

ACL & QoS Configuration

Оглавление

| | |
|--------------------|-----|
| 1. CONFIGURING ACL | 3 |
| 1.2 Applications | 3 |
| 1.3 Features | 5 |
| 1.4 Configuration | 28 |
| 1.5 Monitoring | 77 |
| 2. CONFIGURING QOS | 79 |
| 2.1 Overview | 79 |
| 2.3 Features | 82 |
| 2.4 Configuration | 93 |
| 3. CONFIGURING MMU | 126 |
| 3.1 Overview | 126 |
| 3.2 Applications | 126 |
| 3.3 Features | 128 |
| 3.4 Configuration | 130 |
| 3.5 Monitoring | 135 |

1.1 Overview

Access control list (ACL) is also called access list or firewall. It is even called packet filtering in some documents. The ACL defines rules to determine whether to forward or drop data packets arriving at a network interface.

ACLs are classified by function into two types:

- Security ACLs: Used to control data flows that are allowed to pass through a network device.
- Quality of service (QoS) ACLs: Used to classify and process data flows by priority. ACLs are configured for a lot of reasons. Major reasons include:
 - Network access control: To ensure network security, rules are defined to limit access of users to some services (for example, only access to the WWW and email services is permitted, and access to other services such as Telnet is prohibited), or to allow users to access services in a specified period of time, or to allow only specified hosts to access the network.
 - QoS: QoS ACLs are used to preferentially classify and process important data flows. For details about the use of QoS ALCs, see the configuration manual related to QoS.

1.2 Applications

| Application | Description |
|---|---|
| Access Control of an Enterprise Network | On an enterprise network, the network access rights of each department, for example, access rights of servers and use permissions of chatting tools (such as QQ and MSN), must be controlled according to requirements. |

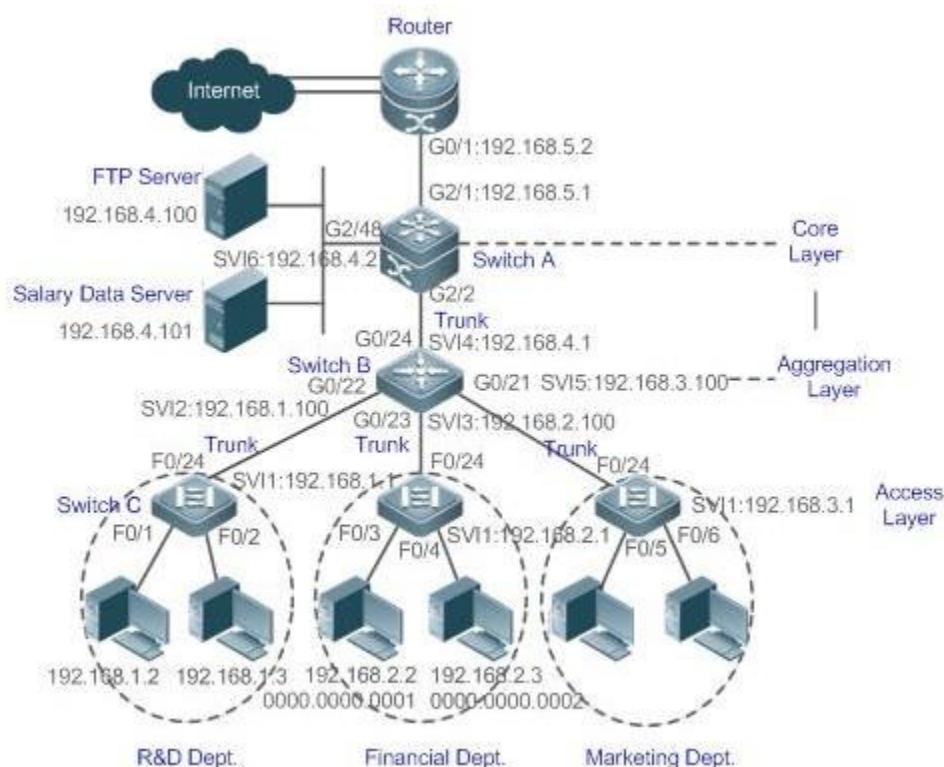
1.2.1 Access Control of an Enterprise Network Scenario

Internet viruses can be found everywhere. Therefore, it is necessary to block ports that are often used by viruses to ensure security of an enterprise network as follows:

- Allow only internal PCs to access the server.
- Prohibit PCs of a non-financial department from accessing PCs of the financial department, and prohibit PCs of a non-R&D department from accessing PCs of the R&D department.

- Prohibit the staff of the R&D department from using chatting tools (such as QQ and MSN) during working hours from 09:00 to 18:00.

Figure 1-1

**Remarks**

Switch C at the access layer:It is connected to PCs of each department and to Switch B at the aggregation layer through the gigabit optical fiber (trunk mode).

Switch B at the aggregation layer:Multiple virtual local area networks (VLANs) are divided. One VLAN is defined for one department. These VLANs are connected to Switch A at the core layer through the 10-gigabit optical fiber (trunk mode).

Switch A at the core layer:It is connected to various servers, such as the File Transfer Protocol (FTP) server and Hypertext Transfer Protocol (HTTP) server, and to the Internet through firewalls.

Deployment

- Configure an extended ACL on the port G2/1 to filter data packets, thus protecting the network against the viruses. This port is located on a core-layer device (Switch A) and used to connect Switch A to the uplink port G2/1 of a router.
- Allow only internal PCs to access servers, and prohibit external PCs from accessing servers. Define and apply the extended IP ACLs on G2/2 or

switch virtual interface (SVI) 2 that is used to connect Switch A to an aggregation layer device or server.

- Prohibit mutual access between specified departments. Define and apply the extended IP ACLs on G0/22 and G0/23 of Switch B.
- Configure and apply the time-based extended IP ACLs on SVI 2 of Switch B to prohibit the R&D department from using chatting tools (such as QQ and MSN) in a specified period of time.

1.3 Features

Basic Concepts

❖ ACL

ACLs include basic ACLs and dynamic ACLs.

You can select basic or dynamic ACLs as required. Generally, basic ACLs can meet the security requirements. However, experienced hackers may use certain software to access the network by means of IP address spoofing. If dynamic ACLs are used, users are requested to pass identify authentication before accessing the network, which prevents hackers from intruding the network. Therefore, you can use dynamic ACLs in some sensitive areas to guarantee network security.

IP address spoofing is an inherent problem of all ACLs, including dynamic ACLs. Hackers may use forged IP addresses to access the network during the validity period of authenticated user identities. Two methods are available to resolve this problem. One is to set the idle time of user access to a smaller value, which increases the difficulty in intruding networks. The other is to encrypt network data using the IPsec protocol, which ensures that all data is encrypted when arriving at a device.

ACLs are generally configured on the following network devices:

- Devices between the internal network and the external network (such as the Internet)
- Devices on the border of two network segments
- Devices connected to controlled ports

ACL statements must be executed in strict compliance with their sequence in the ACL. Comparison starts from the first statement. Once the header of a data packet matches a statement in the ACL, the subsequent statements are ignored and no longer checked.

❖ **Input/Output ACLs, Filtering Field Template, and Rules**

When receiving a packet on an interface, the device checks whether the packet matches any access control entry (ACE) in the input ACL of this interface. Before sending a packet through a interface, the device checks whether the packet matches any ACE in the output ACL of this interface.

When different filtering rules are defined, all or only some rules may be applied

simultaneously. If a packet matches an ACE, this packet is processed according to the action policy (permit or deny) defined in this ACE. ACEs in an ACL identify Ethernet packets based on the following fields in the Ethernet packets:

Layer 2 (L2) fields:

- 48-bit source MAC address (containing all 48 bits)
- 48-bit destination MAC address (containing all 48 bits)
- 16-bit L2 type field
- Layer 3 (L3) fields:
 - Source IP address field (All source IP address values can be specified, or the subnet can be used to define a type of data flows.)
 - Destination IP address field (All destination IP address values can be specified, or the subnet can be used to define a type of data flows.)
 - Protocol type field
- Layer 4 (L4) fields:
 - Either a TCP source or destination port is specified, or both are specified, or the range of the source or destination port is specified.
 - Either a UDP source or destination port is specified, or both are specified, or the range of the source or destination port is specified.

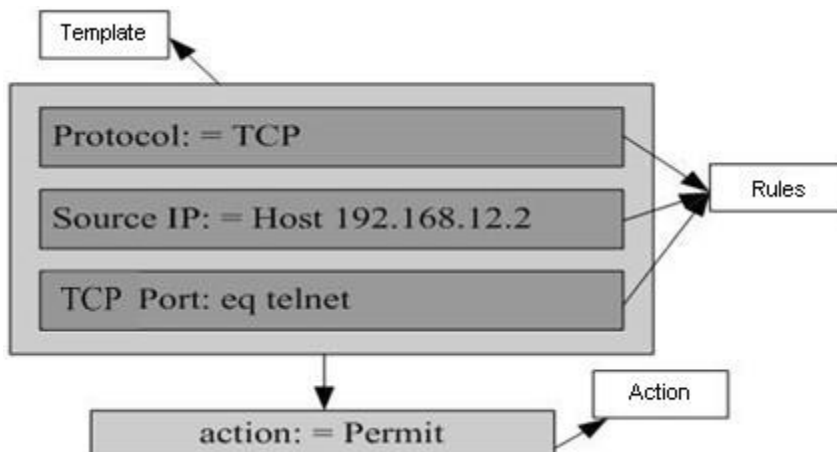
Filtering fields refer to the fields in packets that can be used to identify or classify packets when an ACE is generated. A filtering field template is a combination of these fields. For example, when an ACE is generated, packets are identified and classified based on the destination IP address field in each packet; when another ACE is generated, packets are identified and classified based on the source IP address field and UDP source port field in each packet. The two ACEs use different filtering field templates.

Rules refer to values of fields in the filtering field template of an ACE. For example, the content of an ACE is as follows:

```
permit tcp host 192.168.12.2 any eq telnet
```

In this ACE, the filtering field template is a combination of the following fields: source IP address field, IP protocol field, and TCP destination port field. The corresponding values (rules) are as follows: source IP address = Host 192.168.12.2; IP protocol = TCP; TCP destination port = Telnet.

Figure 1-2 Analysis of the ACE: permit tcp host 192.168.12.2 any eq telnet



On a switch, if ACLs are applied to the outgoing direction of a physical port or an aggregate port (AP), the ACLs can filter only well-known packets (unicast or multicast packets), but not unknown unicast packets. That is, for unknown or broadcast packets, ACLs configured in the outgoing direction of a port does not take effect.

On a switch, if the input ACL and DOT1X, global IP+MAC binding, port security, and IP source guard are shared among all ports, the permit and default deny ACEs do not take effect, but other deny ACEs take effect.

On a switch, if the input ACL and QoS are shared, the permit ACEs do not take effect, other deny ACEs take effect, and the default deny ACE takes effect after the QoS ACE takes effect.

On a switch, you can run the **norgos-security compatible** command to make the permit and deny ACEs take effect at the same time when the port-based input ACL and DOT1X, global IP+MAC binding, port security, and IP source guard are shared.

If ACEs are added to an ACL and then the switch is restarted after an ACL is applied to the incoming direction of multiple SVIs, the ACL may fail to be configured on some SVIs due to the limited hardware capacity.

If an expert ACL is configured and applied to the outgoing direction of an interface, and some ACEs in this ACL contain the L3 matching information (e.g. the IP address and L4 port), non-IP packets sent to the device from this interface cannot be controlled by the permit and deny ACEs in this ACL.

If ACEs of an ACL (IP ACL or expert extended ACL) are configured to match non-L2 fields (such as SIP and DIP), the ACL does not take effect on tagged MPLS packets.

❖ ACL Logging

To allow users better learn the running status of ACLs on a device, you can determine whether to specify the ACL logging option as required when adding ACEs. If this option is specified, logs are output when packets matching ACEs are found. ACL logs are displayed based on ACEs. That is, the device periodically displays ACEs with matched packets and the number of matched packets. An example of the log is as follows:

```
*Sep 9 16:23:06: %ACL-6-MATCH: ACL 100 ACE 10 permit icmp any any, match 78 packets.
```

To control the amount of logs and output frequency, you can configure the log update interval respectively for the IPv4 ACL and the IPv6 ACL.

An ACE containing the ACL logging option consumes more hardware resources. If all configured ACEs contain this option, the ACE capacity of a device will be reduced by half.

By default, the log update interval is 0, that is, no log is output. After the ACL logging option is specified in an ACE, you need to configure the log update interval to output related logs.

For an ACE containing the ACL logging option, if no packet is matched in the specified interval, no packet matching log related to this ACE will be output. If matched packets are found in the specified interval, packet matching logs related to

this ACE will be output when the interval expires. The number of matched packets is the total number of packets that match the ACE during the specified interval, that is, the period from the previous log output to the current log output.

Only switches support the ACL logging function.

❖ ACL Packet Matching Counters

To implement network management, users may want to know whether an ACE has any matched packets and how many packets are matched. ACLs provide the ACE-based packet matching counters. You can enable or disable packet matching counters for all ACEs in an ACL, which can be an IP ACL, MAC ACL, expert ACL, or IPv6 ACL. In addition, you can run the **clear counters access-list [acl-id | acl-name]** command to reset ACL counters for a new round of statistics.

Enabling ACL counters requires more hardware entries. In an extreme case, this will reduce by half the number of ACEs that can be configured on a device.

Only switches support the ACL packet matching counters.

Overview

| Feature | Description |
|-------------------------------------|--|
| IP ACL | Control incoming or outgoing IPv4 packets of a device based on the L3 or L4 information in the IPv4 packet header. |
| MAC Extended ACL | Control incoming or outgoing L2 packets of a device based on the L2 information in the Ethernet packet header. |
| Expert Extended ACL | Combine the IP ACL and MAC extended ACL into an expert extended ACL, which controls (permits or denies) incoming or outgoing packets of a device using the same rule based on the L2, L3, and L4 information in the packet header. |
| IPv6 ACL | Control incoming or outgoing IPv6 packets of a device based on the L3 or L4 information in the IPv6 packet header. |

| | |
|-------------------------------------|---|
| ACL80 | Customize the matching fields and mask for scenarios where fixed matching fields cannot meet the requirements. |
| ACL Redirection | Redirect incoming packets of a device that match ACEs to a specified outgoing interface. |
| Global Security ACL | Make an ACL take effect in the incoming direction of all interfaces, instead of applying the ACL on every interface. |
| Security Channel | Allow packets to bypass the check of access control applications, such as DOT1X and Web authentication, to meet requirements of some special scenarios. |
| SVI Router ACL | Enable users in the same VLAN to communicate with each other. |
| Feature | Description |
| ACL Logging | Output ACL packet matching logs at a specified interval according to requirements. The logs help users learn the packet matching result of a specified ACE. |

1.3.1 IP ACL

The IP ACL implements refined control on incoming and outgoing IPv4 packets of a device. You can permit or deny the entry of specific IPv4 packets to a network according to actual requirements to control access of IP users to network resources.

Working Principle

Define a series of IP access rules in the IP ACL, and then apply the IP ACL either in the incoming or outgoing direction of an interface or globally. The device checks whether the incoming or outgoing IPv4 packets match the rules and accordingly forwards or blocks these packets.

To configure an IP ACL, you must specify a unique name or ID for the ACL of a protocol so that the protocol can uniquely identify each ACL. The following table lists the protocols that can use IDs to identify ACLs and the range of IDs.

| Protocol | ID Range |
|--------------------|--------------------|
| Standard IP | 1–99, 1300–1999 |
| Extended IP | 100–199, 2000–2699 |

Basic ACLs include the standard IP ACLs and extended IP ACLs. Typical rules defined in an ACL contain the following matching fields:

- Source IP address

- Destination IP address
- IP protocol number
- L4 source port ID or ICMP type
- L4 destination port ID or ICMP code

The standard IP ACL (ID range: 1–99, 1300–1999) is used to forward or block packets based on the source IP address, whereas the extended IP ACL (ID range: 100–199, 2000–2699) is used to forward or block packets based on a combination of the preceding matching fields.

For an individual ACL, multiple independent ACL statements can be used to define multiple rules. All statements reference the same ID or name so that these statements are bound with the same ACL. However, more statements mean that it is increasingly difficult to read and understand the ACL.

For routing products, the ICMP code matching field in an ACL rule is ineffective for ICMP packets whose ICMP type is 3.

If the ICMP code of ICMP packets to be matched is configured in an ACL rule, the ACL matching result of incoming ICMP packets of a device whose ICMP type is 3 may be different from the expected result.

❖ **Implicit "Deny All Traffic" Rule Statement**

At the end of every IP ACL is an implicit "deny all traffic" rule statement. Therefore, if a packet does not match any rule, the packet will be denied.

For example:

```
access-list 1 permit host 192.168.4.12
```

This ACL permits only packets sent from the source host 192.168.4.12, and denies packets sent from all other hosts. This is because the following statement exists at the end of this ACL: **access-list 1 deny any**.

If the ACL contains only the following statement:

```
access-list 1 deny host 192.168.4.12
```

Packets sent from any host will be denied when passing through this port.

When defining an ACL, you must consider the routing update packets. As the implicit "deny all traffic" statement exists at the end of an ACL, all routing update packets may be blocked.

❖ **Input Sequence of Rule Statements**

Every new rule is added to the end of an ACL and in front of the default rule statement. The input sequence of statements in an ACL is very important. It determines the priority of each statement in the ACL. When determining whether to forward or block packets, a device compares packets with rule statements based on the sequence that rule statements are created.

After locating a matched rule statement, the device does not check any other rule

statement.

If a rule statement is created and denies all traffic, all subsequent statements will not be checked. For example:

```
access-list 101 deny ip any any
```

```
access-list 101 permittcp 192.168.12.0 0.0.0.255 eqtelnetany
```

The first rule statement denies all IP packets. Therefore, Telnet packets from the host on the network 192.168.12.0/24 will be denied. After the device finds that packets match the first rule statement, it does not check the subsequent rule statements any more.

Related Configuration

❖ Configuring an IP ACL

By default, no IP ACL is configured on a device.

Run the **ip access-list { standard | extended } {acl-name | acl-id}** command in global configuration mode to create a standard or an extended IP ACL and enter standard or extended IP ACL mode.

❖ Adding ACEs to an IP ACL

By default, a newly created IP ACL contains an implicit ACE that denies all IPv4 packets. This ACE is hidden from users, but takes effect when the ACL is applied to an interface. That is, all IPv4 packets will be discarded. Therefore, if you want the device to receive or send some specific IPv4 packets, add some ACEs to the ACL.

For a standard IP ACL, add ACEs as follows:

- No matter whether the standard IP ACL is a named or number ACL, you can run the following command in standard IP ACL mode to add an ACE:
`[sn] { permit | deny } {hostsource| any | sourcesource-wildcard } [time-range time-range-name] [log]`
- For a numbered standard IP ACL, you can also run the following command in global configuration mode to add an ACE:
`access-list acl-id { permit | deny } {hostsource| any | sourcesource-wildcard } [time-range tm-rng-name] [log]`

For an extended IP ACL, you can add ACEs as follows:
- No matter whether the extended IP ACL is a named or numbered ACL, you can run the following command in extended IP ACL mode to add an ACE:
`[sn] { permit | deny } protocol { hostsource | any | sourcesource-wildcard } { hostdestination | any | destination destination-wildcard } [[precedence precedence [tos tos]] | dscp dscp] [fragment] [time-range time-range-name] [log]`
- For a numbered extended IP ACL, you can also run the following command in global configuration mode to add an ACE: `access-list acl-id { permit | deny } protocol { hostsource | any | sourcesource-wildcard } { hostdestination | any |`

```
destination destination-wildcard } [ [ precedence precedence [ tos tos ] ] |
dscp dscp ] [ fragment ]
[ time-range time-range-name ] [ log ]
```

❖ Applying an IP ACL

By default, the IP ACL is not applied to any interface/VXLAN, that is, the IP ACL does not filter incoming or outgoing IP packets of the device.

Run the **ip access-group** { *acl-id* | *acl-name* } { *in* | *out* } [**reflect**] command in interface/VXLAN configuration mode to apply a standard or an extended IP ACL to a specified interface/VXLAN. By default, a reflexive ACL is disabled on a router. You can run the **reflect** command to enable the reflexive ACL. The working principle of the reflexive ACL is as follows:

- a. A temporary ACL is automatically generated based on the L3 and L4 information of the traffic originated by the internal network. The temporary ACL is created according to the following principles: The IP protocol number remains unchanged, the source and destination IP addresses are swapped, and the TCP/UDP source and destination ports are also swapped.
- b. The router allows traffic to enter the internal network only when the L3 and L4 information of the returned traffic exactly matches that of the temporary ACL previously created based on the outgoing traffic.

1.3.2 MAC Extended ACL

The MAC extended ACL implements refined control on incoming and outgoing packets based on the L2 header of packets. You can permit or deny the entry of specific L2 packets to a network, thus protecting network resources against attacks or control users' access to network resources.

Working Principle

Define a series of MAC access rules in the MAC extended ACL, and then apply the ACL to the incoming or outgoing direction of an interface. The device checks whether the incoming or outgoing packets match the rules and accordingly forwards or blocks these packets.

To configure an MAC extended ACL, you must specify a unique name or ID for this ACL to uniquely identify the ACL. The following table lists the range of IDs that identify MAC extended ACLs.

| Protocol | ID Range |
|------------------|----------|
| MAC extended ACL | 700–799 |

Typical rules defined in an MAC extended ACL include:

- Source MAC address
- Destination MAC address
- Ethernet protocol type

The MAC extended ACL (ID range: 700–799) is used to filter packets based on the source or destination MAC address and the Ethernet type in the packets.

For an individual MAC extended ACL, multiple independent ACL statements can be used to define multiple rules. All statements reference the same ID or name so that these statements are bound with the same ACL. However, more statements mean that it is increasingly difficult to read and understand the ACL.

If ACEs in an MAC extended ACL are not defined specifically for IPv6 packets, that is, the Ethernet type is not specified or the value of the Ethernet type field is not 0x86dd, the MAC extended ACL does not filter IPv6 packets. If you want to filter IPv6 packets, use the IPv6 extended ACL.

❖ Implicit "Deny All Traffic" Rule Statement

At the end of every MAC extended ACL is an implicit "deny all traffic" rule statement. Therefore, if a packet does not match any rule, the packet will be denied.

For example:

```
access-list 700 permit host 00d0.f800.0001 any
```

This ACL permits only packets from the host with the MAC address 00d0.f800.0001, and denies packets from all other hosts. This is because the following statement exists at the end of this ACL: **access-list 700 deny any any.**

Related Configuration

❖ Configuring an MAC Extended ACL

By default, no MAC extended ACL is configured on a device.

Run the **mac access-list extended {acl-name | acl-id }** command in global configuration mode to create an MAC extended ACL and enter MAC extended ACL mode.

❖ Adding ACEs to an MAC Extended ACL

By default, a newly created MAC extended ACL contains an implicit ACE that denies all L2 packets. This ACE is hidden from users, but takes effect when the ACL is applied to an interface. That is, all L2 packets will be discarded. Therefore, if you want the device to receive or send some specific L2 packets, add some ACEs to the ACL.

You can add ACEs to an MAC extended ACL as follows:

- No matter whether the MAC extended ACL is a named or numbered ACL, you can run the following command in MAC extended ACL mode to add an ACE:


```
[sn] { permit | deny } {any | host src-mac-addr | src-mac-addrmask}{any | host dst-mac-addr | dst-mac-addrmask} [ethernet-type] [coscos ] [innercos] [ time-range tm-rng-name ]
```
- For a numbered MAC extended ACL, you can also run the following

command in global configuration mode to add an ACE:

```
access-list acl-id { permit | deny } {any | host src-mac-addr | src-mac-addrmask } {any | host dst-mac-addr | dst-mac-addrmask } [ethernet-type] [coscos] [innercos] [time-rangetime-range-name ]
```

❖ Applying an MAC Extended ACL

By default, the MAC extended ACL is not applied to any interface, that is, the created MAC extended ACL does not filter incoming or outgoing L2 packets of a device.

Run the **mac access-group { *acl-id* | *acl-name* } { in| out }** command in interface/VXLAN configuration mode to apply an MAC extended ACL to a specified interface/VXLAN.

1.3.3 Expert Extended ACL

You can create an expert extended ACL to match the L2 and L3 information in packets using the same rule. The expert extended ACL can be treated as a combination and enhancement of the IP ACL and the MAC extended ACL because the expert extended ACL can contain ACEs in both the IP ACL and the MAC extended ACL. In addition, the VLAN ID can be specified in the expert extended ACL to filter packets.

Working Principle

Define a series of access rules in the expert extended ACL, and then apply the ACL in the incoming or outgoing direction of an interface. The device checks whether incoming or outgoing packets match the rules and accordingly forwards or blocks these packets.

To configure an expert extended ACL, you must specify a unique name or ID for this ACL so that the protocol can uniquely identify each ACL. The following table lists the ID range of the expert extended ACL.

| Protocol | ID Range |
|---------------------|-----------|
| Expert extended ACL | 2700–2899 |

When an expert extended ACL is created, defined rules can be applied to all packets. The device determines whether to forward or block packets by checking whether packets match these rules.

Typical rules defined in an expert extended ACL include:

- All information in the basic ACL and MAC extended ACL
- VLAN ID

The expert extended ACL (ID range: 2700–2899) is a combination of the basic ACL and MAC extended ACL, and can filter packets based on the VLAN ID.

For an individual expert extended ACL, multiple independent statements can be used to define multiple rules. All statements reference the same ID or name so that these statements are bound with the same ACL.

If rules in an expert extended ACL are not defined specifically for IPv6 packets, that is, the Ethernet type is not specified or the value of the Ethernet type field is not 0x86dd, the expert extended ACL does not filter IPv6 packets. If you want to filter IPv6 packets, use the IPv6 extended ACL.

❖ Implicit "Deny All Traffic" Rule Statement

At the end of every expert extended ACL is an implicit "deny all traffic" rule statement. Therefore, if a packet does not match any rule, the packet will be denied.

For example:

```
access-list 2700 permit 0x0806 any any any any any
```

This ACL permits only ARP packets whose Ethernet type is 0x0806, and denies all other types of packets. This is because the following statement exists at the end of this ACL: **access-list 2700 deny any any any any**.

Related Configuration

❖ Configuring an Expert Extended ACL

By default, no expert extended ACL is configured on a device.

Run the **expert access-list extended {acl-name | acl-id}** command in global configuration mode to create an expert extended ACL and enter expert extended ACL mode.

❖ Adding ACEs to an Expert Extended ACL

By default, a newly created expert extended ACL contains an implicit ACE that denies all packets. This ACE is hidden from users, but takes effect when the ACL is applied to an interface. That is, all L2 packets will be discarded. Therefore, if you want the device to receive or send some specific L2 packets, add some ACEs to the ACL.

You can add ACEs to an expert extended ACL as follows:

- No matter whether the expert extended ACL is a named or numbered ACL, you can run the following command in expert extended ACL mode to add an ACE:


```
[sn] { permit | deny } [ protocol ] [ ethernet-type ] [ cos [ out ] [ inner in ] ] [ [ VID [ out ] [ inner in ] ] ]
{ source source-wildcard | host source | any } { host source-mac-address | any }
{ destination destination-wildcard |
host destination | any } { host destination-mac-address | any }
[ precedence precedence ] [ tos tos ] [ fragment ] [ range lower upper ]
[ time-range time-range-name ]
```
- For a numbered expert extended ACL, you can also run the following command in expert extended ACL mode to add an ACE:

```
access-list acl-id{ permit |deny }[[protocol] [ethernet-type][ cos[out] [inner in]]
[[VID [out][inner in]]]
{sourcesource-wildcard | hostsource | any}{host source-mac-
address|any } {destination destination-wildcard | hostdestination | any}
{host destination-mac-address | any} [[precedence precedence] [tos
tos] | [dscp dscp] ][fragment] [range|lowerupper] [time-range|time-
range-name]]
```

❖ Applying an Expert Extended ACL

By default, the expert extended ACL is not applied to any interface, that is, the created expert extended ACL does not filter incoming or outgoing L2 or L3 packets of a device.

Run the **expert access-group { acl-id | acl-name } { in| out }** command in interface/VXLAN configuration mode to apply an expert extended ACL to a specified interface/VXLAN.

1.3.4 IPv6 ACL

The IPv6 ACL implements refined control on incoming and outgoing IPv6 packets of a device. You can permit or deny the entry of specific IPv6 packets to a network according to actual requirements to control access of IPv6 users to network resources.

Working Principle

Define a series of IPv6 access rules in the IPv6 ACL, and then apply the ACL in the incoming or outgoing direction of an interface. The device checks whether the incoming or outgoing IPv6 packets match the rules and accordingly forwards or blocks these packets.

To configure an IPv6 ACL, you must specify a unique name for this ACL.

Unlike the IP ACL, MAC extended ACL, and expert extended ACL, you can specify only a name but not an ID for the IPv6 ACL created.

Only one IP ACL, or one MAC extended ACL, or one expert extended ACL can be applied to the incoming or outgoing direction of an interface. Besides, one more IPv6 ACL can be applied.

❖ Implicit "Deny All Traffic" Rule Statement

At the end of every IPv6 ACL is an implicit "deny all IPv6 traffic" rule statement. Therefore, if a packet does not match any rule, the packet will be denied.

For example:

```
ipv6 access-list ipv6_acl
10 permit ipv6 host 200::1 any
```

This ACL permits only IPv6 packets from the source host 200::1, and denies IPv6 packets from all other hosts. This is because the following statement

exists at the end of this ACL: deny ipv6 any any.

Although the IPv6 ACL contains the implicit "deny all IPv6 traffic" rule statement by default, it does not filter ND packets

❖ Input Sequence of Rule Statements

Every new rule is added to the end of an ACL and in front of the default rule statement. The input sequence of statements in an ACL is very important. It determines the priority of each statement in the ACL. When determining whether to forward or block packets, a device compares packets with rule statements based on the sequence that rule statements are created. After locating a matched rule statement, the device does not check any other rule statement.

If a rule statement is created and permits all IPv6 traffic, all subsequent statements will not be checked. For example:

```
ipv6 access-list ipv6_acl 10 permit ipv6 any any
20 deny ipv6 host 200::1 any
```

As the first rule statement permits all IPv6 packets, all IPv6 packets sent from the host 200::1 does not match the subsequent deny rule with the serial number of 20, and therefore will not be denied. After the device finds that packets match the first rule statement, it does not check the subsequent rule statements any more.

Related Configuration

❖ Configuring an IPv6 ACL

By default, no IPv6 ACL is configured on a device.

Run the **ipv6 access-list *acl-name*** command in global configuration mode to create an IPv6 ACL and enter IPv6 ACL mode.

❖ Adding ACEs to an IPv6 ACL

By default, a newly created IPv6 ACL contains an implicit ACE that denies all IPv6 packets. This ACE is hidden from users, but takes effect when the ACL is applied to an interface. That is, all IPv6 packets will be discarded. Therefore, if you want the device to receive or send some specific IPv6 packets, add some ACEs to the ACL.

Run the following command in IPv6 ACL mode to add an ACE:

```
[sn]{permit | deny }protocol{src-ipv6-prefix/prefix-len|hostsrc-ipv6-addr|
any}{dst-ipv6-pfix/pfix-len|hostdst-ipv6-addr|any} [range]lower
upper][dscp]dscp][flow-label]flow-label][fragment][time-range]tm-rng-
name][log]
```

❖ Applying an IPv6 ACL

By default, the IPv6 ACL is not applied to any interface, that is, the IPv6 ACL

does not filter incoming or outgoing IPv6 packets of a device.

Run the **ipv6 traffic-filter *acl-name* { in| out }** command in interface/VXLAN configuration mode to apply an IPv6 ACL to a specified interface/VXLAN.

1.3.5 ACL80

ACL80 refers to the expert advanced ACL, and is also called custom ACL. It filters packets based on the first 80 bytes of every packet.

Working Principle

A packet consists of a number of bytes. ACL80 allows you to match by bit in the first 80 bytes of a packet. Any bit of a field can be set to a value (**0** or **1**), indicating whether the bit is compared. When any byte is filtered, three factors are considered: content of the matching field, mask of the matching field, and the start position for matching. Bits of the matching field content are in one-to-one mapping relationship with bits of the matching field mask. The filtering rule specifies the value of the field to be filtered. The filtering field template specifies whether the corresponding field in the filtering rule should be filtered. (**1** indicates that the bit specified in the filtering rule should be matched; **0** indicates that the bit specified in the filtering rule is not matched.) Therefore, when it is required to match a specific bit, you must set the corresponding bit to 1 in the filtering field template. For example, if the bit is set to **0** in the filtering field template, no bit is matched no matter which bit is specified in the filtering rule.

For example,

```
QTECH(config)#expert access-list advanced name QTECH(config-exp-dacl)#permit
00d0f8123456 ffffffff 0
QTECH(config-exp-dacl)#deny 00d0f8654321 ffffffff 6
```

The custom ACL matches any byte of the first 80 bytes in a L2 data frame according to user' definition, and filters packets accordingly. To properly use a custom ACL, you must have an in-depth understanding about the structure of a L2 data frame. The following shows the first 64 bytes of a L3 data frame (every letter represents a hexadecimal number, and every two letters represent one byte):

```
AA AA AA AA AA AA BB BB BB
BB BB BB CC CC DD DD DD
DD EE FF GG HH HH HH II II JJ
KK LL LL MM MM
NN NN OO PP QQ QQ RR RR
RR RR SS SS SS SS TT TT UU
UU VV VV VV VV WW WW WW
WW XY ZZ aa aa bb bb
```

The following table describes the meaning and offset of each letter:

| Letter | Meaning | Offset | Letter | Meaning | Offset |
|--------|-------------------------|--------|--------|--------------------------|--------|
| A | Destination MAC address | 0 | O | Time To Live (TTL) field | 34 |

| | | | | | |
|---|---|----|----|-----------------------------------|----|
| B | Source MAC address | 6 | P | Protocol number | 35 |
| C | VLAN tag field | 12 | Q | IP checksum | 36 |
| D | Data frame length | 16 | R | Source IP address | 38 |
| E | Destination service access point (DSAP) field | 18 | S | Destination IP address | 42 |
| F | Source service access point (SSAP) field | 19 | T | TCP source port | 46 |
| G | Cntl field | 20 | U | TCP destination port | 48 |
| H | Org Code field | 21 | V | Serial number | 50 |
| I | Encapsulated data type | 24 | W | Acknowledgment field | 54 |
| J | IP version number | 26 | XY | IP header length and reserved bit | 58 |
| K | TOS field | 27 | Z | Reserved bit and flags bit | 59 |
| L | IP packet length | 28 | a | Windows size field | 60 |
| M | ID | 30 | b | Miscellaneous | 62 |
| N | Flags field | 32 | | | |

In the above table, the offset of each field is the offset of this field in the tagged 802.3 SNAP packet. In a custom ACL, you can use the rule mask and offset jointly to extract any byte from the first 80 bytes of a data frame, compare the byte with the rule customized in the ACL, and then filter matched data frames for further processing. Customized rules may be some fixed

attributes of data. For example, to obtain all TCP packets, you can define the rule as "06", rule mask as "FF", and offset as "35". Then, the device can use the rule mask and offset jointly to extract the content of TCP protocol number field in a received data frame, and compare the extracted content with the rule to obtain all TCP packets.

Only switches support the ACL80.

The ACL80 supports filtering of the Ethernet, 803.3 SNAP, and 802.3 LLC packets. If the values of the fields from DSAP to cntl are set to AAAA03, the ACL is used to filter the 803.3 SNAP packets. If the values of the fields from DSAP to cntl are set to E0E003, the ACL is used to filter the 803.3 LLC packets. The value of the cntl

field cannot be configured to filter Ethernet packets.

ACL80 can not match any bytes in the first 80 bytes due to hardware reason. It only support matching destination/source MAC, VID, ETYPE, IP protocol number, destination/source IP, destination/source port, ICMP type, ICMP code and PPPoE IType.

Related Configuration

❖ Configuring an Expert Advanced ACL

By default, no expert advanced ACL is configured on a device.

Run the **expert access-list advanced *acl-name*** command in global configuration mode to create an expert advanced ACL and enter expert advanced ACL mode.

❖ Adding ACEs to an Expert Advanced ACL

By default, a newly created expert advanced ACL contains an implicit ACE that denies all packets. This ACE is hidden from users, but takes effect when the ACL is applied to an interface. That is, all L2 packets will be discarded. Therefore, if you want the device to receive or send some specific L2 packets, add some ACEs to the ACL.

- Run the **[sn] { permit | deny } hex hex-mask offset** command in expert advanced ACL mode to add an ACE to the expert advanced ACL.

❖ Applying an Expert Advanced ACL

By default, the expert advanced ACL is not applied to any interface, that is, the created expert advanced ACL does not filter incoming or outgoing packets of a device.

Run the **expert access-group {acl-id | acl-name} { in| out }** command in interface configuration mode to apply an expert advanced ACL to a specified interface.

1.3.6 ACL Redirection

ACL redirection allows a device to analyze received packets and redirect the packets to a specified port for forwarding. To analyze specific incoming packets of a device, you can configure the ACL redirection function to redirect packets meeting rules to a specified port and capture packets on this port for analysis. Bind different ACL policy to an interface and specify an output destination interface for each policy. When receiving packets on this interface, the device searches ACL policies bound to this interface one by one. If packets match criteria described in a certain policy, the device forwards packets on the destination interface specified by the policy, thus redirecting packets based on traffic.

Only switches support the ACL redirection function.

Related Configuration

❖ Configuring an ACL

Before configuring ACL redirection, configure an ACL. For details about how to

configure an ACL, see the earlier descriptions about ACL configuration.

❖ Adding ACEs to an ACL

For details about how to add ACEs to an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

❖ Configuring ACL Redirection

By default, ACL redirection is not configured on a device.

Run the **redirect destinationinterface** *interface-name* **acl** {*acl-id* | **acl-name** } in command in interface configuration mode to configure ACL redirection.

You can configure the ACL redirection function only on an Ethernet interface, AP, or SVI.

1.3.7 Global Security ACL

To meet the requirements of security deployment, the port-based ACL is often configured to filter out virus packets and obtain packets with certain characteristics, for example, packets that attack the TCP port. Various virus packets exist in a global network environment, and the identification features of virus packets under each port are identical or similar. Therefore, an ACL is generally created. After the deny ACE for matching virus signatures is added to the ACL, the port-based ACL is applied to each port on the switch to filter out virus packets.

For two reasons, it is not convenient to use the port-based ACLs in antivirus scenarios such as virus filtering. The first reason is that the port-based ACL must be configured on every port, which results in repeated configuration, poor operation performance, and over-consumption of ACL resources. The second reason is that the access control function of the ACL is weakened. As the port-based ACL is used for virus filtering, basic functions of the ACL, such as route update restriction and network access restriction, cannot be used properly. The global security ACL can be used for global antivirus deployment and defense without affecting the port-based ACL. By running only one command, you can make the global security ACL takes effect on all L2 interfaces. In contrast, the port-based ACL must be configured on every interface.

The global security ACL takes effect on all L2 interfaces. When both the global security ACL and the port-based ACL are configured, both take effect. Packets that match the global security ACL are directly filtered out as virus packets. Packets that do not match the global security ACL are still controlled by the port-based ACL. You can disable the global security ACL on some ports so that these ports are not controlled by the global security ACL.

The global security ACL is mainly used for virus filtering. Therefore, in an ACL associated with the global security ACL, only the deny ACEs take effect, and the permit ACEs do not take effect.

Unlike the secure ACL applied to a port, the global security ACL does not contain the default "deny all traffic" ACE, that is, all packets that do not match the ACL

are permitted.

A global secure ACL can take effect either on a L2 port or a routed port. That is, it takes effect on all the following types of ports: access port, trunk port, hybrid port, routed port, and AP (L2 or L3). The global secure ACL does not take effect on an SVI.

You can disable the global security ACL on an individual physical port or AP, but not on a member port of an AP.

The global secure ACL supports only the associated IP standard ACL, IP extended ACL, MAC extended ACL and Expert extended ACL.

Related Configuration

❖ Configuring an ACL

Before configuring the global security ACL, configure an ACL. For details about how to configure an ACL, see the earlier descriptions about ACL configuration.

❖ Adding ACEs to an ACL

For details about how to add ACEs to an ACL, see the earlier descriptions about the IP ACL.

❖ Configuring a Global Security ACL

By default, no global security ACL is configured on a device.

Run the `{ip | mac | expert} access-group acl-id { in | out }` command in global configuration mode to enable the global security ACL.

Run the `no global access-group` command in interface configuration mode to disable the global security ACL.

1.3.8 Security Channel

In some application scenarios, packets meeting some characteristics may need to bypass the checks of access control applications. For example, before DOT1X authentication, users are allowed to log in to a specified website to download the DOT1X authentication client. The security channel can be used for this purpose. When the security channel configuration command is executed to apply a secure ACL globally or to an interface or VXLAN, this ACL becomes a security channel.

Working Principle

The security channel is also an ACL, and can be configured globally or for a specified interface or VXLAN. When arriving at an interface, packets are checked on the security channel. If meeting the matching conditions of the security channel, packets

directly enters a switch without undergoing the access control, such as port security, Web authentication, 802.1x, and IP+MAC binding check. A globally applied security channel takes effect on all interfaces except exclusive interfaces.

The deny ACEs in an ACL that is applied to a security channel do not take effect. In addition, this ACL does not contain an implicit "deny all traffic" rule statement at the end of the ACL. If packets do not meet matching conditions of the security channel, they are checked according to the access control rules in compliance with the relevant process.

You can configure up to eight exclusive interfaces for the global security channel. In addition, you cannot configure interface-based security channel on these exclusive interfaces.

If both port-based migratable authentication mode and security channel are applied to an interface, the security channel does not take effect.

An IPv6 ACL cannot be configured as a security channel.

Only switches support the security channel.

Related Configuration

❖ Configuring an ACL

Before configuring the security channel, configure an ACL. For details about how to configure an ACL, see the earlier descriptions about ACL configuration.

❖ Adding ACEs to an ACL

For details about how to add ACEs to an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, or expert extended ACL.

❖ Configuring a Security Channel on an Interface

By default, no security channel is configured on an interface of a device.

Run the **security access-group** {*acl-id* | *acl-name* } command in interface configuration mode to configure the security channel on an interface.

❖ Configuring a Global Security Channel

By default, no global security channel is configured on a device.

Run the **security global access-group** {*acl-id* | *acl-name* } command in global configuration mode to configure a global security channel.

❖ Configuring an Exclusive Interface for the Global Security Channel

By default, no exclusive interface is configured for the global security channel on a device.

Run the **security uplink enable** command in interface configuration mode to configure a specified interface as the exclusive interface of the global security channel.

1.3.9 SVI Router ACL

By default, an ACL that is applied to an SVI also takes effect on L2 packets forwarded within a VLAN and L3 packets forwarded between VLANs. Consequently, users in the same VLAN may fail to communicate with each other. Therefore, a switchover method is provided so that the ACL that is applied to an SVI takes effect only on routing packets between VLANs.

Working Principle

By default, the SVI router ACL function is disabled, and an SVI ACL takes effect on L3 packets forwarded between VLANs and L2 packets forwarded within a VLAN. After the SVI router ACL function is enabled, the SVI ACL takes effect only on L3 packets forwarded between VLANs.

Only switches support the SVI router ACL.

Related Configuration

❖ Configuring an ACL

Before configuring the SVI router ACL, configure and apply an ACL. For details about how to configure an ACL, see the earlier descriptions about ACL configuration.

❖ Adding ACEs to an ACL

For details about how to add ACEs to an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

❖ Applying an ACL

For details about how to apply an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL. Apply the ACL in SVI configuration mode.

❖ Configuring the SVI Router ACL

Run the **svi router-acls enable** command in global configuration mode to enable the SVI router ACL so that the ACL that is applied to an SVI takes effect only on packets forwarded at L3, and not on packets forwarded at L2 within a VLAN.

1.3.10 ACL Logging

ACL logging is used to monitor the running status of ACEs in an ACL and provide essential information for routine network maintenance and optimization.

Working Principle

To better learn the running status of ACLs on a device, you can determine whether to specify the ACL logging option as required when adding ACEs. If this option is specified, logs are output when packets matching ACEs are found. ACL logs are displayed based on ACEs. That is, the device periodically displays ACEs

with matched packets and the number of matched packets. An example of the log is as follows:

```
*Sep 9 16:23:06: %ACL-6-MATCH: ACL 100 ACE 10 permit icmp any any, match 78 packets.
```

To control the amount of logs and output frequency, you can configure the log update interval.

An ACE containing the ACL logging option consumes more hardware resources. If all configured ACEs contain this option, the ACE capacity of a device will be reduced by half.

By default, the log update interval is 0, that is, no log is output. After the ACL logging option is specified in an ACE, you need to configure the log update interval to output related logs; otherwise, logs are not output.

For an ACE containing the ACL logging option, if no packet is matched in the specified interval, no packet matching log related to this ACE will be output. If matched packets are found in the specified interval, packet matching logs related to

this ACE will be output when the interval expires. The number of matched packets is the total number of packets that match the ACE during the specified interval, that is, the period from the previous log output to the current log output.

Only switches support the ACL logging function.

You can configure the ACL logging option only for an IP ACL or an IPv6 ACL.

Related Configuration

❖ Configuring an ACL

Configure an ACL before configuring ACEs containing the ACL logging option. For details about how to configure an ACL, see the earlier descriptions about ACL configuration.

❖ Adding ACEs to an ACL

For details about how to add ACEs to an ACL, see the earlier descriptions about the IP ACL and IPv6 ACL. Note that the ACL logging option must be configured.

❖ Configuring the Log Update Interval

Run the `{ip | ipv6} access-list log-update interval time` command in the configuration mode to configure the interval at which the ACL logs are output.

❖ Applying an ACL

For details about how to apply an ACL, see the earlier descriptions about the IP ACL and IPv6 ACL.

1.3.11 Packet Matching Counters

In addition to ACL logs, packet matching counters provide another choice for routine network maintenance and optimization.

Working Principle

To implement network management, users may want to know whether an ACE has any matched packets and how many packets are matched. ACLs provide the ACE-based packet matching counters. You can enable or disable packet matching counters for all ACEs in an ACL. When a packet matches the ACE, the corresponding counter increments by 1. You can run the **clear counters access-list [acl-id | acl-name]** command to reset counters of all ACEs in an ACL for a new round of statistics.

Enabling ACL counters requires more hardware entries. In an extreme case, this will reduce by half the number of ACEs that can be configured on a device.

You can enable packet matching counters on an IP ACL, MAC ACL, expert ACL, or IPv6 ACL.

Only switches support the ACL packet matching counters.

Related Configuration

❖ Configuring an ACL

Configure an ACL before configuring ACEs containing the ACL logging option. For details about how to configure an ACL, see the earlier descriptions about ACL configuration.

❖ Adding ACEs to an ACL

For details about how to add ACEs to an ACL, see the earlier descriptions about the IP ACL and IPv6 ACL. Note that the ACL logging option must be configured.

❖ Enabling Packet Matching Counters

To enable packet matching counters on an IP ACL, MAC ACL, or expert ACL, run the **{mac | expert | ip} access-list counter { acl-id | acl-name }** command in global configuration mode.

To enable packet matching counters on an IPv6 ACL, run the **ipv6 access-list counter acl-name** command in global configuration mode.

❖ Applying an ACL

For details about how to apply an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

❖ Clearing Packet Matching Counters

Run the **clear counters access-list [acl-id | acl-name]** command in privileged EXEC mode to reset packet matching counters.

1.3.12 Fragmented Packet Matching Mode

In fragmented packet matching mode, an ACL can implement more refined control on fragmented packets.

Working Principle

IP packets may be fragmented when transmitted on the network. When fragmentation occurs, only the first fragment of the packet contains the L4 information, such as the TCP/UDP port number, ICMP type, and ICMP code, and other fragmented packets do not contain the L4 information. By default, if an ACE contains the fragment flag, fragmented packets except the first fragments are filtered. If an ACE does not contain the fragment flag, all fragmented packets (including the first fragments) are filtered. In addition to this default fragmented packet matching mode, a new fragmented packet matching mode is provided. You can switch between the two fragmented packet matching modes as required on a specified ACL. In the new fragmented packet matching mode, if an ACE does not contain the fragment flag and packets are fragmented, the first

fragments are compared with all the matching fields (including L3 and L4 information) defined in the ACE, and other fragmented packets are compared with only the non-L4 information defined in the ACE.

In the new fragmented packet matching mode, if an ACE does not contain the fragment flag and the action is Permit, this type of ACE occupies more hardware entries. In an extreme case, this will reduce by half the number of hardware entries. If Established is configured for filter the TCP flag in an ACE, more hardware entries will be occupied.

The ACL will be temporarily ineffective during switchover of the fragmented packet matching mode.

In the new fragmented packet matching mode, if an ACE does not contain the fragment flag, the L4 information of packets needs to be compared, and the action is Permit, the ACE checks the L3 and L4 information of the first fragments of packets, and checks only the L3 information of other fragmented packets. If the action is Deny, the ACE checks only the first fragments of packets, and ignores other fragmented packets.

In the new fragmented packet matching mode, if an ACE contains the fragment flag, the ACE checks only fragmented packets but not the first fragments of packets no matter whether the action in the ACE is Permit or Deny.

Only the IP extended ACL and the expert extended ACL support switching between the two fragmented packet matching modes.

Only switches support filtering of fragmented packets.

Related Configuration

❖ Configuring an ACL

For details about how to configure an ACL, see the earlier descriptions about the IP ACL and expert extended ACL.

❖ Adding ACEs to an ACL

For details about how to add ACEs to an ACL, see the earlier descriptions about

the IP ACL and expert extended ACL. Note that the fragment option must be added.

❖ **Switching the Fragmented Packet Matching Mode**

Run the [no] {ip | expert} **access-list new-fragment-mode** { acl-id | acl-name } command in global configuration mode to switch the fragmented packet matching mode.

❖ **Applying an ACL**

For details about how to apply an ACL, see the earlier descriptions about the IP ACL and expert extended ACL.

1.4 Configuration

| Configuration Item | Description and Command | |
|---|---|---|
| Configuring an IP ACL | (Optional) It is used to filter IPv4 packets. | |
| | ip access-list standard | Configures a standard IP ACL. |
| | ip access-list extended | Configures an extended IP ACL. |
| Configuration Item | Description and Command | |
| | permit host any time-range log | Adds a permit ACE to a standard IP ACL. |
| | deny host any time-range log | Adds a deny ACE to a standard IP ACL. |
| | permit host any host any tos dscp precedence fragment time-range log | Adds a permit ACE to an extended IP ACL. |
| | deny host any host any tos dscp precedence fragment time-range log | Adds a deny ACE to an extended IP ACL. |
| | ip access-group in out | Applies a standard or an extended IP ACL. |
| Configuring an MAC Extended ACL | (Optional) It is used to filter L2 packets. | |
| | mac access-list extended | Configures an MAC extended ACL. |

| | | |
|--|--|--|
| | permit any host any host cos inner time-range | Adds a permit ACE to an MAC extended ACL. |
| | deny any host any host cos inner time-range | Adds a deny ACE to an MAC extended ACL. |
| | mac access-group in out | Applies an MAC extended ACL. |
| Configuring an Expert Extended ACL | (Optional) It is used to filter L2 and L3 packets. | |
| | expert access-list extended | Configures an expert extended ACL. |
| | permit cos inner VID inner host any host any host any host any precedence tos fragment range time-range | Adds a permit ACE to an expert extended ACL. |
| | deny cos inner VID inner host any host any host any host any precedence tos fragment range time-range | Adds a deny ACE to an expert extended ACL. |
| | expert access-group in out | Applies an expert extended ACL. |
| Configuring an IPv6 ACL | (Optional) It is used to filter IPv6 packets. | |
| | ipv6 access-list | Configures an IPv6 ACL. |
| | permit host any host any range dscp flow-label fragment time-range log | Adds a permit ACE to an IPv6 ACL. |
| | deny host any host any range dscp flow-label fragment time-range log | Adds a deny ACE to an IPv6 ACL. |
| | ipv6 traffic-filter in out | Applies an IPv6 ACL. |
| Configuring an ACL80 | (Optional) It is used to customize the fields for filter L2 and L3 packets. | |

| | | |
|---|---|--|
| | expert access-list advanced | Configures an expert advanced ACL. |
| | permit | Adds a permit ACE to an expert advanced ACL. |
| | deny | Adds a deny ACE to an expert advanced ACL. |
| Configuration Item | Description and Command | |
| | expert access-group in out | Applies an expert advanced ACL |
| Configuring ACL Redirection | (Optional) It is used to redirect packets meeting the rules to a specified interface. | |
| | redirect destination interface acl in | Configures ACL redirection. |
| Configuring a Global Security ACL | (Optional) It is used to make an ACL take effect globally. | |
| | ip access-group in out | Applies a global security ACL in global configuration mode. |
| | no global access-group | Configures an interface as the exclusive interface of the global security ACL in interface configuration mode. |
| Configuring a Security Channel | (Optional) It is used to enable packets meeting some characteristics to bypass the checks of access control applications, such as the DOT1X and Web authentication. | |
| | security access-group | Enables the security channel in interface configuration mode. |
| | security global access-group | Enables the security channel in global configuration mode. |

| | | |
|---|--|--|
| | security uplink enable | Configures an interface as the exclusive interface of the global security channel in interface configuration mode. |
| Configuring Comments for ACLs | (Optional) It is used to configure comments for an ACL or ACE so that users can easily identify the functions of the ACL or ACE. | |
| | list-remark | Configures a comment for an ACL in ACL configuration mode. |
| | access-list list-remark | Configures a comment for an ACL in global configuration mode. |
| | remark | Configures a comment for an ACE in ACL configuration mode. |

1.4.1 Configuring an IP ACL

Configuration Effect

Configure and apply an IP ACL to an interface/VXLAN to control all incoming and outgoing IPv4 packets of this interface/VXLAN. You can permit or deny the entry of specific IPv4 packets to a network to control access of IP users to network resources.

Notes

N/A

Configuration Steps

❖ Configuring an IP ACL

- (Mandatory) Configure an IP ACL if you want to control access of IPv4 users to network resources.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The IP ACL takes effect only on the local device, and does not affect other devices on the network.

❖ Adding ACEs to an IP ACL

- (Optional) An ACL may contain zero or multiple ACEs. If no ACE is configured, all incoming IPv4 packets of the device are denied by default.

❖ Applying an IP ACL

- (Mandatory) Apply an IP ACL to a specified interface/VXLAN if you want this ACL take effect.
- You can apply an IP ACL on a specified interface/VXLAN of an access, an aggregate, or a core device based on the distribution of users.

Verification

- Use the following methods to verify the configuration effects of the IP ACL:
- Run the **ping** command to verify that the IP ACL takes effect on the specified interface. For example, if an IP ACL is configured to prohibit a host with a specified IP address or hosts in a specified IP address range from accessing the network, run the **ping** command to verify that the host(s) cannot be successfully pinged.
- Access related network resources to verify that the IP ACL takes effect on the specified interface. For example, access the Internet or access the FTP resources on the network through FTP.

Related Commands

❖ Configuring an IP ACL

| | |
|-----------------------|---|
| Command | <code>ip access-list { standard extended } {<i>acl-name</i> <i>acl-id</i> }</code> |
| Parameter Description | <p>standard: Indicates that a standard IP ACL is created.</p> <p>extended: Indicates that an extended IP ACL is created.</p> <p><i>acl-name:</i> Indicates the name of a standard or an extended IP ACL. If this option is configured, a named ACL is created. The name is a string of 1 to 99 characters. The ACL name cannot start with numbers (0–9), "in", or "out".</p> <p><i>acl-id:</i> Indicates the ID that uniquely identifies a standard or extended IP ACL. If this option is configured, a numbered ACL is created. If a standard IP ACL is created, the value range of <i>acl-id</i> is 1–99 and 1300–1999.</p> <p>If an extended IP ACL is created, the value range of <i>acl-id</i> is 100–199 and 2000–2699.</p> |
| Command Mode | Global configuration mode |
| Usage Guide | <p>Run this command to configure a standard or an extended IP ACL and enter standard or extended IP ACL configuration mode. If you want to control access of users to network resources by checking the source IP</p> <p>address of each packet, configure a standard IP ACL. If you want to control access of users to network resources by checking the source or destination IP address, protocol number, and TCP/UDP source or destination port, configure an extended IP ACL.</p> |

- ❖ Adding ACEs to an IP ACL
 - Add ACEs to a standard IP ACL.

Use either of the following methods to add ACEs to a standard IP ACL:

| | |
|-----------------------|---|
| Command | <code>[sn] { permit deny } { host <i>source</i> any <i>source source-wildcard</i> } [time-range <i>time-range-name</i>] [log]</code> |
| Parameter Description | <p>sn: Indicates the sequence number of an ACE. The value ranges from 1 to 2,147,483,647. This sequence number determines the priority of this ACE in the ACL. A smaller sequence number indicates a higher priority. An ACE with a higher priority will be preferentially used to match packets. If you do not specify the sequence number when adding an ACE, the system automatically allocates a sequence number, which is equal to an increment (10 by default) plus the sequence number of the last ACE in the current ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a newly-added ACE will be 110 by default. You can adjust the increment using a command.</p> <p>permit: Indicates that the ACE is a permit ACE.</p> <p>deny: Indicates that the ACE is a deny ACE.</p> <p>host source: Indicates that IP packets sent from a host with the specified source IP address are filtered.</p> <p>any: Indicates that IP packets sent from any host are filtered.</p> <p>source source-wildcard: Indicates that IP packets sent from hosts in the specified IP network segment are filtered.</p> <p>time-range time-range-name: Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range. log: Indicates that logs will be periodically output if packets matching the ACEs are found. For details about logs, see "ACL Logging" in this document.</p> |
| Command Mode | Standard IP ACL configuration mode |
| Usage Guide | Run this command to add ACEs in standard IP ACL configuration mode. The ACL can be a named or numbered ACL. |
| Command | <code>access-list <i>acl-id</i> { permit deny } { host <i>source</i> any <i>source source-wildcard</i> } [time-range <i>tm-rng-name</i>] [log]</code> |
| Parameter Description | acl-id : Indicates the ID of a numbered ACL. It uniquely identifies an ACL. The value range of <i>acl-id</i> is 100–199 and 1300–1999. |

| | |
|---------------------|--|
| | <p>permit: Indicates that the ACE is a permit ACE.</p> <p>deny: Indicates that the ACE is a deny ACE.</p> <p>host source: Indicates that IP packets sent from a host with the specified source IP address are filtered.</p> <p>any: Indicates that IP packets sent from any host are filtered.</p> <p>source source-wildcard: Indicates that IP packets sent from hosts in the specified IP network segment are filtered.</p> |
| | <p>time-range time-range-name: Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range. log: Indicates that logs will be periodically output if packets matching the ACEs are found. For details about logs, see "ACL Logging" in this document.</p> |
| Command Mode | Standard IP ACL configuration mode |
| Usage Guide | Run this command to add ACEs to a numbered IP ACL in global configuration mode. It cannot be used to add ACEs to a named IP ACL. |

- Add ACEs to an extended IP ACL.

Use either of the following methods to add ACEs to an extended IP ACL:

| | |
|---------|---|
| Command | <pre>[sn] { permit deny } protocol { host source any source source-wildcard } { host destination any destination destination-wildcard } [[precedence precedence [tos tos]] dscp dscp] [fragment] [time-range time-range-name] [log]</pre> |
|---------|---|

| | |
|------------------------------|---|
| Parameter Description | <p><i>sn</i>: Indicates the sequence number of an ACE. The value ranges from 1 to 2,147,483,647. This sequence number determines the priority of this ACE in the ACL. A smaller sequence number indicates a higher priority. An ACE with a higher priority will be preferentially used to match packets. If you do not specify the sequence number when adding an ACE, the system automatically allocates a sequence number, which is equal to an increment (10 by default) plus the sequence number of the last ACE in the current ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a newly-added ACE will be 110 by default. You can adjust the increment using a command.</p> <p>permit: Indicates that the ACE is a permit ACE.</p> <p>deny: Indicates that the ACE is a deny ACE.</p> <p><i>protocol</i>: Indicates the IP protocol number. The value ranges from 0 to 255. To facilitate the use, the system provides frequently-used abbreviations to replace the specific IP protocol numbers, including eigrp, gre, icmp, igmp, ip, ipinip, nos, ospf, tcp, and udp.</p> <p>host source: Indicates that IP packets sent from a host with the specified source IP address are filtered. <i>source source-wildcard</i>: Indicates that IP packets sent from hosts in the specified IP network segment are filtered.</p> <p>host destination: Indicates that IP packets sent to a host with the specified destination IP address are filtered. If the any keyword is configured, IP packets sent to any host are filtered.</p> <p><i>destination destination-wildcard</i>: Indicates that IP packets sent to hosts in a specified IP network segment are filtered.</p> <p>any: Indicates that IP packets sent to or from any host are filtered.</p> <p>precedence precedence: Indicates that IP packets with the specified precedence field in the header are filtered.</p> <p>tos tos: Indicates that IP packets with the specified the type of service (TOS) field in the header are filtered.</p> <p>dscp dscp: Indicates that IP packets with the specified the dcsp field in the header are filtered.</p> <p>fragment: Indicates that only fragmented IP packets except the first fragments are filtered.</p> <p>time-range time-range-name: Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range.</p> <p>log: Indicates that logs will be periodically output if packets matching the ACEs are found. For details about logs, see "ACL Logging" in this document.</p> |
| Command Mode | Extended IP ACL configuration mode |

| | |
|--------------------|--|
| Usage Guide | Run this command to add ACEs in extended IP ACL configuration mode. The ACL can be a named or numbered ACL. |
| Command | access-list <i>acl-id</i> { permit deny } <i>protocol</i> {host <i>source</i> any <i>source source-wildcard</i> } {host <i>destination</i> any <i>destination destination-wildcard</i> } [[precedence <i>precedence</i> [tos <i>tos</i>]] dscp <i>dscp</i>] [fragment] [time-range <i>time-range-name</i>] [log] |

| Parameter Description | |
|-----------------------|---|
| | <p>acl-id: Indicates the ID of a numbered ACL. It uniquely identifies an ACL. The value range of <i>acl-id</i> is 100–199 and 2000–1999.</p> <p>sn: Indicates the sequence number of an ACE. The value ranges from 1 to 2,147,483,647. This sequence number determines the priority of this ACE in the ACL. A smaller sequence number indicates a higher priority. An ACE with a higher priority will be preferentially used to match packets. If you do not specify the sequence number when adding an ACE, the system automatically allocates a sequence number, which is equal to an increment (10 by default) plus the sequence number of the last ACE in the current ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a newly-added ACE will be 110 by default. You can adjust the increment using a command.</p> <p>permit: Indicates that the ACE is a permit ACE.</p> <p>deny: Indicates that the ACE is a deny ACE.</p> <p>protocol: Indicates the IP protocol number. The value ranges from 0 to 255. To facilitate the use, the system provides frequently-used abbreviations to replace the specific IP protocol numbers, including eigrp, gre, icmp, igmp, ip, ipinip, nos, ospf, tcp, and udp.</p> <p>host source: Indicates that IP packets sent from a host with the specified source IP address are filtered. source source-wildcard: Indicates that IP packets sent from hosts in the specified IP network segment are filtered.</p> <p>host destination: Indicates that IP packets sent to a host with the specified destination IP address are filtered. If the any keyword is configured, IP packets sent to any host are filtered.</p> <p>destination destination-wildcard: Indicates that IP packets sent to hosts in a specified IP network segment are filtered.</p> <p>any: Indicates that IP packets sent to or from any host are filtered.</p> <p>precedence precedence: Indicates that IP packets with the specified precedence field in the header are filtered.</p> <p>tos tos: Indicates that IP packets with the specified the type of service (TOS) field in the header are filtered.</p> <p>dscp dscp: Indicates that IP packets with the specified the dscp field in the header are filtered.</p> <p>fragment: Indicates that only fragmented IP packets except the first fragments are filtered.</p> <p>time-range time-range-name: Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range.</p> <p>log: Indicates that logs will be periodically output if packets matching the ACEs are found. For details about logs, see "ACL Logging" in this document.</p> |

| | |
|---------------------|--|
| Command Mode | Extended IP ACL configuration mode |
| Usage Guide | Run this command to add ACEs to a numbered IP ACL in extended IP ACL configuration mode. It cannot be used to add ACEs to a named extended IP ACL. |

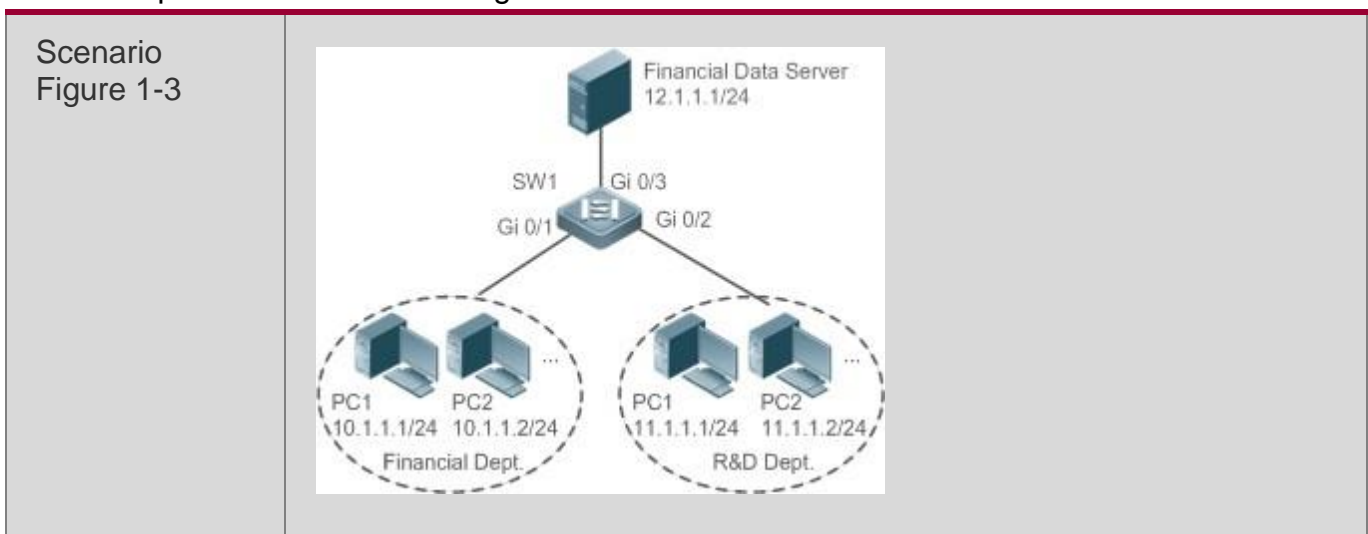
❖ Applying an IP ACL

| | |
|------------------------------|---|
| Command | <code>ip access-group { <i>acl-id</i> <i>acl-name</i> } { in out }</code> |
| Parameter Description | <i>acl-id</i> : Indicates that a numbered standard or extended IP ACL will be applied to the interface. <i>acl-name</i> : Indicates that a named standard or extended IP ACL will be applied to the interface. in : Indicates that this ACL controls incoming IP packets of the interface. out : Indicates that this ACL controls outgoing IP packets of the interface. reflect : Indicates that the reflexive ACL is enabled. |
| Command Mode | Interface/VXLAN configuration mode |
| Usage Guide | This command makes an IP ACL take effect on the incoming or outgoing packets of a specified interface/VXLAN. |

Configuration Example

The following configuration example describes only ACL-related configurations.

- ❖ Configuring an IP ACL to Prohibit Departments Except the Financial Department from Accessing the Financial Data Server



| | |
|----------------------------|---|
| Configuration Steps | <ul style="list-style-type: none"> ▪ Configure an IP ACL. ▪ Add ACEs to the IP ACL. ▪ Apply the IP ACL to the outgoing direction of the interface connecting the financial data server. |
| SW1 | <pre>sw1(config)#ip access-list standard 1 sw1(config-std- nacl)#permit 10.1.1.0 0.0.0.255 sw1(config-std- nacl)#deny 11.1.1.1 0.0.0.255 sw1(config-std- nacl)#exit sw1(config)#int gigabitEthernet 0/3 sw1(config-if-GigabitEthernet 0/3)#ip access-group 1 out</pre> |
| Verification | <ul style="list-style-type: none"> ▪ On a PC of the R&D department, ping the financial data server. Verify that the ping operation fails. ▪ On a PC of the financial department, ping the financial data server. Verify that the ping operation succeeds. |
| SW1 | <pre>sw1(config)#show access-lists ip access-list standard 1 10 permit 10.1.1.0 0.0.0.255 20 deny 11.1.1.0 0.0.0.255 sw1(config)#sh ow access- group ip access-group 1 out Applied On interface GigabitEthernet 0/3</pre> |

1.4.2 Configuring an MAC Extended ACL

Configuration Effect

Configure and apply an MAC extended ACL to an interface/VXLAN to control all incoming and outgoing IPv4 packets of this interface/VXLAN. You can permit or deny the entry of specific L2 packets to a network to control access of users to network resources based on L2 packets.

Notes

N/A

Configuration Steps

❖ Configuring an MAC Extended ACL

- (Mandatory) Configure an MAC extended ACL if you want to control users' access to network resources based on the L2 packet header, for example, the MAC address of each user's PC.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The MAC extended ACL takes effect only on the local device, and does not affect other devices on the network.

❖ Adding ACEs to an MAC Extended ACL

- (Optional) An ACL may contain zero or multiple ACEs. If no ACE is configured, all incoming L2 Ethernet packets of the device are denied by default.

❖ Applying an MAC extended ACL

- (Mandatory) Apply an MAC extended ACL to a specified interface if you want this ACL take effect.
- You can apply an MAC extended ACL on a specified interface of an access, an aggregate, or a core device based on the distribution of users.

Verification

- Use the following methods to verify the configuration effects of the MAC extended ACL:
- If an MAC extended ACL is configured to permit or deny some IP packets, run the **ping** command to check whether ACEs of this ACL takes effect on the specified interface. For example, an MAC extended ACL is configured to prevent a device interface from receiving IP packets (Ethernet type is 0x0800), run the **ping** command for verification.
- If an MAC extended ACL is configured to permit or deny some non-IP packets (e.g. ARP packets), also run the **ping** command to check whether ACEs of this ACL takes effect on the specified interface. For example, to filter out ARP packets, run the **ping** command for verification.
- You can also construct L2 packets meeting some specified characteristics to check whether the MAC extended ACL takes effect. Typically, prepare two PCs, construct and send L2 packets on one PC, enable packet capturing on another PC, and check whether packets are forwarded as expected (forwarded or blocked) according to the action specified in the ACEs.

Related Commands

❖ Configuring an MAC Extended ACL

| | |
|------------------------------|---|
| Command | mac access-list extended {acl-name acl-id } |
| Parameter Description | <p><i>acl-name</i>: Indicates the name of an MAC extended ACL. If this option is configured, a named ACL is created. The name is a string of 1 to 99 characters. The ACL name cannot start with numbers (0–9), "in", or "out".</p> <p><i>acl-id</i>: Indicates the ID that uniquely identifies an MAC extended ACL. If this option is configured, a numbered ACL is created. The value range of <i>acl-id</i> is 700–799.</p> |
| Command Mode | Global configuration mode |
| Usage Guide | Run this command to configure an MAC extended ACL and enter MAC extended ACL configuration mode. You can configure an MAC extended ACL to control users' access to network resources by checking the L2 information of Ethernet packets. |

❖ Adding ACEs to an MAC Extended ACL

Use either of the following methods to add ACEs to an MAC extended ACL:

- Add ACEs in MAC extended ACL configuration mode.

| | |
|----------------|--|
| Command | <p>[sn] { permit deny } {any host <i>src-mac-addr</i> / <i>src-mac-addr mask</i> } {any host <i>dst-mac-addr</i> / <i>dst-mac-addr mask</i> } [<i>ethernet-type</i>] [cos <i>cos</i> [inner <i>cos</i>]] [time-range <i>tm-rng-name</i>]</p> |
|----------------|--|

| | |
|------------------------------|---|
| Parameter Description | <p><i>sn</i>: Indicates the sequence number of an ACE. The value ranges from 1 to 2,147,483,647. This sequence number determines the priority of this ACE in the ACL. A smaller sequence number indicates a higher priority. An ACE with a higher priority will be preferentially used to match packets. If you do not specify the sequence number when adding an ACE, the system automatically allocates a sequence number, which is equal to an increment (10 by default) plus the sequence number of the last ACE in the current ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a newly-added ACE will be 110 by default. You can adjust the increment using a command.</p> <p>permit: Indicates that the ACE is a permit ACE.</p> <p>deny: Indicates that the ACE is a deny ACE.</p> <p>any: Indicates that L2 packets sent from any host are filtered.</p> <p>host src-mac-addr: Indicates that IP packets sent from a host with the specified source MAC address are filtered.</p> <p><i>src-mac-addr mask</i>: Indicates that the source MAC address is reversed.</p> <p>any: Indicates that L2 packets sent to any host are filtered.</p> <p>host dst-mac-addr: Indicates that IP packets sent to a host with the specified destination MAC address are filtered.</p> <p><i>dst-mac-addr mask</i>: Indicates that the destination MAC address is reversed.</p> <p><i>ethernet-type</i>: Indicates that L2 packets of the specified Ethernet type are filtered.</p> <p>cos cos: Indicates that L2 packets with the specified class of service (cos) field in the outer tag are filtered.</p> <p>inner cos: Indicates that L2 packets with the specified cos field in the inner tag are filtered.</p> <p>time-range time-range-name: Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range.</p> |
| Command Mode | MAC extended ACL configuration mode |
| Usage Guide | Run this command to add ACEs in MAC extended ACL configuration mode. The ACL can be a named or numbered ACL. |

- Add ACEs to an MAC extended ACL in global configuration mode.

| | |
|----------------|---|
| Command | <pre>access-list <i>acl-id</i> { permit deny } {any host <i>src-mac-addr</i> / <i>src-mac-addr mask</i> } {any host <i>dst-mac-addr</i> / <i>dst-mac-addr mask</i> } [<i>ethernet-type</i>] [cos <i>cos</i> [inner <i>cos</i>]] [</pre> |
|----------------|---|

| | |
|------------------------------|--|
| | time-range <i>tm-rng-name</i>] |
| Parameter Description | <p><i>acl-id</i>: Indicates the ID of a numbered ACL. It uniquely identifies an ACL. The value range of <i>acl-id</i> is 700–799.</p> <p>permit: Indicates that the ACE is a permit ACE.</p> <p>deny: Indicates that the ACE is a deny ACE.</p> <p>host src-mac-addr: Indicates that IP packets sent from a host with the specified source MAC address are filtered.</p> <p><i>src-mac-addr mask</i>: Indicates that the source MAC address is reversed.</p> |
| | <p>any: Indicates that L2 packets sent to any host are filtered.</p> <p>host dst-mac-addr: Indicates that IP packets sent to a host with the specified destination MAC address are filtered.</p> <p><i>dst-mac-addr mask</i>: Indicates that the destination MAC address is reversed.</p> <p><i>ethernet-type</i>: Indicates that L2 packets of the specified Ethernet type are filtered.</p> <p>cos cos: Indicates that L2 packets with the specified cos field in the outer tag are filtered.</p> <p>inner cos: Indicates that L2 packets with the specified cos field in the inner tag are filtered.</p> <p>time-range time-range-name: Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range.</p> |
| Command Mode | Global configuration mode |
| Usage Guide | Run this command to add ACEs to a numbered MAC extended ACL in global configuration mode. It cannot be used to add ACEs to a named MAC extended ACL. |

❖ Applying an MAC Extended ACL

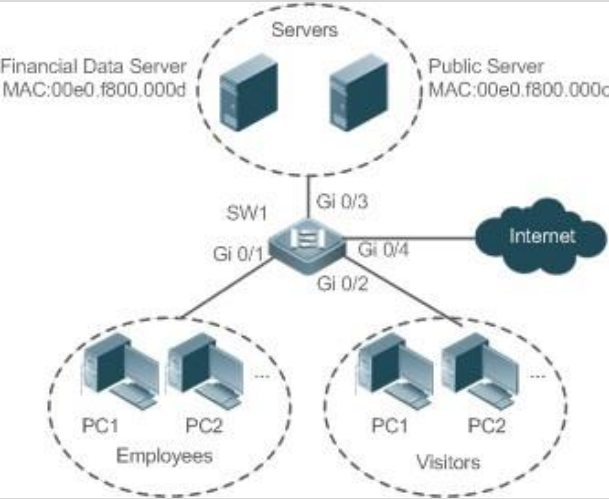
| | |
|------------------------------|---|
| Command | mac access-group { <i>acl-id</i> <i>acl-name</i> } { in out } |
| Parameter Description | <p><i>acl-id</i>: Indicates that a numbered MAC extended IP ACL will be applied to the interface. <i>acl-name</i>: Indicates that a named MAC extended IP ACL will be applied to the interface. in: Indicates that this ACL controls incoming L2 packets of the interface.</p> <p>out: Indicates that this ACL controls outgoing L2 packets of the interface.</p> |

| | |
|---------------------|--|
| Command Mode | Interface configuration mode |
| Usage Guide | This command makes an MAC extended ACL take effect on the incoming or outgoing packets of a specified interface. |

Configuration Example

The following configuration example describes only ACL-related configurations.

❖ Configuring an MAC Extended ACL to Restrict Resources Accessible by Visitors

| | |
|-----------------------------------|--|
| <p>Scenario Figure 1-4</p> |  |
| <p>Configuration Steps</p> | <ul style="list-style-type: none"> ▪ Configure an MAC extended ACL. ▪ Add ACEs to the MAC extended ACL. ▪ Apply the MAC extended ACL to the outgoing direction of the interface connected to the visitor area so that visitors are allowed to access Internet and the public server of the company, but prohibited from accessing the financial data server of the company. That is, visitors cannot access the server with the MAC address 00e0.f800.000d. |
| <p>SW1</p> | <pre>sw1(config)#mac access-list extended 700 sw1(config-mac- nacl)#deny any host 00e0.f800.000d sw1(config- mac-nacl)#permit any any sw1(config-mac- nacl)#exit sw1(config)#int gigabitEthernet 0/2 sw1(config-if-GigabitEthernet 0/2)#mac access-group 700 in</pre> |

| | |
|---------------------|--|
| Verification | <ul style="list-style-type: none"> ▪ On a visitor's PC, ping the financial data server. Verify that the ping operation fails. ▪ On a visitor's PC, ping the public resource server. Verify that the ping operation succeeds. ▪ On a visitor's PC, access the Internet, for example, visit the Baidu website. Verify that the webpage can be opened. |
| SW1 | <pre>sw1(config)#sh ow access-lists mac access-list extended 700 10 deny any host 00e0.f800.000d etype-any 20 permit any any etype- any sw1(config)#show access-group mac access-group 700 in</pre> |
| | Applied On interface GigabitEthernet 0/2 |

1.4.3 Configuring an Expert Extended ACL

Configuration Effect

Configure and apply an expert extended ACL to an interface/VXLAN to control incoming and outgoing packets of the interface/VXLAN based on the L2 and L3 information, and allow or prohibit the entry of specific packets to the network. In addition, you can configure an expert extended ACL to control all L2 packets based on the VLAN to permit or deny the access of users in some network segments to network resources. Generally, you can use an expert extended ACL if you want to incorporate ACEs of the IP ACL and MAC extended ACL into one ACL.

Configuration Steps

❖ Configuring an Expert Extended ACL

- (Mandatory) Configure an expert extended ACL if you want to control users' access to network resources based on the L2 packet header, for example, the VLAN ID.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The expert extended ACL takes effect only on the local device, and does not affect other devices on the network.

❖ Adding ACEs to an Expert Extended ACL

- (Optional) An ACL may contain zero or multiple ACEs. If no ACE is configured, all incoming packets of the device are denied by default.

❖ Applying an Expert Extended ACL

- (Mandatory) Apply an expert extended ACL to a specified interface if you want this ACL take effect.
- You can apply an expert extended ACL in the incoming or outgoing direction of a specified interface of an access, an aggregate, or a core device based on the distribution of users.

Verification

- Use the following methods to verify the configuration effects of the expert extended ACL:
- If IP-based access rules are configured in an expert extended ACL to permit or deny some IP packets, run the **ping** command to verify whether these rules take effect.
- If MAC-based access rules are configured in an expert extended ACL to permit or deny some L2 packets (e.g. ARP packets), also run the **ping** command to check whether ACEs of this ACL takes effect on the specified interface. For example, to filter out ARP packets, run the **ping** command for verification.
- If VLAN ID-based access rules are configured in an expert extended ACL to permit or deny some L2 packets in some network segments (e.g., to prevent communication between VLAN 1 users and VLAN 2 users), ping PCs of VLAN 2 on a PC of VLAN 1. If the ping operation fails, the rules take effect.

Related Commands

❖ Configuring an Expert Extended ACL

| | |
|-----------------------|--|
| Command | expert access-list extended { <i>acl-name</i> <i>acl-id</i> } |
| Parameter Description | <p><i>acl-name</i>: Indicates the name of an expert extended ACL. If this option is configured, a named ACL is created. The name is a string of 1 to 99 characters. The ACL name cannot start with numbers (0–9), "in", or "out".</p> <p><i>acl-id</i>: Indicates the ID of an expert extended ACL. If this option is configured, a numbered ACL is created.</p> <p>The value range of <i>acl-id</i> is 2700-2899.</p> |
| Command Mode | Global configuration mode |
| Usage Guide | Run this command to configure an expert extended ACL and enter expert extended ACL configuration mode. |

❖ Adding ACEs to an Expert Extended ACL

Use either of the following methods to add ACEs to an expert extended ACL:

- Add ACEs in expert extended ACL configuration mode.

| | |
|-----------------------|---|
| Command | <pre>[sn]{ permit deny }[protocol [ethernet-type][cos [out] [inner in]]] [[VID [out][inner in]]] {source source-wildcard host source any}{host source-mac-address any } {destination destination-wildcard host destination any} {host destination-mac-address any} [[precedence precedence] [tos tos] [dscp dscp]] [fragment] [range lower upper] [time-range time-range- name]]</pre> |
| Parameter Description | <p>sn: Indicates the sequence number of an ACE. The value ranges from 1 to 2,147,483,647. This sequence number determines the priority of this ACE in the ACL. A smaller sequence number indicates a higher priority. An ACE with a higher priority will be preferentially used to match packets. If you do not specify the sequence number when adding an ACE, the system automatically allocates a sequence number, which is equal to an increment (10 by default) plus the sequence number of the last ACE in the current ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a newly-added ACE will be 110 by default. You can adjust the increment using a command.</p> <p>permit: Indicates that the ACE is a permit ACE.</p> <p>deny: Indicates that the ACE is a deny ACE.</p> <p>protocol: Indicates the IP protocol number. The value ranges from 0 to 255. To facilitate the use, the system provides frequently-used abbreviations to replace the specific IP protocol numbers, including eigrp, gre, icmp, igmp, ip, ipinip, nos, ospf, tcp, and udp.</p> <p>ethernet-type: Indicates that L2 packets of the specified Ethernet type are filtered.</p> <p>cos out: Indicates that L2 packets with the specified cos field in the outer tag are filtered.</p> <p>cos inner in: Indicates that L2 packets with the specified cos field in the inner tag are filtered.</p> <p>VID out: Indicates that L2 packets with the specified VLAN ID field in the outer tag are filtered.</p> <p>VID inner in: Indicates that L2 packets with the specified VLAN ID field in the inner tag are filtered.</p> <p>source source-wildcard: Indicates that IP packets sent from hosts in the specified IP network segment are filtered.</p> <p>host source: Indicates that IP packets sent from a host with the specified source IP address are filtered.</p> <p>any: Indicates that IP packets sent from any host are filtered.</p> <p>host source-mac-address: Indicates that IP packets sent from a host with the specified source MAC address are filtered.</p> <p>any: Indicates that L2 packets sent to any host are filtered.</p> |

| | |
|---------------------|--|
| | <p><i>destination destination-wildcard</i>: Indicates that IP packets sent to hosts in a specified IP network segment are filtered.</p> <p>host destination: Indicates that IP packets sent to a host with the specified destination IP address are filtered.</p> <p>any: Indicates that IP packets sent to any host are filtered.</p> <p>host destination-mac-address: Indicates that IP packets sent to a host with the specified destination MAC address are filtered.</p> <p>any: Indicates that L2 packets sent to any host are filtered.</p> <p>precedence precedence: Indicates that IP packets with the specified precedence field in the header are filtered.</p> <p>tos tos: Indicates that IP packets with the specified the TOS field in the header are filtered. dscp dscp: Indicates that IP packets with the specified the dscp field in the header are filtered. fragment: Indicates that only fragmented IP packets except the first fragments are filtered.</p> <p>time-range time-range-name: Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range.</p> |
| Command Mode | Expert extended ACL configuration mode |
| Usage Guide | Run this command to add ACEs in expert extended ACL configuration mode. The ACL can be a named or numbered ACL. |

- Add ACEs to an expert extended ACL in global configuration mode.

| | |
|------------------------------|--|
| Command | <pre>access-list <i>acl-id</i>{ permit deny }<i>[protocol] [ethernet-type][cos [out] [inner in]]</i> <i>[[VID [out][inner in]]]</i> <i>{source source-wildcard hostsource any}{host source-mac-address any } {destination destination-wildcard hostdestination any} {host destination-mac-address any} <i>[[precedence precedence] [tos tos] [dscp dscp]][fragment] [range lowerupper][time-range time- range-name]]</i></i></pre> |
| Parameter Description | <p><i>acl-id</i>: Indicates the ID of a numbered ACL. It uniquely identifies an ACL. The value range of <i>acl-id</i> is 2700-2899.</p> <p>permit: Indicates that the ACE is a permit ACE.</p> <p>deny: Indicates that the ACE is a deny ACE.</p> <p><i>protocol</i>: Indicates the IP protocol number. The value ranges from 0 to 255. To facilitate the use, the system provides frequently-used abbreviations to replace the specific IP protocol numbers, including eigrp, gre, icmp, igmp, ip, ipinip, nos, ospf, tcp, and udp.</p> |

| | |
|---------------------|---|
| | <p><i>ethernet-type</i>: Indicates that L2 packets of the specified Ethernet type are filtered.</p> <p>cos out: Indicates that L2 packets with the specified cos field in the outer tag are filtered.</p> <p>cos inner in: Indicates that L2 packets with the specified cos field in the inner tag are filtered.</p> <p>VID out: Indicates that L2 packets with the specified VLAN ID field in the outer tag are filtered.</p> <p>VID inner in: Indicates that L2 packets with the specified VLAN ID field in the inner tag are filtered.</p> <p><i>source source-wildcard</i>: Indicates that IP packets sent from hosts in the specified IP network segment are filtered.</p> <p>host source: Indicates that IP packets sent from a host with the specified source IP address are filtered.</p> <p>any: Indicates that IP packets sent from any host are filtered.</p> <p>host source-mac-address: Indicates that IP packets sent from a host with the specified source MAC address are filtered.</p> <p>any: Indicates that L2 packets sent to any host are filtered.</p> <p><i>destination destination-wildcard</i>: Indicates that IP packets sent to hosts in a specified IP network segment are filtered.</p> <p>host destination: Indicates that IP packets sent to a host with the specified destination IP address are filtered.</p> <p>any: Indicates that IP packets sent to any host are filtered.</p> <p>host destination-mac-address: Indicates that IP packets sent to a host with the specified destination MAC address are filtered.</p> <p>any: Indicates that L2 packets sent to any host are filtered.</p> <p>precedence precedence: Indicates that IP packets with the specified precedence field in the header are filtered.</p> <p>tos tos: Indicates that IP packets with the specified the TOS field in the header are filtered. dscp dscp: Indicates that IP packets with the specified the dscp field in the header are filtered. fragment: Indicates that only fragmented IP packets except the first fragments are filtered.</p> <p>time-range time-range-name: Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range.</p> |
| Command Mode | Global configuration mode |
| Usage Guide | Run this command to add ACEs to a numbered expert extended ACL in global configuration mode. It cannot |

be used to add ACEs to a named expert extended ACL.

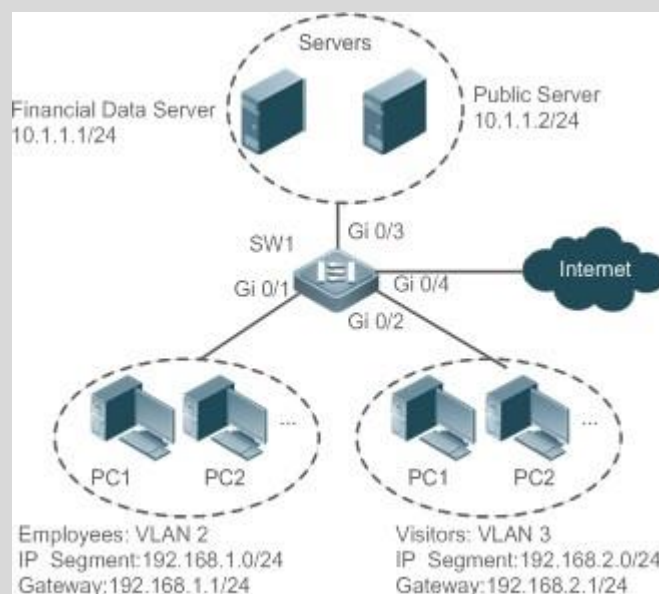
❖ Applying an Expert Extended ACL

| | |
|------------------------------|--|
| Command | <code>expert access-group { <i>acl-id</i> <i>acl-name</i> } { in out }</code> |
| Parameter Description | <ul style="list-style-type: none"> ▪ <i>acl-id</i>: Indicates that a numbered expert extended ACL will be applied to the interface. ▪ <i>acl-name</i>: Indicates that a named expert extended ACL will be applied to the interface. ▪ in: Indicates that this ACL controls incoming L2 packets of the interface. ▪ out: Indicates that this ACL controls outgoing L2 packets of the interface. |
| Command Mode | Interface configuration mode |
| Usage Guide | This command makes an expert extended ACL take effect on the incoming or outgoing packets of a specified interface. |

Configuration Example

The following configuration example describes only ACL-related configurations.

- ❖ Configuring an Expert Extended ACL to Restrict Resources Accessible by Visitors (It is required that visitors and employees cannot communicate with each other, visitors can access the public resource server but not
- ❖ the financial data server of the company.)

Scenario
Figure 1-5**Configuration Steps**

- Configure an expert extended ACL.
- Add an ACE to deny packets sent from PCs in the visitor area (VLAN 3) to employee PCs in VLAN2.
- Add an ACE to prevent visitors from accessing the financial data server of the company.
- Add an ACE to permit all packets.
- Apply the ACL to the incoming direction of the interface of the switch that connects to the visitor area.

SW1

```
sw1(config)#expert access-list extended 2700

sw1(config-exp-nacl)#deny ip any any
192.168.1.0 0.0.0.255 any sw1(config-
exp-nacl)#deny ip any any host 10.1.1.1
any sw1(config-exp-nacl)#pemit any any
any any
sw1(config-exp-
nacl)#exit
sw1(config)#int
gigabitEthernet
0/2
sw1(config-if-GigabitEthernet 0/2)#expert access-group 2700 in
```

Verification

- On a visitor's PC, ping the financial data server. Verify that the ping operation fails.
- On a visitor's PC, ping the public resource server. Verify that the ping operation succeeds.
- On a visitor's PC, ping the gateway address 192.168.1.1 of an employee. Verify that the ping operation fails.

| | |
|------------|--|
| | <ul style="list-style-type: none"> On a visitor's PC, access the Internet, for example, visit the Baidu website. Verify that the webpage can be opened. |
| SW1 | <pre>sw1(config)#show access-lists expert access-list extended 2700 10 deny ip any any 192.168.1.0 0.0.0.255 any 20 deny ip any any host 10.1.1.1 any 30 permit ip any any any any sw1(config)#show access-group expert access-group 2700 in</pre> |

1.4.4 Configuring an IPv6 Extended ACL

Configuration Effect

Configure and apply an IPv6 ACL to an interface/VXLAN to control all incoming and outgoing IPv5 packets of this interface/VXLAN. You can permit or deny the entry of specific IPv6 packets to a network to control access of IPv6 users to network resources.

Configuration Steps

❖ Configuring an IPv6 ACL

- (Mandatory) Configure an IP ACL if you want to access of IPv4 users to network resources.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The IPv6 ACL takes effect only on the local device, and does not affect other devices on the network.

❖ Adding ACEs to an IPv6 ACL

- (Optional) An ACL may contain zero or multiple ACEs. If no ACE is configured, all incoming IPv6 packets of the device are denied by default.

❖ Applying an IPv6 ACL

- (Mandatory) Apply an IPv6 ACL to a specified interface on a device if you want this ACL take effect.
- You can apply an IPv6 ACL on a specified interface/VXLAN of an access, an aggregate, or a core device based on the distribution of users.

Verification

- Use the following methods to verify the configuration effects of the IPv6 ACL:
- Run the **ping** command to verify that the IPv6 ACL takes effect on the specified interface. For example, if an IPv6 ACL is configured to prohibit a host with a specified IP address or hosts in a specified IPv6 address range from accessing the network, run the **ping** command to verify that the host(s) cannot be successfully pinged.

- Access network resources, for example, visit an IPv6 website, to check whether the IPv6 ACL takes effect on the specified interface.

Related Commands

❖ Configuring an IPv6 ACL

| | |
|------------------------------|---|
| Command | <code>ipv6 access-list <i>acl-name</i></code> |
| Parameter Description | <i>acl-name</i> : Indicates the name of a standard or an extended IP ACL. The name is a string of 1 to 99 characters. The ACL name cannot start with numbers (0–9), "in", or "out". |
| Command Mode | Global configuration mode |
| Usage Guide | Run this command to configure an IPv6 ACL and enter IPv6 configuration mode. |

❖ Adding ACEs to an IPv6 ACL

- To filter TCP or UDP packets, add ACEs to an IPv6 ACL as follows:

| | |
|----------------|---|
| Command | <code>[<i>sn</i>] {permit deny } <i>protocol</i> {<i>src-ipv6-prefix/prefix-len</i> host <i>src-ipv6-addr</i> any} {<i>dst-ipv6-pfix/pfix-len</i> host <i>dst-ipv6-addr</i> any} [<i>op dstport</i> range <i>lower upper</i>] [dscp <i>dscp</i>] [flow-label <i>flow-label</i>] [fragment] [time-rangetm-rng-name][log]</code> |
|----------------|---|

| Parameter Description | |
|-----------------------|--|
| | <p><i>sn</i>: Indicates the sequence number of an ACE. The value ranges from 1 to 2,147,483,647. This sequence number determines the priority of this ACE in the ACL. A smaller sequence number indicates a higher priority. An ACE with a higher priority will be preferentially used to match packets. If you do not specify the sequence number when adding an ACE, the system automatically allocates a sequence number, which is equal to an increment (10 by default) plus the sequence number of the last ACE in the current ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a newly-added ACE will be 110 by default. You can adjust the increment using a command.</p> <p>permit: Indicates that the ACE is a permit ACE.</p> <p>deny: Indicates that the ACE is a deny ACE.</p> <p><i>protocol</i>: Indicates the IPv6 protocol number. The value ranges from 0 to 255. To facilitate the use, the system provides frequently-used abbreviations of IPv6 protocol numbers to replace the specific IP protocol numbers, including icmp, ipv6, tcp, and udp.</p> <p><i>src-ipv6-prefix/prefix-len</i>: Indicates that IP packets sent from hosts in the specified IPv6 network segment are filtered.</p> <p>host <i>src-ipv6-addr</i>: Indicates that IPv6 packets sent from a host with the specified source IP address are filtered.</p> <p>any: Indicates that IPv6 packets sent from any host are filtered.</p> <p><i>dst-ipv6-pfx/pfx-len</i>: Indicates that IPv6 packets sent from hosts in the specified IPv6 network segment are filtered.</p> <p>host <i>dst-ipv6-addr</i>: Indicates that IPv6 packets sent to a host with the specified destination IP address are filtered.</p> <p>any: Indicates that IPv6 packets sent to any host are filtered.</p> <p><i>op dstport</i>: Indicates that TCP or UDP packets are filtered based on the L4 destination port number. The value of the op parameter can be eq (equal to), neq (not equal to), gt (greater than), or lt (smaller than). range <i>lower upper</i>: Indicates that TCP or UDP packets with the L4 destination port number in the specified range are filtered.</p> <p>dscp <i>dscp</i>: Indicates that IPv6 packets with the specified the dscp field in the header are filtered.</p> <p>flow-label <i>flow-label</i>: Indicates that IPv6 packets with the specified the flow label field in the header are filtered.</p> <p>fragment: Indicates that only fragmented IPv6 packets except the first fragments are filtered.</p> <p>time-range <i>time-range-name</i>: Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range. log: Indicates that logs will be periodically output if packets matching the ACEs are found. For details about logs, see "ACL Logging" in this document.</p> |

| | |
|---------------------|--|
| Command Mode | IPv6 ACL configuration mode |
| Usage Guide | Run this command to add ACEs in IPv6 ACL configuration mode. |

- To filter IPv6 packets except for the TCP or UDP packets, add ACEs to an IPv6 ACL as follows:

| | |
|------------------------------|---|
| Command | <code>[sn] { permit deny } protocol { src-ipv6-prefix/prefix-len host src-ipv6-addr any } { dst-ipv6-pfix/pfix-len host dst-ipv6-addr any } [dscp dscp] [flow-label flow-label] [fragment] [time-rangetm-rng-name] [log]</code> |
| Parameter Description | <p>sn: Indicates the sequence number of an ACE. The value ranges from 1 to 2,147,483,647. This sequence number determines the priority of this ACE in the ACL. A smaller sequence number indicates a higher priority. An ACE with a higher priority will be preferentially used to match packets. If you do not specify the sequence number when adding an ACE, the system automatically allocates a sequence number, which is equal to an increment (10 by default) plus the sequence number of the last ACE in the current ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a newly-added ACE will be 110 by default. You can adjust the increment using a command.</p> <p>permit: Indicates that the ACE is a permit ACE.</p> <p>deny: Indicates that the ACE is a deny ACE.</p> <p>protocol: Indicates the IPv6 protocol number. The value ranges from 0 to 255. To facilitate the use, the system provides frequently-used abbreviations of IPv6 protocol numbers to replace the specific IP protocol numbers, including icmp, ipv6, tcp, and udp.</p> <p>src-ipv6-prefix/prefix-len: Indicates that IP packets sent from hosts in the specified IPv6 network segment are filtered.</p> <p>host src-ipv6-addr: Indicates that IPv6 packets sent from a host with the specified source IP address are filtered.</p> <p>any: Indicates that IPv6 packets sent from any host are filtered.</p> <p>dst-ipv6-pfix/pfix-len: Indicates that IPv6 packets sent from hosts in the specified IPv6 network segment are filtered.</p> <p>host dst-ipv6-addr: Indicates that IPv6 packets sent to a host with the specified destination IP address are filtered.</p> <p>any: Indicates that IPv6 packets sent to any host are filtered.</p> |

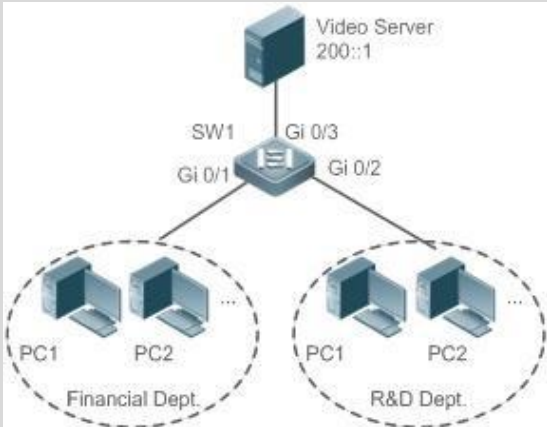
| | |
|---------------------|--|
| | <p>dscp <i>dscp</i>: Indicates that IPv6 packets with the specified the dscp field in the header are filtered.</p> <p>flow-label <i>flow-label</i>: Indicates that IPv6 packets with the specified the flow label field in the header are filtered.</p> <p>fragment: Indicates that only fragmented IPv6 packets except the first fragments are filtered.</p> <p>time-range <i>time-range-name</i>: Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range. log: Indicates that logs will be periodically output if packets matching the ACEs are found. For details about logs, see "ACL Logging" in this document.</p> |
| Command Mode | IPv6 ACL configuration mode |
| Usage Guide | Run this command to add ACEs in IPv6 ACL configuration mode. |

❖ Applying an IPv6 ACL

| | |
|------------------------------|---|
| Command | ipv6 traffic-filter <i>acl-name</i> { in out } |
| Parameter Description | <p><i>acl-name</i>: Indicates the name of an IPv6 ACL.</p> <p>in: Indicates that this ACL controls incoming IPv6 packets of the interface.</p> <p>out: Indicates that this ACL controls outgoing IPv6 packets of the interface.</p> |
| Command Mode | Interface configuration mode |
| Usage Guide | This command makes an IPv6 ACL take effect on the incoming or outgoing packets of the specified interface. |

Configuration Example

- ❖ Configuring an IPv6 ACL to Prohibit the R&D Department from Accessing the Video Server

| | |
|-----------------------------------|---|
| <p>Scenario Figure 1-6</p> |  |
| <p>Configuration Steps</p> | <ul style="list-style-type: none"> ▪ Configure an IPv6 ACL. ▪ Add an ACE to the IPv6 ACL to prevent access to the video server. ▪ Add an ACE to the IPv6 ACL to permit all IPv6 packets. ▪ Apply the IPv6 ACL to the incoming direction of the interface connected to the R&D department. |
| <p>SW1</p> | <pre>sw1(config)#ipv6 access-list dev_deny_ipv6video sw1(config-ipv6-nacl)#deny ipv6 any host 200::1 sw1(config-ipv6-nacl)#permit ipv6 any any sw1(config-ipv6-nacl)#exit sw1(config)#int gigabitEthernet 0/2 sw1(config-if-GigabitEthernet 0/2)# ipv6 traffic-filter dev_deny_ipv6video in</pre> |
| <p>Verification</p> | <p>On a PC of the R&D department, ping the video server. Verify that the ping operation fails.</p> |
| <p>SW1</p> | <pre>sw1(config)#show access-lists ipv6 access-list dev_deny_ipv6vid eo 10 deny ipv6 any host 200::1 20 permit ipv6 any any sw1(config)#show access-group ipv6 traffic-filter dev_deny_ipv6video in Applied On interface GigabitEthernet 0/2</pre> |

1.4.5 Configuring an ACL80 Configuration Effect

When the IP ACL, MAC extended ACL, expert extended ACL, and IPv6 ACL with fixed matching fields cannot meet requirements, configure the ACL80 to customize the packet fields that need to be matched.

Configuration Steps

❖ Configuring an Expert Advanced ACL

- (Mandatory) Configure an expert advanced ACL if you want to implement the ACL80 function. For details about how to configure the expert advanced ACL, see the related descriptions.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The expert advanced ACL takes effect only on the local device, and does not affect other devices on the network.

❖ Adding ACEs to an Expert Advanced ACL

- (Mandatory) Add ACEs to an expert advanced ACL to customize matching fields. If no ACE is added to the expert advanced ACL, the deny ACEs will drop all packets by default. For details about how to add an ACE to an expert advanced ACL, see the related descriptions.

❖ Applying an Expert Advanced ACL

- (Mandatory) Apply an expert advanced ACL to a specified interface if you want this ACL take effect.
- You can apply an expert advanced ACL on a specified interface of an access, an aggregate, or a core device based on the distribution of users.

Verification

- Use the following methods to verify the configuration effects of the expert advanced ACL:
- Run the **ping** command to check whether the configurations take effect.
- Construct packets matching the ACEs to check whether ACEs take effect.

Related Commands

❖ Configuring an Expert Advanced ACL

| | |
|-----------------------|---|
| Command | expert access-list advanced <i>acl-name</i> |
| Parameter Description | <i>acl-name</i> : Indicates the name of an expert advanced ACL. The name is a string of 1 to 99 characters. The ACL name cannot start with numbers (0–9), "in", or "out". |

| | |
|---------------------|--|
| Command Mode | Global configuration mode |
| Usage Guide | Run this command to configure an expert advanced ACL and enter expert advanced ACL configuration mode. |

❖ Adding ACEs to an Expert Advanced ACL

| | |
|------------------------------|---|
| Command | [sn] { permit deny } hex hex-mask offset |
| Parameter Description | <p><i>sn</i>: Indicates the sequence number of an ACE. The value ranges from 1 to 2,147,483,647. This sequence number determines the priority of this ACE in the ACL. A smaller sequence number indicates a higher priority. An ACE with a higher priority will be preferentially used to match packets. If you do not specify the sequence number when adding an ACE, the system automatically allocates a sequence number, which is equal to an increment (10 by default) plus the sequence number of the last ACE in the current ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a newly-added ACE will be 110 by default. You can adjust the increment using a command.</p> <p>permit: Indicates that the ACE is a permit ACE.</p> <p>deny: Indicates that the ACE is a deny ACE.</p> <p><i>hex</i>: Indicates the customized matching rule expressed in hexadecimal format, for example, 00d0f800.</p> <p><i>hex-mask</i>: Indicates the matching mask.</p> <p><i>offset</i>: Indicates the start position of matching. For example, if the matching content is 00d0f800, the matching mask is 00ff0000, and start position is 6, the destination MAC address of each packet is compared. All packets whose second byte of the destination MAC address is d0 match this ACE.</p> |
| Command Mode | Expert advanced ACL configuration mode |
| Usage Guide | Run this command to add ACEs in expert advanced ACL configuration mode. |

❖ Applying an Expert Advanced ACL

| | |
|----------------|--|
| Command | expert access-group <i>acl-n</i> { in out } |
|----------------|--|

| | |
|------------------------------|---|
| Parameter Description | <p><i>acl-id</i>: Indicates that a numbered expert advanced ACL will be applied to the interface. <i>acl-name</i>: Indicates that a named expert advanced ACL will be applied to the interface. in: Indicates that this ACL controls incoming L2 packets of the interface.</p> <p>out: Indicates that this ACL controls outgoing L2 packets of the interface.</p> |
| Command Mode | Interface configuration mode |
| Usage Guide | This command makes an expert advanced ACL take effect on the incoming or outgoing packets of a specified interface. |

Configuration Example

The following configuration example describes only ACL-related configurations.

- ❖ Configuring an ACL80 to Restrict Resources Accessible **by** Visitors (It is required that visitors and employees cannot communicate with each other, visitors can access the public resource server but not the financial data server of the company.)
- ❖ server of the company.)

| | |
|----------------------------|---|
| Scenario Figure 1-7 | |
| Configuration Steps | <ul style="list-style-type: none"> ▪ Configure an expert advanced ACL. ▪ Add an ACE to deny packets sent from PCs in the visitor area (VLAN 3) to employee PCs in VLAN2. ▪ Add an ACE to prevent visitors from accessing the financial data server of the company. |

| | |
|---------------------|---|
| | <ul style="list-style-type: none"> ▪ Add an ACE to permit all packets. ▪ Apply the ACL to the incoming direction of the interface of the switch that connects to the visitor area. |
| SW1 | <pre>sw1(config)#expert access-list advanced acl80-guest sw1(config-exp- dacl)#deny COA801 FFFFFFFF 42 sw1(config-exp-dacl)#deny 0A010101 FFFFFFFF 42 sw1(config-exp-dacl)#permit 0806 FFFF 24 sw1(config-exp-dacl)#permit 0800 FFFF 24 sw1(config-exp-dacl)#exit sw1(config)#int gigabitEthernet 0/2 sw1(config-if-GigabitEthernet 0/2)#expert access-group acl80-guest in</pre> |
| Verification | <ul style="list-style-type: none"> ▪ On a visitor's PC, ping the financial data server. Verify that the ping operation fails. ▪ On a visitor's PC, ping the public resource server. Verify that the ping operation succeeds. ▪ On a visitor's PC, ping the gateway address 192.168.1.1 of an employee. Verify that the ping operation fails. ▪ On a visitor's PC, access the Internet, for example, visit the Baidu website. Verify that the webpage can be opened. |
| SW1 | <pre>sw1(config)#show access-lists expert access-list advanced sss 10 deny COA801 FFFFFFFF 42 20 deny 0A010101 FFFFFFFF 42 30 permit 0806 FFFF 24 40 permit 0800 FFFF 24 expert access-group acl80-guest in Applied On interface GigabitEthernet 0/2</pre> |

1.4.6 Configuring ACL Redirection

Configuration Effect

Configure the ACL redirection function on a specified interface to directly redirect specified packets on the interface to a specified port for further forwarding.

Configuration Steps

❖ Configuring an ACL

- (Mandatory) To implement ACL redirection, you must first configure an ACL, for example, an IP, MAC extended, or expert extended ACL. For details about how to configure an ACL, see the related descriptions.
- You can configure this ACL on an access, an aggregate, or a core device

based on the distribution of users. The IPv6 ACL takes effect only on the local device, and does not affect other devices on the network.

❖ Adding ACEs to an ACL

- (Optional) An ACL may contain zero or multiple ACEs. If no ACE is configured, the ACL redirection function is not available. For details about how to add an ACE to an ACL, see the related descriptions.

❖ Configuring ACL Redirection

- (Mandatory) Enable ACL redirection on a specified interface if you want to implement ACL redirection.
- You can configure the ACL redirection function on a specified interface of an access, an aggregate, or a core device based on the distribution of users.

Verification

Send packets matching ACEs on the port where ACL redirection is enabled, and then use the packet capturing software on the destination port to check whether the ACL redirection function takes effect.

Related Commands

❖ Configuring an ACL

For details about how to configure an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

❖ Adding ACEs to an ACL

For details about how to add ACEs to an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

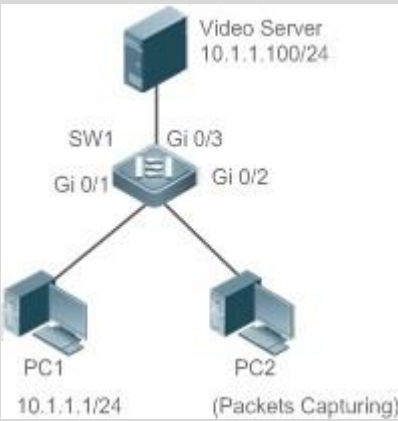
❖ Configuring ACL Redirection on Interface

| | |
|-----------------------|---|
| Command | redirect destination interface <i>interface-name</i> acl { <i>acl-id</i> <i>acl-name</i> } in |
| Parameter Description | <p>interface <i>interface-name</i>: Indicates the name of the destination port for redirection.</p> <p><i>acl-id</i>: Indicates the ID of an ACL.</p> <p><i>acl-name</i>: Indicates the name of an ACL.</p> <p>in: Indicates that incoming packets of the interface are redirected.</p> |
| Command Mode | Interface configuration mode |
| Usage Guide | Run this command to redirect incoming packets of the interface that match ACEs to the destination port for further forwarding. |

Configuration Example

The following configuration example describes only ACL-related configurations.

- ❖ Enabling ACL Redirection to Redirect Packets Sent from the Host 10.1.1.1 to the Packet Capturing Device for Analysis

| | |
|-----------------------------------|--|
| <p>Scenario Figure 1-8</p> |  |
| <p>Configuration Steps</p> | <ul style="list-style-type: none"> ▪ Configures an IP ACL. ▪ Add an ACE to the IP ACL to permit packets sent from the host 10.1.1.1. ▪ Enable ACL redirection on the port Gi 0/1, and set the destination port to Gi 0/2. |
| <p>SW1</p> | <pre>sw1(config)#ip access-list standard 1 sw1 (config-std-nacl)#permit host 10.1.1.1 sw1(config-std-nacl)#exit sw1(config)#int gigabitEthernet 0/1 sw1(config-if-GigabitEthernet 0/1)# redirect destination interface gigabitEthernet 0/2 acl 1</pre> |
| <p>Verification</p> | <p>Capture packets on PC 2. Ping the video server on PC 1. Verify that ICMP requests sent from PC 1 are captured on PC 2.</p> |

SW1

```

sw1#show
access-lists
ip access-
list standard
1 10 permit
host
10.1.1.1
sw1#show redirect interface gigabitEthernet 0/1
acl redirect configuration on interface gigabitEthernet 0/1

redirect destination interface gigabitEthernet 0/2 acl 1 in

```

1.4.7 Configuring a Global Security ACL

Configuration Effect

Configure a global security ACL to prevent internal PCs of a company from accessing illegal websites or prevent virus from attacking the company's internal network. You can also configure exclusive interfaces to allow specified departments of the company to access external websites.

Configuration Steps

❖ Configuring an ACL

- (Mandatory) Configure an ACL if you want to protect the internal network globally. For details about the configuration method, see the earlier descriptions about the ACL.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The configurations take effect only on the local device, and do not affect other devices on the network.

❖ Adding ACEs to an ACL

- (Optional) An ACL may contain zero or multiple ACEs. If no ACE is configured, it is equivalent that the global security ACL does not exist. For details about how to add an ACE to an ACL, see the related descriptions.

❖ Configuring a Global Security ACL

- (Mandatory) Enable the global security function if you want to make the global security ACL take effect.
- You can configure a global security ACL on an access, an aggregate, or a core device based on the distribution of users.

Verification

On the internal network protected by the global security ACL, ping the website or device that are denied by ACEs to check whether the global security ACL takes effect.

Related Commands

❖ Configuring an ACL

For details about the configuration method, see the earlier descriptions about the ACL.

❖ Adding ACEs to an ACL

For details about the configuration method, see the earlier descriptions about the ACL.

❖ Configuring a Global Security ACL

| | |
|-----------------------|--|
| Command | { ip mac expert } access-group acl-id { in out } |
| Parameter Description | acl-id : Indicates the ID of an ACL. in : Filters the incoming packets of the device. out : Filters the outgoing packets of the device. |
| Command Mode | Global configuration mode |
| Usage Guide | Run this command to enable the global security ACL so that the ACL takes effect on all L2 interfaces of the device. |

❖ Configuring an Exclusive Interface of the Global Security ACL

| | |
|-----------------------|--|
| Command | no global ip access-group |
| Parameter Description | N/A |
| Command Mode | Interface configuration mode |
| Usage Guide | Run this command to invalidate a global security ACL on a specified interface. |

Configuration Example

The following configuration example describes only ACL-related configurations.

- ❖ Configuring a Global Security ACL to Prevent the R&D Department From Accessing the Server of the Sales Department but Allow the Sales Department to Access This Server

| | |
|-----------------------------------|---|
| <p>Scenario Figure 1-9</p> | |
| <p>Configuration Steps</p> | <ul style="list-style-type: none"> Configure an extended IP ACL "ip_ext_deny_dst_sale_server". Add the ACE that prevents the device to forward packets to the destination host 10.1.1.3/24. Configure the ACL "ip_ext_deny_dst_sale_server" as a global security ACL. Configure the interface directly connected to the sales department as the exclusive interface of the global security ACL. |
| <p>SW1</p> | <pre>sw1(config)#ip access-list extended ip_ext_deny_dst_sale_server sw1(config-ext-nacl)# deny ip any host 10.1.1.3 sw1(config-ext-nacl)#exit sw1(config)#ip access-group ip_ext_deny_dst_sale_server in sw1(config)#int gigabitEthernet 0/1 sw1(config-if-GigabitEthernet 0/1)# no global ip access-group</pre> |
| <p>Verification</p> | <ul style="list-style-type: none"> On a PC of the sales department, ping the server of the sales department. Verify that the ping operation succeeds. On the PCs of R&D department 1 and R&D department 2, ping the server of the sales department. Verify that the ping operations fail. |

```
sw1#show access-lists

ip access-list extended ip_ext_deny_dst_sale_server 10 deny ip any host
10.1.1.3

sw1#show running
.....
!
ip access-group ip_ext_deny_dst_sale_server in
!
!
!
!
!
!
!
!
!
!
interface GigabitEthernet 0/1 no global ip access-group
!
.....
```

1.4.8 Configuring a Security Channel

Configuration Effect

Configure a security channel to enable packets meeting the security channel rules to bypass the checks of access control applications. Configure the security channel if an access control application (such as DOT1X) is enabled on an uplink interface of a user, but the user should be allowed to log in to a website to download some resources (for example, downloading the QTECH SU client) before the DOT1X authentication.

Configuration Steps

❖ Configuring an ACL

- (Mandatory) Configure an ACL before configuring the security channel. For details about the configuration method, see the earlier descriptions.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The configurations take effect only on the local device, and do not affect other devices on the network.

❖ Adding ACEs to an ACL

- (Optional) An ACL may contain zero or multiple ACEs. If no ACE is configured for an ACL, it is equivalent that the security channel does not take effect. For details about how to add an ACE to an ACL, see the related descriptions.

❖ Configuring a Security Channel on a Specified Interface, VXLAN or Globally

- Configure a security channel on an interface if you want this security channel to

take effect on the interface. Configure a VXLAN security channel if you want this security channel to take effect on VNI. Configure a global security channel if you want this security channel to take effect globally. You must configure either the interface-based security channel or the global security channel.

- You can configure a security channel on an access, an aggregate, or a core device based on the distribution of users.

❖ **Configuring an Exclusive Interface for the Global Security Channel**

- (Optional) Configure an interface as the exclusive interface for the global security channel if you do not want the global security channel to take effect on this interface.

❖ **Configuring an Access Control Application**

- (Optional) You can enable the DOT1X or Web authentication function to verify the security channel function.
- You can configure the access control function on an access, an aggregate, or a core device based on the distribution of users.

Verification

On a PC that is subject to the control of an access control application, ping the resources (devices or servers) that are allowed to bypass the check of the access control application to verify the configuration of the security channel.

Related Commands

❖ **Configuring an ACL**

For details about how to configure an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

❖ **Adding ACEs to an ACL**

For details about how to add ACEs to an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

❖ **Configuring a Security Channel on an Interface**

| | |
|-----------------------|---|
| Command | security access-group { <i>acl-id</i> <i>acl-name</i> } |
| Parameter Description | <p><i>acl-id</i>: Indicates that ID of the ACL that is configured as the security channel.</p> <p><i>acl-name</i>: Indicates that name of the ACL that is configured as the security channel.</p> |
| Command | Interface configuration mode |

| | |
|--------------------|---|
| Mode | |
| Usage Guide | Run this command to configure a specified ACL as the security channel on the specified interface. |

❖ Configuring a VXLAN Security Channel

| | |
|------------------------------|--|
| Command | security access-group { <i>acl-id</i> <i>acl-name</i> } |
| Parameter Description | <i>acl-id</i> : Indicates that ID of the ACL that is configured as the security channel. <i>acl-name</i> : Indicates that name of the ACL that is configured as the security channel. |
| Command Mode | VXLAN configuration mode |
| Usage Guide | Run this command to configure a specified ACL as the security channel on the specified VXLAN. |

❖ Configuring a Global Security Channel

| | |
|------------------------------|--|
| Command | security global access-group { <i>acl-id</i> <i>acl-name</i> } |
| Parameter Description | <i>acl-id</i> : Indicates that ID of the ACL that is configured as the security channel. <i>acl-name</i> : Indicates that name of the ACL that is configured as the security channel. |
| Command Mode | Global configuration mode |
| Usage Guide | Run this command to configure the specified ACL as the global security channel. |

❖ Configuring an Exclusive Interface for the Global Security Channel

| | |
|------------------------------|------------------------------|
| Command | security uplink enable |
| Parameter Description | N/A |
| Command Mode | Interface configuration mode |

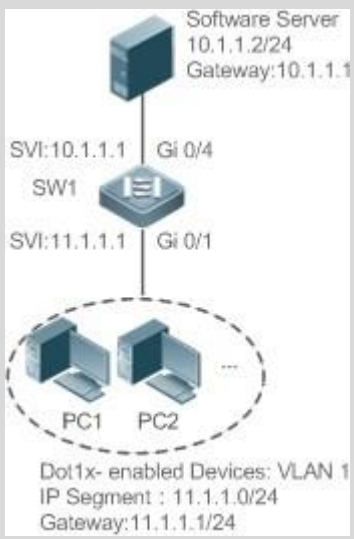
Usage Guide

Run this command to configure the specified interface as the exclusive interface of the global security channel.

Configuration Example

The following configuration example describes only ACL-related configurations.

- ❖ Enabling DOT1X Authentication and Configuring a Security Channel to Allow Users to Download the SU Software From the Server Before Authentication

| | |
|-----------------------------------|--|
| <p>Scenario Figure 1-10</p> |  |
| <p>Configuration Steps</p> | <ul style="list-style-type: none"> ● Configure an expert extended ACL "exp_ext_esc". ● Add an ACE to allow forwarding packets to the destination host 10.1.1.2. ● Add an ACE to permit the DHCP packets. ● Add an ACE to permit the ARP packets. ● On the interface where DOT1X authentication is enabled, configure the ACL "exp_ext_esc" as the security channel. |
| <p>SW1</p> | <pre>sw1(config)#expert access-list extended exp_ext_esc sw1(config- exp-nacl)# permit ip any any host 10.1.1.2 any sw1(config-exp-nacl)# permit 0x0806 any any any any any sw1(config-exp-nacl)# permit tcp any any any any eq 67 sw1(config-exp-nacl)# permit tcp any any any any eq 68 sw1(config)#int gigabitEthernet 0/1</pre> |

| | |
|---------------------|--|
| | sw1(config-if-GigabitEthernet 0/1)# security access-group exp_ext_esc |
| Verification | <ul style="list-style-type: none"> On a PC of the sales department, ping the server of the sales department. Verify that the ping operation succeeds. |
| | <p>On the PCs of R&D department 1 and R&D department 2, ping the server of the sales department.</p> <p>Verify that the ping operations fail.</p> |
| | <pre>sw1#show access-lists expert access-list extended exp_ext_esc 10 permit ip any any host 10.1.1.2 any 20 permit arp any any any any any 30 permit tcp any any any any eq 67 40 permit tcp any any any any eq 68..... sw1#show running-config interface gigabitEthernet 0/1 Building configuration... Current configuration : 59 bytes interface GigabitEthernet 0/1 security access-group exp_ext_esc</pre> |

1.4.9 Configuring the Time Range-Based ACEs

Configuration Effect

Configure the time range-based ACEs if you want some ACEs to take effect or to become invalid in a specified period of time, for example, in some time ranges during a week.

Configuration Steps

❖ Configuring an ACL

- (Mandatory) Configure an ACL if you want ACEs to take effect in the specified time range. For details about the configuration method, see the earlier descriptions.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The configurations take effect only on the local device, and do not affect other devices on the network.

❖ Adding an ACE with the Time Range Specified

- (Mandatory) Specify the time range when adding an ACE. For details about how to configure the time range, see the configuration manual related to the time range.

❖ **Applying an ACL**

- (Mandatory) Apply the ACL to a specified interface if you want to make ACEs take effect in the specified time range.
- You can apply an IP ACL on a specified interface of an access, an aggregate, or a core device based on the distribution of users.

Verification

In the time range that the configured ACE takes effect or becomes invalid, run the **ping** command or construct packets matching the ACE to check whether the ACE takes effect or becomes invalid.

Related Commands

❖ **Configuring an ACL**

For details about the ACL configuration commands, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

❖ **Adding an ACE with the Time Range Specified**

For details about the ACE configuration commands, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

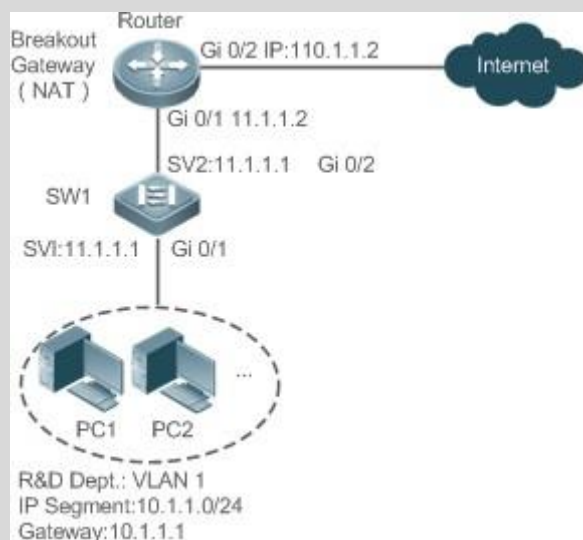
❖ **Applying an ACL**

For details about the command for applying an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

Configuration Example

The following configuration example describes only ACL-related configurations.

- ❖ **Adding an ACE With the Time Range Specified to Allow the R&D Department to Access the Internet Between 12:00 and 13:30 Every Day**

Scenario Figure 1-11

| | |
|----------------------|---|
| Configuration | Configure a time range named "access-internet", and add an entry of the time range between 12:00 |
| Steps | <p>and 13:30 every day.</p> <ul style="list-style-type: none"> ▪ Configure an IP ACL "ip_std_internet_acl". ▪ Add an ACE to allow packets with the source IP address in the network segment 10.1.1.0/24, and associate this ACE with the time zone "access-internet". ▪ Add an ACE to deny packets with the source IP address the network segment 10.1.1.0/24. Access to the Internet is not allowed except in the specified time range. ▪ Add an ACE to permit all packets. ▪ Apply the ACL to the outgoing direction of the interface connected to the breakout gateway. |
| SW1 | <pre>QTECH(config)# time-range access-internet QTECH(config-time-range)# periodic daily 12:00 to 13:30 QTECH(config-time-range)# exit sw1(config)# ip access-list standard ip_std_internet_acl sw1(config-std-nacl)# permit 10.1.1.0 0.0.0.255 time-range access- internet sw1(config-std-nacl)# deny 10.1.1.0 0.0.0.255 sw1(config-std-nacl)# permit any sw1(config-std-nacl)# exit sw1(config)#int gigabitEthernet 0/2 sw1(config-if-GigabitEthernet 0/2)# ip access-group ip_std_internet_acl out</pre> |
| Verification | <ul style="list-style-type: none"> ● Within the time range between 12:00 and 13:30, visit the Baidu website on a PC of the R&D department. Verify that the website can be opened normally. ● Beyond the time range between 12:00 and 13:30, visit the Baidu website on a PC of the R&D |

| | |
|------------|---|
| | department. Verify that the website cannot be opened. |
| SW1 | <pre>sw1#show time-range time-range entry: access-internet (inactive) periodic Daily 12:00 to 13:30 sw1#show access-lists ip access-list standard ip_std_internet_acl 10 permit 10.1.1.0 0.0.0.255 time-range access-internet (inactive) 20 deny 10.1.1.0 0.0.0.255 30 permit any</pre> |
| | <pre>sw1#show access-group ip access-group ip_std_internet_acl out Applied On interface GigabitEthernet 0/2</pre> |

1.4.10 Configuring Comments for ACLs

Configuration Effect

During network maintenance, if a lot of ACLs are configured without any comments, it is difficult to distinguish these ACLs later on. You can configure comments for ACLs to better understand the intended use of ACLs.

Configuration Steps

❖ Configuring an ACL

- (Mandatory) Configure an ACL before configuring the security channel. For details about the configuration method, see the earlier descriptions.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The configurations take effect only on the local device, and do not affect other devices on the network.

❖ Configuring Comments for ACLs

- (Optional) Configure comments for ACLs so that it is easy to manage and understand the configured ACLs.

❖ Adding ACEs to an ACL

- (Optional) An ACL may contain zero or multiple ACEs. If no ACE is configured, it is equivalent that the security channel does not take effect. For details about how to add an ACE to an ACL, see the related descriptions.

❖ Configuring Comments for ACEs

- (Optional) To facilitate understanding of a configured ACL, you can configure comments for ACEs in addition to comments for the ACL.

Verification

Run the **show access-lists** command on the device to display the comments configured for ACLs.

Related Commands

❖ Configuring an ACL

For details about how to configure an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

❖ Configuring a Comment for an ACL

Use either of the following two methods to configure a comment for an ACL:

| | |
|-----------------------|--|
| Command | list-remark <i>comment</i> |
| Parameter Description | <i>comment</i> : Indicates the comment. The value is a string of 1 to 100 characters. A comment longer than 100 characters will be truncated to 100 characters. |
| Command Mode | ACL configuration mode |
| Usage Guide | Run this command to configure the comment for a specified ACL. |

| | |
|-----------------------|--|
| Command | access-list <i>acl-id</i> list-remark <i>comment</i> |
| Parameter Description | <i>acl-id</i> : Indicates the ID of an ACL. <i>comment</i> : Indicates the comment. The value is a string of 1 to 100 characters. A comment longer than 100 characters will be truncated to 100 characters. |

| | |
|---------------------|--|
| Command Mode | Configuration mode |
| Usage Guide | Run this command to configure the comment for a specified ACL. |

❖ Adding ACEs to an ACL

For details about how to add ACEs to an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

❖ Configuring Comments for ACEs

Use either of the following two methods to configure a comment for an ACE:

| | |
|------------------------------|---|
| Command | <code>[sn] remark <i>comment</i></code> |
| Parameter Description | <i>comment</i> : Indicates the comment. The value is a string of 1 to 100 characters. A comment longer than 100 characters will be truncated to 100 characters. sn: Indicates the sequence number of ACE. |
| Command Mode | ACL configuration mode |
| Usage Guide | Run this command to configure the comment for a specified ACE. If sn is not specified, the remark is applied to the last ACE. |

| | |
|------------------------------|---|
| Command | <code>access-list <i>acl-id</i> sn remark <i>comment</i></code> |
| Parameter Description | <i>acl-id</i> : Indicates the ID of an ACL. <i>comment</i> : Indicates the comment. The value is a string of 1 to 100 characters. A comment longer than 100 characters will be truncated to 100 characters. sn: Indicates the sequence number of ACE. |
| Command Mode | Global configuration mode |
| Usage Guide | Run this command to configure the comment for a specified ACE. If sn is not specified, the remark is applied to the last ACE. |

1.5 Monitoring

Clearing

| Description | Command |
|--|---|
| Clears the ACL packet matching counters. | clear counters access-list [<i>acl-id</i> <i>acl-name</i>] |
| Clears the counters of packets matching the deny ACEs. | clear access-list counters [<i>acl-id</i> <i>acl-name</i>] |

Displaying

| Description | Command |
|--|--|
| Displays the basic ACLs. | show access-lists [<i>acl-id</i> <i>acl-name</i>] [summary] |
| Displays the redirection ACEs bound to a specified interface. If the interface is not specified, redirection ACEs bound to all interfaces are displayed. | show redirect [interface <i>interface-name</i>] |
| Displays the ACL configurations applied to an interface. | show access-group [interface <i>interface-name</i>] |
| Displays the IP ACL configurations applied to an interface. | show ip access-group [interface <i>interface-name</i>] |
| Displays the MAC extended ACL configurations applied to an interface. | show mac access-group [interface <i>interface-name</i>] |
| Displays the expert extended ACL configurations applied to an interface. | show expert access-group [interface <i>interface-name</i>] |
| Displays the IPv6 ACL configurations applied to an interface. | show ipv6 traffic-filter [interface <i>interface-name</i>] |

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

| Description | Command |
|---|-----------------------------------|
| Debugs the ACL running process. | debug acl acld event |
| Debugs the ACL clients. | debug acl acld client-show |
| Debugs the ACLs created by all ACL clients. | debug acl acld acl-show |

2.1 Overview

Quality of Service (QoS) indicates that a network can provide a good service capability for specified network communication by using various infrastructure technologies.

When the network bandwidth is sufficient, all data streams can be properly processed; when network congestion occurs, all data streams may be discarded. To meet users' requirements for different applications and different levels of service quality, a network must be able to allocate and schedule resources based on users' requirements and provide different levels of service quality for different data streams. To be specific, the network can process real-time and important data packets in higher priorities, and process non-real-time and common data packets in lower priorities and even discard the data packets upon network congestion.

The "doing the best" forwarding mechanism used by traditional networks cannot meet the requirements any longer and then QoS comes into being. QoS-enabled devices provide transmission QoS quality service. A transmission priority can be assigned to data streams of a type to identify the importance of the data streams. Then, the devices provide forwarding policies for different priorities, congestion mitigation and other mechanisms to provide special transmission services for these data streams. A network environment configured with QoS can provide predictability for network performance, effectively allocate network bandwidth, and reasonably utilize network resources.

2.2 Applications

| Application | Description |
|--|--|
| Interface Rate Limit + Priority Relabeling | Based on different service requirements for a campus network, provide rate control and priority-based processing for outgoing traffic of the teaching building, laboratories and dormitory building. |
| Priority Relabeling + Queue Scheduling | Provide priority-based processing and bandwidth control for traffic of internal access to servers of an enterprise. |

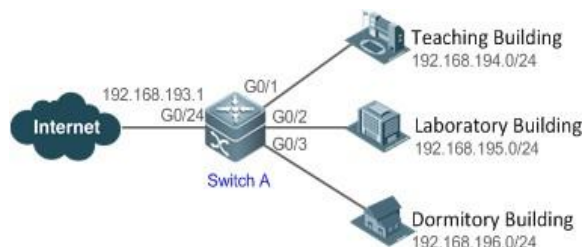
2.2.1 Interface Rate Limit + Priority Relabeling Scenario

To meet the service requirements of normal teaching, a school puts forwards the

following requirements:

- Control the Internet access traffic under 100M and discard packets out of control.
- Control the outgoing traffic of the dormitory building under 50M and discard packets out of control.
- Control the rate of packets with DSCP priority 7 sent from laboratories under 20M, and change the DSCP priorities of these packets whose rates exceed 20M to 16.
- Control the outgoing traffic of the teaching building under 30M and discard packets out of control.

Figure 2-1



| | |
|---------|--|
| Remarks | A school connects GigabitEthernet 0/24 of Switch A to the Internet in the uplink and connects GigabitEthernet 0/1, GigabitEthernet 0/2 and GigabitEthernet 0/3 of Switch A to the teaching building, laboratory and dormitory building in the downlink respectively |
|---------|--|

Deployment

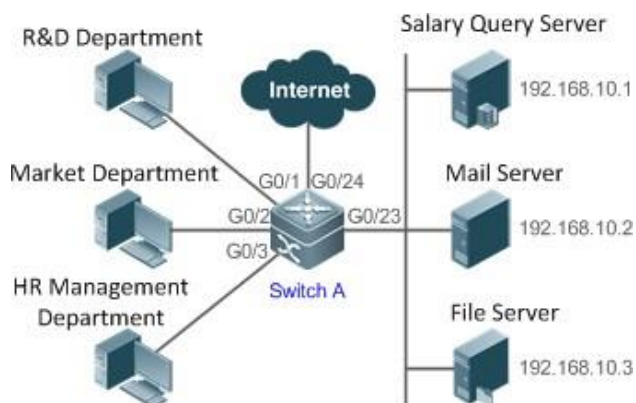
- Configure the QoS interface rate limit for the interface G0/24 of Switch A for connecting the Internet.
- Configure the QoS rate limit for packets sent from the dormitory building on Switch A.
- Set the rate limit for packets with the DSCP priority 7 sent from the laboratory to 20M and relabel the DSCP priority of packets out of the rate limit to 16.
- Configure the QoS rate limit for packets sent from the teaching building on Switch A.

2.2.2 Priority Relabeling + Queue Scheduling Scenario

Configure priority relabeling and queue scheduling to meet the following requirements:

- When the R&D department and market department access servers, the priorities of the server packets are as follows: mail server > file server > salary query server.
- No matter when the HR management department accesses the Internet or servers, the switch processes the corresponding packets in the highest priority.
- Since network congestion often occurs in switch running, in order to ensure smooth business operation, WRR queue scheduling must be used to schedule IP packets for the R&D and market departments to access the mail database, file database, and salary query database based on the ratio of 6:2:1.

Figure 2-2



Remarks

The R&D, market and HR management departments access the interfaces GigabitEthernet 0/1, GigabitEthernet 0/2 and GigabitEthernet 0/3 of Switch A respectively. The salary query server, mail server and file server are connected to GigabitEthernet 0/23 of Switch A.

Deployment

- Configure the CoS values of data streams for accessing different servers to ensure that the switch processes packets for different servers in different priorities.
- Set the default CoS value of the interface to a specific value to ensure that the switch processes packets sent by the HR management department in the highest priority.
- Configure WRR queue scheduling to ensure that data packets are transmitted in a specific quantity ratio.

2.3 Features

Basic Concept

❖ DiffServ

The Differentiated Services (DiffServ) Mode is an IETF system based on which QoS is implemented in QTECH products. The DiffServ system classifies all packets transmitted in a network into different types. The classification information is included in layer-2/3 packet headers, including 802.1P, IP and IP DSCP priorities.

In a DiffServ-compliant network, all devices apply the same transmission service policy to packets containing the same classification information and apply different transmission service policies to packets containing different classification information. Classification information of packets is either assigned by hosts or other devices in the network or assigned based on different application policies or different packet contents. Based on the classification information carried by packets, a device may provide different transmission priorities for different packet streams, reserve bandwidth for a kind of packet streams, discard certain packets with lower priorities, or take some other actions.

❖ 802.1P(PRI) priority

The 802.1 P priority is located at the header of a layer-2 packet with the 802.1Q header, and is used in scenarios where layer-3 headers do not need to be analyzed and QoS needs to be implemented at layer 2. Figure 2-3 shows the structure of a layer-2 packet.

Figure 2-3

| | | | | | | |
|---------------------|----------------|---------------|---------|---------------|---------|-------------|
| Destination Address | Source Address | 802.1Q header | | Length/Type | Data | FCS(CRC-32) |
| | | TPID | TCI | | | |
| 6 bytes | 6 bytes | 4 bytes | 2 bytes | 46~1500 bytes | 4 bytes | |

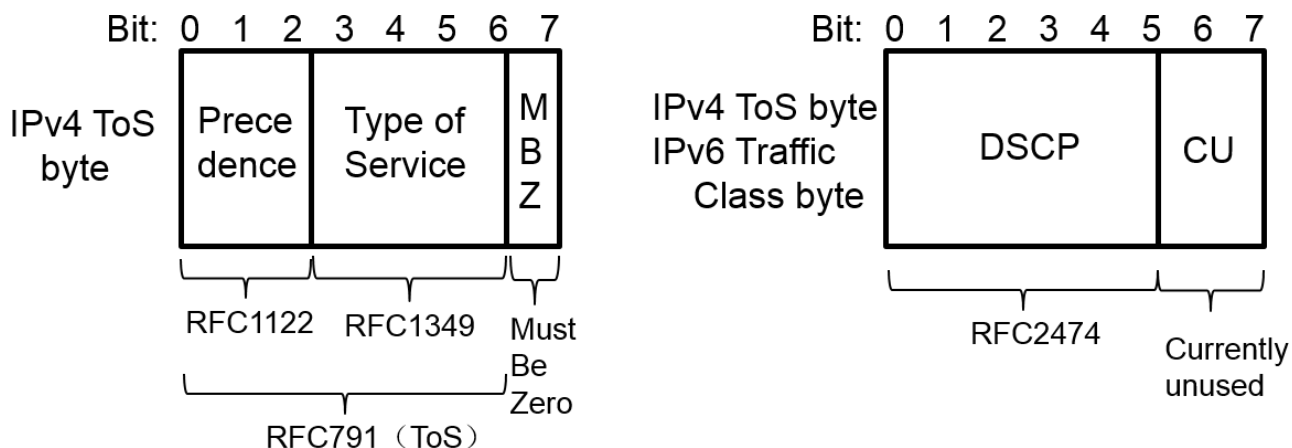
As shown in Figure 2-3, the 4-byte 802.1Q header contains 2-byte Tag Protocol Identifier (TPID) whose value is 0x8100 and 2-byte Tag Control Information (TCI). The first three bits of the TCI indicate the 802.1P priority.

❖ IP priority (IP PRE) and DSCP priority

The priorities of IP packets are identified by the IP PRE and DSCP priority. The Type Of Service (ToS) field of the IPv4 header comprises 8 bits; where the first three bits indicate the IP precedence (IP PRE), ranging from 0 to 7. RFC 2474 redefines the ToS field of the IPv4 header, which is called the Differentiated Services (DS) field. The Differentiated Services Code Point (DSCP) priority is identified by the first 6 bits (bits 0 to 5) of the DS field, and by the first 6 bits of the

Traffic Class field in the IPv6 header. Figure 2-4 shows the locations of the IP PRE and DSCP priorities in IPv4/IPv6 packets.

Figure 2-4



❖ CoS

Class of Service (COS). QTECH products convert packet priorities into CoS values to identify the local priorities of the packets and determine the input queue ID when packets are sent from the output interface.

Overview

| Feature | Description |
|---|---|
| Stream Classification | Stream classification uses certain rules to identify packets with same characteristics and is the prerequisite and basis for distinguishing network services. |
| Priority Labeling and Mapping | Label packet priorities with specified values and map the values to corresponding CoS values. |
| Traffic Supervision | Supervise the specification of traffic flowing into a network, limit the traffic within a reasonable range, and discard the traffic out of the limit or modify the priority of the traffic. |
| Congestion Management | Determine the sequence of data packets sent from an interface based on the priorities of the data packets and ensure that key services can be processed in time when congestion occurs. |
| Congestion Mitigation | Monitor the usage of the output interface queue and reduce the network load by actively discarding packets and adjusting the network traffic when network congestion occurs. |

2.3.1 Stream Classification

Stream classification uses certain rules to identify packets with same characteristics and is the prerequisite and basis for distinguishing network services. Stream classification rules are used to distinguish different packets in the network and specify different QoS parameters for packets at different service levels.

Working Principle

Stream classification rules can be matching the PRE or DSCP priorities of IP packets or classifying packets by identifying packet content through an ACL. You can define the binding between multiple streams and stream behaviors by using commands to form policies which can be applied to interfaces for stream classification and processing.

❖ QoS policy

A QoS policy comprises three elements: class, stream behavior and policy.

- Class

A class identifies streams and comprises the class name and class rules. You can define the class rules by using commands to classify packets.

- Stream behavior

Stream behaviors define the QoS actions taken for packets, including priority labeling and traffic supervision for packets.

- Policy

A policy binds a specific class and specific stream behaviors and comprises the policy name, names of the classes bound, and stream behaviors. You can bind a specified class and stream behaviors by using a QoS policy and apply the policy to one or more interfaces.

❖ QoS logical interface group

You can specify a series of interfaces as a QoS logical interface group (including both APs and Ethernet interfaces) and associate policies with the logical interface group for QoS processing. Take rate limit for stream behaviors for example. For packets that meet the rate limit conditions, all interfaces in the same logical interface group share the bandwidth specified by the policy.

Related Configuration

❖ Creating a class

No class is defined by default.

You can run the **class-map** command to create a class and enter the class configuration mode.

❖ Matching an ACL

No rules are defined for a class by default.

In the class configuration mode, you can run the **match access-group** command to define a class rule as matching an ACL. You need to create ACL rules first.

❖ **Matching DSCP priorities of IP packets**

No rules are defined for a class by default.

In the class configuration mode, you can run the **match ip dscp** command to define a class rule as matching DSCP priorities of IP packets. The value range of DSCP priorities is 0 to 63.

❖ **Creating a policy**

No policy is defined by default.

You can run the **policy-map** command to create a policy and enter the policy configuration mode.

❖ **Associating a class**

A policy is not associated with any class by default.

In the policy configuration mode, you can run the **class** command to associate a class and enter the policy-class configuration mode.

❖ **Binding a stream behavior**

A class is not bound to any stream behavior by default.

In the policy-class configuration mode, you can run the **set** command to modify the CoS, DSCP or VID values of a specified stream; where, the CoS value ranges from 0 to 7, the DSCP value ranges from 0 to 63 and the VID value ranges from 1 to 4094. You can run the **police** command to limit the bandwidth and process streams out of the limit for specified streams. The bandwidth limit ranges are determined by products.

❖ **Configuring a logical interface group**

No logical interface group is defined and an interface is not added to any logical interface group by default. In the global configuration mode, you can run the **virtual-group** command to create a logical interface group. In the interface configuration mode, you can run the **virtual-group** command to add an interface to a logical interface group. If this logical interface group is not created, you can create the logical interface group and add the interface to the group. You can create 128 logical interface groups, ranging from 1 to 128.

❖ **Applying a policy to an interface**

No policy is applied to an interface by default.

In the interface configuration mode, you can run the **service-policy** command to apply a policy in the input/output directions of the interface. In the global configuration mode, you can run the **service-policy** command to apply a policy in the input/output directions of all interfaces.

2.3.2 Priority Labeling and Mapping

Priorities are used to label the scheduling weights of packets or the priorities of the packets in forwarding. Different packet types have different priority types including 802.1P(PRI), IP PRE and DSCP priorities. Priority labeling and mapping refer to labeling packet priorities with specified values and mapping the values to corresponding CoS values.

Working Principle

After data streams of packets enter a device interface, the device assigns priorities to the packets based on the trust mode configured for the interface. The following describes several trust modes:

- When the interface trust mode is untrust, which means not trusting the priority information carried in packets:

Modify the CoS value according to the default CoS value (0, which is configurable), COS-DSCP mapping table and DSCP-COS mapping table of the interface and put the packets into queues based on the final CoS value. For output packets carrying the 802.1Q tag, the packet priority will be modified to the corresponding CoS value.

- When the interface trust mode is trusting CoS:

For packets carrying the 802.1Q tag, modify the CoS value according to the PRI value, CoS-DSCP mapping table, and DSCP-CO mapping table, and put the packets into queues based on the final CoS value. For output packets carrying the 802.1Q tag, the packet priority will be modified to the corresponding CoS value.

For packets not carrying the 802.1Q tag, modify the CoS value according to the default CoS value (0, which is configurable), COS-DSCP mapping table and DSCP-COS mapping table of the interface, and put the packets into queues based on the final CoS value. For output packets carrying the 802.1Q tag, the packet priority will be modified to the corresponding CoS value.

- When the interface trust mode is trusting DSCP:

For non-IP packets, the processing is the same as that for trusting CoS.

For IP packets, modify the CoS value according to the DSCP value of the packets and the DSCP-CoS mapping table and put the packets into queues based on the final CoS value.

- When the interface trust mode is trusting IP PRE:

For non-IPv4 packets, the processing is the same as that for trusting CoS.

For IPv4 packets, obtain and modify the DSCP priority of the packets according to the IP PRE value of the packets and the IP-PRE-DSCP mapping table, obtain the CoS value according to the DSCP-CoS mapping table, and then put the packets into queues based on the final CoS value.

- When the trust mode and the applied policy of an interface work together:

When the trust mode and the applied policy of an interface work together,

the trust mode has a lower priority than the policy and the CoS priority can be obtained according to the DSCP-CoS mapping table.

If a policy is applied to the interface but the policy does not have a configuration for modifying the DSCP and CoS values, the processing will be performed based on the trust mode of the interface.

Related Configuration

❖ Configuring the trust mode of an interface

The default trust mode of an interface is untrust.

In the interface configuration mode, run the **mls qos trust** command to modify the trust mode. The trust mode can be trusting CoS, trusting DSCP or trusting IP PRE.

❖ Configuring the default CoS value of an interface

The default CoS value of an interface is 0.

In the interface configuration mode, run the **mls qos cos** command to modify the default CoS value of the interface, which ranges from 0 to 7.

❖ Labeling the priority of streams

The priorities of streams are not relabeled by default.

In the policy-class configuration mode, run the **set** command to modify the CoS, DSCP and VID values of streams. The CoS value ranges from 0 to 7; the DSCP value ranges from 0 to 63; the VID value ranges from 1 to 4094.

❖ Configuring CoS-to-DSCP Map

By default, the CoS values 0, 1, 2, 3, 4, 5, 6 and 7 are mapped to the DSCP values 0, 8, 16, 24, 32, 40, 48 and 56 respectively.

Run the **mls qos map cos-dscp** command to configure the CoS-DSCP mapping. The DSCP value ranges from 0 to 63.

❖ Configuring DSCP-to-CoS Map

By default, DSCP 0 to 7 are mapped to CoS 0, DSCP 8 to 15 mapped to CoS 1, DSCP 16 to 23 mapped to CoS 2, DSCP 24

to 31 mapped to CoS 3, DSCP 32 to 39 mapped to CoS 4, DSCP 40 to 47 mapped to CoS 5, DSCP 48 to 55 mapped to CoS

6, and DSCP 56 to 63 mapped to CoS 7.

Run the **mls qos map dscp-cos** command to configure the DSCP-CoS mapping. The CoS value ranges from 0 to 7 and the DSCP value ranges from 0 to 63.

❖ Configuring IP-PRE-to-DSCP Map

By default, the IP PRE values 0, 1, 2, 3, 4, 5, 6 and 7 are mapped to the DSCP values 0, 8, 16, 24, 32, 40, 48 and 56 respectively.

Run the **mls qos map ip-prec-dscp** command to configure the IP PRE-DSCP mapping. The DSCP value ranges from 0 to 63.

2.3.3 Traffic Supervision

Supervise the specification of traffic flowing into a network, limit the traffic within a reasonable range, and discard the traffic out of the limit or modify the priority of packets. In addition, the total traffic of an interface can be monitored and the traffic out of the limit will be discarded.

Working Principle

Traffic supervision is used to monitor the specification of traffic flowing into a network and conduct preset supervision actions based on different assessment results. These actions can be:

- Forwarding: Normally forward packets within the traffic limit.
- Discarding: discard packets out of the traffic limit.
- Changing the priority and forwarding: modify the priorities of packets out of the traffic limit and then forward the packets. Directly discard packets out of the total traffic limit of an interface.

Related Configuration

❖ Configuring the action to be conducted for traffic out of limit

No action to be conducted for traffic out of limit is configured by default.

In the policy-class configuration mode, run the **police** command to configure the action to be conducted for traffic out of limit to discarding traffic out of limit, or modifying the CoS value or DSCP value. The traffic limit range is determined by products. When the traffic is out of the limit, you can modify the CoS value in the range of 0 to 7 and the DSCP value in the range of 0 to 63.

❖ Configuring the total traffic limit for an interface

The total traffic limit for an interface is not configured by default.

In the interface configuration mode, run the **rate-limit** command to configure the total traffic limit for an interface in the input and output directions. The traffic limit range is determined by products.

2.3.4 Congestion Management

When the receiving rate of packets exceeds the sending rate of packets, congestion will occur on the sending interface. If no sufficient buffer is provided to store these packets, the packets may be lost. The congestion management mechanism determines the sequence of data packets to be sent from an interface based on the priorities of the data packets. The congestion management function allows for congestion control by increasing the priorities of important data packets. When congestion occurs, the important data packets are sent in higher priorities to ensure that key services are implemented in time.

Working Principle

A queue scheduling mechanism is used for congestion management and the process is as follows:

- After each packet passes all QoS processing in a switch, the packet will obtain a CoS value finally.
- At the output interface, the device classifies the packets into corresponding sending queues based on the CoS values.
- The output interface selects packets in a queue for sending based on various scheduling policies (SP, WRR, DRR, SP+WRR and SP+DRR).

❖ Scheduling policy

The queue scheduling policies include SP, WRR, DRR, SP+WRR and SP+DRR.

- Strict-Priority (SP) scheduling means scheduling packets strictly following queue IDs. Before sending packets each time, check whether a queue with the first priority has packets to be sent. If yes, the packets in this queue are sent first. If not, check whether a queue with the second priority has packets. Follow the same rules for packets in other queues.
- Weighted Round Robin (WRR) scheduling means scheduling queues in turn to ensure that all queues have certain service time. For example, a 1000 Mbps interface has 8 output queues. The WRR configures a weighted value (5, 5, 10, 20, 20, 10, 20 and 10, which indicate the proportions of obtained resources) for each queue. This scheduling method ensures that a queue with the lowest priority is assigned with at least 50 Mbps bandwidth, which avoids that packets in the queue with the lowest priority are not served for long time when the SP scheduling method is used.
- Deficit Round Robin (DRR) scheduling is similar to the WRR, but applies weight values based on bytes, but not based on time slices.
- SP+WRR scheduling means configuring the SP scheduling for one or more sending queues and configuring the WRR scheduling for the other queues. Among SP queues, only after all packets in the SP queue with the first priority are sent, the packets in the SP queue with the second priority can be sent. Among SP and WRR queues, only after the packets in all SP queues are sent, the packets in WRR queues can be sent.
- SP+DRR scheduling means configuring the SP scheduling for one or more sending queues and configuring the DRR scheduling for the other queues. Among SP queues, only after all packets in the SP queue with the first priority are sent, the packets in the SP queue with the second priority can be sent. Among SP and DRR queues, only after the packets in all SP queues are sent, the packets in DRR queues are sent.

❖ QoS multicast queue

On some products, interface queues are classified into unicast queues and multicast queues. There are 8 unicast queues. All known unicast packets enter corresponding

unicast queues for forwarding based on their priorities. There are 1 to 8 multicast queues (depending on products. Certain products do not support multicast queues). Except for known unicast packets, all packets (such as broadcast packets, multicast packets, unknown unicast packets, and mirroring packets) enter corresponding multicast queues for forwarding based on their priorities. Similar to unicast queues, you can configure priority mappings and scheduling algorithms for multicast queues. The **Cos-to-Mc-Queue** command can be used to configure mapping from priorities to multicast queues. At present, multicast queues support the SP, WRR and SP+WRR scheduling algorithms.

❖ Queue bandwidth

Some products allow for configuring the guaranteed minimum bandwidth and the limited maximum bandwidth for a queue. A queue configured with the guaranteed minimum bandwidth ensures that the bandwidth for this queue is not smaller than the configured value. A queue configured with the limited maximum bandwidth ensures that the bandwidth for this queue is not greater than the configured value and packets out of the bandwidth limit will be discarded. The bandwidth limits for unicast and multicast queues are configured together on some products whereas configured separately on some other products. In addition, some products allow for configuring bandwidth only for unicast queues. Supported types are determined by products.

Related Configuration

❖ Configuring CoS-to-Queue Map

By default, the CoS values 0, 1, 2, 3, 4, 5, 6 and 7 are mapped to the queues 1, 2, 3, 4, 5, 6, 7 and 8 respectively.

Run the **priority-queue cos-map** command to configure the CoS-to-queue mapping. The CoS value ranges from 0 to 7 and the queue value ranges from 1 to 8.

❖ Configuring the scheduling policy for an output queue

By default, the scheduling policy for a global output queue is WRR.

Run the **mls qos scheduler** command to configure the output scheduling policy for a queue. Configurable scheduling policies include SP, WRR and DRR. You can also run the **priority-queue** command to configure the scheduling policy as SP.

❖ Configuring the round robin weight corresponding to the WRR scheduling policy for an output queue

By default, the weight of a global queue is 1:1:1:1:1:1:1.

Run the **wrr-queue bandwidth** command to configure the round robin weight corresponding to the WRR scheduling policy for an output queue. The configurable weight range is determined by products.

A higher weight means longer output time.

❖ Configuring the round robin weight corresponding to the DRR scheduling

policy for an output queue

By default, the weight of a global queue is 1:1:1:1:1:1:1.

Run the **drr-queue bandwidth** command to configure the round robin weight corresponding to the DRR scheduling policy for an output queue. The configurable weight range is determined by products.

A higher weight means more packet bytes that can be sent.

❖ Configuring CoS-to-MC-Queue Map

By default, the CoS-to-multicast queue mapping is determined by products.

Run the **qos mc-queue cos-map** command to configure the CoS-to-multicast queue mapping. The CoS value ranges from 0 to 7 and the multicast queue value range is determined by products.

❖ Configuring the bandwidth for a queue

Run the **qos queue** command to configure the guaranteed minimum bandwidth and the limited maximum bandwidth for each queue. The queue value ranges from 1 to 8 and the guaranteed minimum bandwidth and limited maximum bandwidth value ranges are determined by products. Supported queue types are determined by products.

2.3.5 Congestion Mitigation

Monitor the usage of the output interface queue and reduce the network load by actively discarding packets and adjusting the network traffic when network congestion occurs.

Working Principle

Mitigate congestion by effectively monitoring the network traffic and forecasting occurrence of congestion. Packets need to be discarded to mitigate congestion. Discarding policies include Tail-Drop, Random Early Detection (RED), and Weighted Random Early Detection (WRED).

❖ Tail-Drop

Traditional packet loss policies include Tail-Drop. Tail-Drop is effective for all traffic and cannot distinguish service levels. When congestion occurs, data packets at the tail of a queue will be discarded until the congestion is removed.

❖ RED and WRED

Hosts running TCP will decrease the rate of sending packets to respond to massive packet loss. After congestion is removed, the hosts increase the rate of sending packets. In this way, Tail-Drop may cause TCP Global Synchronization. When a queue discards multiple TCP packets simultaneously, multiple TCP connections enter the congestion mitigation and slow startup state simultaneously, and the traffic is reduced and adjusted. When congestion is removed, traffic peaks may appear. The process repeats constantly, the network traffic goes up and down

suddenly, and the line traffic always fluctuates between the lowest quantity and the highest quantity. When TCP global synchronization occurs, the connection bandwidth cannot be adequately used, which causes bandwidth waste.

To avoid this circumstance, you can use the RED/WRED packet discarding policy. This policy provides a mechanism for discarding packets in random, which avoids TCP global synchronization. When packets of a TCP connection are discarded and sent at a lower rate, packets of other TCP connections are still sent at higher rates. In this way, there are always some TCP connections whose packets are sent at higher rates, which increases the utilization of line bandwidth.

When WRED is used, you can set the lower threshold value and maximum discarding probability for a queue. When the queue length is smaller than the lower threshold, WRED does not discard packets. When the queue length is between the higher and lower thresholds, WRED discards packets in random (the longer the queue length, the higher probability of packet discarding. There is a maximum discarding probability). When the queue length is greater than the higher threshold value, WRED discards packets at the maximum discarding probability.

Different from RED, WRED uses priorities to distinguish discarding policies. RED is a special example of WRED. When all CoS values of an interface are mapped to the same lower and higher threshold values, WRED becomes RED.

Related Configuration

❖ Enabling the WRED function

The default packet discarding policy is Tail-Drop.

You can run the **queueing wred** command to enable the WRED function.

❖ Configuring the lower threshold value

When 2 groups of lower thresholds in the unit of percentage are supported, the default values are 100 and 80 (the number of threshold value groups are determined by products).

In the interface configuration mode, you can run the **wrr-queue random-detect min-threshold** command to configure the lower thresholds in the unit of percentage for packets discarded by WRED in each queue. The queue value ranges from 1 to

8. The lower threshold value ranges from 1 to 100.

❖ Configuring the maximum discarding probability

When 2 groups of maximum discarding probabilities are supported, the default values are 100 and 80 (the number of threshold value groups are determined by products).

In the interface configuration mode, you can run the **wrr-queue random-detect probability** command to configure the maximum discarding probabilities for packets discarded by WRED in each queue. The queue value ranges from 1 to

8. The maximum discarding probability ranges from 1 to 100.

❖ **Configuring the CoS-to-threshold mapping**

By default, all CoS values are mapped to the first group of threshold values (the number of threshold groups is determined by products).

In the interface configuration mode, you can run the **wrr-queue cos-map** command to configure the CoS-to-threshold group mapping. The CoS value ranges from 0 to 7 and the number of threshold groups is determined by products. Multiple groups of lower threshold values and maximum discarding probabilities can be configured. By configuring the CoS-to-threshold group mapping, you can select the effective threshold group mapped to a CoS value, for example, CoS 0 mapped to the first threshold group, and CoS 1 mapped to the second threshold group. If the packets of CoS 0 and 1 are added to queue 1 for scheduling, the packets of CoS 0 are processed based on the lower threshold values and maximum discarding probabilities in the first group and the packets of CoS 1 are processed based on the lower threshold values and maximum discarding probabilities of the second group.

When all CoS values of an interface are mapped to the same group of threshold values, the enabled WRED becomes RED.

2.4 Configuration

| Configuration | Description and Command | |
|---|--|---|
| Configuring Stream Classification | (Optional) It is used to create stream classification information. | |
| | class-map | Creates a class. |
| | match access-group | Matches ACL rules. |
| | match ip dscp | Matches the DSCP priorities of IP packets. |
| | policy-map | Creates a policy. |
| Configuration | Description and Command | |
| | class | Associates a class. |
| | police | Binds the bandwidth limit for streams and the action for processing packets out of the limit. |
| | set | Binds the behaviors for modifying the CoS, DSCP and VID values of streams. |

| | | |
|---|--|---|
| | virtual-group | Creates a logical interface group and adds interfaces to the logical interface group. |
| | service-policy | Applies a policy to an interface. |
| Configuring Priority Labeling and Mapping for Packets | (Optional) It is used to configure the trust mode, default CoS value and various mappings for an interface. | |
| | mls qos trust | Modifies the trust mode of an interface. |
| | mls qos cos | Modifies the default CoS value of the interface. |
| | mls qos map cos-dscp | Configures the CoS-to-DSCP mapping. |
| | mls qos map dscp-cos | Configures the DSCP-to-CoS mapping. |
| | mls qos map ip-precedence-dscp | Configures the IP PRE-to-DSCP mapping. |
| Configuring Interface Rate Limit | (Optional) It is used to configure the rate limit for an interface. | |
| | rate-limit | Configures the traffic limit for an interface. |
| Configuring Congestion Management | (Optional) It is used to configure the CoS-to-queue mapping, queue scheduling policies and round robin weight. | |
| | priority-queue cos-map | Configures the CoS-to-queue mapping. |
| | priority-queue | Configures the output scheduling policy for a queue to SP. |
| | mls qos scheduler | Configures the output scheduling policy for a queue. |
| | wrr-queue bandwidth | Configures the round robin weight corresponding to the WRR scheduling policy |

| | | |
|---|---|---|
| | | for an output queue. |
| | drp-queue bandwidth | Configures the round robin weight corresponding to the DRP scheduling policy for an output queue. |
| | qos mc-queue cos-map | Configures the CoS-to-multicast queue mapping. |
| | qos queue bandwidth | Configures the guaranteed minimum bandwidth and limited maximum bandwidth for a queue. |
| Configuring Congestion Mitigation | (Optional) It is used to prevent network congestion by setting packet discarding. | |
| | queueing wred | Enables the WRED function. |
| | wrr-queue random-detect min-threshold | Configures the lower threshold value for packets discarded by WRED (in the unit of percentage). |
| | wrr-queue random-detect probability | Configures the maximum discarding probability for packets discarded by WRED. |
| | wrr-queue cos-map | Configures the threshold-to-CoS mapping. |

2.4.1 Configuring Stream Classification

Configuration Effect

- Create a class and match classification rules.
- Create a policy, bind a class and stream behaviors, and associate with an interface.

Notes

- The class and policy names cannot comprise more than 31 characters.
- Interface configurations allow for only AP and Ethernet interface

configurations. Certain products support policies applied to SVI interfaces through the **service-policy** command. When both physical interfaces and SVI interfaces are configured with policies, the priority of the physical interfaces is higher than that of the SVI interfaces.

- If run the **service-policy** command in global configuration mode, policies will be applied to all interfaces which can be configured with policies.

Configuration Steps

❖ Creating a class and matching ACL rules

- Optional.
- Create a class. In the class configuration mode, match ACL, IP PRE or DSCP.

❖ Creating a policy

- Optional.
- Create a policy. In the policy configuration mode, bind the class and stream behaviors.

❖ Creating a logical interface group and adding interfaces to the logical interface group

- Optional.
- Create a logical interface group and add interfaces to the logical interface group.

❖ Applying a policy to an interface

- Optional.
- Associate a configured policy with a specified interface or logical interface group.

Verification

- Run the **show class-map** command to check whether the class is successfully created and whether rules are successfully matched.
- Run the **show policy-map** command to check whether the policy is successfully created and whether the class and stream behaviors are successfully bound.
- Run the **show mls qos interface** command to check whether the interface is associated with the policy.
- Run the **show virtual-group** command to check the interfaces in the logical interface group.
- Run the **show mls qos virtual-group** command to check whether the logical interface group is associated with the policy.

Related Commands

❖ Creating a class

| | |
|-----------------------|--|
| Command | class-map <i>class-map-name</i> |
| Parameter Description | <i>class-map-name</i> : Indicates the name of a class to be created. The name cannot comprise more than 31 characters. |
| Command Mode | Global configuration mode |
| Usage Guide | - |

❖ Matching an ACL

| | |
|-----------------------|--|
| Command | match access-group <i>access list</i> |
| Parameter Description | <i>access list</i> : Indicates the ACEs to be matched. |
| Command Mode | Class configuration mode |
| Usage Guide | - |

❖ Matching DSCP of IP packets

| | |
|-----------------------|--|
| Command | match ip dscp <i>dscp-value-list... [dscp-value-list...]</i> |
| Parameter Description | <i>dscp -value</i> : Indicates the DSCP (one or multiple) to be matched, ranging from 0 to 63. |
| Command Mode | Class configuration mode |
| Usage Guide | - |

❖ Creating a policy

| | |
|-----------------------|--|
| Command | policy-map <i>policy-map-name</i> |
| Parameter Description | <i>policy-map-name</i> : Indicates the name of a policy to be created. The name cannot comprise more than 31 characters. |
| Command Mode | Global configuration mode |

Usage Guide

-

❖ Associating a class

| | |
|------------------------------|---|
| Command | class <i>class-map-name</i> |
| Parameter Description | <i>class-map-name</i> : Indicates the name of a class to be associated. |
| Command Mode | Policy configuration mode |
| Usage Guide | - |

❖ Binding the behaviors for modifying the CoS, DSCP and VID values of streams

| | |
|------------------------------|--|
| Command | set { ip dscp <i>new-dscp</i> cos <i>new-cos</i> vid <i>new-vid</i> } |
| Parameter Description | <p>ip dscp <i>new-dscp</i>: Changes the DSCP value of streams to new-dscp, ranging from 0 to 63.</p> <p>cos <i>new-cos</i>: Changes the CoS value of streams to new-cos, ranging from 0 to 7.</p> <p>vid <i>new-vid</i>: Changes the VLAN ID of streams to new-vid, ranging from 1 to 4094.</p> |
| Command Mode | Class configuration mode |
| Usage Guide | - |

❖ Binding the bandwidth limit for streams and the action for processing packets out of the limit

| | |
|------------------------------|---|
| Command | police <i>rate-bps burst-byte</i> [exceed-action { drop dscp <i>new-dscp</i> cos <i>new-cos</i> [none-tos] }] |
| Parameter Description | <p><i>rate-bps</i>: Indicates the bandwidth limit per second (KBits). The value range is determined by products.</p> <p><i>burst-byte</i>: Indicates the burst traffic limit (Kbytes). The value range is determined by products.</p> <p>drop: Discards packets out of the bandwidth limit.</p> <p>dscp <i>new-dscp</i>: Changes the DSCP value of packets out of the bandwidth limit to new-dscp, ranging from 0 to 63.</p> <p>cos <i>new-cos</i>: Changes the CoS value of packets out of the bandwidth limit to new-cos, ranging from 0 to 7.</p> |

| | |
|---------------------|--|
| | none-tos: Does not change the DSCP value of packets when changing the CoS value of the packets. |
| Command Mode | Class configuration mode |
| Usage Guide | - |

- ❖ Creating a logical interface group and adding interfaces to the logical interface group

| | |
|---------------------|---|
| Command | virtual-group <i>virtual-group-number</i> |
| Parameter | <i>virtual-group-number</i> : Indicates the logical interface group number, ranging from 1 to 128. |
| Description | |
| Command Mode | Create the logical interface group in the global configuration mode, add the interface to the logical interface group in the interface configuration mode. If no logical interface group exists, you need to create a logical interface group first and then add interfaces to the logical interface group. |
| Usage Guide | - |

- ❖ Applying a policy to an interface

| | |
|------------------------------|--|
| Command | service-policy { input output } <i>policy-map-name</i> |
| Parameter Description | input: Indicates the input direction of the interface. output: Indicates the output direction of the interface. <i>policy-map-name:</i> Indicates the name of the policy applied to the interface. |
| Command Mode | Interface configuration mode/Global configuration mode/Logical port group mode |
| Usage Guide | - |

Configuration Example

- ❖ Creating three stream classes and matching ACL, IP PRE and DSCP

| | |
|----------------------------|--|
| Configuration Steps | <ul style="list-style-type: none"> ▪ Create ACL rules. ▪ Create 3 stream classes and match ACL, IP PRE and DSCP. |
| | <pre>QTECH# configure terminal QTECH(config)# access-list 11 permit host 192.168.23.61</pre> |
| | <pre>QTECH(config)# class-map cmap1 QTECH(config-cmap)# match access-group 11 QTECH(config-cmap)# exit QTECH(config)# class-map cmap2 QTECH(config-cmap)# match ip dscp 21 QTECH(config-cmap)# exit QTECH(config)# class-map cmap3 QTECH(config-cmap)# match ip precedence 5 QTECH(config-cmap)# exit</pre> |
| Verification | Check whether the created ACL rules and stream class rules are successful. |
| | <pre>QTECH# show access-lists ip access- list standard 11 10 permit host 192.168.23.61 QTECH# show class-map Class Map cmap1 Match access-group 11 Class Map cmap2 Match ip dscp 21</pre> |

- ❖ Creating a policy, binding a class and stream behaviors, and associating with an interface

| | |
|----------------------------|---|
| <p>Configuration Steps</p> | <ul style="list-style-type: none"> ▪ Create the stream class cmap1, and match packets whose DSCP value is 18. Create cmap2 and match packets whose IP PRE is 7. Create cmap3 and apply ACL 11. ▪ Create the policy pmap1, associate the policy with cmap1, and bind the behavior of changing the CoS value of the stream to 6. Associate the policy with cmap2, bind the behavior of changing the DSCP value of the stream to 16, limiting the traffic per second within 10,000 Kbits and trigger traffic within 1024 Kbits per second, and changing the DSCP value for traffic out of limit to 7. Associate cmap3 and bind its behavior to drop. ▪ Apply the policy pmap1 to the output direction of the interface gigabitEthernet0/0. ▪ Create virtual logical group 1, add the interfaces gigabitEthernet 0/1 and gigabitEthernet 0/2 to the group, and apply the policy pmap1 to the input interface of the virtual logicalgroup. |
| | <pre>QTECH# configure terminal QTECH(config)# class-map cmap1 QTECH(config-cmap)# match ip dscp 18 QTECH(config-cmap)# exit QTECH(config)# class-map cmap2 QTECH(config-cmap)# match ip precedence 7 QTECH(config-cmap)# exit QTECH(config)# access-list 11 permit host 192.168.23.61 QTECH(config)# class-map cmap3 QTECH(config-cmap)# match access-group 11 QTECH(config-cmap)# exit</pre> |
| | <pre>QTECH(config)# policy-map pmap1 QTECH(config-pmap)# class cmap1 QTECH(config-pmap-c)# set cos 6</pre> |
| | <pre>QTECH(config-pmap-c)# exit QTECH(config-cmap)# class cmap2 QTECH(config-cmap-c)# set ip dscp 15 QTECH(config-pmap-c)# police 10000 1024 exceed-action dscp 7 QTECH(config-pmap-c)# exit QTECH(config-pmap)# exit</pre> |
| | <pre>QTECH(config)# interface gigabitEthernet 0/0 QTECH(config-if-GigabitEthernet 0/0)# service-policy output pmap1 QTECH(config-if-GigabitEthernet 0/0)# exit</pre> |
| | <pre>QTECH(config)# interface gigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)# virtual-group 1 QTECH(config-if-GigabitEthernet 0/1)# exit QTECH(config)# interface gigabitEthernet 0/2 QTECH(config-if-GigabitEthernet 0/2)# virtual-group 1 QTECH(config-if-GigabitEthernet 0/2)# exit QTECH(config)# virtual-group 1 QTECH(config-VirtualGroup)# service-policy input pmap1 QTECH(config-VirtualGroup)# exit</pre> |

| | |
|---------------------|--|
| Verification | <ul style="list-style-type: none"> ▪ Check whether the stream class rules are successfully created. ▪ Check whether the policy is successfully created, and whether the stream and stream behaviors are successfully bound. ▪ Check whether the policy is applied to the interface. ▪ Check whether the logical interface group is successfully created, whether interfaces are successfully associated and whether the policy is successfully applied to the interface. |
| | <pre>QTECH# show class-map Class Map cmap1 Match ip dscp 18 Class Map cmap2 Match ip precedence 7 Class Map cmap3 Match access-group 11</pre> |
| | <pre>QTECH# show policy-map Policy Map pmap1 Class cmap1 set cos 6 Class cmap2 set ip dscp 15 police 10000 1024 exceed-action dscp 7</pre> |
| | <pre>QTECH# show mls qos interface gigabitEthernet 0/0 Interface: GigabitEthernet 0/0 Ratelimit input: Ratelimit output: Attached input policy-map: Attached output policy-map: pmap1 Default trust: none Default cos: 0</pre> |
| | <pre>QTECH# show virtual-group 1 virtual-group member 1 Gi0/1 Gi0/2 QTECH# show mls qos virtual-group 1 Virtual-group: 1 Attached input policy-map: pmap1</pre> |

2.4.2 Configuring Priority Labeling and Mapping for Packets

Configuration Effect

- Configure the trust mode and default CoS value of an interface.
- Configure the CoS-to-DSCP, DSCP-to-CoS, and IP-PRE-to-DSCP mappings.

Notes

- Interface configurations allow for only AP and Ethernet interface configurations.

Configuration Steps

❖ Configuring the trust mode and default CoS value of an interface

- Optional.
- In the interface configuration mode, configure the trust mode and default CoS value of an interface.

❖ Configuring the CoS-to-DSCP, DSCP-to-CoS, and IP-PRE-to-DSCP mappings

- Optional.
- Configure various mappings.

Verification

- Run the **show mls qos interface** command to display the trust mode and default CoS value of the interface.
- Run the **show mls qos maps** command to display the CoS-to-DSCP, DSCP-to-CoS and IP-PRE-to-DSCP mappings.

Related Commands

❖ Configuring the trust mode of an interface

| | |
|-----------------------|---|
| Command | <code>mls qos trust { cos ip-precedence dscp }</code> |
| Parameter Description | cos : Configures the trust mode of an interface to CoS. ip-precedence : Configures the trust mode of an interface to IP PRE. dscp : Configures the trust mode of an interface to DSCP. |
| Command Mode | Interface configuration mode |
| Usage Guide | - |

❖ Configuring the default CoS value of an interface

| | |
|---------|---|
| Command | <code>mls qos cos <i>default-cos</i></code> |
|---------|---|

| | |
|------------------------------|---|
| Parameter Description | <i>default-cos</i> : Configures the default CoS value, ranging from 0 to 7. The default value is 0. |
| Command Mode | Interface configuration mode |
| Usage Guide | - |

❖ Configuring CoS-to-DSCP MAP

| | |
|------------------------------|--|
| Command | <code>mls qos map cos-dscp <i>dscp1...dscp8</i></code> |
| Parameter Description | <i>dscp1...dscp8</i> : Indicates the DSCP values mapped to the CoS values. The default CoS values 0~7 are mapped to DSCP 0, 8, 16, 24, 32, 40, 48 and 56 respectively. The DSCP value ranges from 0 to 63. |
| Command Mode | Global configuration mode |
| Usage Guide | - |

❖ Configuring DSCP-to-CoS MAP

| | |
|------------------------------|--|
| Command | <code>mls qos map dscp-cos <i>dscp-list to cos</i></code> |
| Parameter Description | <i>dscp-list</i> : Indicates the DSCP list mapped to the CoS values. The default DSCP 0~7 are mapped to CoS 0, DSCP 8~15 mapped to CoS 1, DSCP 16~23 mapped to CoS 2, DSCP 24~31 mapped to CoS 3, DSCP 32~39 mapped to CoS 4, DSCP 40~47 mapped to CoS 5, DSCP 48~55 mapped to CoS 6, and DSCP 56~63 mapped to CoS 7. The DSCP value ranges from 0 to 63. <i>cos</i> : Indicates the CoS values mapped to the dscp-list, ranging from 0 to 7. |
| Command Mode | Global configuration mode |
| Usage Guide | - |

❖ Configuring IP-PRE-to-DSCP MAP

| | |
|------------------------------|--|
| Command | <code>mls qos map ip-prec-dscp <i>dscp1...dscp8</i></code> |
| Parameter Description | <i>dscp1...dscp8</i> : Indicates the DSCP values mapped to the IP PRE values. The default IP PRE 0~7 are |

| | |
|---------------------|--|
| | mapped to DSCP 0, 8, 16, 24, 32, 40, 48 and 56 respectively. The DSCP value ranges from 0 to 63. |
| Command Mode | Global configuration mode |
| Usage Guide | - |

Configuration Example

- ❖ Configuring the trust mode and default CoS value of an interface

| | |
|----------------------------|---|
| Configuration Steps | <ul style="list-style-type: none"> ▪ Modify the trust mode of the interface gigabitEthernet 0/0 to DSCP. ▪ Change the default CoS value of the interface gigabitEthernet 0/1 to 7. |
| | <pre>QTECH# configure terminal QTECH(config)# interface gigabitEthernet 0/0 QTECH(config-if-GigabitEthernet 0/0)# mls qos trust dscp QTECH(config-if- GigabitEthernet 0/0)# exit QTECH(config)# interface gigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)# mls qos cos 7 QTECH(config-if-GigabitEthernet 0/1)# exit</pre> |
| Verification | Check whether the trust mode and default CoS value are successfully configured for the interface. |
| | <pre>QTECH# show mls qos interface gigabitEthernet 0/0 Interface: GigabitEthernet 0/0 Ratelimit input: Ratelimit output:</pre> |

```

Attached      input
policy-map:
Attached      output
policy-map: Default
trust: dscp
Default cos: 0

QTECH# show mls qos interface
gigabitEthernet 0/1 Interface:
GigabitEthernet 0/1
Ratelimit
input:
Ratelimit
output:
Attached      input
policy-map:
Attached      output
policy-map: Default
trust: none
Default cos: 7

```

❖ Configuring the CoS-to-DSCP, DSCP-to-CoS, and IP-PRE-to-DSCP mappings

| | |
|----------------------------|---|
| Configuration Steps | <p>Configure CoS-to-DSCP to map CoS 0, 1, 2, 3, 4, 5, 6, and 7 to DSCP 7, 14, 21, 28, 35, 42, 49, and 56 respectively.</p> <p>Configure DSCP-to-CoS to map DSCP 0, 1, 2, 3, and 4 to CoS 4 and DSCP 11, 12, 13 and 14 to CoS 7.</p> |
| | <p>Configure IP-PRE-to-DSCP to map IP PRE 0, 1, 2, 3, 4, 5, 6, and 7 to DSCP 31, 26, 21, 15, 19, 45, 47, and 61 respectively.</p> |
| | <pre> QTECH# configure terminal QTECH(config)# mls qos map cos-dscp 7 14 21 28 35 42 49 56 QTECH(config)# mls qos map dscp-cos 0 1 2 3 4 to 4 QTECH(config)# mls qos map dscp-cos 11 12 13 14 to 7 QTECH(config)# mls qos map ip-precedence-dscp 31 26 21 15 19 45 47 61 </pre> |
| Verification | <p>Check whether all mappings are successfully configured.</p> |
| | <pre> QTECH# show mls qos maps cos-dscp </pre> |

```
cos dscp

0 7
1 14
2 21
3 28
4 35
5 42
6 49
7 56

QTECH# show mls qos maps dscp-cos
dscp cos dscp cos dscp cos dscp cos

 0 4 1 4 2 4 3 4
 4 4 5 0 6 0 7 0
 8 1 9 1 10 1 11 7
12 7 13 7 14 7 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

QTECH# show mls qos maps ip-prec-dscp
ip-precedence dscp

0 31
1 26
2 21
3 15
4 15
5 19
6 47
7 61
```

2.4.3 Configuring Interface Rate Limit Configuration Effect

- Configure the traffic limit for an interface.

Notes

- The configuration is supported only by Ethernet and aggregate interfaces.

Configuration Steps

❖ Configuring the traffic limit for an interface

- Optional.
- Configure the limit on the traffic and burst traffic for an interface.

Verification

- Run the **show mls qos rate-limit** command to display the rate limit information about the interface.

Related Commands

❖ Configuring the traffic limit for an interface

| | |
|-----------------------|--|
| Command | <code>rate-limit { input output } <i>bps burst-size</i></code> |
| Parameter Description | <p>input: Indicates the input direction of the interface.</p> <p>output: Indicates the output direction of the interface.</p> <p><i>bps:</i> Indicates the bandwidth limit per second (Kbits). The value range is determined by products.</p> <p><i>burst-size:</i> Indicates the burst traffic limit (Kbytes). The value range is determined by products.</p> |
| Command Mode | Interface configuration mode |
| Usage Guide | - |

Configuration Example

- ❖ Typical application – Interface rate limit + priority relabeling

| | |
|----------------------------|--|
| <p>Configuration Steps</p> | <ul style="list-style-type: none"> ▪ For Internet access by using the output interface, configure the output traffic limit on the interface G0/24, and set the bandwidth limit to 102,400 Kbits per second and burst traffic limit to 256 Kbytes per second. ▪ For the dormitory building, configure the input traffic limit on the interface G0/3, and set the bandwidth limit to 51,200 Kbits per second and burst traffic limit to 256 Kbytes per second. ▪ For the teaching building, configure the input traffic limit on the interface G0/1, and set the bandwidth limit to 30,720 Kbits per second and burst traffic limit to 256 Kbytes per second. ▪ For the laboratory, create the class <code>cmap_dscp7</code> to match DSCP priority 7, create the policy <code>pmap_shiyan</code> to associate with <code>cmap_dscp7</code>, bind the stream behavior of changing the DSCP value for packets whose rates exceed 20M to 16, apply <code>pmap_shiyan</code> to the interface G0/2, and configure the interface to trusting DSCP. |
| | <pre>QTECH# configure terminal QTECH(config)# interface gigabitEthernet 0/24 QTECH(config-if-GigabitEthernet 0/24# rate-limit output 102400 256 QTECH(config-if-GigabitEthernet 0/24)# exit QTECH(config)# interface gigabitEthernet 0/3 QTECH(config-if-GigabitEthernet 0/3# rate-limit input 51200 256 QTECH(config-if-GigabitEthernet 0/3)# exit QTECH(config)# interface gigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1# rate-limit input 30720 256 QTECH(config-if-GigabitEthernet 0/1)# exit</pre> |
| | <pre>QTECH(config)# class-map cmap_dscp7 QTECH(config-cmap)# match ip dscp 7 QTECH(config-cmap)# exit QTECH(config)# policy-map pmap_shiyan QTECH(config-pmap)# class cmap_dscp7 QTECH(config-pmap-c)# police 20480 128 exceed-action dscp 16 QTECH(config-pmap-c)# exit QTECH(config-pmap)# exit QTECH(config)# interface gigabitEthernet 0/2 QTECH(config-if-GigabitEthernet 0/2# service-policy input pmap_shiyan QTECH(config-if-GigabitEthernet 0/2)# mls qos trust dscp QTECH(config- if-GigabitEthernet 0/2)# exit</pre> |
| <p>Verification</p> | <p>Check whether the interface rate limit is successfully configured.</p> |
| | <p>Check whether the class and policy are successfully created and successfully applied to the interface.</p> |

```
QTECH# show mls qos
rate-limit
Interface:
GigabitEthernet 0/1
  rate limit input Kbps =
30720 burst = 256 Interface:
GigabitEthernet 0/3
  rate limit input Kbps = 51200 burst = 256 Interface: GigabitEthernet
0/24
  rate limit output Kbps = 102400 burst = 256
QTECH# show class-map cmap_dscp7

Class Map cmap_dscp7

Match ip dscp 7

QTECH# show policy-map pmap_shiyan

Policy Map pmap_shiyan

Class cmap_dscp7

  police 20480 128 exceed-action
dscp 16 QTECH# show mls qos
interface gigabitEthernet 0/2
Interface: GigabitEthernet 0/2
Ratelimit input: Ratelimit output:
Attached input policy-map: pmap_shiyan Attached output policy-map:
Default trust: dscp

Default cos: 0
```

2.4.4 Configuring Congestion Management Configuration Effect

- Configure the CoS-to-queue mapping.
- Configure the scheduling policy and round robin weight for an output queue.
- Configure the guaranteed minimum bandwidth and limited maximum bandwidth for a queue.

Notes

- Interface configurations allow for only AP and Ethernet interface configurations.

Configuration Steps

❖ Configuring the CoS-to-unicast and CoS-to-multicast mappings

- Optional.

- Configure the CoS-to-queue mappings. On products supporting multicast queues, you can configure the CoS-to-multicast queue mapping.
- ❖ **Configuring the scheduling policies and round robin weight for output queues**
 - Optional.
 - Configure the scheduling policy for an output queue and modify the round robin weight.
- ❖ **Configuring the guaranteed minimum bandwidth and limited maximum bandwidth for a queue**
 - Optional.
 - Configure the guaranteed minimum bandwidth and limited maximum bandwidth for a queue.

Verification

- Run the **show mls qos queueing** command to display the output queue information.
- Run the **show mls qos scheduler** command to display the scheduling policy for the output queue.
- Run the **show qos mc-queue scheduler** command to display the scheduling policy for the multicast queue.
- Run the **show qos bandwidth** command to display the queue bandwidth.

Related Commands

❖ **Configuring CoS-to-Queue MAP**

| | |
|------------------------------|--|
| Command | <code>priority-queue cos-map <i>qid</i> <i>cos0</i> [<i>cos1</i> [<i>cos2</i> [<i>cos3</i> [<i>cos4</i> [<i>cos5</i> [<i>cos6</i> [<i>cos7</i>]]]]]]]</code> |
| Parameter Description | <i>qid</i> : Indicates the queue ID to be mapped, ranging from 1 to 8. <i>cos0~cos7</i> : Indicates the CoS values to be mapped to the <i>qid</i> . The default CoS values 0~7 are mapped to queues 1~8. The value range is 0 to 7. |
| Command Mode | Global configuration mode |
| Usage Guide | - |

- ❖ **Configuring the scheduling policy for an output queue to SP**

| | |
|----------------|-----------------------------|
| Command | <code>priority-queue</code> |
|----------------|-----------------------------|

| | |
|------------------------------|---------------------------|
| Parameter Description | - |
| Command Mode | Global configuration mode |
| Usage Guide | - |

❖ Configuring the scheduling policy for an output queue

| | |
|------------------------------|---|
| Command | <code>mls qos scheduler { sp wrr drr }</code> |
| Parameter Description | sp: Sets the scheduling algorithm for an output queue to SP. wrr: Sets the scheduling algorithm for an output queue to WRR. drr: Sets the scheduling algorithm for an output queue to DRR. |
| Command Mode | Global configuration mode |
| Usage Guide | - |

❖ Configuring the scheduling policy and round robin weight for an output queue

| | |
|------------------------------|---|
| Command | <code>{ drr-queue wrr-queue } bandwidth <i>weight1...weight8</i></code> |
| Parameter Description | drr-queue: Configures the round robin weight corresponding to the DRR scheduling policy for an output queue. wrr-queue: Configures the round robin weight corresponding to the WRR scheduling policy for an output queue. <i>weight1...weight8:</i> Indicates the weight of queues 1 to 8. The value range is determined by products. The value 0 indicates that the queue uses the SP scheduling algorithm. The default weight for global/interface queues is 1:1. |
| Command Mode | Global configuration mode |
| Usage Guide | - |

❖ Configuring CoS-to-Queue MAP for multicast queues

| | |
|------------------------------|---|
| Command | <code>qos mc-queue cos-map <i>cos0-qid...cos7-qid</i></code> |
| Parameter Description | <i>cosN-qid:</i> Indicates the queue ID to be mapped by CoS N. The specific number of multicast queues is |

| | |
|---------------------|--|
| | determined by products. The default value is determined by products. |
| Command Mode | Global/Interface configuration mode |
| Usage Guide | - |

- ❖ Configuring the guaranteed minimum bandwidth and limited maximum bandwidth for a queue

| | |
|------------------------------|---|
| Command | <code>qos queue <i>queue-id</i> bandwidth { minimum maximum } <i>bandwidth</i></code> |
| Parameter Description | <p>queue: configures the guaranteed minimum bandwidth or limited maximum bandwidth for devices that allow for configuring both the unicast and multicast queue bandwidth limits.</p> <p>queue-id: Indicates the queue ID to be configured, ranging from 1 to 8.</p> <p>minimum bandwidth: Indicates the guaranteed minimum bandwidth Kbps. The value range is determined by products. It is not configured by default.</p> |
| | <p>maximum bandwidth: Indicates the limited maximum bandwidth Kbps. The value range is determined by products. It is not configured by default.</p> |
| Command Mode | Interface configuration mode |
| Usage Guide | - |

Configuration Example

- ❖ Configuring the CoS-to-queue mapping and modifying the scheduling policy and its round robin weight

| | |
|----------------------------|--|
| Configuration Steps | <ul style="list-style-type: none"> ▪ Configure the CoS-to-queue mapping to the mapping from the CoS values 0, 1, 2, 3, 4, 5, 6, and 7 to queues 1, 2, 5, 5, 5, 5, 7, and 8. ▪ Configure the output scheduling policy for a queue to DRR and the round robin weight to 2:1:1:1:6:6:6:8. |
| | <pre>QTECH# configure terminal QTECH(config)# priority-queue cos-map 1 2 5 5 5 5 7 8 QTECH(config)# mls qos scheduler drr QTECH(config)# drr-queue bandwidth 2 1 1 1 6 6 6 8</pre> |

| Verification | Check whether the CoS-to-queue mapping is successfully created, and whether the output scheduling policy and round robin weight are successfully configured for the queue. |
|--------------|---|
| | <pre> QTECH# show mls qos scheduler Global Multi-Layer Switching scheduling Deficit Round Robin QTECH# show mls qos queueing CoS-to-queue map: cos qid --- --- 0 1 1 2 2 5 3 5 4 5 5 5 6 7 7 8 </pre> |
| | <pre> wrr bandwidth weights: qid weights 1 1 2 1 3 1 4 1 5 1 6 1 7 1 8 1 drr bandwidth weights: qid weights 1 2 2 1 3 1 4 1 5 6 6 6 7 6 8 8 </pre> |

- ❖ Taking products that support separate configuration of unicast and multicast queues for example and configuring the guaranteed minimum bandwidth and limited maximum bandwidth for a queue

| | |
|----------------------------|---|
| Configuration Steps | Configure the limited maximum bandwidth to 10M and guaranteed minimum bandwidth to 5M for unicast queue 1 on the interface gigabitEthernet 0/1. Configure the guaranteed minimum bandwidth to 2M for unicast queue 2. Configure the limited maximum bandwidth to 5M and guaranteed minimum bandwidth to 1M for multicast queue 1. |
| | <pre> QTECH# configure terminal QTECH(config)# interface gigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)# qos queue ucast 1 bandwidth maximum 10240 QTECH(config-if-GigabitEthernet 0/1)# qos queue ucast 1 bandwidth minimum 5120 QTECH(config-if-GigabitEthernet 0/1)# qos queue ucast 2 bandwidth minimum 2048 QTECH(config-if-GigabitEthernet 0/1)# exit </pre> |
| Verification | Check whether the guaranteed minimum bandwidth and limited maximum bandwidth are successfully configured for the interface. |
| | <pre> QTECH# show qos bandwidth interface gigabitEthernet 0/1 Interface: GigabitEthernet 0/1 ----- uc-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 Interface: GigabitEthernet 0/1 ----- mc-queue-id minimum-bandwidth maximum-bandwidth ----- 1 1024 5120 2 0 0 3 0 0 4 0 2048 </pre> |

❖ Typical application – Priority relabeling + queue scheduling

| | |
|----------------------------|---|
| <p>Configuration Steps</p> | <p>Create ACLs for accessing various servers and create classes for matching these ACLs.</p> <ul style="list-style-type: none"> ▪ Create policies for associating with the classes and specify new CoS values for packets accessing various servers. Associate the CoS values with the input interfaces for the R&D and market departments and configure the interfaces to trusting CoS. ▪ Configure the default CoS value for the HR management department interface to the highest priority 7 to ensure that packets from the HR management department are sent in the highest priority. ▪ Configure the output scheduling policy to <code>WR</code> and the round robin weight to <code>1:1:1:2:6:1:1:0</code> for the queues. This means that the <code>SP</code> scheduling algorithm is used for packets of the HR management department, and the packets of the R&D and market departments for accessing the mail database, file database and salary query database are scheduled based on the ratio of <code>6:2:1</code>. |
| | <pre>QTECH# configure terminal QTECH(config)# ip access-list extended salary QTECH(config-ext-nacl)# permit ip any host 192.168.10.1 QTECH(config-ext-nacl)# exit QTECH(config)# ip access-list extended mail QTECH(config-ext-nacl)# permit ip any host 192.168.10.2 QTECH(config-ext-nacl)# exit QTECH(config)# ip access-list extended file QTECH(config-ext-nacl)# permit ip any host 192.168.10.3 QTECH(config-ext-nacl)# exit</pre> |
| | <pre>QTECH(config)# class-map salary QTECH(config-cmap)# match access-group salary QTECH(config-cmap)# exit QTECH(config)# class-map mail QTECH(config-cmap)# match access-group mail QTECH(config-cmap)# exit QTECH(config)# class-map file QTECH(config-cmap)# match access-group file</pre> |

| | |
|---------------------|--|
| | <pre> QTECH(config)# policy-map toserver QTECH(config-pmap)# class mail QTECH(config-pmap- c)# set cos 4 QTECH(config- pmap-c)# exit QTECH(config- pmap)# class file QTECH(config-pmap-c)# set cos 3 QTECH(config-pmap-c)# exit QTECH(config-pmap)# class salary QTECH(config-pmap-c)# set cos 2 QTECH(config-pmap-c)# end </pre> |
| | <pre> QTECH(config)# interface gigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)# service-policy input toserver QTECH(config-if-GigabitEthernet 0/1)# mls qos trust cos QTECH(config-if- GigabitEthernet 0/1)# exit QTECH(config)# interface gigabitEthernet 0/2 QTECH(config-if-GigabitEthernet 0/2)# service-policy input toserver QTECH(config-if-GigabitEthernet 0/2)# mls qos trust cos QTECH(config-if- GigabitEthernet 0/2)# exit </pre> |
| | <pre> QTECH(config)# interface gigabitEthernet 0/3 QTECH(config-if-GigabitEthernet 0/3)# mls qos cos 7 </pre> |
| | <pre> QTECH(config)#wrr-queue bandwidth 1 1 1 2 6 1 1 0 QTECH(config)#mls qos scheduler wrr </pre> |
| Verification | <ul style="list-style-type: none"> ▪ Check whether the ACLs are successfully created and whether the classes are successfully associated with the ACLs. ▪ Check whether the policies are successfully created, whether the classes and stream behaviors are successfully bound, and whether policies are successfully applied to the interfaces. ▪ Check whether the default CoS value is successfully configured for the interface and whether the scheduling policy and the round robin weight are successfully configured. |
| | <pre> QTECH# show access-lists ip access-list extended file </pre> |

| | |
|--|---|
| | <pre> 10 permit ip any host 192.168.10.3 ip access-list extended mail 10 permit ip any host 192.168.10.2 ip access-list extended salary 10 permit ip any host 192.168.10.1 </pre> |
| | <pre> QTECH# show class-map Class Map salary Match access-group salary Class Map mail Match access-group mail Class Map file Match access-group file </pre> |
| | <pre> QTECH# show policy-map Policy Map toserver Class mail set cos 4 Class file set cos 3 Class salary set cos 2 </pre> |
| | <pre> QTECH# show mls qos interface gigabitEthernet 0/1 Interface: GigabitEthernet 0/1 Ratelimit input: Ratelimit output: Attached input policy-map: toserver Attached output policy-map: Default trust: cos </pre> |

| | |
|--|---|
| | <pre> Default cos: 0 QTECH# show mls qos interface gigabitEthernet 0/2 Interface: GigabitEthernet 0/3 Ratelimit input: Ratelimit output: Attached input policy- map: toserver Attached output policy-map: Default trust: cos Default cos: 0 </pre> |
| | <pre> QTECH# show mls qos interface gigabitEthernet 0/3 Interface: GigabitEthernet 0/2 Ratelimit input: Ratelimit output: Attached input policy-map: Attached output policy-map: Default trust: none Default cos: 7 QTECH# show mls qos scheduler Global Multi-Layer Switching scheduling Weighted Round Robin QTECH# QTECH#show mls qos queueing CoS-to-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 1 3 1 4 2 5 6 6 1 7 1 8 0 drr bandwidth weights: qid </pre> |

| weights | |
|---------|---|
| 1 | 1 |
| 2 | 1 |
| 3 | 1 |
| 4 | 1 |
| 5 | 1 |
| 6 | 1 |
| 7 | 1 |
| 8 | 1 |

2.4.5 Configuring Congestion Mitigation

Configuration Effect

- Configure the lower threshold value for WRED. When the length of packets in a queue is smaller than the lower threshold value, WRED does not discard packets.
- Configure the maximum discarding probability. When the length of packets in the queue is between the lower and higher threshold values, WRED discards packets in random. The maximum probability for discarding packets is configured.
- Configure the CoS-to-threshold mapping.

Notes

- Interface configurations allow for only AP and Ethernet interface configurations.

Configuration Steps

❖ Enabling the WRED function

- Optional.
- Enable the WRED function if necessary.

❖ Configuring the lower threshold value

- Optional.
- Configure the lower threshold value if necessary.

❖ Configuring the maximum discarding probability

- Optional.
- Configure the maximum discarding probability if necessary.

❖ Configuring the CoS-to-threshold mapping

- Optional.
- Configure the CoS-to-threshold mapping if necessary.

Verification

- Run the **show queueing wred interface** command to display the WRED configuration.

Related Commands

❖ Enabling the WRED function

| | |
|-----------------------|---------------------------|
| Command | queueing wred |
| Parameter Description | - |
| Command Mode | Global configuration mode |
| Usage Guide | - |

- ❖ Configuring the lower threshold value(in the unit of percentage)

| | |
|-----------------------|---|
| Command | wrr-queue random-detect min-threshold <i>queue_id</i> <i>thr1</i> [<i>thr2</i>] |
| Parameter Description | <i>queue_id</i> : Indicates the queue ID for an interface, ranging from 1 to 8. <i>thrN</i> : Supports 2 groups of lower threshold values, ranging from 1 to the specified higher threshold. |
| Command Mode | Interface configuration mode |
| Usage Guide | Because the maximum value of the configuration range is equal to the current higher threshold, you need to pay attention to the setting of the higher threshold when configuring the lower threshold. |

- ❖ Configuring the maximum discarding probability

| | |
|-----------------------|---|
| Command | wrr-queue random-detect probability <i>queue_id</i> <i>prob1</i> [<i>prob2</i>] |
| Parameter Description | <i>queue_id</i> : Indicates the queue ID for an interface, ranging from 1 to 8. <i>probN</i> : Supports 2 groups of maximum discarding probabilities, ranging from 1 to 100. |
| Command Mode | Interface configuration mode |
| Usage Guide | - |

- ❖ Configuring the CoS-to-threshold mapping

| | |
|------------------------------|---|
| Command | wrr-queue cos-map <i>threshold_id cos1</i> [<i>cos2</i> [<i>cos3</i> [<i>cos4</i> [<i>cos5</i> [<i>cos6</i> [<i>cos7</i> [<i>cos8</i>]]]]]]]] |
| Parameter Description | <i>threshold_id</i> : Indicates the threshold group ID, ranging from 1 to 2. Two threshold groups are supported. <i>cos1...cos8</i> : Indicates the CoS values to be mapped to the threshold group, ranging from 0 to 7. By default, all CoS values are mapped to the first threshold group. |
| Command Mode | Interface configuration mode |
| Usage Guide | - |

Configuration Example

- ❖ Enabling the WRED function and configuring the lower threshold, maximum discarding probability, and the CoS-to-threshold mappings (assuming that there are 2 groups of thresholds for a product)

| | |
|----------------------------|--|
| Configuration Steps | <ul style="list-style-type: none"> ▪ Enable the WRED function. ▪ Configure the lower thresholds for queue 2 of the interface gigabitEthernet 0/2 to 10 and 20. ▪ Configure the higher thresholds for queue 2 of the interface gigabitEthernet 0/2 to 60 and 90. ▪ Configure the maximum discarding probabilities for queue 2 of the interface gigabitEthernet 0/2 to 60 and 80. ▪ Configure the CoS values 0, 1, 2, and 3 on the interface gigabitEthernet 0/2 to use the threshold group 2. |
| | <pre>QTECH# configure terminal</pre> |
| | <pre>QTECH(config)# queueing wred QTECH(config)# interface gigabitEthernet 0/2 QTECH(config-if-GigabitEthernet 0/2)# wrr-queue random-detect min- threshold 2 10 20 QTECH(config-if-GigabitEthernet 0/2)# wrr-queue random-detect max- threshold 2 60 90 QTECH(config-if-GigabitEthernet 0/2)# wrr-queue random-detect probability 2 60 80 QTECH(config-if-GigabitEthernet 0/2)# wrr-queue cos-map 2 0 1 2 3</pre> |

| | |
|---------------------|---|
| Verification | <ul style="list-style-type: none"> Check whether the WRED function is enabled, whether the thresholds are successfully configured, and whether the CoS-to-threshold mapping is successfully configured. |
| | <pre>QTECH# show running-config Building configuration... Current configuration : 1654 bytes version 11.0(1C2B1) (09/11/13 00:16:26 CST -ngcf78) queueing wred QTECH#show queueing wred interface gigabitEthernet 0/1 qid min_1 prob_1 min_2 rob_2 1 100 60 80 80 2 100 60 80 80 3 100 60 80 80 4 100 60 80 80 5 100 60 80 80 6 100 60 80 80 7 100 60 80 80 8 100 60 80 80</pre> |
| | <pre>cos qid hreshold_id 0 1 1 1 2 1 2 3 1 3 4 1 4 5 1 5 6 1 6 7 1 7 8 1</pre> |

2.5 Monitoring

Displaying

| Description | Command |
|---|---|
| Displays stream classification information. | show class-map [<i>class-map-name</i>] |

| | |
|---|--|
| Displays QoS policy information. | show policy-map [<i>policy-map-name</i> [class <i>class-map-name</i>]] |
| Displays the policy applied to an interface. | show policy-map interface <i>interface-id</i> |
| Displays logical interface group information. | show virtual-group [<i>virtual-group-number</i> summary] |
| Displays the policy applied to a logical interface group. | show mls qos virtual-group [<i>virtual-group-number</i> policers] |
| Displays various mappings. | show mls qos maps [cos-dscp dscp-cos ip-prec-dscp] |
| Displays interface rate limit information. | show mls qos rate-limit [interface <i>interface-id</i>] |
| Displays the QoS queue, scheduling policy and round robin weight information. | show mls qos queueing [interface <i>interface-id</i>] |
| Displays the scheduling information of an output queue. | show mls qos scheduler |
| Displays the priority mapping for a multicast queue. | show qos mc-queue cos-map |
| Displays the output scheduling policy for a multicast queue. | show qos mc-queue scheduler |
| Displays the configurations of WRED. | show queueing wred interface <i>interface-id</i> |
| Displays the QoS information of an interface. | show mls qos interface <i>interface-id</i> [policers] |
| Displays the bandwidth information of an interface. | show qos bandwidth [interfaces <i>interface-id</i>] |

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

| Description | Command |
|--------------------------------------|---|
| Debugs the QoS library. | debug qos lib [event message] |
| Debugs the QoS communication server. | debug qos server [event message] |
| Debugs QoS user command processing. | debug qos mls |
| Debugs VMSUP configurations. | debug qos vmsup |

3.1 Overview

The Memory Management Unit (MMU) means that the chip buffer is distributed reasonably so that the switching equipment can better deal with all kinds of burst flows.

Flows not steady all the time and various burst flows exist on the network. When the network flow is steady and the bandwidth is sufficient, all the data flows are processed better; when burst flows exist on the network, data flows may be discarded even if the average flow rate does not exceed the bandwidth.

Data packets that enter the switching equipment are stored in the buffer of switching equipment before being forwarded. Normally, data packets stay for a short period of time in the buffer and will be forwarded in microseconds; when there is a burst flow, if the instantaneous rate of burst flow exceeds the processing capacity of the switching equipment, the data packets that cannot be processed in time will be piled up in the switching equipment and packet loss will take place once the buffer is insufficient. In this case, the MMU can be used to reasonably configure the buffer and allocate different buffer sizes to respective services, with a view to optimizing the network.

3.2 Applications

| Application | Description |
|--|--|
| Configuring Large Buffer Application Based on Egress Queue | An enterprise needs a buffer large enough in the SkyDrive service to avoid packet loss for the service flow. |

3.2.1 Configuring Large Buffer Application Based on Egress Queue Scenario

An enterprise needs a buffer large enough in the SkyDrive service to avoid packet loss for the service flow.

As shown in the following figure, equipment A is connected to 5 clients and 35 service servers, where 15 service servers virtualize 15 front end servers.

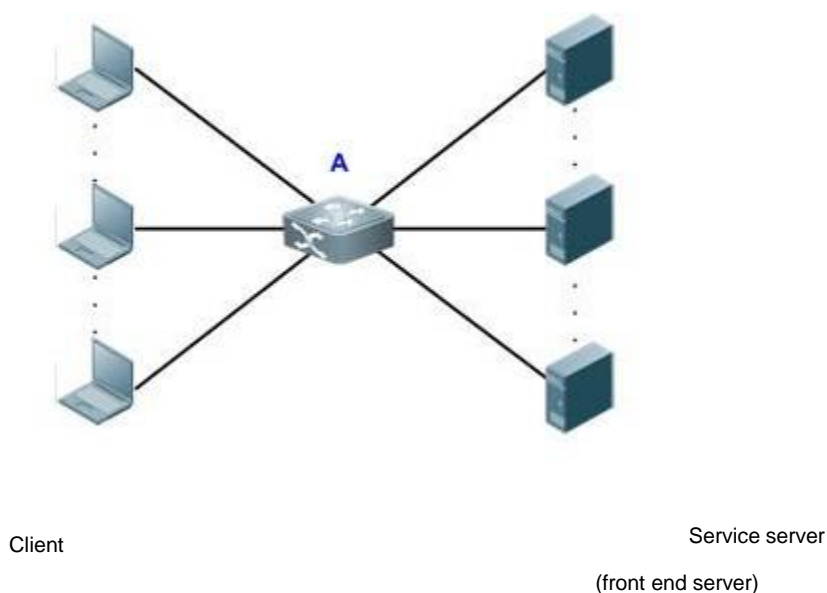
The main service flow is as follows:

- The client server sends a request packet to the front end server.
- The front end server sends the received request packet to the service server.

- After receiving the request packet, the service server sends a response packet to the front end server.
- After receiving the response packet, the front end server sends it to the client server.
- After receiving the response packet, the client indicates that a session is created successfully. A many-to-one flow transmission mode exists under this service model:
 - The request flows of multiple clients are sent to one front end server.
 - The request flows of multiple front end servers are sent to one service server.
 - The response flows of multiple service servers are sent to one front end server.
 - The response flows of multiple front end servers are sent to one client.

These flows are transmitted through equipment A basically, easily leading to network congestion. Such a problem can be fixed by configuring a large buffer on the equipment.

Figure 3-1



Deployment

- In all the service ports (namely, the ports connecting clients to servers), configure the shared buffer of the queue where the service is as 100%.
- In all the service ports, configure the minimum value for the guaranteed buffer of the queue not in use.
- In all the ports not in use, configure the minimum value for the guaranteed buffers of all the queues.

For the specific configuration, see the configuration examples in "Configuration".

3.3 Features

Basic Concepts

❖ Cell

Cell is a buffer unit, i.e., the minimum unit for the switching equipment to store packets. The size of each cell varies with the product. One packet can use multiple cells, while one cell can be used by only one packet.

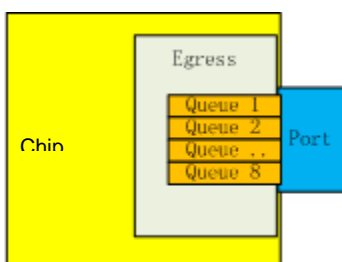
❖ Port group

All the ports physically belonging to one switching chip are collectively called a port group, the buffer of switching equipment is managed in the port group. Take the board card M18000_40XS_CB as an example, this version has two switching chips, so there are two port groups. The first 20 ports belong to Port Group 1, and the back 20 ports belong to Port Group 2.

❖ Egress queue

Port egress queues are classified into unicast queues and multicast queues (the number of queues depends on the product). Logically the switching chip is divided into the ingress (incoming direction) and egress (outgoing direction). The egress queue is in the egress direction. Before packets go out of the egress, the enqueue operation needs to be performed for them at the egress queue. Some of our products implement buffer management based on the egress queue.\

Figure 3-2



Currently there are three types of egress queue models:

- There are 8 unicast queues and 8 multicast queues at the egress. The well-known unicast packets follow the unicast queue, and all the other packets follow the multicast queue.
- There are 8 unicast queues and 4 multicast queues at the egress. The well-known unicast packets follow the unicast queue, and all the other packets follow the multicast queue.
- There are only 8 queues at the egress, without differentiating unicast and multicast.

Overview

| Feature | Description |
|-----------------------------------|---|
| Buffer Adjustment | The buffer is adjusted based on the queue. It is the foundation of MMU. |
| Buffer Monitoring | Buffer monitoring actually means monitoring on the use of the buffer capacity, which facilitates buffer adjustment. |
| Queue Counting | The received and sent packets of each queue are counted so that the buffer adjustment result can be displayed easily. |

3.3.1 Configuring Buffer Adjustment

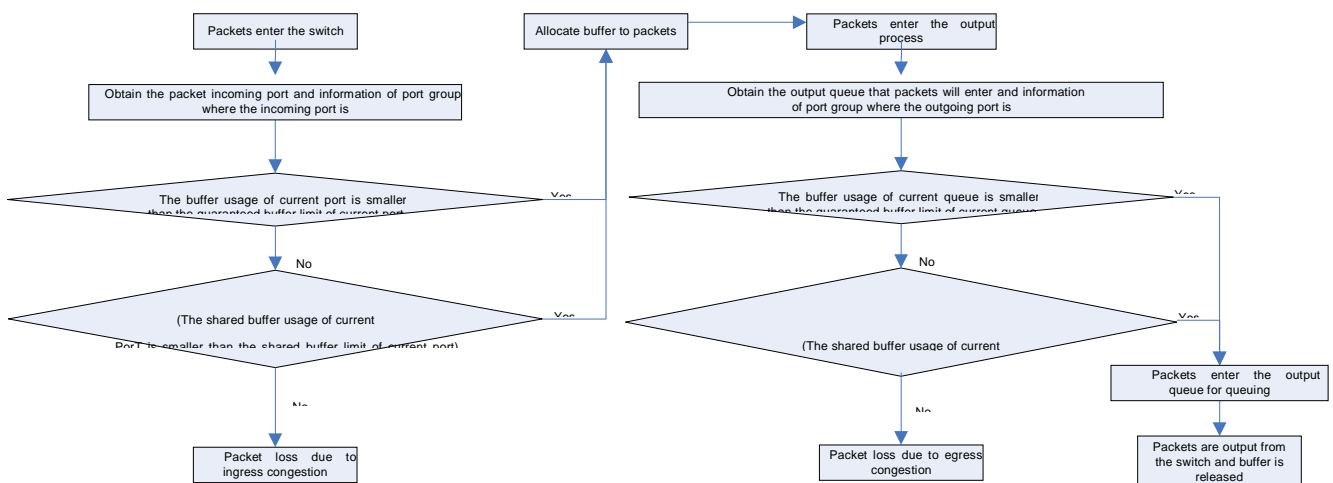
Buffer adjustment means that the queue of each service has different buffer sizes through some adjustment of the queue buffer so that each service is treated differently and services at different priorities are served differently.

Working Principle

❖ Working mechanism of caching in hardware

In terms of hardware, the buffer is managed in the input direction and output direction. The processing mechanism is shown below:

Figure 3-3



During buffer management, the input direction is adjusted to the maximum value to prevent packet loss in the input direction and make packet loss take place in the output direction. Therefore, adjustment is not opened for the buffer in the input direction, and CLI provides buffer adjustment in the output direction only, including the queue guaranteed buffer and queue shared buffer. Buffer adjustment configures the guaranteed buffer threshold and shared buffer threshold of queues to allocate different buffer sizes to queues.

❖ Guaranteed buffer

Guaranteed buffer is also called exclusive buffer. This part of buffer is distributed based on each queue. The guaranteed buffer of a queue can be used by this queue only. A fixed guaranteed buffer is allocated to each queue by default. This part of queue enables this queue to forward packets at the normal line rate under the stable flow.

❖ **Shared buffer**

In the total buffer of port group, the remaining part is the total shared buffer after the guaranteed buffer of each queue is deducted. The shared buffer can be used by all the queues. A shared queue threshold can be set for each queue. This threshold restricts the maximum shared buffer quantity that can be used by this queue. When the shared buffer sum configured for each queue in the port group exceeds the total shared queue of port group, the "First Come First Served" buffer occupancy mechanism is adopted.

3.3.2 Configuring Buffer Monitoring

Buffer monitoring implements monitoring on the use amount of each queue and shared buffer, with a view to providing data support for network optimization and reasonable buffer configuration.

Working Principle

Buffer monitoring adopts the polling mode to read the buffer use amount of each queue and the use situation of total buffer regularly and display the buffer use situation of current equipment in real time.

❖ **Queue buffer utilization alarm threshold**

When the buffer utilization of queue exceeds this threshold, syslog will be printed to remind the user.

3.3.3 Configuring Queue Counting

Queue counting monitors the forwarding and packet loss data of each queue, and push the alarm when packet loses, so as to provide data support for network optimization and reasonable buffer configuration.

Working Principle

The queue adopts the polling mode to read the number of forwarded packets/number of bytes and the number of lost packets/number of bytes of each queue regularly, and then use the data to calculate each kind of statistics of the queue.

3.4 Configuration

| Configuration | Description and Command |
|---------------|-------------------------|
|---------------|-------------------------|

| | | |
|-----------------------------------|--|--|
| Buffer Adjustment | (Optional) It is used to configure buffer. | |
| | mmu queue-guarantee | Configures guaranteed buffer |
| | mmu queue-threshold | Configures shared buffer |
| | mmu buffer-mode | Configures buffer mode |
| | mmu fc-threshold | Configure flow control threshold based on inbound port |
| Buffer Monitoring | (Optional) It is used to configure buffer. | |
| | mmu usage-warn-limit | Configures the buffer utilization alarm threshold |

3.4.1 Configuring Buffer Adjustment

Configuration Effect

- Configure guaranteed buffer so that the queue can share this part of buffer exclusively.
- Configure shared buffer so as to control the shared buffer use amount of the queue.

Notes

- Configuration on the interface can be made on the physical port only.

Configuration Steps

❖ Configuring guaranteed buffer

- Optional.
- In the interface mode, use the **mmu queue-guarantee** command to configure guaranteed buffer for each queue and ensure that the buffer configuration range varies with the product.
- Use the **no** or **default** command of this command to restore the default value of buffer.

| | |
|---------|---|
| Command | <code>mmu queue-guarantee output { unicast } [queue-id1 [queue-id2 [queue-idN]] set value</code> |
|---------|---|

| | |
|------------------------------|---|
| Parameter Description | output: performs buffer management on the egress queue unicast: performs buffer management on the egress unicast queue <i>queue-id:</i> queue ID, in the range from 1 to 8 <i>value:</i> number of guaranteed buffers, in cells; the range depends on the product. |
| Defaults | A fixed number of guaranteed buffers are allocated to each queue by default. The specific configuration depends on the product. |
| Command Mode | Interface mode |
| Usage Guide | The effective way of this command varies with the equipment and depends on the product. |

❖ Configuring buffer mode

- Optional.
- Under the global configuration mode, use the **mmu buffer-mode** command to configure the buffer mode.

| | |
|------------------------------|---|
| Command | mmu buffer-mode { normal burst-enhance qos-enhance flowctrl-enhance } |
| Parameter Description | normal: normal buffer mode burst-enhance: Burst enhanced buffer mode qos-enhance: QoS enhanced buffer support mode flowctrl-enhance: flow control enhanced buffer support mode |
| Defaults | Normal buffer mode is applied by default. |
| Command Mode | Global configuration mode |
| Usage Guide | The effective way of this command varies with the equipment and depends on the product. |

❖ Configuring shared buffer

- Optional.
- Use the **no** or **default** command of this command to restore the default value of buffer.

| | |
|------------------------------|---|
| Command | mmu queue-threshold output { unicast } [<i>queue-id1</i> [<i>queue-id2</i> [<i>queue-idN</i>]] set <i>thr%</i> |
| Parameter Description | output: performs buffer management on the egress queue unicast: performs buffer management on the egress unicastqueue <i>queue-id:</i> queue ID, in the range from 1 to 8 <i>thr%:</i> percentage, in the range from 1 to 100 |
| Defaults | A shared buffer use threshold is allocated to each queue by default. This threshold is a percentage. The calculation method of the maximum available shared buffer for the queue is as follows: Maximum available shared buffer for the queue = Total number of shared buffers of the port group * Threshold percentage |
| | The default value depends on the product. |
| Command Mode | Interface configuration mode |
| Usage Guide | The effective way of this command varies with the equipment and depends on the product. |

❖ Configuring flow control threshold

- Optional.
- Use the **no** or **default** form of the command to restore the default value of buffer.

| | |
|------------------------------|---|
| Command | mmu fc-threshold set <i>thr%</i> |
| Parameter Description | <i>value:</i> flow control threshold in the unit of percentage, range: 1-100 |
| Defaults | Vary with products |
| Command Mode | Interface configuration mode |
| Usage Guide | <ol style="list-style-type: none"> 1. The effective way of this command varies with the product. 2. The configuration takes effect only when flow control/PFC is enabled. 3. If flow control/PFC is not enabled, the shared buffer threshold of the PG is according to the value of ingress-threshold. 4. The user-configured value is displayed when the show running- |

config command is executed, even if the user-configured value is the default value.

Verification

- Use the **show running** command to check whether the MMU under the corresponding interface is configured successfully.

3.4.2 Configuring Buffer Monitoring

Configuration Effect

- Configure the buffer utilization alarm threshold of queue. The log alarm will be printed when the buffer utilization of queue exceeds this configured value.

Notes

- Configuration on the interface can be made on the physical port only.

Configuration Steps

❖ Configuring the queue buffer utilization alarm threshold

- Optional.
- In the interface configuration mode, use the **mmu usage-warn-limit { unicast | multicast } [queue-id1 [queue-id2 [queue-idN]] set value** command to configure the buffer utilization alarm threshold for each queue.
- Use the **no** or **default** command of this command to restore the default value of buffer.

| | |
|-----------------------|---|
| Command | mmu usage-warn-limit { unicast } [queue-id1 [queue-id2 [queue-idN]] set value |
| Parameter Description | unicast: performs buffer management on the egress unicast queue <i>queue-id:</i> queue ID, in the range from 1 to 8 <i>value:</i> percentage, in the range from 1 to 100 |
| Defaults | The default value is 0, indicating that no alarm is reported. |
| Command Mode | Interface configuration mode |
| Usage Guide | |

Verification

- Use the **show running** command to check whether the MMU under the corresponding interface is configured successfully.
- Use the **show queue-buffer** command to check whether the configuration succeeds.

Configuration Examples

❖ Configuring the buffer utilization alarm limit based on egress queue

| Configuration Steps | Configure the buffer utilization alarm threshold as 70% at the unicast queues 6 and 8 of port 1/1 on the switch. |
|---------------------|---|
| | <pre>QTECH# configure terminal QTECH(config)# int tel1/1 QTECH(config-if)#mmu usage-warn-limit unicast 6 8 set 70</pre> |
| Verification | Check whether the created guaranteed buffer has been configured successfully. |
| | <pre>QTECH#show queue-buffer interface gigabitEthernet 0/9 Dev/slot Port-group Total-shared(%) Guarantee-used(%) Share-used(%) Available(%) Warn-limit(%) 1/- 1 74.5271 0.0822 14.7615 85.1562 NA Interface GigabitEthernet 0/9: Type Queue Admin-shared(%) Total-used(%) Available(%) Warn-limit(%) Peak-usage(%) Peak-time Unicast 1 (default) 7.4836 0.0103 NA 7.5041 2015/7/14 20:7:14 Unicast 2 (default) 0.0000 7.4938 NA 0.0000 NA Unicast 3 (default) 0.0000 7.4938 NA 0.0000 NA Unicast 4 (default) 0.0000 7.4938 NA 0.0000 NA Unicast 5 (default) 0.0000 7.4938 NA 0.0000 NA Unicast 6 (default) 0.0000 7.4938 70% 0.0000 NA Unicast 7 (default) 0.0000 7.4938 NA 0.0000 NA Unicast 8 (default) 0.0000 7.4938 70% 0.0000 NA</pre> |

3.5 Monitoring

Clearing

Running the **clear** command during operation of the equipment may lead to service interruption due to loss of important information.

| Description | Command |
|------------------------------------|--------------------------------------|
| Clears the queue counter value. | clear queue-counter |
| Clears the historical buffer peak. | clear mmu queue-buffer peaked |

Displaying

| Description | Command |
|--|-------------------------------------|
| Displays the buffer use information of panel interface. | show queue-buffer interface |
| Displays the queue counter information of panel interface. | show queue-counter interface |