

# Table of Contents

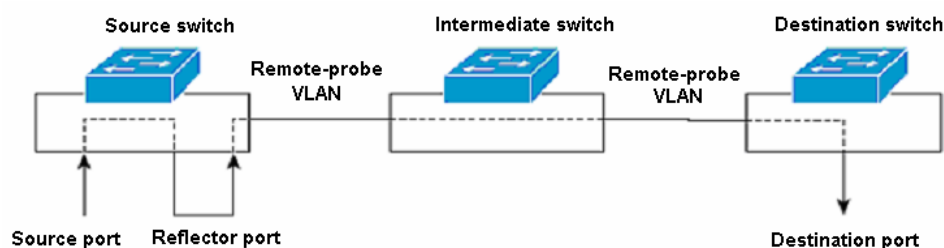
<b>Chapter 1 Configuration for QoS Newly Added Features .....</b>	<b>1-1</b>
1.1 RSPAN Features .....	1-1
1.1.1 Configuration Prerequisite.....	1-2
1.1.2 Configuration Procedures in the Source Switch .....	1-3
1.1.3 Configuration Procedures in the Intermediate Switch.....	1-4
1.1.4 Configuration Procedures in the Source Switch .....	1-4
1.1.5 Configuration Example.....	1-5
1.2 Newly Added Features of Traffic Statistics.....	1-7
1.3 Improving the Depth First Order of ACL Matching .....	1-7
1.4 Newly Added Displaying Information of the display acl command .....	1-8
1.5 Subdividing DSCP while Defining ACL Rules .....	1-8
1.6 Delivery of ACL by RADIUS .....	1-9
1.7 The Synchronization Feature of Queue Scheduling for Aggregation Ports.....	1-9
1.8 Configuring the Priority for Protocol Packets.....	1-10
1.9 Configuring Control Over Telnet.....	1-11
1.9.1 Configuration Preparation .....	1-11
1.9.2 Controlling Telnet via Source IP.....	1-11
1.9.3 Controlling Telnet via Source IP and Destination IP .....	1-12
1.9.4 Controlling Telnet via Source MAC .....	1-13
1.9.5 Configuration Example.....	1-14
<b>Chapter 2 QoS Commands for Newly Added Features .....</b>	<b>2-1</b>
2.1 QoS Commands for Newly Added Features .....	2-1
2.1.1 display mirroring-group .....	2-1
2.1.2 display protocol-priority .....	2-2
2.1.3 mirroring-group.....	2-2
2.1.4 mirroring-group mirroring-port.....	2-3
2.1.5 mirroring-group monitor-port .....	2-4
2.1.6 mirroring-group reflector-port .....	2-4
2.1.7 mirroring-group remote-probe vlan .....	2-5
2.1.8 protocol-priority protocol-type.....	2-6
2.1.9 remote-probe vlan .....	2-6

# Chapter 1 Configuration for QoS Newly Added Features

## 1.1 RSPAN Features

Remote switched port analyzer (RSPAN) refers to remote port mirroring. It breaks through the limitation that the mirrored port and the mirroring port have to be located in the same switch, and makes it possible that the mirrored and mirroring ports be located across several devices in the network, and greatly enhances the way that the network administrator can manage the switch.

The application of RSPAN is illustrated in the following figure:



**Figure 1-1** RSPAN application

There are three types of switches with the RSPAN enabled.

- Source switch: the switch to which the monitored port belong.
- Intermediate switch: the switches that are between the source and destination switches on the network.
- Destination switch: the switch to which the remote mirroring destination port belong.

The following figure gives an illustration of how various ports are involved in the mirroring operation.

**Table 1-1** The ports involved in the mirroring

Switch	The ports involved	Function
Source switch	Source port	The port to be mirrored. By means of local port mirroring, the users' data packets can be copied to the reflector port. There could be more than one source port.
	Reflector port	Receive users' data packets that are mirrored on a local port.
	Trunk port	Send the mirrored packets to the intermediate switch or the destination switch.
Intermediate switch	Trunk port	Send the mirrored packets to the destination switch. Two Trunk ports are necessary for the intermediate switch in order to connect with devices from both the source and destination switches.
Destination switch	Trunk port	Receive remote mirrored packets.
	Destination port	Monitor the remote mirrored packets

To implement the remote port management, a special VLAN, called Remote-probe VLAN, needs to be defined in all three types of switches. All the mirrored packets will be forwarded to destination switch from the source switch via this VLAN, and therefore the destination switch can monitor the port packets sent from the source switch.

Remote-probe VLAN has the following characteristics:

- None of the ports in this VLAN should have their PVID (Port VLAN ID) set as Remote-probe VLAN ID.
- All the ports in this VLAN must be Trunk ports, rather than Access ports or Hybrid ports.
- The default VLAN, Management VLAN, Fabric VLAN, and Protocol VLAN cannot be configured as Remote-probe VLAN.
- Remote-probe VLAN cannot have the source ports of remote mirroring.

### 1.1.1 Configuration Prerequisite

- Specify the source switch, intermediate switch, and the destination switch.
- Specify the source port, the reflector port, the destination port, and the Remote-probe VLAN.
- Specify whether the packets to be monitored are inbound or outbound.
- Intermediate switch and source switch support the function of MAC-learning-disabled-based-on-VLAN, which also is enabled for Remote-probe VLAN.

## 1.1.2 Configuration Procedures in the Source Switch

**Table 1-2** Configuration procedures in the source switch

Operation	Command	Description
Enter system view	<b>system-view</b>	—
Establish Remote-probe VLAN, and enter VLAN view	<b>vlan</b> <i>vlan-id</i>	The parameter <i>vlan-id</i> represents the ID of the Remote-probe VLAN.
Define the current VLAN as Remote-probe VLAN	<b>remote-probe enable</b>	Required.
Exit the current view	<b>quit</b>	—
Enter the Ethernet port view of Trunk ports	<b>interface</b> <i>interface-type</i> <i>interface-number</i>	—
Configure Trunk ports so that packets of the Remote-probe VLAN can pass through	<b>port trunk permit vlan</b> <i>remote-probe-vlan-id</i>	Required.
Exit the current view	<b>quit</b>	—
Configure the source group of remote mirroring	<b>mirroring-group</b> <i>group-id</i> <b>remote-source</b>	Required.
Configure the source ports of remote mirroring	<b>mirroring-group</b> <i>group-id</i> <b>mirroring-port</b> <i>mirroring-port-list</i> { <b>both</b>   <b>inbound</b>   <b>outbound</b> }	Required.
Configure the reflector ports of remote mirroring	<b>mirroring-group</b> <i>group-id</i> <b>reflector-port</b> <i>reflector-port</i>	Required. The reflector ports of remote mirroring cannot enable STP, and have to be Access ports. The reflector ports cannot have the <i>vlan-vpn</i> commands configured.
Configure the remote-probe VLAN for the source group of remote mirroring	<b>mirroring-group</b> <i>group-id</i> <b>remote-probe vlan</b> <i>remote-probe-vlan-id</i>	Required.
Display the configuration for the source group of remote mirroring	<b>display mirroring-group</b> <b>remote-source</b>	Optional. The <b>display</b> command can be used under any view.

### 1.1.3 Configuration Procedures in the Intermediate Switch

**Table 1-3** Configuration procedures in the intermediate switch

Operation	Command	Description
Enter system view	<b>system-view</b>	—
Establish remote-probe VLAN, and enter VLAN view	<b>vlan</b> <i>vlan-id</i>	The parameter <i>vlan-id</i> represents the ID of the remote-probe VLAN.
Exit the current view	<b>quit</b>	—
Enter the Ethernet port view of Trunk ports	<b>interface</b> <i>interface-type</i> <i>interface-number</i>	—
Configure Trunk ports so that packets in the remote-probe VLAN can pass through	<b>port trunk permit vlan</b> <i>remote-probe-vlan-id</i>	Required. This configuration is necessary for ports of intermediate switch that are connected with the source switch or the destination switch.

### 1.1.4 Configuration Procedures in the Source Switch

**Table 1-4** Configuration procedures in the source switch

Operation	Command	Description
Enter system view	<b>system-view</b>	—
Establish remote-probe VLAN, and enter VLAN view	<b>vlan</b> <i>vlan-id</i>	The parameter <i>vlan-id</i> represents the ID of the remote-probe VLAN.
Define the current VLAN as remote-probe VLAN.	<b>remote-probe enable</b> <b>vlan</b>	Required.
Exit the current view	<b>quit</b>	—
Enter the Ethernet port view of Trunk ports	<b>interface</b> <i>interface-type</i> <i>interface-number</i>	—
Configure Trunk ports so that packets in the remote-probe VLAN can pass through	<b>port trunk permit vlan</b> <i>remote-probe-vlan-id</i>	Required.
Exit the current view	<b>quit</b>	—
Configure the destination group of remote mirroring	<b>mirroring-group</b> <i>group-id</i> <b>remote-destination</b>	Required.

Operation	Command	Description
Configure the destination ports of remote mirroring	<b>mirroring-group</b> <i>group-id</i> <b>monitor-port</b> <i>monitor-port</i>	Required. The destination ports of remote mirroring cannot enable STP. Once a port has been configured as a destination port of remote mirroring, its port type and default VLAN ID can no longer be modified.
Configure the remote-probe VLAN for the destination group of remote mirroring	<b>mirroring-group</b> <i>group-id</i> <b>remote-probe vlan</b> <i>remote-probe-vlan-id</i>	Required.
Display the configuration of destination group of remote mirroring	<b>display mirroring-group remote-destination</b>	Optional. The <b>display</b> command can be used under any view.

## 1.1.5 Configuration Example

### I. Network diagram requirements

The network description is as follows:

- Switch A is connected to the data monitoring device via GigabitEthernet1/0/2.
- GigabitEthernet, the Trunk port of Switch A, is connected to GigabitEthernet 1/0/1, the Trunk port of Switch B.
- GigabitEthernet1/0/2, the Trunk port of Switch B, is connected to GigabitEthernet 1/0/1, the Trunk port of Switch C.
- GigabitEthernet1/0/2, the port of Switch C, is connected to PC1.

The requirement is to monitor and analyze the packets sent to PC1 via the data monitoring device.

To meet the above requirement using the RSPAN function, perform the following configurations:

- Define VLAN10 as remote-probe VLAN.
- Configure Switch A to be the destination switch, GigabitEthernet1/0/2, the port that connects the data monitoring device, to be the destination port of remote mirroring. Disable the STP function for GigabitEthernet1/0/2.
- Configure Switch B to be the intermediate switch.
- Configure Switch C to be the source switch, GigabitEthernet1/0/2 to be the source port of remote mirroring, and GigabitEthernet1/0/5 to be the reflector port. Set GigabitEthernet1/0/5 to be Access port, with STP disabled.

## II. Network Diagram

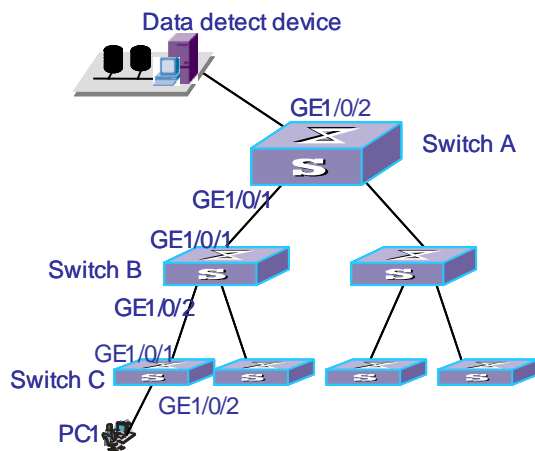


Figure 1-2 Network diagram for RSPAN

## III. Configuration Procedure

### # Configure Switch C.

```
<Quidway> system-view
[Quidway] vlan 10
[Quidway-vlan10] remote-probe vlan enable
[Quidway-vlan10] quit
[Quidway] interface gigabitEthernet1/0/1
[Quidway-GigabitEthernet1/0/1] port trunk permit vlan 10
[Quidway-GigabitEthernet1/0/1] quit
[Quidway] mirroring-group 1 remote-source
[Quidway] mirroring-group 1 mirroring-port gigabitEthernet1/0/2 outbound
[Quidway] mirroring-group 1 reflector-port gigabitEthernet1/0/5
[Quidway] mirroring-group 1 remote-probe vlan 10
[Quidway] display mirroring-group remote-source
```

### # Configure Switch B.

```
<Quidway> system-view
[Quidway] vlan 10
[Quidway-vlan10] quit
[Quidway] interface gigabitEthernet1/0/1
[Quidway-GigabitEthernet1/0/1] port trunk permit vlan 10
[Quidway-GigabitEthernet1/0/1] quit
[Quidway] interface gigabitEthernet1/0/2
[Quidway-GigabitEthernet1/0/2] port trunk permit vlan 10
```

### # Configure Switch A.

```
<Quidway> system-view
```

```
[Quidway] vlan 10
[Quidway-vlan10] remote-probe vlan enable
[Quidway-vlan10] quit
[Quidway] interface gigabitethernet1/0/1
[Quidway-GigabitEthernet1/0/1] port trunk permit vlan 10
[Quidway-GigabitEthernet1/0/1] quit
[Quidway] mirroring-group 1 remote-destination
[Quidway] mirroring-group 1 monitor-port gigabitethernet1/0/2
[Quidway] mirroring-group 1 remote-probe vlan 10
[Quidway] display mirroring-group remote-destination
```

## 1.2 Newly Added Features of Traffic Statistics

Traffic statistics is employed to count data packets within a specified traffic flow. Traffic statistics counts data information in the data packets that match a defined access control list (ACL).

The newly added features of traffic statistics allow the switch to count data packets with their action defined as deny in the ACL rules.

For detailed configuration regarding traffic statistics, refer to the QoS/ACL part of *Quidway S5600 Series Ethernet Switches Operation Manual*.

## 1.3 Improving the Depth First Order of ACL Matching

The depth first order of ACL matching can be configured by selecting auto option while defining the ACL matching order.

The priority sequence is determined based on the following rules:

- 1) Compare the protocol range of the ACL rules first. The range for IP protocol is 0 to 255 and those of other protocols are the same as their protocol numbers. The smaller the protocol range, the higher the priority.
- 2) Compare the range of source IP addresses. Those with smaller source IP address range have higher priority.
- 3) Compare the range of destination IP addresses. Those with smaller destination IP address range have higher priority.
- 4) Compare the Layer 4 port numbers (the TCP/UDP port numbers). Those with smaller range have higher priority.
- 5) While all the above checks show the same priority, sort according to the configuration order.

In the new version of the software, improvements have been made based on the above matching order, as illustrated below.

- If rule A is rule B's proper subset, then rule B has a higher priority.
- If based on the original matching order, rule A and rule B are the same in all the following aspects: the range of their protocols, the range of their source IP address,



the range of their destination IP address, and their Layer 4 port numbers, and furthermore, their numbers of other elements to be considered in deciding their priority order are also the same, weighting principles will be used in deciding their priority order.

The weighting principles work as follows:

- Each element is given a fixed weighting value. This weighting value and the value of the element itself will jointly decide the final matching order.
- The weighting value for each element ranks in the following descending order: DSCP, ToS, ICMP, established, VPN-instance, precedence, fragment.
- A fixed weighting value is deducted from the weighting value of each element of the rule. The rule with the smallest weighting value left has the highest priority.
- If the number and type of elements are the same for all rules, then the rule with the smallest sum value of all its elements has the highest priority.

For more ACL configuration, refer to the QoS/ACL part of the *Quidway S5600 Series Ethernet Operation Manual*.

## 1.4 Newly Added Displaying Information of the display acl command

The **display acl** command has included the total number of ACLs as newly added displaying information:

For example:

```
<Quidway> display acl all
Total ACL Number: 1
Advanced ACL 3000, 1 rule
Acl's step is 1
rule 0 permit ip
```

For more information on the **display acl** command, refer to the QoS/ACL part of the *Quidway S5600 Series Ethernet Command Manual*.

## 1.5 Subdividing DSCP while Defining ACL Rules

The new version has subdivided the value range of DSCP while defining the ACL rules, as illustrated in the following table:

**Table 1-5** Detailed information on subdivision of DSCP Priority

Before subdivision	After subdivision	DSCP value(in binary format)	DSCP value(in decimal format)
af1	af11	001010	10
	af12	001100	12
	af13	001110	14

Before subdivision	After subdivision	DSCP value(in binary format)	DSCP value(in decimal format)
af2	af21	010010	18
	af22	010100	20
	af23	010110	22
af3	af31	011010	26
	af32	011100	28
	af33	011110	30
af4	af41	100010	32
	af42	100100	34
	af43	100110	36

When updating the software, the device automatically converts the fields af1, af2, af3, af4 in the old DSCP configuration into af11, af21, af31, af41 respectively.

For more information on the ACL commands, refer to the QoS/ACL part of the *Quidway S5600 Series Ethernet Command Manual*.

## 1.6 Delivery of ACL by RADIUS

Delivery of ACL by RADIUS requires corporation of devices and the CAMS server.

Users need to first define the ACL which is of numeric type, and then deliver the ACL to the hardware of the devices in the CAMS server through the configuration of external groups.

For information on how to define ACL of numeric type, refer to *Quidway S5600 Series Ethernet Switch Operation Manual*.

## 1.7 The Synchronization Feature of Queue Scheduling for Aggregation Ports

This feature provides the synchronization function of queue scheduling on each individual port of the aggregation port group, as illustrated as follows:

- 1) The new feature supports the synchronization of queue scheduling within the aggregation port group.

When users modify or delete the queue scheduling mode for a given port under Ethernet port view, if the port belongs to an aggregation port group, then the queue scheduling modes for all the other ports will be modified or deleted; if the port does not belong to any aggregation port group, then only the queue scheduling mode for this port will be modified or deleted.

## 2) Queue scheduling supports dynamic aggregation.

If the port is in the UP state, and the LACP feature of the port is also enabled, then ports with the same queue scheduling information can be aggregated as a group.

Queue scheduling of ports supports static and manual aggregation.

Users can include those ports with their queue scheduling features configured in a static or manual aggregation group. This operation can be done either on a local device or in an IRF across various devices.

The new feature also supports the use of the **copy** command to copy the queue scheduling configuration.

For more configurations on queue scheduling, refer to the QoS/ACL part of the *Quidway S5600 Series Ethernet Operation Manual*. For further information on the **copy** command, refer to *Quidway S5600 Series Ethernet Operation Manual*.

## 1.8 Configuring the Priority for Protocol Packets

Each protocol packet has its own priority. Users can modify the priority of the protocol packet, and, with the help of relevant QoS commands, perform corresponding QoS operations.

Configuration procedures are as follows:

**Table 1-6** Configure the priority for a protocol packet

Operation	Command	Description
Enter system view	<b>system-view</b>	—
Configure the priority of the protocol packet	<b>protocol-priority</b> <b>protocol-type</b> <i>protocol-type</i> { <b>ip-precedence</b>   <b>dscp</b> <i>ip-precedence</i>   <i>dscp-value</i> }	Required. Users can modify the IP priority or DSCP priority of the protocol packet.
Display the priority of a protocol packet.	<b>display protocol-priority</b>	Optional. The <b>display</b> command can be used under any view.

To remove the relevant configuration, use the **undo** command.



### Caution:

Currently only packets of OSPF, LNET, MP, and MP can have their priorities modified.

---

## I. Configuration example for setting priority of a protocol packet

- 1) Change OSPF protocol packets' IP priority to be 3. Enter system view.

```
<Quidway> system-view
```

```
[Quidway]
```

- 2) Set OSPF protocol packets' IP priority to be 3.

```
[Quidway] protocol-priority protocol-type OSPF ip-precedence 3
```

- 3) Display the priority of protocol packets.

```
[Quidway] display protocol-priority
```

## 1.9 Configuring Control Over Telnet

**Table 1-7** Control over logged in users

Login mode	Control Method	Implementation	Relevant links
Telnet	Control Telnet via source IP	Implement by means of basic ACL	<a href="#">1.9.2 Controlling Telnet via Source IP</a>
	Control Telnet via source IP and destination IP	Implement by means of advanced ACL	<a href="#">1.9.3 Controlling Telnet via Source IP and Destination IP</a>
	Control Telnet via source MAC	Implement by means of Layer 2 ACL	<a href="#">1.9.3 Controlling Telnet via Source MAC</a>

### 1.9.1 Configuration Preparation

Decide the control policy over Telnet, configuring the source IP, destination IP, and source MAC to control over. Also specify whether the control action is permitting or denying access.

### 1.9.2 Controlling Telnet via Source IP

This configuration can be implemented by means of basic ACL, which ranges from 2000 to 2999.

**Table 1-8** Control Telnet via source IP

Configuration Procedure	Command	Description
Enter system view	system-view	—
Create or enter basic ACL view	<b>acl number</b> <i>acl-number</i> [ <b>match-order</b> { <b>config</b>   <b>auto</b> } ]	By default, the matching order is <b>config</b> .

Configuration Procedure	Command	Description
Define the rule	<b>rule</b> [ <i>rule-id</i> ] { <b>permit</b>   <b>deny</b> } [ <b>source</b> { <i>sour-addr</i> <i>sour-wildcard</i>   <b>any</b> } ] [ <b>time-range</b> <i>time-name</i> ] [ <b>fragment</b> ]	Required.
Exit ACL view	<b>quit</b>	—
Enter user interface view	<b>user-interface</b> [ <i>type</i> ] <i>first-number</i> [ <i>last-number</i> ]	—
Reference an ACL, and control Telnet via source IP	<b>acl</b> <i>acl-number</i> { <b>inbound</b>   <b>outbound</b> }	Required. <b>inbound</b> : Performs ACL control over users Telnetting to the local switch.. <b>outbound</b> : Performs ACL control over users Telnetting to other switches from the local switch..

### 1.9.3 Controlling Telnet via Source IP and Destination IP

This configuration can be implemented by means of advanced ACL, which ranges from 3000 to 3999. For the definition of ACL, refer to ACL part.

**Table 1-9** Control Telnet via source IP and destination IP

Configuration Procedure	Command	Description
Enter system view	<b>system-view</b>	—
Create or enter advanced ACL view	<b>acl</b> <b>number</b> <i>acl-number</i> [ <b>match-order</b> { <b>config</b>   <b>auto</b> } ]	By default, the matching order is <b>config</b> .

Configuration Procedure	Command	Description
Define the rule	<b>rule</b> [ <i>rule-id</i> ] { <b>permit</b>   <b>deny</b> } <i>protocol</i> [ <b>source</b> { <i>source-addr wildcard</i>   <b>any</b> } ] [ <b>destination</b> { <i>dest-addr wildcard</i>   <b>any</b> } ] [ <b>source-port</b> <i>operator port1</i> [ <i>port2</i> ] ] [ <b>destination-port</b> <i>operator port1</i> [ <i>port2</i> ] ] [ <b>icmp-type</b> <i>type code</i> ] [ <b>established</b> ] [ [ { <b>precedence</b> <i>precedence tos tos</i>   <b>dscp</b> <i>dscp</i> }* ]   <b>vpn-instance</b> <i>instance</i> ]   <b>fragment</b>   <b>time-range</b> <i>name</i> ]*	Required. Users can configure the filtering rules for the related source IP and destination IP based on actual requirements.
Exit ACL view	<b>quit</b>	—
Enter user interface view	<b>user-interface</b> [ <i>type</i> ] <i>first-number</i> [ <i>last-number</i> ]	—
Refer to ACL, and control Telnet via source IP and destination IP	<b>acl</b> <i>acl-number</i> { <b>inbound</b>   <b>outbound</b> }	Required. <b>inbound</b> : Performs ACL control over users Telnetting from the local switch. <b>outbound</b> : Performs ACL control over users Telnetting to other switches from the local switch.

### 1.9.4 Controlling Telnet via Source MAC

This configuration can be implemented by means of Layer 2 ACL, which ranges from 4000 to 4999. For the definition of ACL, refer to ACL part.

**Table 1-10** Control Telnet via Source MAC

Configuration Procedure	Command	Description
Enter system view	<b>system-view</b>	—
Create or enter Layer 2 ACL view	<b>acl number</b> <i>acl-number</i>	—

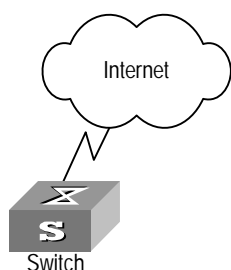
Configuration Procedure	Command	Description
Define the subset principle	<pre>rule [ rule-id ] { permit   deny } [ [ type protocol-type type-mask / lsap lsap-type type-mask ]   format-type   cos cos   source { source-vlan-id   source-mac-addr source-mac-mask }*   dest { dest-mac-addr dest-mac-mask }   time-range name ]*</pre>	Required. Users can configure the filtering rules for the related source MAC based on actual requirements.
Exit ACL view	<b>quit</b>	—
Enter user interface view	<b>user-interface</b> [ type ] first-number [ last-number ]	—
Reference an ACL, and control Telnet via source MAC	<b>acl</b> acl-number { <b>inbound</b>   <b>outbound</b> }	Required. <b>inbound:</b> Perform ACL control over users Telnetting to the local switch. <b>outbound:</b> Performs ACL control over users Telnetting to other switches from the local switch.

## 1.9.5 Configuration Example

### I. Network requirements

Only Telnet users from 10.110.100.52 and 10.110.100.46 can access the switch.

### II. Network diagram



**Figure 1-3** Perform ACL control over Telnet users of the switch

### III. Configuration Procedure

#### # Define the basic ACL.

```
[Quidway] acl number 2000 match-order config
[Quidway-acl-basic-2000] rule 1 permit source 10.110.100.52 0
[Quidway-acl-basic-2000] rule 2 permit source 10.110.100.46 0
[Quidway-acl-basic-2000] rule 3 deny source any
[Quidway-acl-basic-2000] quit
```

#### # Reference an ACL.

```
[Quidway] user-interface vty 0 4
[Quidway-ui-vty0-4] acl 2000 inbound
```



## Chapter 2 QoS Commands for Newly Added Features

### 2.1 QoS Commands for Newly Added Features

#### 2.1.1 display mirroring-group

##### Syntax

```
display mirroring-group { group-id | all | local | remote-destination | remote-source }
```

##### View

Any view

##### Parameter

None

##### Description

Use the **display mirroring-group** command to display the parameter setting of a port mirroring group.

Local mirroring group information includes:

- Group number
- Group type: **local**
- Group state
- Information of the monitored port
- Information of the monitoring port

Information displayed on the destination mirroring group of remote mirroring includes:

- Group number
- Group type: **remote-destination**
- Group state
- Information of the destination port
- remote-probe vlan information

Information displayed on the source mirroring group of remote mirroring includes:

- Group number
- Group type: **remote-source**
- Group state
- Information of the source port

- Information of the reflector port
- remote-probe vlan information

### Example

# Display the parameter setting of the mirroring group.

```
<Quidway> display mirroring-group all
mirroring-group 1:
    type: local
    status: active
    mirroring port:
        GigabitEthernet1/0/1 inbound
    monitor port: GigabitEthernet1/0/2
```

## 2.1.2 display protocol-priority

### Syntax

**display protocol-priority**

### View

Any view

### Parameter

None

### Description

Use the **display protocol-priority** command to display the priority of protocol packets.

### Example

# Display the priority of protocol packets.

```
<Quidway> display protocol-priority
```

## 2.1.3 mirroring-group

### Syntax

**mirroring-group** *group-id* { **local** | **remote-destination** | **remote-source** }  
**undo mirroring-group** { *group-id* | **all** | **local** | **remote-destination** | **remote-source** }

### View

System view

Parameter *group-id*: Group number of a port mirroring group, in the range of 1 to 20.

**local**: The specified mirroring group is a local port mirroring group.

**remote-destination:** The specified mirroring group is the destination group of remote mirroring.

**remote-source:** The specified mirroring group is the source group of remote mirroring.

**all:** A parameter used while deleting the mirroring group, indicating all groups are being deleted

## Description

Use the **mirroring-group** command to configure the port mirroring group.

Use the **undo mirroring-group** command to delete the port mirroring group.

## Example

# Configure the mirroring group on the local switch.

```
<Quidway> system-view  
System View: return to User View with Ctrl+Z.  
[Quidway] mirroring-group 1 local
```

### 2.1.4 mirroring-group mirroring-port

#### Syntax

**mirroring-group** *group-id* **mirroring-port** *mirroring-port-list* { **both** | **inbound** | **outbound** }

**undo mirroring-group** *group-id* **mirroring-port** *mirroring-port-list* { **both** | **inbound** | **outbound** }

#### View

System view

#### Parameter

*group-id*: Group number of a port mirroring group, in the range of 1 to 20.

**mirroring-port** *mirroring-port-list*: The specified ACL for the monitored port.

**both**: Monitors both the inbound and outbound information of the port.

**inbound**: Only monitors inbound information of the port.

**outbound**: Only monitors outbound information of the port.

## Description

Use the **mirroring-group mirroring-port** command to configure the monitored port.

Use the **undo mirroring-group mirroring-port** command to remove the configuration of the monitored port.

## Example

# Configure GigabitEthernet1/0/1 to be the monitored port, monitor and control all the inbound information of this port.

```
<Quidway> system-view
```

System View: return to User View with Ctrl+Z.

```
[Quidway] mirroring-group 1 mirroring-port gigabitethernet1/0/1 inbound
```

## 2.1.5 mirroring-group monitor-port

### Syntax

**mirroring-group** *group-id* **monitor-port** *monitor-port*

**undo mirroring-group** *group-id* **monitor-port** *monitor-port*

### View

System view

### Parameter

*group-id*: Group number of a port mirroring group, in the range of 1 to 20.

**monitor-port** *monitor-port*: The specified port to be monitored.

### Description

Use the **mirroring-group monitor-port** command to configure the monitoring port.

Use the **undo mirroring-group monitor-port** command to remove the configuration of the monitoring port.

When a port is configured as a destination port of remote mirroring, its port type or default VLAN ID can no longer be modified.

## Example

# Configure GigabitEthernet1/0/2 to be the monitoring port.

```
<Quidway> system-view
```

System View: return to User View with Ctrl+Z.

```
[Quidway] mirroring-group 1 monitor-port gigabitethernet1/0/2
```

## 2.1.6 mirroring-group reflector-port

### Syntax

**mirroring-group** *group-id* **reflector-port** *reflector-port*

**undo mirroring-group** *group-id* **reflector-port** *reflector-port*

ViewSystem view

## Parameter

*group-id*: Group number of a port mirroring group, in the range of 1 to 20.

**reflector-port** *reflector-port*: The specified reflector port.

## Description

Use the **mirroring-group reflector-port** command to configure reflector port.

Use the **undo mirroring-group reflector-port** command to remove the configuration of the reflector port.

## Example

# Configure GigabitEthernet1/0/1 to be the reflector port, monitor and control all the inbound and outbound information of this switch.

```
<Quidway> system-view
```

```
System View: return to User View with Ctrl+Z.
```

```
[Quidway] mirroring-group 1 reflector-port gigabitethernet1/0/1
```

## 2.1.7 mirroring-group remote-probe vlan

### Syntax

**mirroring-group** *group-id* **remote-probe vlan** *remote-probe-vlan-id*

**undo mirroring-group** *group-id* **remote-probe vlan** *remote-probe-vlan-id*

### View

System view

### Parameter

*group-id*: The group number of a mirroring group, in the range of 1 to 20.

**remote-probe vlan** *remote-probe-vlan-id*: The remote-probe VLAN for a specified mirroring group.

### Description

Use the **mirroring-group remote-probe vlan** command to specify the remote-probe VLAN for a given mirroring group.

Use the **undo mirroring-group remote-probe vlan** command to delete the remote-probe VLAN configuration for a given mirroring group.

### Example

# Configure the remote-probe VLAN of mirroring group to be VLAN 100.

```
<Quidway> system-view
```

```
System View: return to User View with Ctrl+Z.
```

```
[Quidway] mirroring-group 1 remote-probe vlan 100
```

## 2.1.8 protocol-priority protocol-type

### Syntax

```
protocol-priority protocol-type protocol-type { ip-precedence ip-precedence | dscp dscp-value }  
undo protocol-priority protocol-type protocol-type
```

### View

System view

### Parameter

**protocol-type** *protocol-type*: Represents the protocol type, currently only supports OSPF, TELNET, SNMP, ICMP ( to be input in the form of strings in the command line).

**ip-precedence** *ip-precedence*: IP priority, in the range of 0 to 7.

**dscp** *dscp-value*: DSCP priority, in the range of 0 to 63.

### Description

Use the **protocol-priority** command to set the global traffic priority that applies to a given protocol.

Use the **undo protocol-priority** command to remove such a configuration.

### Example

# Set the IP priority of OSPF protocol to be 3.

```
<Quidway> system-view
```

System View: return to User View with Ctrl+Z.

```
[Quidway] protocol-priority protocol-type OSPF ip-precedence 3
```

## 2.1.9 remote-probe vlan

### Syntax

```
remote-probe vlan enable  
undo remote-probe vlan enable
```

### View

VLAN view

### Parameter

None

## Description

Use the **remote-probe vlan enable** command to enable the remote-probe port mirroring on the VLAN of a switch.

Use the **undo remote-probe vlan enable** command to disable the remote-probe port mirroring.

## Example

# Configure VLAN 5 to be remote-probe VLAN.

```
<Quidway> system-view
```

System View: return to User View with Ctrl+Z.

```
[Quidway] vlan 5
```

```
[Quidway-vlan5] remote-probe vlan enable
```