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

## 2.11 radius-server attribute 31

Use this command to specify the MAC-based format of RADIUS Calling-Station-ID attribute.

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

**radius-server attribute 31 mac format { ietf | normal | unformatted }**

**no radius-server attribute 31 mac format**

**Parameter  
Description**

Parameter	Description
<b>ietf</b>	The standard format specified by the IETF RFC3580. '-' is used as the separator, for example: 00-D0-F8-33-22-AC.
<b>normal</b>	Normal format representing the MAC address. ';' is used as the separator. For example: 00d0.f833.22ac.
<b>unformatted</b>	No format and separator. By default, unformatted is used. For example: 00d0f83322ac.

**Defaults**

The default format is unformatted.

**Command Mode**

Global configuration mode

**Usage Guide**

Some RADIUS security servers (mainly used to 802.1x authentication) may identify the IETF format only. In this case, the RADIUS Calling-Station-ID attribute shall be set as the IETF format type.

**Configuration**

The following example defines the RADIUS Calling-Station-ID attribute as IETF format.

**Examples**

```
Ruijie(config)# radius-server attribute 31 mac format ietf
```

**Related Commands**

Command	Description
<b>radius-server host</b>	Defines the RADIUS server.

**Platform**

N/A

**Description**

## 2.12 radius-server authentication attribute

Use this command to enable access-request packets to contain a specified RADIUS attribute.

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

**radius-server authentication attribute *type* package**

**no radius-server authentication attribute *type* package**

**default radius-server authentication attribute *type* package**

Use this command to disable access-request packets to contain a specified RADIUS attribute.

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

**radius-server authentication attribute** *type* **unpackage**

**no radius-server authentication attribute** *type* **unpackage**

**default radius-server authentication attribute** *type* **unpackage**

Parameter Description	Parameter	Description
	<i>type</i>	RADIUS attribute in the range from 1 to 255

**Defaults** RFC-compliant

**Command Mode** Global configuration mode

**Usage Guide** Use this command to enable access-request packets to contain a specified RADIUS attribute.

**Configuration Examples** The following example disables access-request packets to contain attribute NAS-PORT-ID.

```
Ruijie(config)# radius-server authentication attribute 87 unpackage
```

**Platform Description** N/A

## 2.13 radius-server authentication vendor

Use this command to enable access-request packets to contain vendor-specific RADIUS attributes.

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

**radius-server authentication vendor** *vendor\_name* **package**

**no radius-server authentication vendor** *vendor\_name* **package**

**default radius-server authentication vendor** *vendor\_name* **package**

Parameter Description	Parameter	Description
	<i>vendor_name</i>	<b>cmcc/ microsoft/cisco</b>

**Defaults** Access-request packets do not contain vendor- specific RADIUS attributes by default.

**Command Mode** Global configuration mode

**Usage Guide** Use this command to enable access-request packets to contain vendor- specific RADIUS attributes.

**Configuration** The following example enables access-request packets to contain “cmcc”.

**Examples**

```
Ruijie(config)# radius-server authentication vendor cmcc package
```

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

## 2.14 radius-server dead-criteria

Use this command to configure criteria on a device to determine that the RADIUS server is unreachable.

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

**radius-server dead-criteria** { **time** *seconds* [ **tries** *number* ] | **tries** *number* }

**no radius-server dead-criteria** { **time** *seconds* [ **tries** *number* ] | **tries** *number* }

Parameter Description	Parameter	Description
	<b>time</b> <i>seconds</i>	Configures the timeout value. If the device does not receive a correct response packet from the RADIUS server within the specified time, the RADIUS server is considered to be unreachable. The value is in the range from 1 to 120 in the unit of seconds.
	<b>tries</b> <i>number</i>	Configures the successive timeout times. When sending a request from the device to the RADIUS server times out for the specified times, the device considers that the RADIUS server is unreachable. The value is in the range from 1 to 100 in the unit of seconds.

**Defaults** The default **time** *seconds* is 60 and **tries** *number* is 10.

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

**Usage Guide** If a RADIUS server meets the timeout and timeout times at the same time, it is considered to be unreachable. This command is used to adjust the parameter conditions of timeout and timeout times.

**Configuration** The following example sets the timeout to 120 seconds and timeout times to 20.

**Examples**

```
Ruijie(config)# radius-server dead-criteria time 120 tries 20
```

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

<b>radius-server host</b>	Defines the RADIUS security server.
<b>radius-server deadtime</b>	Defines the duration when a device stops sending any requests to an unreachable RADIUS server.
<b>radius-server timeout</b>	Defines the timeout for the packet re-transmission.

**Platform** N/A

**Description**

## 2.15 radius-server deadtime

Use this command to configure the duration when a device stops sending any requests to an unreachable RADIUS server.

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

**radius-server deadtime** *minutes*

**no radius-server deadtime**

Parameter Description	Parameter	Description
	<i>minutes</i>	Defines the duration in minutes when the device stops sending any requests to the unreachable RADIUS server. The value is in the range from 1 to 1,440 in the unit of minutes.

**Defaults** The default value of minutes is 0, that is, the device keeps sending requests to the unreachable RADIUS server.

**Command Mode** Global configuration mode

**Usage Guide** If active RADIUS server detection is enabled on the device, the time parameter of this command does not take effect on the RADIUS server. Otherwise, the RADIUS server becomes reachable when the duration set by this command is shorter than the unreachable time.

**Configuration Examples** The following example sets the duration when the device stops sending requests to 1 minute.

```
Ruijie(config)# radius-server deadtime 1
```

Related Commands	Command	Description
	<b>radius-server host</b>	Defines the RADIUS security server.

<b>radius-server dead-criteria</b>	Defines the criteria to determine that a RADIUS server is unreachable.
------------------------------------	--

**Platform** N/A

**Description**

## 2.16 radius-server host

Use this command to specify a RADIUS security server host.

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

**radius-server host** { *ipv4-address* | *ipv6-address* } [ **auth-port** *port-number* ] [ **acct-port** *port-number* ] [ **test username** *name* [ **ignore-auth-port** ] [ **ignore-acct-port** ] [ **idle-time** *time* ] ] [ **key** [ **0** | **7** ] *text-string* ]

**no radius-server host** { *ipv4-address* | *ipv6-address* }

**Parameter Description**

Parameter	Description
<i>ipv4-address</i>	IPv6 address of the RADIUS security server host.
<i>ipv6-address</i>	IPv4 address of the RADIUS security server host.
<i>auth-port</i>	UDP port used for RADIUS authentication.
<i>port-number</i>	Number of the UDP port used for RADIUS authentication. If it is set to 0, this host does not perform authentication.
<i>acct-port</i>	UDP port used for RADIUS accounting.
<i>port-number</i>	Number of the UDP port used for RADIUS accounting. If it is set to 0, this host does not perform accounting.
<b>test username</b> <i>name</i>	(Optional) Enables the active detection to the RADIUS security server and specify the username used by the active detection.
<b>ignore-auth-port</b>	(Optional) Disables the detection to the authentication port on the RADIUS security server. It is enabled by default.
<b>ignore-acct-port</b>	(Optional) Disables the detection to the authentication port on the RADIUS security server. It is enabled by default.
<b>idle-time</b> <i>time</i>	(Optional) Sets the interval of sending the test packets to the reachable RADIUS security server, which is 60 minutes by default and in the range of 1 to 1440 minutes (namely 24 hours).
<b>key</b> [ <b>0</b>   <b>7</b> ] <i>text-string</i>	Configure a shared key for the server. The type of encryption can be specified. 0 is no encryption and 7 is simple encryption. The default is 0.

**Defaults** No RADIUS host is specified by default.

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

**Usage Guide** In order to implement the AAA security service using RADIUS, you must define a RADIUS security server. You can define one or more RADIUS security servers using the **radius-server host** command.

**Configuration** The following example defines a RADIUS security server host:

**Examples**

```
Ruijie(config)# radius-server host 192.168.12.1
```

The following example defines a RADIUS security server host in the IPv4 environment, enable the active detection with the detection interval 60 minutes and disable the accounting UDP port detection:

```
Ruijie(config)# radius-server host 192.168.100.1 test username viven
ignore-acct-port idle-time 60
```

The following example defines a RADIUS security server host in the IPv6 environment

```
Ruijie(config)# radius-server host 3000::100
```

**Related  
Commands**

Command	Description
<b>aaa authentication</b>	Defines the AAA authentication method list
<b>radius-server key</b>	Defines a shared password for the RADIUS security server.
<b>radius-server retransmit</b>	Defines the number of RADIUS packet retransmissions.

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

## 2.17 radius-server key

Use this command to define a shared password for the network access server (device) to communicate with the RADIUS security server.

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

**radius-server key** [ 0 | 7 ] *text-string*

**no radius-server key**

**Parameter  
Description**

Parameter	Description
<i>text-string</i>	Text of the shared password



<b>0   7</b>	Password encryption type. 0: no encryption; 7: Simply-encrypted.
--------------	--

**Defaults** No shared password is specified by default.

**Command**

**Mode** Global configuration mode.

**Usage Guide** A shared password is the basis for communications between the device and the RADIUS security server. In order to allow the device to communicate with the RADIUS security server, you must define the same shared password on the device and the RADIUS security server.

**Configuration** The following example defines the shared password **aaa** for the RADIUS security server:

**Examples** Ruijie(config)# radius-server key aaa

**Related  
Commands**

Command	Description
<b>radius-server host</b>	Defines the RADIUS security server.
<b>radius-server retransmit</b>	Defines the number of RADIUS packet retransmissions.
<b>radius-server timeout</b>	Defines the timeout for the RADIUS packet.

**Platform** N/A

**Description**

## 2.18 radius-server retransmit

Use this command to configure the number of packet retransmissions before the device considers that the RADIUS security server does not respond.

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

**radius-server retransmit** *retries*

**no radius-server retransmit**

**Parameter  
Description**

Parameter	Description
<i>retries</i>	Number of retransmissions in the range from 1 to 100

**Defaults** The default is 3.

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

**Usage Guide** AAA uses the next method to authenticate users only when the current security server for authentication does not respond. When the device retransmits the RADIUS packet for the specified times and the interval between every two retries is timeout, the device considers that the security sever does not respond.

**Configuration** The following example sets the number of retransmissions to 4.

**Examples** Ruijie(config)# radius-server retransmit 4

**Related  
Commands**

Command	Description
<b>radius-server host</b>	Defines the RADIUS security server.
<b>radius-server key</b>	Defines a shared password for the RADIUS server.
<b>radius-server timeout</b>	Defines the timeout for the RADIUS packet.

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

## 2.19 radius-server source-port

Use this command to configure the source port to send RADIUS packets.

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

**radius-server source-port** *port*

**no radius-server source-port**

**Parameter  
Description**

Parameter	Description
<i>port</i>	The port ID, in the range from 1 to 65535.

**Defaults** The default is a random number.

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

**Usage Guide** The source port is random by default. This command is used to specify a source port.

**Configuration** The following example configures source port 10000 to send RADIUS packets.

**Examples** `Ruijie(config)# radius-server source-port 10000`

**Related  
Commands**

Command	Description
N/A	N/A

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

## 2.20 radius-server timeout

Use this command to set the time for the device to wait for a response from the security server after retransmitting the RADIUS packet.

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

**radius-server timeout** *seconds*

**no radius-server timeout**

**Parameter  
Description**

Parameter	Description
<i>seconds</i>	Timeout in the range from 0 to 1,000 in the unit of seconds.

**Defaults** The default is 5 seconds.

**Command**

**Mode** Global configuration mode

**Usage Guide** This command is used to change the timeout of packet retransmission.

**Configuration** The following example sets the timeout to 10 seconds.

**Examples** `Ruijie(config)# radius-server timeout 10`

**Related  
Commands**

Command	Description
<b>radius-server host</b>	Defines the RADIUS security server.
<b>radius-server retransmit</b>	Defines the number of the RADIUS packet retransmissions.
<b>radius-server key</b>	Defines a shared password for the RADIUS server.

**Platform** N/A

## Description

## 2.21 server auth-port acct-port

Use this command to add the server of the AAA server group.

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

**server** { *ipv4-addr* | *ipv6-addr* } [ **auth-port** *port1* ] [ **acct-port** *port2* ]

**no server** { *ipv4-addr* | *ipv6-addr* } [ **auth-port** *port1* ] [ **acct-port** *port2* ]

Parameter  
Description

Parameter	Description
<i>ip-addr</i>	Server IP address
<i>ipv6-addr</i>	Server IPv6 address
<i>port1</i>	Server authentication port
<i>port2</i>	Server accounting port

**Defaults** No server is configured by default.

**Command Mode** Server group configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example adds server 192.168.4.12 to server group ss and sets the accounting port and authentication port to 5 and 6 respectively.

```
Ruijie(config)# aaa group server radius ss
Ruijie(config-gs-radius)# server 192.168.4.12 acct-port 5 auth-port 6
Ruijie(config-gs-radius)# end
Ruijie# show aaa group
Type      Reference Name
-----
radius    1          radius
tacacs+   1          tacacs+
radius    1          ss
```

Related  
Commands

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 2.22 show radius acct statistics

Use this command to display RADIUS accounting statistics.

**show radius acct statistics**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

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

**Usage Guide** N/A

**Configuration Examples** The following example displays RADIUS accounting statistics.

```
Ruijie#show radius acct statistics
Accounting Servers:

Server Index..... 1
Server Address..... 192.168.1.1
Server Port..... 1813
Msg Round Trip Time..... 0 (msec)
First Requests..... 1
Retry Requests..... 1
Accounting Responses..... 0
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Pending Requests.....
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 2.23 show radius attribute

Use this command to display standard RADIUS attributes.

**show radius attribute**

Parameter Description	Parameter	Description
	N/A	N/A

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

**Usage Guide** N/A

**Configuration Examples** The following example displays standard RADIUS attributes.

```
Ruijie#sh radius attribute
type          implicate
-----
1.....User-Name
2.....User-Password
3.....Chap-Password
4.....NAS-Ip-Addr
5.....Nas-Ip-Port
6.....Service-Type
7.....Framed-Protocol
8.....Frame-Ip-Address
9.....Framed-Ip-Mask
10.....Framed-Routing
11.....Filter-Id
12.....Framed-Mtu
13.....Framed-Compress
14.....Login-Ip-Host
15.....Login-Service
16.....Login-Tcp-Port
18.....Reply-Message
19.....Callback-Num
20.....Callback-Id
22.....Framed-Route
23.....Framed-IPX-Network
24.....State
25.....Class
26.....Vendor-Specific
27.....Session-Timeout
28.....Idle-Timeout
29.....Termination-Action
```

```
30.....Called-Station-Id
31.....Calling-Station-Id
32.....Nas-Id
33.....Proxy-State
34.....Login-LAT-Service
35.....Login-LAT-Node
36.....Login-LAT-Group
37.....Framed-AppleTalk-Link
38.....Framed-AppleTalk-Net
39.....Framed-AppleTalk-Zone
40.....Acct-Status-Type
41.....Acct-Delay-Time
42.....Acct-Input-Octets
43.....Acct-Output-Octets
44.....Acct-Session-Id
45.....Acct-Authentic
46.....Acct-Session-Time
47.....Acct-Input-Packet
48.....Acct-Output-Packet
49.....Acct-Terminate-Cause
50.....Acct-Multi-Session-ID
51.....Acct-Link-Count
52.....Acct-Input-Gigawords
53.....Acct-Output-Gigawords
60.....Chap-Challenge
61.....Nas-Port-Type
62.....Port-Limit
63.....Login-Lat-Port
64.....Tunnel-Type
65.....Tunnel-Medium-Type
66.....Tunnel-Client-EndPoint
67.....Tunnel-Service-EndPoint
79.....eap msg
80.....Message-Authenticator
81.....group id
85.....Acct-Interim-Interval
87.....Nas-Port-Id
89.....cui
95.....Nas-Ipv6-Addr
96.....Framed-Interface-Id
97.....Framed-Ipv6-Prefix
```

```

98.....Login-Ipv6-Host
99.....Framed-Ipv6-Route
100.....Framed-Ipv6-Pool
168.....Framed-Ipv6-Addr
    
```

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

## 2.24 show radius auth statistics

Use this command to display RADIUS authentication statistics.

**show radius auth statistics**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

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

**Usage Guide** N/A

**Configuration** The following example displays RADIUS authentication statistics.

```

Examples Ruijie#show radius auth statistics
Authentication Servers:

Server Index..... 1
Server Address..... 192.168.1.1
Server Port..... 1812
Msg Round Trip Time..... 0 (msec)
First Requests..... 0
Retry Requests..... 0
Accept Responses..... 0
Reject Responses..... 0
Challenge Responses..... 0
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Pending Requests..... 0
    
```



```
Timeout Requests..... 0
Unknowntype Msgs..... 0
Other Drops..... 0
```

Related Commands	Command	Description
		N/A

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

## 2.25 show radius group

Use this command to display RADIUS server group configuration.

**show radius group**

Parameter Description	Parameter	Description
		N/A


**Defaults** N/A

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

**Usage Guide** N/A

**Configuration Examples** The following example displays RADIUS server group configuration.

```
Ruijie#show radius group
=====Radius group radius=====
Vrf:not-set
Server:192.168.1.1
  Server key:ruijie
  Authentication port:1812
  Accounting port:1813
  State:Active
```

 RG-S29 series do not support the VRF parameter. The above example is for reference purpose. Please take the actual device as standard.

Related Commands	Command	Description
	N/A	N/A

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

## 2.26 show radius parameter

Use this command to display global RADIUS server parameters.

**show radius parameter**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

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

**Usage Guide** N/A

**Configuration Examples** The following example displays global RADIUS server parameters.

```
Ruijie# show radius parameter
Server Timeout: 5 Seconds
Server Deadtime: 0 Minutes
Server Retries: 3
Server Dead Criteria:
Time: 10 Seconds
Tries: 10
```

Related Commands	Command	Description
	N/A	N/A

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

## 2.27 show radius server

Use this command to display the configuration of the RADIUS server.

**show radius server**

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 of the RADIUS server.

### Examples

```
Ruijie# show radius server
Server IP: 192.168.4.12
Accounting Port: 23
Authen Port: 77
Test Username: viven
Test Idle Time: 10 Minutes
Test Ports: Authen
Server State: Active
    Current duration 765s, previous duration 0s
Dead: total time 0s, count 0
Statistics:
Authen: request 15, timeouts 1
Author: request 0, timeouts 0
Account: request 0, timeouts 0

Server IP: 192.168.4.13
Accounting Port: 45
Authen Port: 74
Test Username: <Not Configured>
Test Idle Time: 60 Minutes
Test Ports: Authen and Accounting
Server State: Active
Current duration 765s, previous duration 0s
```

```
Dead: total time 0s, count 0
Statistics:
Authen: request 0, timeouts 0
Author: request 0, timeouts 0
Account: request 20, timeouts 0
```

**Related Commands**

Command	Description
<b>radius-server host</b>	Defines the RADIUS security server.
<b>radius-server retransmit</b>	Defines the number of RADIUS packet retransmissions.
<b>radius-server key</b>	Defines a shared password for the RADIUS server.
<b>radius-server timeout</b>	Defines the packet transmission timeout.

**Platform** N/A

**Description**

## 2.28 show radius vendor-specific

Use this command to display the configuration of the private vendors.

**show radius vendor-specific**

**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 of the private vendors.

**Examples**

```
Ruijie#show radius vendor-specific
id  vendor-specific  type-value
-----
1   max-down-rate    1
2   port-priority    2
```

3	user-ip	3
4	vlan-id	4
5	last-supPLICANT-vers	5
	ion	
6	net-ip	6
7	user-name	7
8	password	8
9	file-directory	9
10	file-count	10
11	file-name-0	11
12	file-name-1	12
13	file-name-2	13
14	file-name-3	14
15	file-name-4	15
16	max-up-rate	16
17	current-supPLICANT-version	17
18	flux-max-high32	18
19	flux-max-low32	19
20	proxy-avoid	20
21	dialup-avoid	21
22	ip-privilege	22
23	login-privilege	42
26	ipv6-multicast-addre	79
	ss	
27	ipv4-multicast-addre	87
	ss	

**Related  
Commands**

Command	Description
<b>radius-server host</b>	Defines the RADIUS security server.
<b>radius-server retransmit</b>	Defines the number of RADIUS packet retransmissions.
<b>radius-server key</b>	Defines a shared password for the RADIUS server.
<b>radius-server timeout</b>	Defines the packet transmission timeout.

**Platform  
Description** N/A

## 3 TACACS+ Commands(beta)

### 3.1 aaa group server tacacs+

Use this command to configure different groups of TACACS+ server hosts.

Use the **no** form of this command to remove a specified TACACS server group.

**aaa group server tacacs+ group\_name**

**no aaa group server tacacs+ group\_name**

Parameter Description	Parameter	Description
	<i>group_name</i>	TACACS+ server group name, which cannot be <b>radius</b> or <b>tacacs+</b> . The two names are the built-in group name.

**Defaults** No TACACS+ server group is configured.

**Command Mode** Global configuration mode

**Usage Guide** After you group different TACACS+ servers, the tasks of authentication, authorization and accounting can be implemented by different server groups.

**Configuration Examples** The following example configures a TACACS+ server group named tac1, and configures a TACACS+ server with IP address 1.1.1.1 in this group:

```
Ruijie(config)#aaa group server tacacs+ tac1
Ruijie(config-gs-tacacs+)# server 1.1.1.1
```

Related Commands	Command	Description
	<b>server</b>	Configures server list of TACACS+ server group.

**Platform** N/A

**Description**

### 3.2 ip tacacs source-interface

Use this command to use the IP address of a specified interface for all outgoing TACACS+ packets.

Use the **no** form of this command to disable use of the specified interface IP address.

**ip tacacs source-interface** *interface-name*  
**no ip tacacs source-interface** *interface-name*

**Parameter  
Description**

Parameter	Description
<i>interface-name</i>	Interface for the outgoing TACACS+ packets

**Defaults**

The source IP address of TACACS+ packets is set on the network layer.

**Command  
Mode**

Global configuration mode

**Usage Guide**

To decrease the work of maintaining massive NAS messages in TACACS+ server, use this command to use the IP address of a specified interface for all outgoing TACACS+ packets. This command specifies the primary IP address of the specified interface as the source address of TACACS+ packets on Layer 3 devices.

**Configuration  
Examples**

The following example specifies the IP address of GigabitEthernet 0/1 for the outgoing TACACS+ packets.

```
Ruijie(config)# ip tacacs source-interface gigabitEthernet 0/1
```

**Related  
Commands**

Command	Description
<b>tacacs-server host</b>	Defines a TACACS+ server.
<b>ip address</b>	Configures the IP address of an interface.

**Platform**

N/A

**Description**

### 3.3 server

Use this command to configure the IP address of the TACACS+ server for the group server.

Use the **no** form of this command to remove the TACACS+ server.

**server** { *ipv4-address* | *ipv6-address* }

**no server** { *ipv4-address* | *ipv6-address* }

**Parameter  
Description**

Parameter	Description
<i>ipv4-address</i>	IPv4 address of the TACACS+ server
<i>ipv6-address</i>	IPv6 address of the TACACS+ server

- Defaults** No TACACS+ server is configured by default.
- Command Mode** TACACS+ server group configuration mode
- Usage Guide** You must configure the **aaa group server tacacs+** command before configuring this command. To configure server address in TACACS+ group server, you must use the **tacacs-server host** command in global configuration mode. If there is no response from the first host entry, the next host entry is tried.

**Configuration Examples** The following example configures a TACACS+ server group named tac1 and a TACACS+ server address 1.1.1.1 in this group.

```
Ruijie(config)#aaa group server tacacs+ tac1
Ruijie(config-gs-tacacs+)# server 1.1.1.1
```

**Related Commands**

Command	Description
<b>aaa group server tacacs+</b>	Configures a TACACS+ server group.

**Platform Description** N/A

### 3.4 show tacacs

Use this command to display the TACACS+ server configuration.

**show tacacs**

**Parameter Description**

Parameter	Description
N/A	N/A

**Defaults** N/A

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

**Usage Guide** N/A



**Configuration** The following example displays the TACACS+ server configuration.

**Examples**

```
Ruijie# show tacacs
Tacacs+ Server : 172.19.192.80/49
Socket Opens: 0
Socket Closes: 0
Total Packets Sent: 0
Total Packets Recv: 0
Reference Count: 0
```

**Related Commands**

Command	Description
<b>tacacs-server host</b>	Defines a TACACS+ secure server host.

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

### 3.5 tacacs-server host

Use this command to configure a TACACS+ host.

Use the **no** form of this command to remove the TACACS+ host.

**tacacs-server host** {*ipv4-address* | *ipv6-address*} [**port** *integer*] [**timeout** *integer*] [**key** [ **0** | **7** ] *text-string* ]

**no tacacs-server host** { *ip-address* | *ipv6-address* }

**Parameter Description**

Parameter	Description
<i>ip-address</i>	IPv4 address of the TACACS+ host
<i>ipv6-address</i>	IPv6 address of the TACACS+ host
<b>port</b> <i>integer</i>	Port number of the server. The range is from 1 to 65,535. The default is 49.
<b>timeout</b> <i>integer</i>	Timeout time of TACACS+ host. The range is from 1 to 1,000.
<b>key</b> <i>string</i>	Configures an authentication and encryption key. The value can be 0 or 7. 0 indicates no encryption, while 7 indicates simple encryption. The default is 0.

**Defaults** No TACACS+ host is specified by default.

**Command** Global configuration mode

**Mode**

**Usage Guide** The TACACS+ host must be configured to implement AAA security service. You can use this command to configure one or multiple TACACS+ hosts.

**Configuration** The following example configures a TACACS+ host.

**Examples**

```
Ruijie(config)# tacacs-server host 192.168.12.1
```

**Related Commands**

Command	Description
N/A	N/A

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

## 3.6 tacacs-server key

Use this command to configure the authentication encryption key used for TACACS+ communications between the access server and the TACACS+ server.

Use the **no** form of this command to remove the authentication encryption key.

**tacacs-server key** [ 0 | 7 ] *string*

**no tacacs-server key**

**Parameter Description**

Parameter	Description
<i>string</i>	Key string
<b>0   7</b>	Encryption type of key 0 indicates no encryption; 7 indicate simple encryption.

**Defaults** No authentication encryption key is configured by default.

**Command** Global configuration mode

**Mode**

**Usage Guide** Use command to configure a global authentication and encryption key for TACACS+ communication. Use the **key** parameter in the **tacacs-server host** command to configure a server-based key.

**Configuration** The following example defines the authentication encryption key of TACACS+ server as aaa:

**Examples**

```
Ruijie(config)# tacacs-server key aaa
```

Related Commands	Command	Description
	<b>tacacs-server host</b>	Defines a TACACS+ host.

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

### 3.7 tacacs-server timeout

Use this command to set the interval for which the server waits for a server host to reply. Use the **no** form of this command to restore the default timeout interval.

**tacacs-server timeout** *seconds*

**no tacacs-server timeout**

Parameter Description	Parameter	Description
	<i>seconds</i>	Timeout interval in the range from 1 to 1,000 in the unit of seconds

**Defaults** The default is 5 seconds.

**Command Mode** Global configuration mode

**Usage Guide** Use command to configure a global timeout interval. Use the **timeout** parameter in the **tacacs-server host** command to configure a server-based interval.

**Configuration Examples** The following example configures the timeout interval to 10 seconds.

```
Ruijie(config)# tacacs-server timeout 10
```

Related Commands	Command	Description
	<b>tacacs-server host</b>	Defines a TACACS+ secure server host.

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

## 4 Global IP-MAC Binding Commands(beta)

### 4.1 address-bind

Use this command to configure global IP-MAC address binding. Use the **no** form of this command to restore the default setting.

**address-bind** *ip-address mac-address*

**no address-bind** *ip-address*

Parameter	Parameter	Description
Description	<i>ip-address</i>	IPv4 address to be bound
	<i>mac-address</i>	MAC address to be bound

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example configures global IP-MAC address binding.

```
Ruijie# configure terminal
Ruijie(config)# address-bind 192.168.5.1 00d0.f800.0001
```

Related Commands	Command	Description
	<b>show address-bind</b>	Displays the IP address-MAC address binding table.

**Platform** N/A

**Description**

### 4.2 address-bind install

Use this command to enable a binding policy globally. Use the **no** form of this command to restore the default setting.

**address-bind install**

**no address-bind install**

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

<b>Description</b>	N/A	N/A				
<b>Defaults</b>	N/A					
<b>Command Mode</b>	Global configuration mode					
<b>Usage Guide</b>	If you bind an IP address to a MAC address, run this command to make the installation policy take effect.					
<b>Configuration Examples</b>	The following example enables a binding policy.					
<b>Examples</b>	<pre>Ruijie# configure terminal Ruijie(config)# address-bind 3.3.3.3 00d0.f811.1112 Ruijie(config)# address-bind install</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					

### 4.3 address-bind uplink

This command is used to configure the exception port. Use the **no** form of this command to restore the default setting.

**address-bind uplink** *interface-id*

**no address-bind uplink** *interface-id*

<b>Parameter Description</b>	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>interface-id</i></td> <td>Switching port or layer 2 aggregate port.</td> </tr> </tbody> </table>	Parameter	Description	<i>interface-id</i>	Switching port or layer 2 aggregate port.
Parameter	Description				
<i>interface-id</i>	Switching port or layer 2 aggregate port.				
<b>Defaults</b>	All ports are non-exception ports by default.				
<b>Command Mode</b>	Global configuration mode.				
<b>Usage Guide</b>	<p>If you have bound an IP address and a MAC address, the switch will discard the packets that have the same source IP address but different source MAC address.</p> <p>If the port is an exceptional port and is installed (see address-bind install), this binding policy does not take effect.</p>				

**Configuration** The following example configures the exception port.

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# address-bind uplink gigabitethernet 0/1
```

**Related Commands**

Command	Description
<b>show address-bind uplink</b>	Displays the exceptional port of address binding.

**Platform** N/A

**Description**

## 4.4 show address-bind

Use this command to display global IP address-MAC address binding.

**show address-bind**

**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 global IPv4 address-MAC address binding.

**Examples**

```
Ruijie# show address-bind
Total Bind Addresses in System : 1
IP Address      Binding MAC Addr
-----
192.168.5.1    00d0.f800.0001
```

Field	Description
Total Bind Addresses in System	IPv4 address-MAC address binding count
IP Address	Bound IP address
Binding MAC Addr	Bound MAC address

**Related**

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

<b>Commands</b>	<b>address-bind</b>	Enables IP address-MAC address binding.
-----------------	---------------------	---

**Platform** N/A

**Description**

## 4.5 show address-bind uplink

Use this command to display the exception port.

**show address-bind uplink**

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

**Defaults** N/A

**Command mode** N/A

**Usage Guide** N/A

**Configuration** The following example displays the exception port.

**Examples**

```
Ruijie# show address-bind uplink
```

```
Port      State
-----  -
Gi0/1     Enabled
Default   Disabled
```

Field	Description
Port	Short for exception ports. All ports are non-exception ports by default.
State	Indicates whether the port is exception port. State Enabled indicates that it is an exception port while state Disabled indicates that it is not.

Related Commands	Command	Description
	<b>address-bind uplink</b>	Sets the exception port.

**Platform** N/A

**Description**

## 5 Password-Policy Commands

### 5.1 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

### 5.2 password policy min-size

Use this command to set the minimum length of the password. Use the **no** form of this command to



restore the default setting.

**password policy min-size** *length*

**no password policy min-size**

**Parameter  
Description**

Parameter	Description
<i>length</i>	Sets the minimum length of the password, in the range from 1 to 31.

**Defaults**


No minimum length of the password is set by default.

**Command  
Mode**

Privileged EXEC mode

**Usage Guide**

This command is used to set the minimum length of the password,

 This function is valid for the global password (the **enable password** and the **enable secret** commands) and the local user password (the **username name password password** command) while not valid for the password in line mode.

**Configuration**

The following example sets the minimum length of the password to 8.

**Examples**

```
Ruijie(config)# password policy min-size 8
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform  
Description**

N/A

## 5.3 password policy no-repeat-times

Use this command to ban the use of passwords used in the past several times. Use the no form of this command to restore the default setting.


**password policy no-repeat-times** *times*

**no password policy no-repeat-times**

**Parameter  
Description**

Parameter	Description
<i>times</i>	The past several times when passwords are configured, in the range from 1 to 31.

- Defaults** This function is disabled by default.
- Command Mode** Global configuration mode
- Usage Guide** After this function is enabled, passwords used in the past several times are recorded. If the new password has been used, the alarm message is displayed and password configuration fails.  
This command is used to set the maximum number of password entries. When the actual number of password entries exceeds the configured number, the new password overwrites the oldest password.

 This function is valid for the global password (the **enable password** and the **enable secret** commands) and the local user password (the **username name password password** command) while not valid for the password in line mode.

**Configuration** The following example bans the use of passwords used in the past five times.

**Examples**

```
Ruijie(config)# password policy no-repeat-times 5
```

Related Commands	Command	Description
	N/A	N/A

## 5.4 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

## 1.7 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**

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

Commands	
<b>enable password</b>	Sets passwords of different privileges.

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

## 5.5 show password policy

Use this command to display the password security policy set by the user.

**show password policy**

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** The following example displays the password security policy set by the user.

**Examples**

```
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	

Related	Command	Description
<b>Commands</b>		

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

**Platform  
Description** N/A

## 6 Port Security Commands(beta)

### 6.1 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
          (Count)      (Count)      (Count)      (Count)
-----
1   Gi0/1   128         2           2           1           protect
-----
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.
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
activ
```

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** N/A  
**Description**

## 6.2 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>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.

**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>	Displays port security settings.

**Platform Description** N/A

## 6.3 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>	Applies the aging time to both manually configured secure addresses and automatically learned addresses. Otherwise, apply it to only the automatically learned secure addresses.
<b>time</b> <i>time</i>	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-GigabitEthernet 0/1)# end
```

**Related Commands**

Command	Description
<b>show port-security</b>	Displays port security settings.

**Platform Description** N/A

## 6.4 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*

**s**

**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
	<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 Examples** The following example binds the IP address 192.168.1.100 on interface GigabitEthernet 0/10:

```
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 GigabitEthernet 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	Command	Description
---------	---------	-------------

Commands	
<b>show port-security</b>	Displays port security settings.
<b>switchport port-security</b>	Enables the port-security.
<b>switchport port-security interface binding</b>	Configures the secure address binding in Global 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**

## 6.5 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*  
**s**

**no switchport port-security interface** *interface-id* **binding** [ *mac-address* **vlan** *vlan-id* ]  
*ipv4-address*

Parameter Description	Parameter	Description
	<i>interface-id</i>	Binds interface ID.
	<i>mac-address</i>	Binds source MAC address.
	<i>vlan-id</i>	VLAN ID of the binding source MAC address
	<i>ipv4-address</i>	Binds IPv4 address.

**Defaults** N/A

**Command Mode** Global 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.

**Configuration** The following example binds the IP address 192.168.1.100 on the interface GigabitEthernet 0/10.

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# switchport port-security interface gigabitethernet 0/10
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 interface gigabitethernet 0/10
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**

## 6.6 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
<i>interface-id</i>	Interface ID
<i>mac-address</i>	Static secure address
<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 gigabitethernet 0/10
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 Description** N/A

## 6.7 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 0/1)# switchport port-security mac-address
00d0.f800.5555 vlan 2
Ruijie(config-if-GigabitEthernet 0/1)# 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 interface mac-address</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

## 6.8 switchport port-security mac-address sticky

Use this command to configure the Sticky MAC secure address.

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

**switchport port-security mac-address sticky** *mac-address* [ **vlan** *vlan-id* ]

**no switchport port-security mac-address sticky** *mac-address* [ **vlan** *vlan-id* ]


Use the command without parameters to enable the Sticky MAC address learning.

Use the **no** form of this command to disable the Sticky MAC address learning.

**switchport port-security mac-address sticky**

**no switchport port-security mac-address sticky**



Parameter Description	Parameter	Description
	<i>mac-address</i>	Static secure address
	<i>vlan-id</i>	Vlan ID of the MAC address   The configuration of vlan-id is only supported on the TRUNK port.

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

**Command Mode** Interface configuration mode

**Usage Guide** Sticky MAC addresses, either static or dynamic, are special addresses free from aging.

**Configuration Examples** The following example sets the MAC address and VLAN ID of TRUNK port 10 to 00d0.f800.5555 to 2 respectively.

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitethernet 0/10
Ruijie(config-if-GigabitEthernet 0/1)# switchport port-security mac-address
00d0.f800.5555 vlan 2
Ruijie(config-if-GigabitEthernet 0/1)# end
```

The following example enables the Sticky MAC address learning on interface GigabitEthernet 0/10.

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitethernet 0/10
Ruijie(config-if-GigabitEthernet 0/1)# switchport port-security mac-address
sticky
Ruijie(config-if-GigabitEthernet 0/1)# 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 interface mac-address</b>	Sets the static secure address in privileged EXEC mode.
	<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**

## 6.9 switchport port-security maximum

Use this command to set the maximum number of port secure addresses.

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

**switchport port-security maximum** *value*

**no switchport port-security maximum**

Parameter Description	Parameter	Description
	<i>value</i>	Maximum number of the secure address, in the range from 1 to 64.

**Defaults** The default is 128.

**Command Mode** Interface configuration mode

**Usage Guide** The number of the secure address contains the sum of static secure address and dynamically learnt secure address, 64 by default.  
If the number of the secure address you set is less than current number, it will prompt this setting failure.

**Configuration Examples** The following example sets the maximum number of the secure address to 2 for interface GigabitEthernet 0/10.

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitethernet 0/10
Ruijie(config-if-GigabitEthernet 0/1)# switchport port-security maximum 2
Ruijie(config-if-GigabitEthernet 0/1)# 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 the interface configuration mode.
	<b>switchport port-security aging</b>	Sets the aging time for the port secure address.

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

## 7 Storm Control Commands

### 7.1 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> <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** N/A

**Description**

### 7.2 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
<b>level</b> <i>percent</i>	Sets the bandwidth percentage, for example, 20 means 20%.
<b>pps</b> <i>packets</i>	Sets the pps, which means packets per second.
<i>rate-bps</i>	Rate allowed

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

**Command** Interface configuration mode

**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)# int gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# storm-control multicast 4096
```

**Related**

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

**Commands**

<b>show storm-control</b>	Displays storm suppression information.

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

## 8 SSH Commands

### 8.1 crypto key generate

Use this command to generate a public key to the SSH server.




**crypto key generate { dsa | rsa }**

Parameter	Parameter	Description
Description	<b>rdsa</b>	Generates a DSA key.
	<b>drsa</b>	Generates an RSA key.

**Defaults** By default, the SSH server does not generate a public key.

**Command Mode** Global configuration 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
	<b>show ip ssh</b>	Displays the current status of the SSH server.
	<b>crypto key zeroize { dsa   rsa }</b>	Deletes DSA and RSA keys and disables the SSH server

	function.
--	-----------

**Platform** N/A

**Description**

## 8.2 crypto key zeroize

Use this command to delete a public key to the SSH server.

**crypto key zeroize { dsa | rsa }**

Parameter	Parameter	Description
<b>Description</b>	<b>rdsa</b>	Deletes the DSA key.
	<b>drsa</b>	Deletes the RSA 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
```

Related Commands	Command	Description
	<b>show ip ssh</b>	Displays the current status of the SSH server.
	<b>crypto key generate { dsa   rsa }</b>	Generates DSA and RSA keys.

**Platform** N/A

**Description**

## 8.3 disconnect ssh

Use this command to disconnect the established SSH connection.

**disconnect ssh [ vty ] session-id**

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



<b>Description</b>	<b>vtty</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
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
		<b>show ssh</b>
	<b>clear line vty</b> <i>line_number</i>	Disconnects the current VTY connection.

**Platform Description** N/A

## 8.4 ip scp server enable

Use this command to enable the SCP server function on a network device.

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

**ip scp server enable**

**no ip scp server enable**

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

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

**Command** Global configuration mode

**Mode**

**Usage Guide** Secure Copy (SCP) enables an authenticated user to transfer files to/from a remote device in an encrypted way, with high security and guarantee.

**Configuration** The following example enables the SCP server function.

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# ip scp server enable
```

Related	Command	Description
Commands	<b>show ip ssh</b>	Displays the current status of the SSH server.

**Platform** N/A

**Description**

## 8.5 ip ssh authentication-retries

Use this command to set the authentication retry times of the SSH server.

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

**ip ssh authentication-retries** *retry-times*

**no ip ssh authentication-retries**

Parameter	Parameter	Description
Description	<i>retry-times</i>	Authentication retry times, ranging from 0 to 5

**Defaults** The default is 3.

**Command** Global configuration mode

**Mode**

**Usage Guide** User authentication is considered failed if authentication is not successful when the configured authentication retry times on the SSH server is exceeded. Use the **show ip ssh** command to display the configuration of the SSH server

**Configuration** The following example sets the authentication retry times to 2.

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# ip ssh authentication-retries 2
```

Related	Command	Description
Commands	<b>show ip ssh</b>	Displays the current status of the SSH server.

**Platform** N/A

**Description**

## 8.6 ip ssh cipher-mode

Use this command to set the SSH server encryption mode.

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

**ip ssh cipher-mode { cbc | ctr | others }**

**no ip ssh cipher-mode**

Parameter	Parameter	Description
<b>Description</b>	<b>cbc</b>	Encryption mode: CBC (Cipher Block Chaining) 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) Encryption algorithm: AES128-CTR, AES192-CTR, AES256-CTR
	<b>others</b>	Encryption mode: Others Encryption algorithm: RC4

**Defaults** All encryption modes are supported by default.

**Command** Global configuration mode

**Mode**

**Usage Guide** This command is used to set the SSH server encryption mode.

For Ruijie Networks, the SSHv1 server supports DES-CBC, 3DES-CBC, and Blowfish-CBC; the SSHv2 server supports AES128-CTR, AES192-CTR, AES256-CTR, DES-CBC, 3DES-CBC, AES-128-CBC, AES-192-CBC, AES-256-CBC, Blowfish-CBC, and RC4. All these algorithms can be grouped into CBC, CTR and Other as shown above.

With the advancement of cryptography study, CBC and Others encryption modes are proved to easily decipher. It is recommended to enable the CTR mode to raise assurance for organizations and enterprises demanding high security.

**Configuration** The following example enables CTR encryption mode.

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# ip ssh cipher-mode ctr
```

**Platform** N/A

**Description**

## 8.7 ip ssh hmac-algorithm

Use this command to set the algorithm for message authentication.

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

**ip ssh hmac-algorithm** { md5 | md5-96 | sha1 | sha1-96 }

**no ip ssh hmac-algorithm**

Parameter	Parameter	Description
Description	md5	MD5 algorithm
	md5-96	MD5-96 algorithm
	sha1	SHA1 algorithm
	sha1-96	SHA1-96 algorithm

**Defaults** SSHv1: all the algorithms are not supported.

SSHv2: all the algorithms are supported.

**Command** Global configuration mode

**Mode**

**Usage Guide** Ruijie SSHv1 servers do not support algorithms for message authentication.

For Ruijie Networks, the SSHv1 server does not support message authentication algorithms; the SSHv2 server supports MD5, MD5-96, SHA1, and SHA1-96 algorithms. Set the algorithm on your demand.

**Configuration** The following example sets the algorithm for message authentication to SHA1.

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# ip ssh hmac-algorithm sha1
```

**Platform** N/A

**Description**

## 8.8 ip ssh peer

Use this command to associate the public key file and the user name on the client. During client login authentication, you can specify a public key file based on the user name.

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

**ip ssh peer** *username* **public-key** { dsa | rsa } *filename*

**no ip ssh peer** *username* **public-key** { dsa | rsa } *filename*

Parameter	Parameter	Description
Description	<i>username</i>	User name

<i>filename</i>	Name of a public key file
<b>rdsa</b>	The public key is a DSA key
<b>drsa</b>	The public key is a RSA 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** N/A

**Description**

## 8.9 ip ssh time-out

Use this command to set the authentication timeout for the SSH server.

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

**ip ssh time-out** *time*

**no ip ssh time-out**

Parameter 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	Command	Description
Commands	<b>show ip ssh</b>	Displays the current status of the SSH server.

**Platform** N/A

**Description**

## 8.10 ip ssh version

Use this command to set the version of the SSH server.

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

**ip ssh version { 1 / 2 }**

**no ip ssh version**

Parameter	Parameter	Description
<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	Command	Description
Commands	<b>show ip ssh</b>	Displays the current status of the SSH server.

**Platform** N/A

**Description**

## 8.11 show crypto key mypubkey

Use this command to display the information about the public key part of the public key to the SSH server.

**show crypto key mypubkey { dsa | rsa }**

Parameter	Parameter	Description
Description	<b>rdsa</b>	Displays the DSA key.
	<b>drsa</b>	Displays the RSA 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 8tOmpWlI XU1QItVN mLdR+G7O
Q10kz+4/
      /IgyR0ge 1sZNg32u dFEifZ6D zfLySPqC MTWlfw==

% Key pair was generated at: 7:1:25 UTC Jan 16 2013
Key name: RSA private
Usage: SSH Purpose Key
Key is not exportable.
Key Data:
      AAAAAwEA AQAAAEAA 0E5w2H0k v744uTIR yZBd/7AM 8pLItnW3 XH3LhEEi
BbZGZvn3
      LEYYfQ9s pgYL0ZQf S0s/GY0X gJOMsc6z i80AkQ==
```

Related	Command	Description
Commands	<code>crypto key generate { dsa   rsa }</code>	Generates DSA and RSA keys.

Platform N/A

Description

## 8.12 show ip ssh

Use this command to display the information of the SSH server.

**show ip ssh**

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Privileged EXEC mode/Global configuration mode  
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 generate rsa and dsa key to enable SSH
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: enabled
```



Related	Command	Description
Commands	<b>ip ssh version { 1   2 }</b>	Configures the version for the SSH server.
	<b>ip ssh time-out time</b>	Sets the authentication timeout for the SSH server.
	<b>ip ssh authentication-retries</b>	Sets the authentication retry times for the SSH server.

**Platform** N/A

**Description**

## 8.13 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

Field	Description
Connection	VTY number
Version	SSH version
Encryption	Encryption algorithm
Hmac	Message authentication algorithm
Compress	Compress algorithm
State	Connection state

Username	Username
----------	----------

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

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

## 9 CPU Protection Commands

### 9.1 clear cpu-protect counters

Use this command to clear the CPP statistics.

**clear cpu-protect counters** [ **device** *device-num* ] [ **slot** *slot-num* ]

<b>Parameter Description</b>	<table border="1"><thead><tr><th>Parameter</th><th>Description</th></tr></thead><tbody><tr><td>N/A</td><td>N/A</td></tr></tbody></table>	Parameter	Description	N/A	N/A
Parameter	Description				
N/A	N/A				
<b>Defaults</b>	N/A				
<b>Command Mode</b>	Privileged EXEC mode				
<b>Usage Guide</b>	N/A				

**Configuration** The following example clears the CPP statistics.

**Examples**

```
Ruijie# show cpu-protect | in arp
arp          4          150          4          0          8605          0
Ruijie# clear cpu-protect counters
Ruijie# show cpu-protect | in arp
arp          4          150          3          0          4          0
```

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 9.2 cpu-protect type bandwidth

Use this command to configure the bandwidth of a specific packet.

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

**cpu-protect type** *packet-type* **bandwidth** *bandwidth-value*

**no cpu-protect type** *packet-type* **bandwidth**

**Parameter Description**

Parameter	Description
<i>packet-type</i>	Packet type, which varies with products
<i>bandwidth-value</i>	An integer number ranges from 0 to 32000 (pps). Indicates the bandwidth value of the CPU port.

**Defaults** The default CPU port bandwidth varies with products.

**Command** Global configuration mode

**Mode**

**Usage Guide** N/A

**Configuration** The following example sets the BPDU bandwidth to 200 pps.

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# cpu-protect type bpdu bandwidth 200
Ruijie(config)# end
```

```
Ruijie# #show cpu-protect | in bpdu
bpdu          10          200          0          0          0          0
tunnel-bpdu   10          128          0          0          0          0
```

**Related  
Commands**

Command	Description
N/A	N/A

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

### 9.3 show cpu-protect

Use this command to display all CPP configuration and statistics.

**show cpu-protect**

**Parameter  
Description**

Parameter	Description
N/A	N/A

**Defaults** N/A**Command  
Mode** All configuraiton mode**Usage Guide** N/A**Configuration  
Examples** N/A**Related  
Commands**

Command	Description
N/A	N/A

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

## 10 DHCP Snooping Commands(beta)

### 10.1 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* ]

Parameter Description	Parameter	Description
	<i>mac</i>	Specifies the user MAC address to be cleared.
	<i>vlan-id</i>	Specifies the ID of the VLAN to be cleared.
	<i>ip</i>	Specifies the IP address to be cleared.
	<i>interface-id</i>	Specifies the ID of the interface to be cleared.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command to clear the current dynamic user information from the DHCP Snooping binding database.

 After this command is used, all the DHCP clients connecting interfaces with IP Source Guard function enabled should request IP addresses again, or they cannot access network.

**Configuration Examples** The following example clears the dynamic database information from the DHCP Snooping binding database.

```
Ruijie# clear ip dhcp snooping binding
Ruijie# show ip dhcp snooping binding
Total number of bindings: 0
MacAddress IpAddress Lease(sec) Type VLAN Interface
-----
```

**Related Commands**

Command	Description
<b>show ip dhcp snooping binding</b>	Displays the information of the DHCP Snooping binding database.

**Platform** N/A

**Description**

## 10.2 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** Global configuration mode

**Mode**

**Usage Guide** The **show ip dhcp snooping** command is used to display whether the DHCP Snooping function is enabled.

**Configuration** The following example enables the DHCP Snooping function.

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping
```

Related Commands	Command	Description
	<b>show ip dhcp snooping</b>	Displays the configuration information of DHCP Snooping.
	<b>ip dhcp snooping vlan</b>	Configures DHCP Snooping enabled VLAN.

**Platform** N/A

**Description**

## 10.3 ip dhcp snooping bootp-bind

Use this command to enable DHCP Snooping BOOTP-bind function.

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

**ip dhcp snooping bootp-bind**

**no ip dhcp snooping bootp-bind**

Parameter Description	Parameter	Description
	N/A	N/A

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

**Command Mode** Global configuration mode

**Usage Guide** By default, the DHCP Snooping only forwards BOOTP packets. With this function enabled, it can Snoop BOOTP packets. After the BOOTP client requests an address successfully, the DHCP Snooping adds the BOOTP user to the static binding database.

**Configuration Examples** The following example enables the DHCP Snooping BOOTP-bind function.

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping bootp-bind
```

Related Commands	Command	Description
	<b>show ip dhcp snooping</b>	Displays the DHCP Snooping configuration.

**Platform Description** N/A

## 10.4 ip dhcp snooping check-giaddr

Use this command to enable DHCP Snooping to support the function of processing Relay requests. Use the **no** form of this command to restore the default setting.

**ip dhcp snooping check-giaddr**  
**no ip dhcp snooping check-giaddr**

Parameter Description	Parameter	Description
	N/A	N/A

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



**Command Mode** Global configuration mode

**Usage Guide** After the feature is enabled, services using DHCP Snooping binding entries generated based on Relay requests, such as IP Source Guard/802.1x authentication, cannot be deployed. Otherwise, users fail to access the Internet.

After the feature is enabled, the **ip dhcp snooping verify mac-address** command cannot be used. Otherwise, DHCP Relay requests will be discarded and as a result, users fail to obtain addresses.

**Configuration 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
```

**Related Commands**

Command	Description
<b>show ip dhcp snooping</b>	Displays the configuration information of the DHCP Snooping.

**Platform Description** N/A

## 10.5 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 Examples** The following example sets the interval at which the switch writes the user information into the flash to 3,600 seconds.

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping database write-delay 3600
```

**Related Commands**

Command	Description
<b>show ip dhcp snooping</b>	Displays the configuration information of the DHCP Snooping.

**Platform** N/A

**Description**

## 10.6 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.

**Configuration Examples** The following example writes the dynamic user information of the DHCP binding database into flash.

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping database write-to-flash
```

Related Commands	Command	Description
	N/A	N/A

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

## 10.7 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>	

**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 Examples** The following example adds option82 to the DHCP request message.

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping information option
```

Related Commands	Command	Description
	<b>show ip dhcp snooping</b>	

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

## 10.8 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** { string *ascii-string* | hostname }

Parameter Description	Parameter	Description
	<b>string</b> <i>ascii-string</i>	The content of the option82 remote-id extension format is customized character string.
	<b>hostname</b>	The content of the option82 remote-id extension format hostname

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

**Command Mode** Global configuration 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
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 10.9 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**

Parameter Description	Parameter	Description
	N/A	N/A

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

**Command Mode** Interface configuration mode

**Usage Guide** This command denies all DHCP request messages under the port, that is, all the users under the port are prohibited to request IP addresses through DHCP.  
This command is only supported on Layer 2 switch interfaces and aggregate ports (APs).

**Configuration Examples** The following example sets GigabitEthernet 0/1 to be in the suppression status.

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip dhcp snooping suppression
```

Related Commands	Command	Description
	<b>show ip dhcp snooping</b>	Displays the DHCP Snooping configuration.

**Platform Description** N/A

## 10.10 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** Interface configuration mode

**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
```

**Related Commands**

Command	Description
<b>show ip dhcp snooping</b>	Displays the DHCP Snooping configuration.

**Platform** N/A

**Description**

## 10.11 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	N/A

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

**Command** Global configuration mode

**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** The following example enables the check of the source MAC address of the DHCP request message.

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping verify mac-address
```

**Related  
Commands**

Command	Description
<b>show ip dhcp snooping</b>	Displays the DHCP Snooping configuration.

**Platform** N/A

**Description**

## 10.12 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  
Mode** Global configuration 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
```

**Related  
Commands**

Command	Description
<b>ip dhcp snooping</b>	Enables DHCP Snooping globally.

**Platform** N/A

**Description**

## 10.13 ip dhcp snooping vlan max-user

Use this command to set the maximum number of users bound with the VLAN.

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

**ip dhcp snooping vlan** *vlan-word* **max-user** *user-number*

**no ip dhcp snooping vlan** *vlan-word* **max-user** *user-number*

**Parameter Description**

Parameter	Description
<i>vlan-word</i>	The VLAN range
<i>user-number</i>	The maximum number of users bound with the VLAN

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

**Command Mode** Interface configuration mode

**Usage Guide** Use this command to set the maximum number of users bound with the VLAN. This function combined with the corresponding topology can prevent illegal DHCP packet attacks.

**Configuration Examples** The following example sets the maximum number of users bound with VLAN 1 to 10 and VLAN 20 to 30 respectively.

```
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
```

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 10.14 ip dhcp snooping vlan information option change-vlan-to vlan

Use this command to enable the option82 sub-option circuit-id and change the VLAN in the circuit-id into the specified VLAN.



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

**ip dhcp snooping vlan *vlan-id* information option change-vlan-to vlan *vlan-id***

**no ip dhcp snooping vlan *vlan-id* information option change-vlan-to vlan *vlan-id***

Parameter Description	Parameter	Description
	<i>vlan-id</i>	The ID of the VLAN to be replaced

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

**Command Mode** Interface configuration 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
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 10.15 ip dhcp snooping vlan information option format-type circuit-id string

Use this command to configure the option82 sub-option circuit-id as user-defined (the storage format is ASCII) and to perform the packet forwarding.

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

**ip dhcp snooping vlan *vlan-id* information option format-type circuit-id string *ascii-string***

**no ip dhcp snooping vlan *vlan-id* information option format-type circuit-id string *ascii-string***

Parameter Description	Parameter	Description
	<i>vlan-id</i>	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 Mode** Interface configuration mode

**Usage Guide** This command is used to add the option82 to the DHCP request packets. The content of the sub-option circuit-id is customized with 3 to 63 bytes, and the DHCP server will assign the addresses according 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
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 10.16 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 Description** N/A

## 10.17 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

**Usage Guide** N/A

**Configuration** The following example displays the DHCP Snooping configuration.

**Examples** Ruijie# show ip dhcp snooping  
Switch DHCP snooping status :ENABLE  
Verification of hwaddr field status :DISABLE  
DHCP snooping database write-delay time: 0 seconds  
DHCP snooping option 82 status: ENABLE

```

DHCP snooping Support Bootp bind status: ENABLE
Interface                               Trusted           Rate
limit (pps)
-----
-----
GigabitEthernet 0/4                     YES              unlimited
Default                                  No

```

**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**

## 10.18 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** 1: 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. It can be a either a wired access interface or wireless access WLAN.

**Related Commands**

Command	Description
<b>ip dhcp snooping binding</b>	Adds the static user information to the DHCP Snooping database.
<b>clear ip dhcp snooping binding</b>	Clears the dynamic user information from the DHCP Snooping binding database.

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

# 11 DHCPv6 Snooping Commands(beta)

## 11.1 clear ipv6 dhcp snooping binding

Use this command to clear all the user information in the DHCPv6 Snooping binding database.

**clear ipv6 dhcp snooping binding** [ *mac* | **vlan** *vlan-id* | *ipv6-address* | **interface** *interface-id* ]

Parameter Description	Parameter	Description
	<i>mac</i>	Specifies the MAC address to be deleted.
	<i>vlan-id</i>	Specifies the ID of the VLAN to be cleared.
	<i>ipv6-address</i>	Specifies the IPv6 address to be cleared.
	<i>interface-id</i>	Specifies the interface to be cleared.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is used to clear the generated user information in the DHCPv6 Snooping binding database.

**Configuration Examples** The following example clears all the user information in the DHCPv6 Snooping binding database.

```
Ruijie# clear ipv6 dhcp snooping binding
Ruijie# show ipv6 dhcp snooping binding
NO. MacAddress      IPv6 Address Lease(sec) VLAN Interface
FilterType FilterStatus
-----
-----
Total number of bindings: 0
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 11.2 clear ipv6 dhcp snooping prefix

Use this command to clear all the user information in the DHCPv6 Snooping prefix list.

**clear ipv6 dhcp snooping prefix** [ *mac* | **vlan** *vlan-id* | *ipv6-prefix* | **interface** *interface-id* ]

Parameter Description	Parameter	Description
	<i>mac</i>	Specifies the MAC address to be deleted.
	<i>vlan-id</i>	Specifies the ID of the VLAN to be cleared.
	<i>ipv6-address</i>	Specifies the IPv6 address to be cleared.
	<i>interface-id</i>	Specifies the interface to be cleared.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is used to clear the generated user information in the DHCPv6 Snooping prefix list.

**Configuration Examples** The following example clears all the user information in the DHCPv6 Snooping binding database

```
Ruijie# clear ipv6 dhcp snooping prefix
Ruijie# show ipv6 dhcp snooping prefix
NO.  MacAddress      IPv6 Prefix  Lease(sec)  VLAN  Interface
FilterType  FilterStatus
-----
-----
Total number of prefixes: 0
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 11.3 clear ipv6 dhcp snooping statistics

Use this command to clear the statistical information of the DHCPv6 packets.

**clear ipv6 dhcp snooping statistics**

Parameter Description	Parameter	Description
		N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is used to clear the statistical information of the DHCPv6 packets.

**Configuration** The following example clears the statistical information of the DHCPv6 packets.

**Examples**

```
Ruijie# clear ipv6 dhcp snooping statistics
Ruijie# show ipv6 dhcp snooping statistics
Packets Processed by DHCPv6 Snooping = 0
Packets Dropped Because
Received on untrusted ports      = 0
Relay forward                    = 0
No binding entry                 = 0
Binding fail                     = 0
Unknown packet                   = 0
Unknown output interface        = 0
No enough memory                 = 0
Admin filter-dhcpv6-pkt         = 0
```

Related Commands	Command	Description
		N/A

**Platform** N/A

**Description**

## 11.4 ipv6 dhcp snooping

Use this command to enable the DHCPv6 Snooping function globally.

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

**ipv6 dhcp snooping**

**no ipv6 dhcp snooping**

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



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

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

**Command Mode** Global configuration mode

**Usage Guide** The **show ip dhcpv6 snooping** command is used to display whether the DHCPv6 Snooping function is enabled.

**Configuration** The following example enables the DHCPv6 Snooping function globally.

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# ipv6 dhcp snooping
```

<b>Related Commands</b>	Command	Description
	<b>show ipv6 dhcp snooping</b>	Displays the DHCPv6 Snooping .

**Platform Description** N/A

## 11.5 ipv6 dhcp snooping binding-delay

Use this command to add the dynamic binding entry to the hardware filtering list after the delay.

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

**ipv6 dhcp snooping binding-delay** *seconds*

**no ipv6 dhcp snooping binding-delay**

<b>Parameter Description</b>	Parameter	Description
	<i>seconds</i>	Sets the binding delay time.

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

**Command Mode** Global configuration mode

**Usage Guide** By default, the dynamic binding entries are added to the hardware filtering list in real time. With this command configured, if no IPv6 address conflict is detected within the specified time, the dynamic

binding entries are added to the hardware filtering list.

**Configuration** The following example sets the delay to 10 seconds.

**Examples**

```
Ruijie(config)# ipv6 dhcp snooping binding-delay 10
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 11.6 ipv6 dhcp snooping database write-delay

Use this command to write the dynamic user information of the DHCPv6 Snooping binding database into the flash periodically.

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

**ipv6 dhcp snooping database write-delay *time***

**no ipv6 dhcp snooping database write-delay**


**Parameter  
Description**

Parameter	Description
<i>time</i>	The interval ranging from 600 to 86,400 in the unit of seconds, at which the system writes the dynamic user information of the DHCP Snooping database into the flash.

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

**Command  
Mode** Global configuration mode

**Usage Guide** This function writes user information into flash and can avoid loss after restart. In that case, users need to obtain IP addresses again for normal communication.

 Too fast writing will reduce flash durability.

**Configuration  
Examples** The following example sets the interval at which the switch writes the user information into the flash to 3,600 seconds.

```
Ruijie# configure terminal
Ruijie(config)# ipv6 dhcp snooping database write-delay 3600
```

Related Commands	Command	Description
		<code>show ipv6 dhcp snooping</code>

Platform N/A

Description

## 11.7 ipv6 dhcp snooping database write-to-flash

Use this command to write the dynamic user information of the DHCPv6 binding database into flash in real time.

**ipv6 dhcp snooping database write-to-flash**

Parameter Description	Parameter	Description
		N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide Use this command to write the dynamic user information of the DHCPv6 binding database into flash in real time.

Configuration Examples The following example writes the dynamic user information of the DHCPv6 binding database into flash.

```
Ruijie# configure terminal
Ruijie(config)# ipv6 dhcp snooping database write-to-flash
```

Related Commands	Command	Description
		N/A

Platform N/A

Description

## 11.8 ipv6 dhcp snooping filter-dhcp-pkt

Use this command to filter all received DHCPv6 request packets.

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

**ipv6 dhcp snooping filter-dhcp-pkt**

**no ipv6 dhcp snooping filter-dhcp-pkt**

**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 filter all received DHCPv6 request packets, that is, to avoid all the DHCPv6 users on this interface to apply for the addresses.

This command is valid only on 2-layer wired switch ports, aggregate ports and sub interfaces as well as in air interfaces.

**Configuration  
Examples**

The following example filters all DHCPv6 request packets on interface GigabitEthernet 0/1 and WLAN 1.

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 dhcp snooping filter-dhcp-pkt
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform  
Description**

N/A

## 11.9 ipv6 dhcp snooping information option

Use this command to add option18/37 to the DHCPv6 request packets.

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

**ipv6 dhcp snooping information option [ standard-format ]**

**no ipv6 dhcp snooping information option [ standard-format ]**

**Parameter  
Description**


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

<b>standard-format</b>	The Option18/37 uses the standard format.
------------------------	---

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

**Command Mode** Global configuration mode

**Usage Guide** With this command configured, the option18/37 will be added to the DHCPv6 request packets and the DHCPv6 server will assign the addresses according to the option18/37 information. Use this command without parameter **standard-format** to enable the standard format.

 DHCPv6 Relay function adds option18/37 by default. Therefore, it is unnecessary to enable functions of DHCP Snooping option18/37 and DHCPv6 Relay at the same time.

**Configuration** The following example adds the option18/37 into the DHCPv6 packets.

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# ipv6 dhcp snooping information option
Ruijie(config)# end
Ruijie# show ipv6 dhcp snooping
Switch DHCPv6 snooping status :ENABLE
DHCPv6 snooping vlan: 1-4094
DHCPv6 snooping database write-delay time: 0 seconds
DHCPv6 snooping option 18/37 status: ENABLE
DHCPv6 snooping link detection :DISABLE
Interface           Trusted   Filter DHCP
-----
GigabitEthernet0/1    yes      DISABLE
```

**Related Commands**

Command	Description
<b>show ipv6 dhcp snooping</b>	Displays the configuration information of the DHCPv6 Snooping.

**Platform** N/A

**Description**

## 11.10 ipv6 dhcp snooping information option format remote-id

Use this command to add option37 remote-id customized character string into the DHCPv6 request packets.

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

**ipv6 dhcp snooping information option format remote-id [ string *ascii-string* | hostname ]**  
**no ipv6 dhcp snooping information option format remote-id [ string *ascii-string* | hostname ]**

**Parameter  
Description**

Parameter	Description
<b>string</b> <i>ascii-string</i>	The content of Option37 remote-id extension format is customized character string.
<b>hostname</b>	The content of Option37 remote-id extension format is hostname.

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

**Command  
Mode** Global configuration mode

**Usage Guide** With this command configured, the option37 remote-id will be added to the DHCPv6 request packets with the content as the customized and the DHCPv6 server will assign the addresses according to the option37 information.

**Configuration  
Examples** The following example adds the option37 remote-id to the DHCPv6 request packets with the content being hostname.

```
Ruijie# configure terminal
Ruijie(config)# ipv6 dhcp snooping information option format remote-id
hostname
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform  
Description** N/A

## 11.11 ipv6 dhcp snooping link-detection

Use this command to clear the dynamic binding entry on an interface when the interface links down.  
 Use the **no** form of this command to restore the default setting.

**ipv6 dhcp snooping link-detection**  
**no ipv6 dhcp snooping link-detection**

**Parameter  
Description**

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

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

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

**Command Mode** Global configuration mode

**Usage Guide** By default, the dynamic binding entries are not cleared on a wired interface when the interface links down. With this function enabled, the dynamic binding entries are auto-cleared on an interface when the interface is in the LINK DOWN status.

**Configuration Examples** The following example clears the dynamic binding entry on a wired interface when the interface is in the LINK DOWN status.

```
Ruijie# configure terminal
Ruijie(config)# ipv6 dhcp snooping link-detection
```

**Related Commands**

Command	Description
<b>show ipv6 dhcp snooping</b>	Displays the configuration information of the DHCPv6 Snooping.

**Platform**

**Description** N/A

## 11.12 ipv6 dhcp snooping trust

Use this command to set the specified DHCPv6 Snooping ports as the trusted ports.

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

**ipv6 dhcp snooping trust**

**no ipv6 dhcp snooping trust**

**Parameter Description**

Parameter	Description
N/A	N/A

**Defaults** All ports are untrusted ports by default.

**Command Mode** Interface configuration mode

- Usage Guide**
1. Use this command to set a port as a trusted port. The DHCPv6 Server response messages received under the trust port are forwarded normally, but the response messages received under the untrusted port will be discarded.
  2. This command is valid only on Layer 2 wired switch ports and aggregate ports.

**Configuration** The following example sets GigabitEthernet 0/1 as a trust port:

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 dhcp snooping trust
```

**Related Commands**

Command	Description
<b>show ipv6 dhcp snooping</b>	Displays the DHCPv6 Snooping configuration.

**Platform** N/A

**Description**

## 11.13 ipv6 dhcp snooping vlan

Use this command to enable DHCPv6 Snooping for the specific VLAN.

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

**ipv6 dhcp snooping vlan** { *vlan-rng* | { *vlan-min* [ *vlan-max* ] } }

**no ipv6 dhcp snooping vlan** { *vlan-rn* | { *vlan-min* [ *vlan-max* ] } }

**Parameter Description**

Parameter	Description
<i>vlan-rng</i>	Sets the valid VLAN range.
<i>vlan-min</i>	Minimum VLAN ID
<i>vlan-max</i>	Maximum VLAN ID

**Defaults** By default, once the DHCPv6 Snooping is enabled globally, it takes effect for all VLANs.

**Command** Global configuration mode

**Mode**

**Usage Guide** With the global DHCPv6 snooping enabled, this function is enabled in all VLANs by default.

**Configuration** The following example enables the DHCPv6 Snooping function in VLAN 1000.

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# ipv6 dhcp snooping vlan 1000
```



The following example enables the DHCPv6 Snooping function in VLAN 1 to VLAN 10.

```
Ruijie# configure terminal
Ruijie(config)# ipv6 dhcp snooping vlan 1-10
```

#### Related Commands

Command	Description
N/A	N/A

#### Platform

N/A

#### Description

## 11.14 ipv6 dhcp snooping vlan information option change-vlan-to vlan

Use this command to enable the function of adding the option18 interface-id into the DHCP request packets and change the VLAN to the specified VLAN for the forwarding.

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

**ipv6 dhcp snooping vlan** *vlan-id* **information option change-vlan-to vlan** *vlan-id*

**no ipv6 dhcp snooping vlan** *vlan-id* **information option change-vlan-to vlan** *vlan-id*

#### Parameter Description

Parameter	Description
<i>vlan-id</i>	Specifies the ID of the VLAN to be replaced.

#### Defaults

This function is disabled by default.

#### Command Mode

Interface configuration mode

#### Usage Guide

With this command enabled, the option18 interface-id will be added into the DHCPv6 request packets and the VLAN will be changed to the specified one and the DHCP server will assign the addresses according to the optionq8 information.

#### Configuration Examples

The following example adds the option18 interface-id into the DHCPv6 request packets and changes the VLAN4094 in the option to VLAN 4093.

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 dhcp snooping vlan 4094
information option change-vlan-to vlan 4093
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

## 11.15 ipv6 dhcp snooping vlan information option format-type interface-id string

Use this command to enable the function of adding the option18 into the DHCP request packets and filling the option18 interface-id with the content being the user-defined (the storage format is ASCII) and performing the packet forwarding.

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

**ipv6 dhcp snooping vlan *vlan-id* information option format-type interface-id string *ascii-string***  
**no ipv6 dhcp snooping vlan *vlan-id* information option format-type interface-id string *ascii-string***

Parameter Description	Parameter	Description
	<i>vlan-id</i>	The VLAN where the DHCPv6 request packets are
	<i>ascii-string</i>	User-defined content for filling the interface-id

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

**Command Mode** Interface configuration mode

**Usage Guide** With this command configured, the option18 interface-id will be added into the DHCPv6 request packets with the content being user-defined and the DHCPv6 server will assign the addresses according to the option18 information.

**Configuration Examples** The following example adds the option18 interface-id to the DHCPv6 request packets with the content being *port-name*.

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 dhcp snooping vlan 4094
information option format-type interface-id string port-name
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A  
Description

## 11.16 renew ipv6 dhcp snooping database

Use this command to import the information in current flash to the DHCPv6 Snooping binding database manually as needed.


**renew ipv6 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 DHCPv6 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 DHCPv6 Snooping database.

Examples 

```
Ruijie# renew ipv6 dhcp snooping database
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A  
Description

## 11.17 show ipv6 dhcp snooping

Use this command to display the setting of the DHCPv6 Snooping.

**show ipv6 dhcp snooping**

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 setting of the DHCPv6 Snooping.

**Examples**

```
Ruijie# show ipv6 dhcp snooping
Switch DHCPv6 snooping status :ENABLE
DHCPv6 snooping vlan: 1-4094
DHCPv6 snooping database write-delay time: 0 seconds
DHCPv6 snooping option 18/37 status: DISABLE
DHCPv6 snooping link detection :DISABLE
Interface           Trusted   Filter DHCP
-----
GigabitEthernet0/1     yes     DISABLE
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** N/A

## 11.18 show ipv6 dhcp snooping binding

Use this command to display the information of the DHCPv6 Snooping binding database.

**show ipv6 dhcp snooping binding** [ *mac* ] [ *vlan* *vlan-id* ] [ *ipv6-address* ] [ **interface** *interface-id* ]

Parameter Description	Parameter	Description
	<i>ipv6-address</i>	Displays the IPv6 address binding entry.
	<i>mac-address</i>	Displays the MAC address binding entry.

<i>vlan</i> <i>vlan_id</i>	Displays the VLAN binding entry.
<b>interface</b> <i>interface_name</i>	Displays the interface binding entry.

**Defaults** N/A

**Command** Privileged EXEC mode

**Mode**

**Usage Guide** N/A

**Configuration** The following example displays the information of the DHCP Snooping binding database.

**Examples**

```
Ruijie# show ipv6 dhcp snooping binding
Total number of bindings: 1
NO.   MacAddress          IPv6 Address          Lease (sec)
VLAN  Interface
-----
1     00d0.f801.0101        2001::10              42368      2
GigabitEthernet 0/1
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 11.19 show ipv6 dhcp snooping prefix

Use this command to display all user information in the DHCPv6 Snooping prefix list.

**show ipv6 dhcp snooping prefix** [ *mac* | **vlan** *vlan-id* | *ipv6-prefix* | **interface** *interface-id* ]

**Parameter  
Description**

Parameter	Description
<i>ipv6-prefix</i>	Displays the IPv6 address prefix entry.
<i>mac-address</i>	Displays the MAC address prefix entry.
<b>vlan</b> <i>vlan_id</i>	Displays the VLAN prefix entry.
<b>interface</b> <i>interface_name</i>	Displays the interface prefix entry.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays all user information in the DHCPv6 Snooping prefix list.

**Examples**

```
Ruijie# show ipv6 dhcp snooping prefix
Total number of prefix: 1

NO.   MacAddress          IPv6 Prefix                Lease(sec)
VLAN  Interface
-----
-----
1     00d0.f801.0101      2001:2002::/64            42368
2     GigabitEthernet 0/1
```

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 11.20 show ipv6 dhcp snooping statistics

Use this command to display the statistical information of the DHCPv6 packets.

**show ipv6 dhcp snooping statistics**

**Parameter Description**

Parameter	Description
N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the statistical information of the DHCPv6 packets.

**Examples**

```
Ruijie# show ipv6 dhcp snooping statistics
Packets Processed by DHCPv6 Snooping = 0
Packets Dropped Because
Received on untrusted ports      = 0
Relay forward                    = 0
No binding entry                 = 0
Binding fail                     = 0
Unknown packet                   = 0
Unknown output interface         = 0
No enough memory                 = 0
Admin filter-dhcpv6-pkt         = 0
```

Field	Description
Received on untrusted ports	The discarded server response packets on the untrust port.
Relay forward	The packets that have been relayed once are discarded.
No binding entry	The binding entries of the release/decline packets are in-existent or error and the packets are discarded.
Binding fail	The entry binding fails and the packets are discarded due to a lack of the hardware resources.
Unknown packet	The unknown DHCP packets.
Unknown output interface	The packets on the unknown output interface. The MAC address for the interface is not found or the trust port is not configured.
No enough memory	There is no enough memory.
Admin filter-dhcpv6-pkt	The filtered DHCPv6 packets configured by the administrator. Use the <b>ipv6 dhcp snooping filter-dhcp-pkt</b> command to filter the packets.

**Related Commands**

Command	Description
N/A	N/A

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

## 11.21 show ipv6 dhcp snooping vlan

Use this command to display the VLAN with DHCPv6 Snooping function disabled.

**show ipv6 dhcp snooping vlan**

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 VLAN with DHCPv6 Snooping function disabled.

**Configuration Examples** The following example displays the VLAN with DHCPv6 Snooping function disabled.

```
Ruijie# show ipv6 dhcp snooping vlan
VLAN Name      Closed
-----
2    VLAN 2      YES
```

Field	Description
VLAN	VLAN ID
NAME	VLAN name
Close	Indicates whether DHCPv6 Snooping is disabled.

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A



## 12 ARP-Check Commands(beta)

### 12.1 arp-check

Use this command to enable the ARP check function on the Layer 2 interface.

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

**arp-check**

**no arp-check**

Parameter Description	Parameter	Description
	N/A	N/A

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

**Command mode** Interface configuration mode

**Usage Guide** The ARP check function generates the ARP filtering information according to legal user information, implementing the illegal ARP packet filtering on the network.

**Configuration Examples** This following example enables the APR check function on interface GigabitEthernet 0/1.

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# arp-check
Ruijie(config-if-GigabitEthernet 0/1)# end
```

Related Commands	Command	Description
	<b>show interfaces arp-check list</b>	Displays the ARP check entries.

**Platform Description** N/A

### 12.2 show interfaces arp-check list

Use this command to display the ARP check entries on the Layer 2 interface.

**show interfaces** [ *interface-type interface-number* ] **arp-check list**

Parameter Description	Parameter	Description
	<i>interface-type</i>	Wired interface type
	<i>interface-number</i>	Wired interface number

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** Use this command to display the ARP check entries.

**Configuration Examples** The following example displays the ARP check entries.

```
Ruijie# show interfaces arp-check list
INTERFACE                SENDER MAC      SENDER IP      POLICY SOURCE
-----
GigabitEthernet 0/1     00D0.F800.0003  192.168.1.3    address-bind
GigabitEthernet 0/1     00D0.F800.0001  192.168.1.1    port-security
GigabitEthernet 0/4                192.168.1.3    port-security
GigabitEthernet 0/5     00D0.F800.0003  192.168.1.3    address-bind
GigabitEthernet 0/7     00D0.F800.0006  192.168.1.6    AAA ip-auth-mode
GigabitEthernet 0/8     00D0.F800.0007  192.168.1.7    GSN
```

Field	Description
INTERFACE	Interface name
SENDER MAC	Source MAC address
SENDER IP	Source IP address
POLICY SOURCE	Source of the entry

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 13 DAI Commands(beta)

### 13.1 ip arp inspection trust

Use this command to configure the L2 port to a trusted port.

Use the **no** form of this command to restore the L2 port to an untrusted port.

**ip arp inspection trust**

**no ip arp inspection trust**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** The L2 port is untrusted.

**Command Mode** Interface configuration mode

**Usage Guide** If it is necessary to make the ARP message received by some interface pass the DAI inspection unconditionally, you can set the interface to a trusted port, indicating that you do not need to check whether the ARP message received by this interface is legal.

**Configuration Examples** The following example sets the GigabitEthernet 0/19 interface as the trusted port.

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitethernet 0/19
Ruijie(config-if-GigabitEthernet 0/19)# ip arp inspection trust
Ruijie(config-if-GigabitEthernet 0/19)# end
```

Related Commands	Command	Description
	<b>show ip arp inspection interface</b>	Displays related DAI information on the interface, including the trust state and rate limit of the interface.

**Platform Description** N/A

## 13.2 ip arp inspection vlan

Use this command to configure the DAI function on the VLAN.

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

**ip arp inspection vlan** { *vlan-id* | *word* }


**no ip arp inspection vlan** { *vlan-id* | *word* }

Parameter Description	Parameter	Description
	<i>vlan-id</i>	VLAN ID, ranging from 1 to 4094
	<i>word</i>	String of the VLAN range, such as 1,3-5,7,9-11

**Defaults** The DAI function on all VLANs is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** To make this command take effect, you need to enable the ARP Check function first,

 Not all ports of the VLAN support the ARP packet detection function. For example, the DHCP Snooping Trust port does not support any security detection, including this function.

**Configuration Examples** The following example detects the received ARP packets on the VLAN1 interfaces:

```
Ruijie# configure terminal
Ruijie(config)# ip arp inspection vlan 1
Ruijie(config)# end
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 13.3 show ip arp inspection interface

Use this command to verify whether the interface is a DAI trust interface.

**show ip arp inspection interface**

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

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

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command to verify whether the interface is a DAI trust interface.

**Configuration** The following example verifies the DAI trust state of all :

**Examples**

```
Ruijie# show ip arp inspection interface
Interface      Trust State
-----
GigabitEthernet 0/1    Untrusted
Default                Untrusted
```

Parameter Description:

Parameter	Description
Interface	Interface name.
Trust State	DAI trust state.

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

**Platform Description** N/A

## 13.4 show ip arp inspection vlan

Use this command to verify whether the DAI function on the VLAN is enabled.

**show ip arp inspection vlan** [ *vlan-id* | *word* ]

<b>Parameter Description</b>	Parameter	Description
	<i>vlan-id</i>	VLAN ID, ranging from 1 to 4094
	<i>word</i>	String of the VLAN range, such as 1,3-5,7,9-11

**Defaults** N/A

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

**Usage Guide** Use this command to verify whether the DAI function on the VLAN is enabled.

**Configuration** The following example verifies whether the DAI function on the VLAN is enabled:

**Examples**

```
Ruijie# show ip arp inspection vlan
Vlan      Configuration
-----  -
1                               Active
```

Parameter Description:

Parameter	Description
Vlan	VLAN number.
Configuration	DAI status (active / inactive)

**Related  
Commands**

Command	Description
N/A	N/A

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

## 14 IP Source Guard Commands(beta)

### 14.1 ip source binding

Use this command to add static user information to IP source address binding database.

Use the **no** form of this command to delete static user information from IP source address binding database.

**ip source binding** *mac-address* **vlan** *vlan-id* *ip-address* { **interface** *interface-id* | **ip-mac** | **ip-only** }

**no ip source binding** *mac-address* **vlan** *vlan-id* *ip-address* { **interface** *interface-id* | **ip-mac** | **ip-only** }


#### Parameter Description


Parameter	Description
<i>mac-address</i>	Adds user MAC address statically.
<i>vlan-id</i>	Adds user VLAN ID statically.
<i>ip-address</i>	Adds user IP address statically.
<i>interface-id</i>	Adds user interface ID statically.
<b>ip-mac</b>	The global binding type is IP+MAC
<b>ip-only</b>	The global binding type is IP only.

**Defaults** No static address is added by default.

**Command Mode** Global configuration mode

**Usage Guide** This command allows specific clients to go through IP source guard detection instead of DHCP. This command is supported on the wired L2 switching port, AP port and sub interface. This command enables global binding for IP source guard so that specific clients will get detected on all interfaces.

 A static IPv6 source binding is valid either on wired and WLAN interfaces or in global configuration mode.

 A new binding will overwrite the old one sharing the same configuration.

**Configuration Examples** The following example adds the interface Id of static users.

```
Ruijie# configure terminal
Ruijie(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 interface
gigabitethernet 0/1
Ruijie(config)# end
```

The following example adds static user information based on IP-MAC binding.

```
Ruijie# configure terminal
Ruijie(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 ip-mac
Ruijie(config)# end
```

The following example adds static user information based on IP binding.

```
Ruijie# configure terminal
Ruijie(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 ip-only
Ruijie(config)# end
```

#### Related Commands

Command	Description
<b>show ip source binding</b>	Displays the binding information of IP source address and database.

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

## 14.2 ip verify source

Use this command to enable IP Source Guard function on the interface.

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

**ip verify source [ port-security ]**

**no ip verify source**

#### Parameter Description

Parameter	Description
<b>port-security</b>	Configures IP Source Guard to do IP+MAC-based detection.

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

**Command Mode** Interface configuration mode

**Usage Guide** This command enables IP Source Guard function on the interface to do IP-based or IP+MAC-based detection.

This command is supported on the wired L2 switching port, AP port and sub interface.

IP Source Guard takes effect only on DHCP Snooping untrusted port. In other words, IP Source Guard does not take effect when configuring it on Trust port or the port which is not controlled by



DHCP Snooping.

**Configuration Examples** The following example enables IP-based IP Source Guard function.

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip verify source
Ruijie(config-if)# end
```

The following example enables IP+MAC-based IP Source Guard function.

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitethernet 0/2
Ruijie(config-if-GigabitEthernet 0/2)# ip verify source port-security
Ruijie(config-if)# end
```

**Related Commands**

Command	Description
<b>show ip verify source</b>	Displays user filtering entry of IP Source Guard.

**Platform** N/A

**Description**

### 14.3 ip verify source exclude-vlan

Use this command to exclude a VLAN from the IP source guard configuration on the port.

Use the **no** form of this command to restore the function.

**ip verify source exclude-vlan** *vlan-id*

**no ip verify source exclude-vlan** *vlan-id*

**Parameter Description**

Parameter	Description
<i>vlan-id</i>	The ID of VLAN excluded from the IP source guard configuration.


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

**Command Mode** Interface configuration mode

**Usage Guide**

- This command is used to exclude a VLAN from the IP source guard configuration. IP packets in this VLAN are forwarded without being checked and filtered.
- Once the IP source guard function is disabled, the excluded VLAN is cleared automatically.

- This command is supported on the wired L2 switching port, AP port and sub interface.

 Only when the IP source guard configuration is enabled on the port can a VLAN be excluded.

**Configuration Examples** The following example configuration configures the IP source guard configuration for the port and excludes a VLAN.

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip verify source
Ruijie(config-if-GigabitEthernet 0/1)# ip verify source exclude-vlan 1
Ruijie(config-if)# end
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** N/A

## 14.4 show ip source binding

Use this command to display the binding information of IP source addresses and database.

**show ip source binding** [ *ip-address* ] [ *mac-address* ] [ **vlan** *vlan-id* ] [ **interface** *interface-id* ] [ **dhcp-snooping** | **static** ]

**Parameter Description**

Parameter	Description
<i>ip-address</i>	Displays user binding information of corresponding IP.
<i>mac-address</i>	Displays user binding information of corresponding MAC.
<i>vlan-id</i>	Displays user binding information of corresponding VLAN.
<i>interface-id</i>	Displays user binding information of corresponding interface.
<b>dhcp-snooping</b>	Displays binding information of dynamic user.
<b>static</b>	Displays binding information of static user.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration**

The following example displays the binding information of IP source guard addresses and database.

**Examples**

```
Ruijie# show ip source binding static
Total number of bindings: 5
NO.    MACADDRESS          IPADDRESS    LEASE(SEC)  TYPE        VLAN  INTERFACE
-----
1      0001.0002.0001     1.2.3.2     Infinite    Static      1     Global
2      0001.0002.0002     1.2.3.3     Infinite    Static      1     GigabitEthernet
0/5
3      0001.0002.0003     1.2.3.4     Infinite    Static      1     Global
4      0001.0002.0004     1.2.3.5     Infinite    Static      1     Global
```

**Related  
Commands**

Command	Description
<b>ip source binding</b>	Sets the binding static user.

**Platform**

N/A

**Description**

## 14.5 show ip verify source

Use this command to display user filtering entry of IP Source Guard.

**show ip verify source** [ **interface** *interface-id* ]

**Parameter  
Description**

Parameter	Description
<i>interface-id</i>	Displays user filtering entry of corresponding interface.

**Defaults**

N/A

**Command**

Privileged EXEC mode

**Mode****Usage Guide**

If IP Source Guard is not enabled on the corresponding interface, the printing information will be shown on the terminal as: "IP source guard is not configured on the interface GigabitEthernet 0/10"

Now, IP Source Guard supports the following filtering modes:

**inactive-restrict-off**: the IP Source Guard is disabled on bound interfaces.

**inactive--not-apply**: the IP Source Guard cannot adds bound entries into filtering entries for system errors.

**active**: the IP Source Guard is active.

**Configuration** The following example displays user filtering entry of IP Source Guard.

**Examples**

```
Ruijie# show ip verify source
Total number of bindings: 7
NO.   INTERFACE          FILTERTYPE  FILTERSTATUS      IPADDRESS
MACADDRESS  VLAN  TYPE
-----
-----
1     Global              IP+MAC     Inactive-not-apply 192.168.0.127
0001.0002.0003 1 Static
2     GigabitEthernet 0/5  IP-ONLY     Active             1.2.3.4
0001.0002.0004 1 DHCP-Snooping
3     Global              IP-ONLY     Active             1.2.3.7
0001.0002.0007 1 Static
4     Global              IP+MAC     Active             1.2.3.6
0001.0002.0006 1 Static
5     GigabitEthernet 0/1  UNSET       Inactive-restrict-off 1.2.3.9
0001.0002.0009 1 DHCP-Snooping
6     GigabitEthernet 0/5  IP-ONLY     Active             Deny-All
```

**Related Commands**

Command	Description
<b>ip verify source</b>	Sets IP Source Guard on the interface.

**Platform** N/A

**Description**

## 15 DoS Protection Commands

### 15.1 ip deny invalid-l4port

Use this command to enable the anti-attack of the self-consumption.

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

**ip deny invalid-l4port**

**no ip deny invalid-l4port**

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 enables the anti-attack of the self-consumption.

```
Ruijie(config)# ip deny invalid-l4port
```

The following example disables the anti-attack of the self-consumption.

```
Ruijie(config)# no ip deny invalid-l4port
```

Related Commands	Command	Description
	<b>show ip deny invalid-l4port</b>	Displays the state of anti-attack of the self-consumption.

**Platform** N/A

**Description**

### 15.2 ip deny invalid-tcp

Use this command to enable the anti-attack of the invalid TCP packets.

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

**ip deny invalid-tcp**

**no ip deny invalid-tcp****Parameter  
Description**

Parameter	Description
N/A	N/A

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

**Command  
Mode** Global configuration mode

**Usage Guide** N/A

**Configuration** The following example enables the anti-attack of the invalid TCP packets:

**Examples** Ruijie(config)# ip deny invalid-tcp

The following example disables the anti-attack of the invalid TCP packets:

Ruijie(config)# no ip deny invalid-tcp

**Related  
Commands**

Command	Description
<b>show ip deny invalid-tcp</b>	Displays the state of anti-attack of the invalid TCP packets.

**Platform** N/A

**Description**

## 15.3 ip deny land

Use this command to enable the anti-land-attack.

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

**ip deny land**

**no ip deny land**

**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 the anti-land-attack:

**Examples** Ruijie(config)# ip deny land

The following example disables the anti-land-attack:

Ruijie(config)# no ip deny land

**Related Commands**

Command	Description
show ip deny land	Displays the anti-land-attack state.

**Platform** N/A

**Description**

## 15.4 show ip deny

Use this command to display the state of the anti-DOS-attack.

**show ip deny**

**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 state of the anti-DOS-attack.

**Examples** Ruijie# show ip deny

```
Protect against Land attack          On
Protect against invalid L4port attack Off
Protect against invalid TCP attack   Off
```

**Related**

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

<b>Commands</b>		
	N/A	N/A

**Platform** N/A

**Description**

## 15.5 show ip deny invalid-l4port

Use this command to display the state of the anti-consumption-attack.

**show ip deny invalid-l4port**

<b>Parameter Description</b>	<b>Parameter</b>	<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 state of the anti-consumption-attack.

**Examples**

```
Ruijie# show ip deny invalid-l4port
  DoS Protection Mode           State
-----
protect against invalid l4port attack Off
```

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

**Platform** N/A

**Description**

## 15.6 show ip deny invalid-tcp

Use this command to display the state of the anti-attack of the invalid TCP packets.

**show ip deny invalid-tcp**



Parameter Description	Parameter	Description
		N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the state of the anti-attack of the invalid TCP packets.

**Examples**

```
Ruijie# show ip deny invalid-tcp
DoS Protection Mode                               State
-----
protect against invalid tcp attack                On
```

Related Commands	Command	Description
		<b>ip deny invalid-tcp</b>

**Platform** N/A

**Description**

## 15.7 show ip deny land

Use this command to display the anti-land-attack state.

**show ip deny land**

Parameter Description	Parameter	Description
		N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the anti-land-attack state.

**Examples**

```
Ruijie# show ip deny land
DoS Protection Mode          State
-----
protect against land attack  On
```

**Related  
Commands**

Command	Description
<b>no ip deny land</b>	Enables the anti-land-attack function.

**Platform** N/A

**Description**

## 16 PPPoE Intermediate Agent Commands(beta)

### 16.1 pppoe intermediate-agent

Use this command to enable PPPoE IA globally.

The the **no** form of this command to restore the default settings.

**pppoe intermediate-agent**

**no pppoe intermediate-agent**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** By default, this function is disabled.

**Command Mode** Global configuration mode and Interface configuration mode

**Usage Guide** If you want to run pppoe intermediate-agent on the ports of a switch, you must enable it globally first, otherwise it is invalid to enable this function on ports.

**Configuration Examples** The following example enables PPPoE IA.

```
Ruijie# configure terminal
Ruijie(config)# pppoe intermediate-agent
Ruijie(config)# end
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

### 16.2 pppoe intermediate-agent trust

Use this command to configure the trusted ports for PPPoE IA.

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

**pppoe intermediate-agent trust**

**no pppoe intermediate-agent trust****Parameter  
Description**

Parameter	Description
N/A	N/A

**Defaults** By default, all ports are untrusted ports.

**Command  
Mode** Interface configuration mode

**Usage Guide** At least one port should be configured as a trusted port that can be connected to a server to copy and forward the PPPoE packets of clients.

**Configuration** The following example configures a GigabitEthernet 0/1 as a trusted port.

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# pppoe intermediate-agent trust
Ruijie(config-if-GigabitEthernet 0/1)# end
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform  
Description** N/A

## 16.3 pppoe intermediate-agent type tr-101 circuit-id access-node-id

Use this command to add the value of the access node id of circuit ID in vendor tag.

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

**pppoe intermediate-agent type tr-101 circuit-id access-node-id** *string*

**no pppoe intermediate-agent type tr-101 circuit-id access-node-id**

**Parameter  
Description**

Parameter	Description
<i>string</i>	The value of the access node id of circuit ID in vendor tag.

**Defaults** By default, it function is disabled.

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

**Usage Guide** Add the value of the access node id of circuit ID in vendor tag.

**Configuration** The following example adds the access node id to PPPoE packets.

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# pppoe intermediate-agent typ tr-101 circuit-id access-node-id
abcd
Ruijie(config)# end
```

Related Commands	Command	Description

**Platform** N/A

**Description**

## 16.4 pppoe intermediate-agent type tr-101 circuit-id identifier-string

Use this command to add the circuit-id of a vendor tag.

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

**pppoe intermediate-agent type tr-101 circuit-id identifier-string** *string* option { **pv** | **sp** | **spv** | **sv** }  
**delimiter** *string*

**no pppoe intermediate-agent type tr-101 circuit-id identifier-string option delimiter**

Parameter Description	Parameter	Description
	<i>string</i>	Custom identifier
	<b>delimiter</b>	Separators between fields

**Defaults** By default, this function is disabled.

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

**Usage Guide** Add the circuit-id of the vendor tag.

**Configuration** The following example adds the circuit-id to PPPoE packets.

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# pppoe intermediate-agent type tr-101 circuit-id
```

```
identifier-string aaa option pv delimiter b
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 16.5 pppoe intermediate-agent type self-defined circuit-id

Use this command to configure a customized circuit-id.

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

```
pppoe intermediate-agent type self-defined circuit-id { id { remote-mac | switch-id { hostname | mac } } | port | string word | vlan }
```

```
no pppoe intermediate-agent type self-defined circuit-id
```

Parameter Description	Parameter	Description
	<b>vlan</b>	
<b>port</b>		The port used to receive PPPoE packets.
<b>id</b>		The MAC address and name of an access device.

**Defaults** By default, this function is disabled.

**Command Mode** Global configuration mode

**Usage Guide** Configure custom circuit-id.

**Configuration Examples** The following example adds the circuit-id to the PPPoE request packets.

```
Ruijie# configure terminal
Ruijie(config)# pppoe intermediate-agent type self-defined circuit-id string abcd
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

## Description

## 16.6 pppoe intermediate-agent type self-defined remoteid

Use this command to configure customized remote-id.

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

```
pppoe intermediate-agent type self-defined remoteid { hostname | mac | string word |
vlan-mac }
no pppoe intermediate-agent type self-defined remote-id
```

**Parameter  
Description**

Parameter	Description
<b>hostname</b>	Adds the hostname as the circuit-id to PPPoE request packets.
<b>mac</b>	Adds the mac as the circuit-id to PPPoE request packets
<b>vlan-mac</b>	Adds the vlan and mac as the circuit-id to PPPoE request packets

**Defaults** By default, this function is disabled.

**Command  
Mode** Global configuration mode

**Usage Guide** Configure a customized remote-id.

**Configuration** The following example adds the customized circuit-id to PPPoE request packets.

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# pppoe intermediate-agent type self-defined remoteid string
aaaa
Ruijie(config)# end
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform  
Description** N/A

## 16.7 pppoe intermediate-agent delimiter

Use this command to configure the separators between the fields of a circuit-id and a remote-id.

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

**pppoe intermediate-agent delimiter** *word*  
**no pppoe intermediate-agent delimiter**

**Parameter  
Description**

Parameter	Description
<i>word</i>	The separators between the fields of a circuit-id and a remote-id.

**Defaults** By default, this function is disabled.

**Command  
Mode** Global configuration mode

**Usage Guide** Configure the separators between the fields of a circuit-id and a remote-id.

**Configuration** Configure the separators between the fields of a circuit-id and a remote-id as '#'.

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# pppoe intermediate-agent delimiter #
Ruijie(config)# end
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform  
Description** N/A

## 16.8 pppoe intermediate-agent vendor-tag strip

Use this command to configure vendor-tag strip function.

Use the no form of this command to restore the default settings.

**pppoe intermediate-agent vendor-tag strip**  
**no pppoe intermediate-agent vendor-tag strip**

**Parameter  
Description**

Parameter	Description
N/A	N/A

**Defaults** By default, this function is disabled.

**Command** Interface configuration mode



**Mode**

**Usage Guide** Strip function must be configured on trusted ports. If the function is configured on untrusted ports, it would fail to take effect.

**Configuration** The following example enables vendor-tag strip function on port 1.

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# pppoe intermediate-agent vendor-tag
strip
Ruijie(config-if-GigabitEthernet 0/1)# end
```

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 16.9 pppoe intermediate-agent circuit-id

Use this command to configure the custom circuit-id of a port.

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

**pppoe intermediate-agent circuit-id** *string*

**no pppoe intermediate-agent circuit-id**

**Parameter Description**

Parameter	Description
N/A	N/A

**Defaults** By default, this function is disabled.

**Command** Interface configuration mode

**Mode**

**Usage Guide** Configure the circuit-id of a port.

**Configuration** The following example configures the custom circuit-id on a port.

**Examples**

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# pppoe intermediate-agent circuit-id
```

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

**Related  
Commands**

Command	Description
N/A	N/A

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

## 16.10 pppoe intermediate-agent remote-id

Use this command to configure the custom remote-id of a port.  
Use the **no** form of this command to restore the default settings.

**pppoe intermediate-agent remote-id** *string*  
**no pppoe intermediate-agent remote-id**

**Parameter  
Description**

Parameter	Description
N/A	N/A

**Defaults** By default, this function is disabled.

**Command Mode** Interface configuration mode

**Usage Guide** Configure the remote-id of a port.

**Configuration** The following example configures the customized remote-id of a port.

**Examples**

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# pppoe intermediate-agent remote-id bbb
Ruijie(config-if-GigabitEthernet 0/1)# end
```

**Related  
Commands**

Command	Description
N/A	N/A

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



## System Commands

---

1. Basic Configuration Management Commands
2. Line Commands
3. File System Commands
4. SYS Commands
5. Time Range Commands
6. HTTP Service Commands
7. Syslog Commands
8. Monitoring Commands

# 1 Basic Configuration Management Commands

## 1.1 <1-99>

Use this command to restore the suspended Telnet Client session.

<1-99>

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** User EXEC mode

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

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

```
Ruijie# 1
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.2 banner exec

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

**banner exec c message c**

**no banner exec**

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

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

**Defaults** N/A

**Command Mode** Global configuration mode

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

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

The messages are for all lines. If you want to disable display the EXEC message on a specific line, configure the **no exec-banner** command on the line.

**Configuration** 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

## 1.3 banner incoming

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

**banner incoming** *c message c*

**no banner incoming**

Parameter Description	Parameter	Description
	<i>c</i>	
<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**

## 1.4 banner login

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

**banner login c message c**

**no banner login**

**Parameter Description**

Parameter	Description
<i>c</i>	Separator of the message contained in the login banner. Delimiters are not allowed in the MOTD.
<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**  
**Description** N/A

## 1.5 banner motd

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

**banner [ motd ] c message c**  
**no banner [ motd ]**

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

**Defaults** N/A

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

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

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

**Examples** Ruijie(config)# **banner motd** \$ *hello,world* \$

Related Commands	Command	Description
	N/A	N/A

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

## 1.6 banner prompt-timeout

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

**banner prompt-timeout c message c**  
**no banner prompt-timeout**

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

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

**Defaults** N/A

**Command Mode** Global configuration mode

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

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

**Examples** Ruijie(config)# banner prompt-timeout \$ authentication \$

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.7 banner slip-ppp

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

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

**no banner slip-pp**

Parameter Description	Parameter	Description
	<i>c</i>	
<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

## 1.8 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

## 1.9 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
		<b>enable</b>

**Platform Description** N/A

## 1.10 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 0
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description**

N/A

## 1.11 do telnet

Use this command to login to Telnet server.

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

**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.
<b>/source</b>	Specifies source IP or source port for Telnet client.
<b>ip</b> <i>A.B.C.D</i>	Specifies source IPv4 address for Telnet client.
<b>ipv6</b> <i>X:X:X:X::X</i>	Specifies source IPv6 address for Telnet client.
<b>interface</b> <i>interface-name</i>	Specifies source port for Telnet client.

**Defaults**

N/A

**Command Mode**

User EXEC mode/Privileged EXEC mode/Interface configuration mode

**Usage Guide**

N/A

**Configuration Examples**

The following example configures destination IP address 1.1.1.1.

**Examples**

```
Ruijie(config)# do telnet 1.1.1.1
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description**

N/A

## 1.12 enable

Use this command to enter privileged EXEC mode.

**Enable** [ *privilege-level* ]

**Parameter  
Description**

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

**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** The following example lowers the privilege level to 14:

**Examples**

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

**Related  
Commands**

Command	Description
N/A	N/A

**Platform  
Description** N/A

## 1.13 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
password	Password for the user to enter the EXEC configuration layer
<b>level</b>	User's level.
<b>0</b>	The password is in plain text.
<b>7</b> <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. The password must contain at least three of the following four types of characters: uppercase letters, lowercase letters, symbols and numbers.

**Configuration** The following example configures the password as **Nihao123!**.

**Examples**

```
Ruijie(config)# enable password Nihao123!
```

**Related Commands**

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

**Platform**

N/A

**Description**

**enable secret** Sets the security password

## 1.14 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
level	User's level.
0	The password is in plain text.
5 encrypted-password	The password is encrypted.

**Defaults**

N/A

**Command** Global configuration mode  
**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 **Nihao123!**.

**Examples** Ruijie(config)# **enable secret 0 Nihao123!**

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

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

## 1.15 enable service

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

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

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

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

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

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

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

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

**Examples** Ruijie(Config) # **enable service ssh-server**

**Related Commands**

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

**Platform Description**

N/A

## 1.16 end

Use this command to return to privileged EXEC mode.

**end**

**Parameter Description**

Parameter	Description
N/A	N/A

**Defaults**

N/A

**Command Mode**

All modes except privileged EXEC mode

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

**Configuration** The following example returns to privileged EXEC 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#
```

**Related**

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

Commands		
	N/A	N/A

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

## 1.17 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** LINE configuration mode  
**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** The following example disables display of the EXEC message on line VTY 1.

**Examples**

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

Related Commands	Command	Description
	N/A	N/A

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



## 1.18 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.
	<b>seconds</b>	(Optional) Timeout in minutes

**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

## 1.19 execute

Use this command to execute a command on the file.

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

Parameter Description	Parameter	Description
	<i>filename</i>	Specifies the file path.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

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

```

Examples
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 vlan 1
Ruijie(config-if-VLAN 1)#ip address 192.168.21.158 24
Ruijie(config-if-VLAN 1)#end
*Sep 29 23:35:49: %SYS-5-CONFIG_I: Configured from console by console

```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform  
Description** N/A

## 1.20 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

## 1.21 help

Use this command to display the help information.

**help****Parameter  
Description**

Parameter	Description
N/A	N/A

**Defaults**

Any mode

**Command  
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  
Examples**

The following example displays brief information about the help system.

```

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 all available commands in interface configuration mode.

```
Ruijie(config-if-GigabitEthernet 0/17)#?
```

Interface configuration commands:

```
arp-check          Port-security arp-check
bandwidth          Set bandwidth informational parameter
bpdu               Bridge Protocol Data Unit
carrier-delay      Specify delay for interface transitions
default            Set a command to its defaults
description        Interface specific description
do                 To run exec commands in config mode
dot1q              The dot1q configuration
dot1q-tunnel       Configure dot1q-tunnel port
duplex             Configure duplex operation
eee                Set eee
efm                Config efm for an interface
end                Exit from interface configuration mode
errdisable         Error disable
exit               Exit from interface configuration mode
expert             Expert extended ACL
flowcontrol        Set the flow-control value for an interface
frame-tag          Server Manufacturer Ethernet Frame Tag
full-duplex        Force full duplex operation
global            Global ACL
gvrp               GVRP configure command
half-duplex        Force half duplex operation
help               Description of the interactive help system
inner-priority-trust Copy inner-tag priority to outer-tag
ip                 Interface Internet Protocol config commands
ipv6               IPv6 information
l2protocol-tunnel Tunnel protocol
lacp               LACP interface subcommands
line-detect        Detect the state of line
link               Configure link
lldp               Link Layer Discovery Protocol
load-interval      Specify interval for load calculation for an
interface
logging            Configure logging for interface
mac                Mac extended ACL
mac-address-learning Modify MAC Address learning for the interface
mac-address-table  Configure mac-address table
mac-vlan           Mac vlan
max-dynamic-mac-count Config dynamic MAC limit of the Interface
```

mls	Configure MultiLayer Switching characteristics
mtu	Set the interface Maximum Transmission Unit (MTU)
nac-author-user	Config max nac user number
negotiation	Set switchport negotiation
no	Negate a command or set its defaults
port-group	Aggregateport/port bundling configuration
pppoe	Pppoe
qos	Configure qos information
rate-limit	Configure rate-limit
redirect	Redirect packets
rldp	Rldp interface configuration
rmon	Rmon command
service-policy	Configure QoS Service Policy
show	Show running system information
shutdown	Shutdown the selected interface
snmp	Modify SNMP interface parameters
spanning-tree	Spanning Tree Subsystem
speed	Configure speed operation
storm-control	Storm configuration
switchport	Set switching mode characteristics
traffic-redirect	Redirect the traffic
virtual-group	Virtual-group
vlan-mapping-in	Vlan mapping in
vlan-mapping-out	Vlan mapping out
wfq-queue	Configure Weighted Fair Queue queues
wrr-queue	Configure weighted round-robin xmt queues

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

## 1.22 hostname

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

**hostname** *name*

<b>Parameter Description</b>	<b>Parameter</b>	<b>Description</b>
	<i>name</i>	Device hostname, string, number or hyphen, up to 63 characters.
<b>Defaults</b>	The default is Ruijie.	
<b>Command Mode</b>	Global configuration mode	
<b>Usage Guide</b>	This hostname is mainly used to identify the device and is taken as the username for the local device during dialup and CHAP authentication.	
<b>Configuration Examples</b>	The following example configures the hostname of the device as BeiJingAgenda.	
	<pre>Ruijie(config)# <b>hostname</b> BeiJingAgenda BeiJingAgenda(config)#</pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	N/A	N/A
<b>Platform Description</b>	N/A	

## 1.23 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*

<b>Parameter Description</b>	<b>Parameter</b>	<b>Description</b>
	<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.
<b>Defaults</b>	N/A	
<b>Command Mode</b>	Global configuration mode	
<b>Usage Guide</b>	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 <b>no ip telnet source-interface</b> command to restore it to the default setting.	

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

**Examples**

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

**Related Commands**

Command	Description
telnet	Logs in a Telnet server.

**Platform Description**

N/A

## 1.24 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
		<b>lockable</b>

**Platform Description** N/A

## 1.25 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

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

```
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
		<b>lock</b>

**Platform Description** N/A



## 1.26 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.

```
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
	<b>password</b>	Configures the line login password

**Platform Description** N/A

## 1.27 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** 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

## 1.28 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
<b>default</b>	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**

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

**Platform  
Description**

N/A

## 1.29 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
<b>username</b>	Configures local user information.

**Platform  
Description**

N/A

## 1.30 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	Parameter	Description
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** N/A

## Description

## 1.31 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

Line configuration mode

## Mode

## Usage Guide

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

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

## Configuration

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

## Examples

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

Related  
Commands

Command	Description
N/A	N/A

## Platform

## Description

N/A

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

**Defaults** N/A

**Command Mode** Line configuration mode

### Usage Guide

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

**Platform Description** N/A

## 1.33 prompt

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

**prompt string**

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

**Defaults** N/A

**Command Mode** Global configuration mode

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

**Configuration** The following example sets the prompt string to rgnos.

**Examples**

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

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.34 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
	<b>0</b>	
<i>password</i>		Sets the password plaintext, a string ranging from 1 to 25 characters.
<b>5 encrypted-secret</b>		Sets the password text encrypted by irreversible MD5 and saves it as the encrypted password after configuration.

**Defaults** N/A

**Command mode** Line configuration mode

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

 If the specified encryption type is 5, the logical length of the cipher text to be entered must be 24 and the 1<sup>st</sup>, 3<sup>rd</sup> and 8<sup>th</sup> 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
<b>login</b>	Sets simple password authentication on the interface as the login authentication mode

**Platform** N/A

**Description**

## 1.35 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>	Timeout in minutes.
<b>output</b>	Regards data output as the input to determine whether the session expires.

**Defaults** The default timeout is 0.

**Command Mode** LINE configuration mode

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

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

**Examples**

```
Ruijie(config-line)#session-timeout 5 output
```

**Related Commands**

Command	Description
N/A	N/A



**Platform**  
**Description**

N/A

## 1.36 show debugging

Use this command to display debugging state.

**show debugging**

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 debugging state.

**Examples**

```
Ruijie#show debugging

debug fw-group detect intf-state
```

Related Commands	Command	Description
	N/A	N/A

**Platform**  
**Description**

N/A

## 1.37 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
	<b>console</b>	Displays the configuration of a console line.
	<b>vty</b>	Displays the configuration of a vty line.
	<i>line-num</i>	Number of the line.

**Defaults** N/A

**Command Mode** Privileged EXEC 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

## 1.38 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**

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

**Examples**

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

**Related Commands**

Command	Description
N/A	N/A

**Platform****Description**

N/A

## 1.39 show running-config

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

**show running-config****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

## 1.40 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

## 1.41 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** User EXEC mode

**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**

N/A

**Description**

## 1.42 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**

Privileged EXEC mode

**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
		<b>boot config</b>

**Platform Description** N/A

## 1.43 show this

Use this command to display effective configuration in the current mode.

**show this**


Parameter Description	Parameter	Description
		N/A

**Defaults** N/A

**Command Mode** All modes.

**Usage Guide** The configuration in the following range modes cannot be displayed. If the **show this** command is run, the outcome is NULL.

1. Use the **line** *first-line last-line* command to configure lines in a continuous group and enter LINE configuration mode.
2. Use the **vlan range** command to configure VLANs and enter vlan range configuration mode.
3. Use the **interface range** command to configure interfaces and enter interface range configuration mode.

 In **vlan range** or **interface range** mode, if the number of VLANs or interfaces exceeds 50, the configuration of the first 50 VLANs or interfaces will be displayed.

**Configuration** Use this command to display effective configuration on interface fastEthernet 0/17.

```

Ruijie (config)#interface fastEthernet 0/17
Ruijie (config-if-FastEthernet 0/17)#show this
Building configuration...
!
spanning-tree link-type point-to-point
spanning-tree mst 0 port-priority 0
!
end
Ruijie (config-if-FastEthernet 0/17)#

```

Use this command to display configuration on interface VLAN 1-3.

```
Ruijie(config-if-range)#show this

Building configuration...
!
interface VLAN 1
 ip address dhcp
interface VLAN 2
 ip address 1.1.1.1 255.255.255.0
interface VLAN 3
 ip address 3.3.3.3 255.255.255.0
!
end
Ruijie(config-if-range)#
```

#### Related Commands

Command	Description
N/A	N/A

#### Platform Description

N/A

## 1.44 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  
Description**

N/A

## 1.45 telnet

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

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

**Parameter  
Description**

Parameter	Description
<i>host</i>	The IP address of the host or host name you want to log in.
<i>port</i>	Selects the TCP port number for login, 23 by default.
<b>/source</b>	Specifies the source IP address or source interface used by the Telnet client.
<b>ip</b> A.B.C.D	Specifies the source IPv4 address used by the Telnet client.
<b>ipv6</b> X:X:X:X::X	Specifies the source IPv6 address used by the Telnet client.
<b>interface</b> interface-name	Specifies the source interface used by the Telnet client.

**Defaults**

N/A

**Command  
Mode**

User EXEC mode

**Usage Guide**

**Configuration** The following example sets telnet to IP address 10.0.0.1.

**Examples**

```
Ruijie# telnet 10.0.0.1
```

**Related  
Commands**

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

**Platform**

N/A



Description

## 1.46 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** ] [ **pwd-modify** ] [ **nopassword** | **password** [ **0** | **7** ] *text-string* | **secret** [ **0** | **5** ] *text-string* ]

**no username** *name*


Parameter Description

Parameter	Description
<i>name</i>	Username
<b>login mode</b>	Sets the login mode.
<b>aux</b>	Sets the login mode to aux.
<b>console</b>	Sets the login mode to console.
<b>ssh</b>	Sets the login mode to ssh.
<b>telnet</b>	Sets the login mode to telnet.
<b>online amount</b> <i>number</i>	Sets the amount of users online simultaneously.
<b>permission</b> <i>oper-mode path</i>	Sets the permission on the specified file. <i>oper-mode</i> refers to the operation mode and <i>path</i> to the file or the directory path.
<b>privilege</b> <i>privilege-level</i>	Sets the privilege level, in the range from 0 to 15.
<b>reject remote-login</b>	Confines the account to remote login.
<b>web-auth</b>	Confines the account to web authentication.
<b>pwd-modify</b>	Allows the web authentication user of this account to change the password. It works only when the <b>web-auth</b> command is configured.
<b>nopassword</b>	The account is not configured with a password.
<b>password</b> [ <b>0</b>   <b>7</b> ] <i>text-string</i>	If the password type is 0, the password is in plain text. If the type is 7, the password is encrypted. The password is in plain text by default.
<b>secret</b> [ <b>0</b>   <b>5</b> ] <i>text-string</i>	If the password type is 0, the password is in plain text. If the type is 5, 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** The following example configures a username and password and binds the user to level 15.

**Examples**

```
Ruijie(config)# username test privilege 15 password 0 Nihao123!
```

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

```
Ruijie(config)# username user1 web-auth password 0 Nihao123!
```

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**

N/A

**Description**

## 1.47 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**

The following example imports user information from the file.

**Examples**

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

**Related  
Commands**

Command	Description
N/A	N/A

**Platform**

N/A

## Description

## 1.48 username export

Use this command to export user information to the file.

**username export** *filename*

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

**Defaults** N/A

**Command Mode** Privileged EXEC mode

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

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

```
Ruijie# username export user.csv
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.49 write

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

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

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

**Defaults** N/A

**Command** Privileged EXEC mode

**Mode**

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

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

The system will ask you whether to save the current configuration in default boot configuration file /config.text and perform an action as required if the device that stores the file does not exist possibly because the boot configuration file is stored on a removable storage device, 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

## 2 LINE Commands

### 2.1 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

### 2.2 access-class

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

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

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

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

**Defaults** N/A

**Command Mode** Line configuration mode

**Usage Guide** N/A

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

**Examples**

```
Ruijie(config)# line vty 0 5
Ruijie(config-line)access-class 20 in
```

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

```
Ruijie(config)# line vty 6 7
Ruijie(config-line)access-class test out
```

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

**Platform** N/A

**Description**

## 2.3 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.
	<b>default</b>	Default authorization list name.
	<i>list-name</i>	Optional list name.

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

**Command Mode** Line configuration mode

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

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

**Examples**

```
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

## 2.4 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 commands { default | list-name }**

**no accounting commands**

**Parameter Description**

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

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

**Command 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**

## 2.5 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 Examples** The following example configures Ctrl+Y (ASCII: 25) for activating the terminal session.

```
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**

## 2.6 authorization commands

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

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

**no authorization commands** *level*

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

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

**Command Mode** Line configuration mode

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

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

```
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 Description** N/A

## 2.7 authorization exec

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

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

**no authorization exec**

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

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

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

**Examples**

```
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

## 2.8 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** The following example enables automatic command execution and connects to line vty 0.

**Examples**

```
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** N/A  
**Description**

## 2.9 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
<b>console</b>	Clears connection status of the console line.
<b>vty</b>	Clears connection status of the virtual terminal line.
<i>line-num</i>	Specifies the line to be cleared.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

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

**Configuration** The following example clears connection status of line VTY 13. The connected session on the client

**Examples** (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

## 2.10 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 Description** N/A

## 2.11 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 Description** N/A

## 2.12 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

## 2.13 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 Examples** The following example bans line VTY 1 from entering the command line interface.

```
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**

## 2.14 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
<b>7</b>	Configures a 7-bit coded character set.
<b>8</b>	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 Examples** The following example configures a 7-bit coded character set for the async line.

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

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 2.15 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
	<b>hardware</b>	Configures hardware flow control.
	<b>none</b>	Configures no flow control.
	<b>software</b>	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 prevents 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 Description** N/A

## 2.16 history

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

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

**no history**



**no history size**

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

**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

**Platform Description** N/A

## 2.17 ipv6 access-class

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

**ipv6 access-class** *access-list-name* { **in** | **out** }

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

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

**Defaults** N/A

**Command Mode** Line configuration mode

**Usage Guide** N/A

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

```
Ruijie(config)# line vty 0 4
Ruijie(config-line)ipv6 access-list test out
```

Related Commands	Command	Description
		show running

**Platform Description** N/A

## 2.18 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>

**Defaults** The default is 24.

**Command Mode** Line configuration mode

**Usage Guide** N/A

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

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

Related Commands	Command	Description
		N/A

**Platform Description** N/A

## 2.19 line

Use this command to enter the specified LINE mode.

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

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

**Defaults** N/A

**Command Mode** Global configuration mode

### Usage Guide

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

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

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 2.20 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>	VTY connection number, in the range from 0 to 35.

**Defaults**

**Command Mode** Global configuration mode.

**Usage Guide**

**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
```

Decrease 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 Description** N/A

## 2.21 location

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

- location** *location*
- no location**

**Parameter Description**

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

**Defaults** N/A

**Command Mode** Line configuration mode

**Usage Guide** N/A

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

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

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 2.22 monitor

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

**monitor**  
**no monitor**

**Parameter Description**

Parameter	Description
N/A	N/A

**Defaults** N/A

**Command Mode** Line configuration mode

**Usage Guide** N/A

**Configuration 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 Description** N/A

## 2.23 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
<b>even</b>	Configures even parity,
<b>none</b>	Configures no parity.
<b>odd</b>	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 Description** N/A

## 2.24 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	N/A
-----	-----

**Platform** N/A

**Description**

## 2.25 refuse-message

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

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

**no refuse-message**

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

**Defaults** N/A

**Command** Line configuration mode

**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)#refuse-message @ Unauthorized user cannot login to the
ruijie device @
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 2.26 show history

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

**show history**

<b>Parameter Description</b>	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table>	Parameter	Description	N/A	N/A
Parameter	Description				
N/A	N/A				
<b>Defaults</b>	N/A				
<b>Command Mode</b>	Privileged EXEC mode				
<b>Usage Guide</b>	N/A				
<b>Configuration Examples</b>	<p>The following example displays the command history of the line.</p> <pre>Ruijie# show history exec: sh privilege sh run show user sh user all show history</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				

## 2.27 show line

Use this command to display line configuration.

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

<b>Parameter Description</b>	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>console</b></td> <td>Displays configuration for the console line.</td> </tr> <tr> <td><b>vty</b></td> <td>Displays configuration for the virtual terminal line.</td> </tr> <tr> <td><i>line-num</i></td> <td>Displays the line.</td> </tr> </tbody> </table>	Parameter	Description	<b>console</b>	Displays configuration for the console line.	<b>vty</b>	Displays configuration for the virtual terminal line.	<i>line-num</i>	Displays the line.
Parameter	Description								
<b>console</b>	Displays configuration for the console line.								
<b>vty</b>	Displays configuration for the virtual terminal line.								
<i>line-num</i>	Displays the line.								
<b>Defaults</b>	N/A								
<b>Command Mode</b>	Privileged EXEC mode								



**Usage Guide** N/A

**Configuration** The following example displays configuration for the 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
```

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

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** N/A

## 2.28 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 Description** N/A

## 2.29 show users

Use this command to display the login user information.

**show users [ all ]**

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

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

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

```

Examples 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      ---          idle            00:00:00      ---
    
```

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 2.30 speed

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

**speed baudrate**

**no speed**

**Parameter Description**

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

**Defaults** The default is 9600.

**Command Mode** LINE configuration mode

**Usage Guide** N/A

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

**Examples**

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

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 2.31 start-character

Use this command to 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>	

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

**Command** LINE configuration mode

**Mode**

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

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

**Examples**

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

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 2.32 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 Mode** LINE configuration 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 Examples** 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 Description** N/A

## 2.33 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 Mode** LINE configuration 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 Description** N/A

## 2.34 terminal databits

Use this command to configure the databit number of the character for the current terminal in flow communication mode. Use the **no** form of this command to restore the default setting.

**terminal databits** *bit*

**terminal no databits**

**Parameter Description**

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

**Defaults** The default is 8.

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the databit number of every character for the current terminal in flow communication mode to 7.

```
Ruijie#terminal databits 7
```

**Related Commands**

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

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

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

## 2.35 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** N/A  
**Description**

## 2.36 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	Parameter	Description
-----------	-----------	-------------

<b>Description</b>		
	<b>7</b>	Configures a 7-bit coded character set.
	<b>8</b>	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

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

**Platform Description** N/A

## 2.37 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 }**

<b>Parameter Description</b>	<b>Parameter</b>	<b>Description</b>
	<b>hardware</b>	Configures hardware flow control.
	<b>none</b>	Configures no flow control.
	<b>software</b>	Configures software flow control.

**Defaults** No flow control is configured by default.

**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**

## 2.38 terminal history

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

- terminal history [ size size ]**
- terminal no history**
- terminal no history size**

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

**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**

## 2.39 terminal length

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

**terminal length** *screen-length*

**terminal no length**

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

**Defaults** The default is 24.

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

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

```
Ruijie# terminal length 10
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 2.40 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** The following example configures location description of the current device as "Swtich's Line Vty 0".

**Examples**

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

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 2.41 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
	<b>even</b>	
<b>none</b>		Configures no parity.
<b>odd</b>		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** The following example configures even parity for the current terminal.

**Examples**

```
Ruijie#terminal parity even
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 2.42 terminal speed

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

**terminal speed** *baudrate*

**terminal no speed**

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

**Defaults** The default is 9600.

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

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

```
Ruijie# terminal speed 115200
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 2.43 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>	Sets the ASCII value corresponding to the start character for software flow control on the current terminal, in the range from 0 to 255.

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

**Command** Privileged EXEC mode

**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**

## 2.44 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

**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** N/A

**Description**

## 2.45 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 Description** N/A

## 2.46 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, such as vt100 and ansi.

**Defaults** The default is vt100.

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

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

```
Ruijie#terminal terminal-type ansi
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 2.47 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 Description** N/A

## 2.48 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 Examples** 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 Description** N/A

## 2.49 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
	<b>response</b>	The time period during which the line waits for the user to enter any message.
	<i>seconds</i>	Timeout value, in the range from 1 to 300 in the unit of seconds.



**Defaults** The default is 30.

**Command Mode** Line configuration mode

**Usage Guide** N/A

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

**Examples**

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

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** N/A

## 2.50 transport input

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

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

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

**Parameter Description**

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

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

**Command Mode** Line configuration mode

**Usage Guide** N/A

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

**Examples**

```
Ruijie(config)# line vty 0 4
Ruijie(config-line) transport input ssh
```

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

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

## 2.51 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>
	<i>message</i>	Logout message.

**Defaults** N/A

**Command Mode** Line configuration mode

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

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

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

Related Commands	Command	Description
		N/A

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

## 2.52 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

### 3 File System Commands

#### 3.1 cd

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

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

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

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

**Command** Privileged EXEC mode.

**Mode**

**Usage Guide**

**Configuration**

**Examples**

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

**Platform** N/A.

**Description**

#### 3.2 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
<b>running-config</b>	Running configuration file.
<b>startup-config</b>	startup configuration file.
<b>flash:</b>	local FLASH file system.
<b>tftp:</b>	The URL of TFTP network server, in the format as follows: <b>tftp:[[/location]/directory]/filename</b>

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

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

**Platform** N/A

**Description**

### 3.3 delete

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

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

**Parameter Description**

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

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

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

**Usage Guide**

**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)
    
```

The following example deletes the non-null file on the FLASH disk recursively.

```

Ruijie#pwd
flash:/
Ruijie#dir
Directory of flash:/
  1 drwx          0  Thu Jan  1 02:02:25 1970  file
  2 -rw-     610019  Tue Aug 14 02:21:13 2012  file-5.11.tar.gz
1 file, 1 directory
58,720,256 bytes total (28,577,792 bytes free)
Ruijie#delete /recursive flash:/file
Ruijie#dir
Directory of flash:/
  1 -rw-     610019  Tue Aug 14 02:21:13 2012  file-5.11.tar.gz
1 file, 0 directories
58,720,256 bytes total (31,358,976 bytes free)
    
```

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

**Platform** N/A

## Description

## 3.4 dir

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

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

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

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

**Command Mode** Privileged EXEC mode.

## Usage Guide

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

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

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

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

**Platform** N/A.

**Description**

### 3.5 mkdir

Use this command to create a directory.

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

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

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

**Command** Privileged EXEC mode.

**Mode**

**Usage Guide**

**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 Commands	Command	Description
	<code>rmdir</code>	Deletes the directory.
	<code>pwd</code>	Displays the present directory.

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

### 3.6 more

Use this command to display the content of a file.

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

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

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

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

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

```
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> <protfamily> <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**

### 3.7 pwd

Use this command to display the working path.

**pwd**

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

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** N/A

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

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

### 3.8 rename

Use this command to move or rename the specified file.

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

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

**Defaults** N/A.

**Command** 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
<b>delete</b>	Deletes the file.
<b>copy</b>	Copies the file.

**Platform** N/A

**Description**

### 3.9 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 <b>flash:</b> , <b>tmp:</b> .
<i>directory</i>	The path name. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.

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

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

**Usage Guide** This command does not support the wildcards, and the directory to be deleted must be empty. Since this command supports abbreviations, you can also use the **rm** command to delete empty directories.

**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**

### 3.10 show file systems

Use this command to display the file system information.  
**show file systems**

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

**Defaults** N/A.

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

**Mode**

**Usage Guide** Use this command to display the file systems supported in the present devices and the available space condition in the file system.

**Configuration** The following example displays the file system information:

**Examples**

```
Ruijie#show file systems
  Size(KB)      Free(KB)    Type  Flags Prefixes
      NA         NA      ram   rw tmp:
      NA         NA  network rw 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"> <li>● ro: read-only</li> <li>● wo: write-only</li> <li>● rw: read and write</li> </ul>
Prefixes	File system prefix

**Related****Commands**

Command	Description
N/A.	N/A.

**Platform**

N/A.

**Description**

### 3.11 show mount

Use this command to display the mounted information.

**show mount****Parameter****Description**

Parameter	Description
N/A	N/A

**Defaults**

N/A

**Command**

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

**Mode****Usage Guide**

N/A

**Configuration**

The following example displays the mounted information.

**Examples**

```
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**

### 3.12 tftp-client source

Use this command to bind a source IP address or source interface with a TFTP client. Use the **no** or **default** form of this command to restore the default setting.

**tftp-client source** { **ip** *ip-address* | **ipv6** *ipv6-address* | *interface* }

**no tftp-client source** { **ip** *ip-address* | **ipv6** *ipv6-address* | *interface* }

**default tftp-client source** { **ip** *ip-address* | **ipv6** *ipv6-address* | *interface* }

**Parameter**

**Description**

Parameter	Description
<i>ip-address</i>	Specifies the IPv4 source address.
<i>ipv6-address</i>	Specifies the IPv6 source address.
<i>interface</i>	Specifies the source interface

**Defaults**

No source interface or IP address is bound with the TFTP client by default.

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

**Usage Guide** N/A

**Configuration** The following example binds source IP address 192.168.23.236 with the TFTP client.

**Examples** Ruijie(config)# tftp-client source ip 192.168.23.236

The following example binds source IPv6 address 2003:0:0:0::2 with the TFTP client.

Ruijie(config)# tftp-client source ipv6 2003:0:0:0::2

The following example binds source interface gigabitEthernet 0/17 with the TFTP client.

Ruijie(config)# tftp-client source gigabitEthernet 0/17

The following example removes the configuration.

Ruijie(config)# no tftp-client source ip 192.168.23.236

The following example restores the default setting.

Ruijie(config)# default tftp-client source ip 192.168.23.236

Related Commands	Command	Description
	N/A	N/A

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

### 3.13 tree

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

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

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

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

**Command** 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**

### 3.14 verify

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

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

Parameter	Parameter	Description
<b>Description</b>	/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 <b>flash:</b> , <b>tmp:</b> .
	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** Privileged EXEC mode.

**Mode**

**Usage Guide** N/A

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

**Examples**

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

The following example computes MD5 of flash:/gcc 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	Command	Description
<b>Commands</b>	N/A	N/A

**Platform** N/A

**Description**

## 4 SYS Commands

### 4.1 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 2069.

**Defaults**

-

**Command Mode**

Privileged EXEC mode

**Default Level**

-

**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 **calendar 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 **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** -

**Platform** -

**Description** -

## 4.2 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
	-	-

**Defaults** -

**Command Mode** Privileged EXEC mode

**Default Level** -

**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** -

**Platform** -

**Description** -

### 4.3 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 2069.

**Defaults** -


**Command Mode** Privileged EXEC mode

**Default Level** -

**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** -

**Platform** -

**Description** -

## 4.4 clock summer-time

Use this command to set the summer time.

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

Use this command to disable the summer time.

**no clock summer-time**

**Parameter Description**

Parameter	Description
<b>zone</b>	Summer time name. It can only be a letter between A and Z or between a and z, which is not case sensitive. The summer time name contains 3 to 31 characters.
<b>start</b>	Indicates the start time of the summer time.
<i>start-month</i>	Start month. Value range: January, February, March, April, May, June, July, August, September, October, November, and December. The value is not case sensitive and you are allowed to enter an incomplete word, for example, Febr and FebRu.
<i>week</i>	Start week in the start month. The range is from 1 to 5.
<b>last</b>	The last week of the specified month.
<i>start-date</i>	Day in the start week of the start month. Value range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday. The value is not case sensitive and you are allowed to enter an incomplete word, for example, Web and WeDne.
<b>hh:mm</b>	Time, in the format of hour : minute.
<b>end</b>	Indicates the end time of the summer time.
<i>end-month</i>	End month. Value range: January, February, March, April, May, June, July, August, September, October, November, and December. The value is not case sensitive and you may enter an incomplete word, for example, Febr and FebRu.
<b>ahead</b>	Indicates how much time for the summer time ahead of the standard time during the effective period of the summer time. By default, the summer time is one hour ahead of the standard time.
<i>hours-offset</i>	Hours ahead of the standard time. The range is from 0 to 12. You are not allowed to set it to 00:00.
<i>minutes-offset</i>	Minutes ahead of the standard time. The range is from 0 to 59. If <i>hours-offset</i> has been set to 0, you are not allowed to set <i>minutes-offset</i> to 0.

**Defaults** -

**Command Mode** Global configuration mode

**Default Level** -

**Usage Guide**

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

09:35 ahead of the UTC time, but non-summer time is still 08:15 ahead of the UTC time.

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

Ruijie(config)# clock summer-time TZA start Feb 1 sat 2:00 end May 3 Monday 18:30 ahead 1 20
*May 10 03:45:58: %SYS-5-CLOCKUPDATE: Set summer-time: TZA from February the 1st Saturday at 2:00
TO May the 3rd Monday at 18:30, ahead 1 hour 20 minute
Set summer-time: TZA from February the 1st Saturday at 2:00 TO May the 3rd Monday at 18:30, ahead
1 hour 20 minute

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

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

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

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

The following example disables summer time.

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

**Check Method**

-

**Platform**

-

**Description**


## 4.5 clock timezone

Use this command to set the time zone.

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

Use this command to remove the time zone settings.

**no clock timezone**

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

**Defaults** -

**Command Mode** Global configuration mode

**Default Level** -

### Usage Guide

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

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

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

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

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

The following example removes the time zone settings.

```
Ruijie(config)# no clock timezone
Set no clock timezone.
```



**Check Method** -

**Platform** -  
**Description** -

## 4.6 clock update-calendar

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

### clock update-calendar

Parameter Description	Parameter	Description
	-	-

**Defaults** -

**Command Mode** Privileged EXEC mode

**Default Level** -

**Usage Guide** 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** -

**Platform** -

**Description**

## 4.7 cpu high-watermark set

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

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

Use this command to disable CPU usage monitoring.

**no cpu high-watermark set**

Use this command to restore the default settings.

**default cpu high-watermark set**

Parameter Description	Parameter	Description
	<b>high</b> <i>high-value</i>	Sets the high watermark of the CPU usage. The range is from 2 to 99.
	<b>range</b> <i>range-value</i>	Sets the watermark fluctuation range. The range is from 1 to 20.
<b>Defaults</b>	By default, the watermark of the CPU usage is 80% and the watermark fluctuation range is 5% (namely, the range of the CPU usage watermark is from 75% and 85%).	
<b>Command Mode</b>	Global configuration mode	
<b>Default Level</b>	-	
<b>Usage Guide</b>	You can use this command to set the high watermark of the CPU usage and enable CPU usage monitoring. When detecting that the CPU usage exceeds the fluctuation range of the highest watermark, the system prints prompts.	
<b>Configuration Examples</b>	<p>The following example sets the CPU usage watermark to the default value and enables CPU usage monitoring (if it is disabled).</p> <pre>Ruijie(config)# default cpu high-watermark set Reset default cpu watermark monitor set system cpu watermark high 80%(75~85%)</pre> <p>The following example disables CPU usage monitoring.</p> <pre>Ruijie(config)# no cpu high-watermark set Close cpu watermark monitor</pre> <p>The following example enables CPU usage monitoring. Keep the defined watermark value.</p> <pre>Ruijie(config)# cpu high-watermark set Open cpu watermark monitor set system cpu watermark high 80%(75~85%)</pre> <p>The following example enables CPU usage monitoring and sets the high watermark to 88% and fluctuation range to 3%.</p> <pre>Ruijie(config)# cpu high-watermark set high 88 range 3 Open cpu watermark monitor set system cpu watermark high 88%(85~91%)</pre> <p>In this case, the high watermark is set to 88%. The upper limit of the high watermark is 91% (88%+3%) and the lower limit is 85% (88%-3%).</p>	
<b>Check Method</b>	-	
<b>Prompt Message</b>	<p>If the high watermark of the CPU usage is allowed to fluctuate from 85% to 91%, the system will print the following warning message when the CPU usage exceeds the upper limit of the high watermark:</p> <pre>*Jan 19 16:23:01: %RG_SYSMON-4-CPU_WATERMARK_HIGH: warning! system cpu usage above high</pre>	

```
watermark(85%),current cpu usage 100%
```

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

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

**Platform**

-

**Description**

## 4.8 memory history clear

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

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

**Parameter Description**

Parameter	Description
<b>one-forth</b>	Clears one fourth entries.
<b>half</b>	Clears a half of entries.
<b>all</b>	Clears all the entries.

**Defaults**

-

**Command Mode**

Global configuration mode

**Default Level**

-

**Usage Guide**

-

**Configuration Examples**

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

```
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** -
- Prompt** -
- Message** -
- Platform** -
- Description** -

## 4.9 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 2069.

- Defaults** -
- Command Mode** Privileged EXEC mode
- Default Level** -
- Usage Guide** -
- Configuration** The following example reloads the device.

**Examples**

```
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** -

**Prompt** -

**Message** -

**Platform** -

**Description** -

### 4.10 show calendar

Use this command to display the hardware calendar.

**show calendar**

Parameter	Parameter	Description
Description	-	-

**Command** Privileged EXEC mode/ global configuration mode

**Mode**

**Default Level** -

**Usage Guide** -

**Configuration** The following example displays the hardware calendar.

**Examples**

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

**Prompt** -

**Message** -

**Platform** -

**Description** -

### 4.11 show clock

Use this command to display the system software clock.

**show clock**

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

<b>Description</b>	
	-

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

**Default Level** -

**Usage Guide** -

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

```
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** -

**Platform Description** -

## 4.12 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
	-	-

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

**Default Level** -

**Usage Guide** 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** -

**Platform** -  
**Description** -



## 4.13 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
	<b>sorted total</b>	Ranked according to the memory usage.
	<b>history</b>	Displays the history of memory usage.
	<b>low-watermark</b>	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> .
	<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** -

**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--
```

Description of some keywords in the command:

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.

Description of the displayed information on each task:

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** -

**Platform** -  
**Description** -

### 4.14 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
<b>5sec   1min   5min   15min</b>	Displays lists of tasks in descending order of CPU usage within the last five seconds, one minute, five minutes, and 15 minutes.
<b>Nonzero</b>	Does not display the task with 0 CPU usage.
<b>History</b>	Displays the CPU usage of the control core within the last 60 seconds, 60 minutes, and 72 hours in histogram.
<b>Table</b>	Displays the CPU usage of the control core within the last 60 seconds, 60 minutes, and 72 hours in table.

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

**Default Level** -

**Usage Guide**

**Configuration**

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

**Examples**

```
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
```

Description of the information displayed in this command:

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
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.

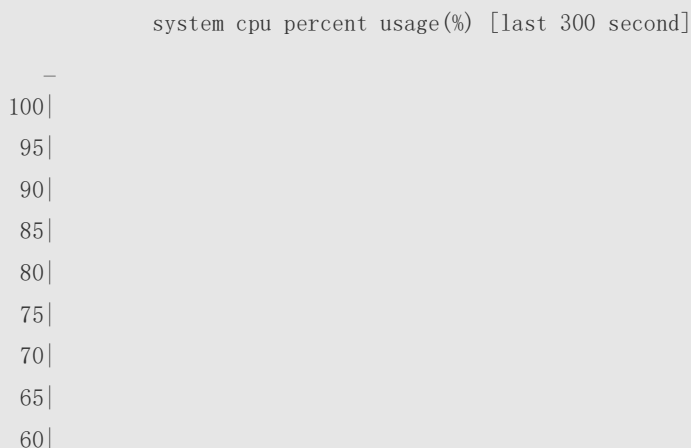
The first histogram displays the CPU usage of the control core within 300 seconds. Every segment in the x-coordinate is five seconds, and every segment in the y-coordinate is 5%. The symbol "\*" indicates the CPU usage at the last specified second. In other words, the first segment on the x-coordinate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

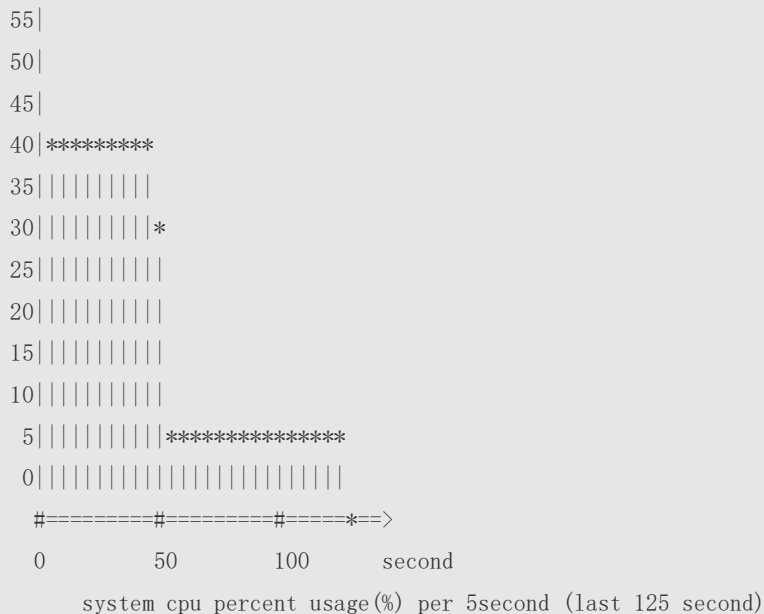
The second histogram displays the CPU usage of the control core within the last 60 minutes, measured in %. Every segment on the x-coordinate is 1 minute.

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
```





system cpu percent usage(%) [last 60 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 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** -  
**Platform** -  
**Description** -

### 4.15 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** -


**Usage Guide**

**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            : ?
```

 **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_procps, do NOT exist, or NOT only one.
```

Description of the displayed information:

Field	Description
-------	-------------

Process Id	Task ID
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** -  
**Platform** -  
**Description** -

### 4.16 show reboot-reason

Use this command to display the reboot reason.

**show reboot-reason** [ *all* ]

Parameter Description	Parameter	Description
	<i>all</i>	Displays the reboot reason of all devices/service modules

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

**Default Level** -

**Usage Guide** -

**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** -

**Platform** -  
**Description** -

### 4.17 show version

Use this command to display the system version information.

**show version**

Parameter	Parameter	Description
Description	-	-

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

**Default Level** -

**Usage Guide** -

**Usage Guide** The following example displays the system version information.

```
Ruijie#show version
System description      : Ruijie Full Gigabit Security Intelligence Access
Switch(RG-HS2310-16GH2GT1XS) By Ruijie Networks
System start time      : 1970-01-01 05:59:59
System uptime          : 0:02:00:09
System hardware version : 1.00
System software version : HS2310_RGOS 11.4(1)B90, Release(10222017)
System patch number    : NA
System serial number    : MACC942570105
System boot version     : 1.0.2
Module information:
  Slot 0 : RG-HS2310-16GH2GT1XS
    Hardware version    : 1.00
    Boot version        : 1.0
    Software version     : HS2310_RGOS 11.4(1)B90, Release(10222017)
    Serial number       : MACC942570105
```

```
Ruijie#
```

**Prompt** -  
**Message**

**Platform** -  
**Description**

## 5 Time Range Commands

### 5.1 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
	<i>start time date</i>	Indicates the start time of the range.
	<i>end time date</i>	Indicates the end time of the range.

**Defaults** The default absolute time range is the maximum range.

**Command Mode** Time range configuration mode

**Default Level** 14

**Usage Guide** Use the **absolute** command to configure a time absolute time range between a start time and an end time to allow a certain function to take effect within the absolute time range.  
The maximum absolute time range is from 00:00 January 1, 0 to 23:59 December 31, 9999.

**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** -

**Platform Description** -

## 5.2 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.

**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** -

**Platform Description** -

## 5.3 show time-range

Use this command to display the time range configuration.

**show time-range** [ *time-range-name* ]

<b>Parameter Description</b>	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>time-range-name</i></td> <td>Displays a specified time range.</td> </tr> </tbody> </table>	Parameter	Description	<i>time-range-name</i>	Displays a specified time range.
Parameter	Description				
<i>time-range-name</i>	Displays a specified time range.				
<b>Command Mode</b>	Privileged EXEC mode				
<b>Default Level</b>	14				
<b>Usage Guide</b>	Use this command to check the time range configuration.				
<b>Configuration Examples</b>	<p>The following example displays the time range configuration.</p> <pre>Ruijie# show time-range time-range entry: test (inactive)   absolute end 01:02 02 February 2012</pre>				
<b>Prompt Message</b>	-				
<b>Platform Description</b>	-				

## 5.4 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*

<b>Parameter Description</b>	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>time-range-name</i></td> <td>Time range name</td> </tr> </tbody> </table>	Parameter	Description	<i>time-range-name</i>	Time range name
Parameter	Description				
<i>time-range-name</i>	Time range name				

**Defaults** No time range is configured by default.

**Command Mode** Global configuration mode

**Default Level** 2

**Usage Guide** Some applications (such as ACL ) may run based on time. For example, an ACL can be effective within certain time ranges of a week. To this end, first you must configure a time range. After the time range is

created, you can configure relevant time control in time range mode.

**Configuration** The following example creates a time range.

**Examples**

```
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** -

**Platform Description** -

## 6 HTTP Service Commands

### 6.1 enable service web-server

Use this command to enable the HTTP service function.

Use the **no** or **default** form of this command to disable the HTTP service function.

**enable service web-server** [ **http** | **https** | **all** ]

**no enable service web-server** [ **http** | **https** ]

**default enable service web-server** [ **http** | **https** ]

Parameter Description	Parameter	Description
	<b>http</b>	Enables the HTTP service.
	<b>https</b>	Enables the HTTPS service.
	<b>all</b>	Enables both the HTTP service and the HTTPS service.

**Defaults** By default, the HTTP service function is disabled.

**Command mode** Global configuration mode.

**Usage Guide** If run a command ends with the keyword **all** or without keyword, it indicates enabling both the HTTP service and the HTTPS service; if run a command ends with keyword **http**, it indicates enabling the HTTP service; if run a command ends with keyword **https**, it indicates enabling the HTTPS service. Use the command **no enable service web-server** to disable the corresponding HTTP service.

**Configuration** The following example enables both the HTTP service and the HTTPS service:

**Examples**

```
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 Description** N/A

### 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

## 6.2 http secure-port

Use this command to configure the HTTPS port number.

Use the **no** form of this command to restore the default HTTPS port number.

**http secure-port** *port-number*  
**no http secure-port**

**Parameter Description**

Parameter	Description
<i>port-number</i>	Configures the HTTPS port number. The value includes 443, 1025 to 65,535.

**Defaults** The default HTTP port number is 443.

**Command mode** Global configuration mode.

**Usage Guide** Use this command to configure the HTTPS port number.



**Configuration** The following example configures the HTTPS port number as 4443:

**Examples** `Ruijie(config)#http secure-port 4443`

Related Commands	Command	Description
		<code>enable service web-server</code>
	<code>show web-server status</code>	Displays the configuration and status of the Web service.

**Platform** N/A

**Description**

### 6.3 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

**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
		<code>enable service web-server</code>
	<code>http port</code>	Configures the HTTP port number.
	<code>http secure-port</code>	Configures the HTTPS port number.

**Platform** N/A

**Description**

## 6.4 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** The following example copies a Web package into the file system and upgrades the package.

**Examples**

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

Related Commands	Command	Description
	<b>enable service web-server</b>	Enables the HTTP service.

**Platform** N/A

**Description**

## 6.5 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
	<b>tftp:</b> <i>path</i>	<i>path</i> indicates the storage path of the Web package on the TFTP server. <b>tftp</b> 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** Global configuration 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
<b>enable service web-server</b>	Enables the HTTP service.

**Platform Description** N/A

## 6.6 webmaster level

Use this command to configure the username and password for Web login authentication. Use the **no** form of this command to restore the default setting.

**webmaster level** *privilege-level* **username** *name* **password** { *password* [ **0** | **7** ] *encrypted-password* }

**no webmaster level** *privilege-level* [ **username** *name* ]

**Parameter Description**

Parameter	Description
<i>privilege-level</i>	Configures the user privilege-level.
<i>name</i>	Username.
<i>password</i>	Password.
<b>0</b>   <b>7</b>	Password type; 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 Nihao123!
```

**Related  
Commands**

Command	Description
<b>enable service web-server</b>	Enables the HTTP service.

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

## 7 Syslog Commands

### 7.1 clear logging

Use this command to clear the logs from the buffer in privileged EXEC mode.

#### clear logging

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command clears the log packets from the memory buffer. You cannot clear the statistics of the log packets.

Configuration The following example clears the log packets from the memory buffer.

Examples Ruijie# **clear logging**

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

Platform Description N/A

### 7.2 logging

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

**logging** { *ip-address* | **ipv6** *ipv6-address* } [ **udp-prot** *port* ]

Use this command to delete the specified syslog server.

**no logging** { *ip-address*] | **ipv6** *ipv6-address* }

Use this command to restore the default port 514.

**no logging** { *ip-address* | **ipv6** *ipv6-address* } **udp-prot**

Parameter Description	Parameter	Description
	<i>ip-address</i>	Sets the IP address of the host receiving log messages.

<i>ipv6-address</i>	Sets the IPv6 address of the host receiving log messages.
<b>udp-port</b> <i>port</i>	Sets the port number of the host receiving log messages. The default is 514.

**Defaults** No log message is sent to syslog server by default.

**Command** Global configuration mode

**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
```

The following example configures a syslog server with IPv6 address AAAA:BBBB::FFFF.

```
Ruijie(config)# logging ipv6 AAAA:BBBB::FFFF
```

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

**Platform** N/A

**Description**

### 7.3 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**

<b>Parameter Description</b>	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
<b>logging on</b>	Turns on the log switch.
<b>show logging</b>	Displays the logs in the buffer.

<b>clear logging</b>	Clears the logs in the log buffer.
----------------------	------------------------------------

**Platform**  
**Description**

N/A

## 7.4 logging console

Use this command to set the severity of logs that are allowed to be displayed on the console in global configuration mode. Use the **no** form of this command to prohibit printing log messages on the console.

**logging console** [ *level* ]

**no logging console**

Parameter	Parameter	Description
<b>Description</b>	<i>level</i>	Severity of log messages, 0 to 7. The name of the severity or the numeral can be used. For the details of log severity, see table 1.

**Defaults** The default is debugging (7).

**Command Mode** Global configuration mode

**Usage Guide** When a log severity is set, the log messages at or below that severity will be displayed on the console.  
The **show logging** command displays the related setting parameters and statistics of the log.

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

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

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

**Platform**  
**Description**

N/A

## 7.5 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
	<b>show logging count</b>	Displays log information about modules of the system.
	<b>show logging</b>	Displays basic configuration of log modules and log information in the buffer.

**Platform Description** N/A

## 7.6 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 23 if the RFC5424 format is enabled (Local7, local use). The default is 16 if the RFC5424 format is disabled (Local0, local use).

**Command Mode** Global configuration mode

**Usage Guide** The following table (Table-2) is the possible device values of Syslog:

Numerical Code	Facility
0 (kern)	Kernel messages
1 (user)	User-level messages
2 (mail)	Mail system
3 (daemon)	System daemons
4 (auth1)	security/authorization messages
5 (syslog)	Messages generated internally by syslogd
6 (lpr)	Line printer subsystem
7 (news)	USENET news
8 (uucp)	Unix-to-Unix copy system
9 (clock1)	Clock daemon
10 (auth2)	security/authorization messages
11 (ftp)	FTP daemon
12 (ntp)	NTP subsystem
13 (logaudit)	log audit
14 (logalert)	log alert
15 (clock2)	clock daemon
16 (local0)	Local use
17 (local1)	Local use
18 (local2)	Local use
19 (local3)	Local use
20 (local4)	Local use
21 (local5)	Local use
22 (local6)	Local use
23 (local7)	Local use

The default device value of RGOS is 23 (local 7).

**Configuration** The following example sets the device value of **Syslog** as **kernel**:

**Examples** Ruijie(config)# logging facility kern

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

**Platform Description** N/A

## 7.7 logging file

Use this command to save log messages in the log file, which can be saved in hardware disk, expanded FLASH, USB or SD card. 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
	<b>flash</b>	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** Global configuration mode

**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** The following example saves the log message in expanded FLASH and sets file name, file size and

**Examples** log level to syslog.txt, 128K and 6 respectively.

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

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 7.8 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 16.

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

**Examples**

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

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 7.9 logging filter direction

Use this command to filter the log messages destined to a certain direction. Use the **no** form of this command to restore the default setting.

**logging filter direction** { **all** | **buffer** | **file** | **server** | **terminal** }

**no logging filter direction** { **all** | **buffer** | **file** | **server** | **terminal** }

Parameter Description	Parameter	Description
	<b>all</b>	Log messages destined to all directions are filtered, including console, VTY terminal, log buffer, log file and log server.
	<b>buffer</b>	Log messages destined to the log buffer are filtered, including log messages displayed by running the <b>show logging</b> command.
	<b>file</b>	Log messages destined to the log file are filtered.
	<b>server</b>	Log messages destined to the log server are filtered.
	<b>terminal</b>	Log messages destined to the console and the VTY terminal (including Telnet and SSH).

**Defaults** Log messages destined to all directions are filtered by default.

**Command Mode** Global configuration mode

**Usage Guide** In general, log messages destined to all directions are filtered, including console, VTY terminal, log buffer, log file and log server. If you want to filter log messages destined to a certain direction, the terminal for instance, configure the **terminal** parameter.

**Configuration Examples** The following example filters log messages destined to the terminal (including the console and the VTY terminal).

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

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 7.10 logging filter rule

Use this command to configure the filter rule of the log message,

**logging filter rule** { **exact-match** **module** *module-name* **mnemonic** *mnemonic-name* **level** *level* |

**single-match** [ **level** *level* | **mnemonic** *mnemonic-name* | **module** *module-name* ] }

Use this command to delete the “exact-match” filter rule.

**no logging filter rule exact-match** [ **module** *module-name* **mnemonic** *mnemonic-name* **level** *level* ]

Use this command to delete the “single-match” filter rule.

**no logging filter rule single-match** [ **level** *level* | **mnemonic** *mnemonic-name* | **module** *module-name* ]

**Parameter Description**

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

**Defaults** No filter rule is configured by default,

**Command** Global configuration mode

**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

## 7.11 logging filter type

Use this command to configure the filter type of log messages. Use the **no** form of this command to restore the default setting.

**logging filter type { contains-only | filter-only }**

**no logging filter type**



Parameter Description	Parameter	Description
	<b>contains-only</b>	The log message containing the key word of the filter rule is printed.
	<b>filter-only</b>	The log message containing the key word of the filter rule is filtered.

**Defaults** The default filter type is filter-only.

**Command Mode** Global configuration mode

**Usage Guide**

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 Description** N/A

## 7.12 logging flash flush

Use this command to write log messages in the system buffer into the flash file immediately.

**logging flash flush**

<b>Parameter Description</b>	Parameter	Description
	N/A	N/A
<b>Defaults</b>	N/A	
<b>Command Mode</b>	Global configuration mode	
<b>Usage Guide</b>	<p>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.</p> <p> The <b>logging flash flush</b> command takes effect only once for each configuration. The log messages cached in the buffer are written into the flash file immediately after configuration.</p>	
<b>Configuration Examples</b>	<p>The following example writes log messages in the system buffer into the flash file immediately.</p> <pre>Ruijie(config)# logging flash flush</pre>	
<b>Related Commands</b>	Command	Description
	N/A	N/A
<b>Platform Description</b>	N/A	

## 7.13 logging flash interval

Use this command to set the interval to write log messages into the flash file, Use the **no** form of this command to restore the default setting.


**logging flash interval** *seconds*

**no logging flash interval**

<b>Parameter Description</b>	Parameter	Description
	<b>interval</b> <i>seconds</i>	The interval to write log messages into the flash file, in the range from 1 to 51840 in the unit of seconds.
<b>Defaults</b>	The default is 3600.	
<b>Command Mode</b>	Global configuration mode	
<b>Usage Guide</b>	This command is used to set the interval to write log messages into the flash file. The timer starts	



after configuration, If you want to restore the interval to 3600 seconds, use the **no logging flash interval** command.

 To avoid writing log messages into the flash file too frequently, it is not recommended to set a short interval.

**Configuration** The following example sets the interval to write log messages into the flash file to 300 seconds.

**Examples**

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

**Related  
Commands**

Command	Description
N/A	N/A

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

## 7.14 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.
<i>days</i>	Sets the preservation duration of logs.

**Defaults** No preservation duration is set by default.

**Command  
Mode** Global configuration mode

**Usage Guide** Due to difference in expanded FLASH size and log level, logs with different levels can be configured with different preservation durations.

 Once log preservation based on time is enabled, log preservation based on file size is disabled automatically. The log files are stored under the syslog/ directory of the expanded FLASH,

**Configuration** 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**

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

<b>Commands</b>		
	N/A	N/A

**Platform** N/A

**Description**

## 7.15 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
<b>Description</b>	<i>level</i>	Severity of the log message. The name of the severity or the numeral can be used. For the details of log severity, see Table-1.

**Defaults** The default is debugging (7).

**Command Mode** Global configuration mode

**Usage Guide** To print log information on the VTY window, run the **terminal monitor** command in privileged EXEC mode. The level of logs to be displayed is defined by **logging monitor**. The log level defined with "Logging monitor" is for all VTY windows.

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

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

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

**Platform** N/A

**Description**

## 7.16 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	Parameter	Description
Description	N/A	N/A

**Defaults** Logs are allowed to be displayed on different devices.

**Command Mode** Global configuration mode

**Usage Guide** Log information can not only be shown in the Console window and VTY window, but also be recorded in different 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
	<b>logging buffered</b>	Records the logs to a memory buffer.
	<b>logging server</b>	Sends logs to the Syslog server.
	<b>logging file flash:</b>	Records logs on the expanded FLASH.
	<b>logging console</b>	Allows the log level to be displayed on the console.
	<b>logging monitor</b>	Allows the log level to be displayed on the VTY window (such as telnet window) .
	<b>logging trap</b>	Sets the log level to be sent to the Syslog server.

**Platform Description** N/A

## 7.17 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.
	<b>all</b>	Sets rate limit to all the logs with severity level 0 to 7.
	<b>console</b>	Sets the amount of logs that can be shown in the console in a second.
	<b>except</b>	By default, the severity level is error (3). The rate of the log whose severity level is less than or equal to error (3) is not controlled.
	<i>severity</i>	Log severity level in the range from 0 to 7. The lower the level is, the higher the severity is.

**Defaults** The log rate limit function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** Use this command to control the syslog output to prevent the massive log output.

**Configuration Examples** The following example sets the number of the logs (including debug) that can be processed in a second as 10. However, the logs with warning or higher severity level are not controlled:

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

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

**Platform Description** N/A

## 7.18 logging server

Use this command to send the logs to the specified Syslog Sever in global configuration mode. Use the **no** form of this command to remove the setting. Use the **default** form of this command to restore the default setting.

**logging server** { *ip-address* | **ipv6** *ipv6-address* } [ **udp-prot** *port* ]

**no logging server** { *ip-address* | **ipv6** *ipv6-address* }

**no logging server** { *ip-address* | **ipv6** *ipv6-address* } **udp-prot**

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

<b>Description</b>	<i>ip-address</i>	IP address of the host that receives log information.
	<i>ipv6-address</i>	Specifies IPv6 address for the host receiving the logs.
	<b>udp-port</b> <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

The following example specifies an ipv6 address as 2001::1:

Ruijie(config)# **logging server ipv6** 2001::1

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

**Platform Description** N/A

## 7.19 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** ]

<b>Parameter Description</b>	Parameter	Description
	<i>interface-type</i>	Interface type.
	<i>interface-number</i>	Interface number.

**Defaults** No source interface is configured by default.

**Command** Global configuration mode

**Mode**

**Usage Guide** By default, the source address of the log messages sent to the syslog server is the address of the sending interface. For easy tracing and management, this command can be used to fix the source address of all log messages as an interface address, so that the administrator can identify which device is sending the message through the unique addresses. If the source interface is not configured on the device, or no IP address is configured for the source interface, the source address of the log messages is the address of the sending interface.

**Configuration** The following example specifies loopback 0 as the source address of the syslog messages:

**Examples**

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

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

**Platform Description** N/A

## 7.20 logging source ip | ipv6

Use this command to configure the source IP address of logs in global configuration mode. Use the **no** form of this command to restore the default setting.

**logging source** {ip *ip-address* | ipv6 *ipv6-address*}

**no logging source** { ip | ipv6 }

Parameter Description	Parameter	Description
	<i>ip-address</i>	Specifies the source IPv4 address sending the logs to IPv4 log server.
	<i>ipv6-address</i>	Specifies the source IPv6 address sending the logs to IPv6 log server.

**Defaults** No source address is configured by default.

**Command Mode** Global configuration mode

**Usage Guide** By default, the source address of the log messages sent to the syslog server is the address of the sending interface. For easy tracing and management, this command can be used to fix the source address of all log messages as an address, so that the administrator can identify which device is sending the message through the unique addresses. If this IP address is not configured on the device, the source address of the log messages is the address of the sending interface.

**Configuration** The following example specifies 192.168.1.1 as the source address of the syslog messages:

**Examples** Ruijie(config)# **logging source ip** 192.168.1.1

Related	Command	Description
Commands	<b>logging server</b>	Sends the logs to the Syslog server.

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

## 7.21 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	Parameter	Description
Description	N/A	N/A

**Defaults** The synchronization function between user input and log output is disabled by default.

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

**Usage Guide** This command enables synchronization function between user input and log output, preventing the user from interrupting when keying in the characters.

**Configuration** Ruijie(config)#**line console** 0

**Examples** 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 0/17, changed state to down
Oct 9 23:40:55 %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/17, changed state to DOWN
Ruijie# configure terminal//----the input command by the user is output again rather than being intererupted.
```

Related	Command	Description
Commands	<b>show running-config</b>	Displays the configuration.

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

## 7.22 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	Parameter	Description
<b>Description</b>	<i>level</i>	Severity of the log message. The name of the severity or the numeral can be used. For the details of log severity, see Table 1.

**Defaults** The default is informational(6)

**Command Mode** Global configuration mode

**Usage Guide** To send logs to the Syslog Server, run the **logging** command in global configuration mode to configure the **Syslog Server**. Then, run the **logging trap** command to specify the severity level of logs to be sent.  
The **show logging** command displays the configured related parameters and statistics of the log.

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

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

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

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



## 7.23 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 Mode** Global configuration mode

**Usage Guide** This command is used to print the log message to remind the administrator of user login. The log message is in the format as follows:

```
Mar 22 14:05:45 %LOGIN-5-LOGIN_SUCCESS: User login from vty0 (192.168.23.68)
OK.
```

**Configuration Examples** The following example enables the logging function to record user log/exit.

```
Ruijie(config)# logging userinfo
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 7.24 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** Global configuration mode  
**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** The following example enables the logging function to record user operation.

**Examples** Ruijie(config)# logging userinfo command-log

**Related  
Commands**

Command	Description
N/A	N/A

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

## 7.25 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** Global configuration mode  
**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

## 7. 26 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 FastEthernet 0/24,
changed state to up.
015488: *Sep 19 02:46:13: Ruijie %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet 0/24, changed state to up.
015489: *Sep 19 02:46:26: Ruijie %LINK-3-UPDOWN: Interface FastEthernet 0/24,
changed state to down.
015490: *Sep 19 02:46:26: Ruijie %LINEPROTO/A5N/AUPDOWN: Line protocol on
Interface FastEthernet 0/24, changed state to down.
015491: *Sep 19 02:46:28: Ruijie %LINKN/A3N/AUPDOWN: Interface FastEthernet
0/24, changed state to up.
015492: *Sep 19 02:46:28: Ruijie %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet 0/24, changed state to up.
```

Log information description:

Field	Description
Syslog logging	Logging flag: enabled or disabled
Console logging	Level of the logs printed on the console, and statistics
Monitor logging	Level of the logs printed on the VTY window, and statistics
Buffer logging	Level of the logs recorded in the memory buffer, and statistics.
Standard format	Standard log format.
Timestamp debug messages	Timestamp format of the Debug messages
Timestamp log messages	Timestamp format of the Log messages
Sequence-number log messages	Serial number switch
Sequence log messages	Attaches system names to the logs.
Count log messages	Log statistics function
Trap logging	Level of the logs sent to the syslog server, and statistics
Log Buffer	Log files recorded in the memory buffer

The following example displays the result of the **show logging** command with RFC5424 format enabled.

```
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
<b>logging on</b>	Turns on the log switch.
<b>clear logging</b>	Clears the log messages in the buffer.

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

## 7.27 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

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

<b>Commands</b>		
	N/A	N/A

**Platform** N/A

**Description**

## 7.28 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

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

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** To use the log packet statistics function, run the **logging count** command in global configuration mode. The **show logging count** command can show the information of a specific log, occurrence times, and the last occurrence time.

You can use the **show logging** command to check whether the log statistics function is enabled.

**Configuration Examples** The following example displays the result of the **show logging count** command:

```
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
```

<b>Related Commands</b>	<b>Command</b>	<b>Function</b>
	<b>logging count</b>	Enables the log statistics function.
	<b>show logging</b>	Displays basic configuration of log modules and log information in the buffer.
	<b>clear logging</b>	Clears the logs in the buffer.

**Platform Description** N/A



## 7.29 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

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

```
Ruijie#show logging reverse
Syslog logging: disabled
  Console logging: level debugging, 14 messages logged
  Monitor logging: level informational, 0 messages logged
  Buffer logging: level debugging, 15 messages logged
  File logging: level informational, 15 messages logged
  File name:syslog.txt, size 128 Kbytes, have written 1 files
  Statistic log messages: disable
  Statistic log messages to terminal: disable
  Delay-send log messages to terminal: disable
  Delay-send file name:syslog_ftp_server, Current write index:0, Current send
index:0, Cycle:3600 seconds
  Count log messages: disable
  Trap logging: level informational, 15 message lines logged,0 fail
  logging to 202.101.11.1
  logging to 202.101.11.22
  logging to 2001::1
  Delay-send logging: 0 message lines logged
Log Buffer (Total 131072 Bytes): have written 1413,
*Jan 1 00:20:31: %SYSLOG-6-DEBUG_PRINT: The debug print time 20 minutes has
expired!
*Jan 1 00:14:19: %SYS-5-CONFIG_I: Configured from console by console
*Jan 1 00:01:52: %DHCP_CLIENT-6-ADDRESS_ASSIGN: Interface VLAN 1 assigned
DHCP address 10.52.24.158, mask 255.255.248.0.
```

```
*Jan 1 00:01:44: %ARP-4-DUPADDR: Duplicate address 192.168.1.200 on interface
VLAN 1 port GigabitEthernet 0/18, sourced by 8005.8800.8249.
*Jan 1 00:01:44: %LINEPROTO-5-UPDOWN: Line protocol on Interface VLAN 1,
changed state to up.
*Jan 1 00:01:42: %LLDP-4-CREATEREM: Port GigabitEthernet 0/18 created one new
neighbor, Chassis ID is 7401.9000.0000, Port ID is Gi0/5.
*Jan 1 00:01:42: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet 0/18, changed state to up.
*Jan 1 00:01:42: %LINK-3-UPDOWN: Interface GigabitEthernet 0/18, changed
state to up.
*Jan 1 00:00:39: %DEV_MONITOR-6-DEVICE_INIT: master role init.
*Jan 1 00:00:32: %SYSMON-5-WARMSTART: System warmstart.
*Jan 1 00:00:32: %DEV_MONITOR-5-CARD_POWER_ON: The power enough, card in slot
0 will be controlled to power on automatically.
*Jan 1 00:00:30: %DP-5-PROB: Board probing has completed.
*Jan 1 00:00:29: %DP-6-MASTER: Module in slot 0 has translated to master.
*Jan 1 00:00:29: %SWITCH-6-INSTALL: Install chassis RG-HS2310-16GH2GT1XS on
switch 1
*Jan 1 00:00:27: %LOCAL_DP-5-LC_PROB: Board information in this chassis has
been collected.
```

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: disabled
  Console logging: level debugging, 14 messages logged
  Monitor logging: level informational, 0 messages logged
  Buffer logging: level debugging, 15 messages logged
  File logging: level informational, 15 messages logged
  File name:syslog.txt, size 128 Kbytes, have written 1 files
  Statistic log messages: disable
  Statistic log messages to terminal: disable
  Delay-send log messages to terminal: disable
  Delay-send file name:syslog_ftp_server, Current write index:0, Current send
index:0, Cycle:3600 seconds
  Count log messages: disable
  Trap logging: level informational, 15 message lines logged,0 fail
    logging to 202.101.11.1
    logging to 202.101.11.22
    logging to 2001::1
  Delay-send logging: 0 message lines logged
Log Buffer (Total 131072 Bytes): have written 1413,
*Jan 1 00:20:31: %SYSLOG-6-DEBUG_PRINT: The debug print time 20 minutes has
expired!
*Jan 1 00:14:19: %SYS-5-CONFIG_I: Configured from console by console
*Jan 1 00:01:52: %DHCP_CLIENT-6-ADDRESS_ASSIGN: Interface VLAN 1 assigned
DHCP address 10.52.24.158, mask 255.255.248.0.
*Jan 1 00:01:44: %ARP-4-DUPADDR: Duplicate address 192.168.1.200 on interface
VLAN 1 port GigabitEthernet 0/18, sourced by 8005.8800.8249.
*Jan 1 00:01:44: %LINEPROTO-5-UPDOWN: Line protocol on Interface VLAN 1,
changed state to up.
*Jan 1 00:01:42: %LLDP-4-CREATEREM: Port GigabitEthernet 0/18 created one new
neighbor, Chassis ID is 7401.9000.0000, Port ID is Gi0/5.
*Jan 1 00:01:42: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet 0/18, changed state to up.
*Jan 1 00:01:42: %LINK-3-UPDOWN: Interface GigabitEthernet 0/18, changed
state to up.
*Jan 1 00:00:39: %DEV_MONITOR-6-DEVICE_INIT: master role init.
*Jan 1 00:00:32: %SYSMON-5-WARMSTART: System warmstart.
*Jan 1 00:00:32: %DEV_MONITOR-5-CARD_POWER_ON: The power enough, card in slot
0 will be controlled to power on automatically.
*Jan 1 00:00:30: %DP-5-PROB: Board probing has completed.
*Jan 1 00:00:29: %DP-6-MASTER: Module in slot 0 has translated to master.
*Jan 1 00:00:29: %SWITCH-6-INSTALL: Install chassis RG-HS2310-16GH2GT1XS on
switch 1
*Jan 1 00:00:27: %LOCAL_DP-5-LC_PROB: Board information in this chassis has
```

been collected.

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

### 7.30 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	Command	Description
Commands	N/A	N/A

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

Command	Version	Description
History	N/A	N/A

## 8 Monitoring Commands

### 8.1 show power

Use this command to display power information including that of its basic condition, redundancy, allocation and version and etc.

**show power**

Parameter Description	Parameter	Description
	N/A	N/A

**Command Mode** Privileged EXEC mode

**Level** 14

**Usage Guide** This command is used to display power information

**Configuration Examples** N/A

**Prompt Messages** N/A

**Platforms** N/A

### 8.2 show temperature

Use this command to display board temperature, threshold configuration and other information.

**show temperature**

Parameter Description	Parameter	Description
	N/A	N/A

**Command Mode** Privileged EXEC mode

**Level** 14

**Usage Guide** Use the command to display the current temperature and threshold configuration of each board. The temperature threshold of CA products involves the alarm threshold and the hazard threshold. Alarm threshold: When the temperature of the board exceeds the alarm threshold, the active supervisor module generates a Syslog message and the Alarm LED on the panel becomes yellow. Hazard threshold: It indicates the power-off temperature. When the temperature of the board exceeds the hazard threshold, the board powers off automatically. In addition, the active supervisor module generates a Syslog message and the Alarm LED on the panel becomes red.

**Configuration** The following example displays the temperature and threshold configuration of all boards of S29XS.

**Examples**

```
Ruijie(config)#show temperature
Slot    Card_type                Temp_name                Current (C)  Status
-----
0       RG-HS2310-16GH2GT1XS    fan_out                  N/A
critical
       RG-HS2310-16GH2GT1XS    ghn_inlet                N/A
critical
       RG-HS2310-16GH2GT1XS    air_inlet                N/A
critical
Ruijie(config)#
```

**Prompt Messages** N/A

**Platforms** N/A

### 8.3 show fan

Use this command to display fan status or speed.  
show fan

Parameter Description	Parameter	Description
	N/A	N/A

**Command Mode** Privileged EXEC mode

**Level** NA

- Usage Guide** Run this command to view the current fan status and speed of each board.
- CA fan thresholds include alarm thresholds and hazard thresholds.
- Alarm threshold: When the speed of a single fan on a board is lower than the alarm threshold, the active monitoring module generates a syslog alarm, and the alarm indicator and status indicator on the panel keep on.
- Danger threshold: When all fan speeds are lower than the alarm threshold, the active monitoring module generates a syslog alarm, the alarm indicator on the panel keeps on, and the status indicator is off.

**Configuration** The following example displays the fan status.

**Examples**

```
Ruijie#show fan
Fan-id Status
-----
1      ok
2      ok
Ruijie#
```

The following example displays the fan speed.

```
Ruijie#show fan speed
Fan-id Status      Speed (R/m)  Speed-level
-----
1      ok          7800        1
2      ok          7680        1
Ruijie#
```

**Prompt Messages** N/A

**Platforms** N/A