H3C S6520X-HI[EI][SI] & S6520-SI & S5560X-HI & S5000-EI & MS4600 Switch Series

ACL and QoS Command Reference

This command reference is applicable to the following switches and software versions:
H3C S6520X-HI switch series (Release 6308 and later)
H3C S6520X-EI switch series (Release 6308 and later)
H3C S6520X-SI switch series (Release 6308 and later)
H3C S6520-SI switch series (Release 6308 and later)
H3C S5560X-HI switch series (Release 6308 and later)
H3C S5000-EI switch series (Release 6308 and later)
H3C MS4600 switch series (Release 6308 and later)

New H3C Technologies Co., Ltd.
http://www.h3c.com

Software version: Release 63xx
Document version: 6W101-20201015

Preface

This command reference describes the configuration commands for ACL and QoS features, including ACL, QoS, data buffer, and time range.

This preface includes the following topics about the documentation:

- Audience.
- Conventions.
- Documentation feedback.

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Documentation feedback

You can e-mail your comments about product documentation to info@h3c.com.

We appreciate your comments.

Contents

ACL commands

acl

Use **acl** to create an ACL and enter its view, or enter the view of an existing ACL.

Use **undo acl** to delete the specified or all ACLs.

Syntax

Command set 1:

acl [**ipv6**] **number** *acl-number* [**name** *acl-name*] [**match-order** { **auto** | **config** }]

undo acl [**ipv6**] **number** *acl-number*

Command set 2:

acl [**ipv6**] { **advanced** | **basic** } { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]

acl mac { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]

undo acl [**ipv6**] { **all** | { **advanced** | **basic** } { *acl-number* | **name** *acl-name* } }

undo acl mac { **all** | *acl-number* | **name** *acl-name* }

Default

No ACLs exist.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6: Specifies the IPv6 ACL type. To specify the IPv4 ACL type, do not use this keyword.

basic: Specifies the basic ACL type.

advanced: Specifies the advanced ACL type.

mac: Specifies the Layer 2 ACL type.

number *acl-number*: Assigns a number to the ACL.

acl-number: Assigns a number to the ACL. The following are available value ranges:

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *acl-name*: Assigns a name to the ACL. The *acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter and to avoid confusion, it cannot be **all**.

match-order: Specifies the order in which ACL rules are compared against packets.

- **auto**: Compares ACL rules in depth-first order.

- **config**: Compares ACL rules in ascending order of rule ID. The rule with a smaller ID has a higher priority. If you do not specify a match order, the **config** order applies by default.

all: Specifies all ACLs of the specified type.

Usage guidelines

If you create a numbered ACL, you can enter the view of the ACL by using either of the following commands:

- The **acl** [**ipv6**] **number** *acl-number* command.
- The **acl** { [**ipv6**] { **advanced** | **basic** } | **mac** } *acl-number* command.

If you create a ACL by using the **acl** [**ipv6**] **number** *acl-number* **name** *acl-name* command, you can enter the view of the ACL by using either of the following commands:

- **acl** [**ipv6**] **name** *acl-name* (for only basic ACLs and advanced ACLs).
- **acl** [**ipv6**] **number** *acl-number* [**name** *acl-name*].
- **acl** { [**ipv6**] { **advanced** | **basic** } | **mac**] } **name** *acl-name*.

If you create a named ACL by using the **acl** { [**ipv6**] { **advanced** | **basic** } | **mac** } **name** *acl-name* command, you can enter the view of the ACL by using only the command that is used to create the ACL.

You can change the match order only for ACLs that do not contain any rules.

Matching packets are forwarded through slow forwarding if an ACL rule contains match criteria or has functions enabled in addition to the following match criteria and functions:

- Source and destination IP addresses.
- Source and destination ports.
- Transport layer protocol.
- ICMP or ICMPv6 message type, message code, and message name.
- Logging.
- Time range.

Slow forwarding requires packets to be sent to the control plane for forwarding entry calculation, which affects the device forwarding performance.

Examples

Create IPv4 basic ACL 2000 and enter its view.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000]
```

Create IPv4 basic ACL **flow** and enter its view.

```
<Sysname> system-view
[Sysname] acl basic name flow
[Sysname-acl-ipv4-basic-flow]
```

Create IPv4 advanced ACL 3000 and enter its view.

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000]
```

Create IPv6 basic ACL 2000 and enter its view.

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2000
[Sysname-acl-ipv6-basic-2000]
```

Create IPv6 basic ACL **flow** and enter its view.

```
<Sysname> system-view
[Sysname] acl ipv6 basic name flow
[Sysname-acl-ipv6-basic-flow]
```

Create IPv6 advanced ACL **abc** and enter its view.

```
<Sysname> system-view
[Sysname] acl ipv6 advanced name abc
[Sysname-acl-ipv6-adv-abc]
```

Create Layer 2 ACL 4000 and enter its view.

```
<Sysname> system-view
[Sysname] acl mac 4000
[Sysname-acl-mac-4000]
```

Create Layer 2 ACL **flow** and enter its view.

```
<Sysname> system-view
[Sysname] acl mac name flow
[Sysname-acl-mac-flow]
```

Related commands

display acl

acl copy

Use **acl copy** to create an ACL by copying an ACL that already exists.

Syntax

acl [**ipv6** | **mac**] **copy** { *source-acl-number* | **name** *source-acl-name* } **to** { *dest-acl-number* | **name** *dest-acl-name* }

Views

System view

Predefined user roles

network-admin

Parameters

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

source-acl-number: Specifies an existing source ACL by its number. The following are available value ranges:

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *source-acl-name*: Specifies an existing source ACL by its name. The *source-acl-name* argument is a case-insensitive string of 1 to 63 characters.

dest-acl-number: Assigns a unique number to the new ACL. The following are available value ranges:

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.

- 4000 to 4999 for Layer 2 ACLs.

name *dest-acl-name*: Assigns a unique name to the new ACL. The *dest-acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter and to avoid confusion, it cannot be **all**.

Usage guidelines

The new ACL and the source ACL must be the same type.

When specifying an ACL by its number, follow these rules:

- To specify an IPv6 ACL, you must specify both its ACL number and the **ipv6** keyword.
- To specify a Layer 2 ACL, you can specify its ACL number without the **mac** keyword.

To specify an IPv6 ACL or Layer 2 ACL by a name, you must specify both the ACL name and the **ipv6** or **mac** keyword.

The new ACL has the same properties and content as the source ACL, but uses a different number or name from the source ACL.

Examples

Create IPv4 basic ACL 2002 by copying IPv4 basic ACL 2001.

```
<Sysname> system-view
[Sysname] acl copy 2001 to 2002
```

Create IPv4 basic ACL **paste** by copying IPv4 basic ACL **test**.

```
<Sysname> system-view
[Sysname] acl copy name test to name paste
```

acl logging interval

Use **acl logging interval** to enable logging for packet filtering and set the interval.

Use **undo acl logging interval** to restore the default.

Syntax

acl logging interval *interval*

undo acl logging interval

Default

The interval is 0. The device does not generate log entries for packet filtering.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the interval at which log entries are generated and output. It must be a multiple of 5, in the range of 0 to 1440 minutes. To disable the logging, set the value to 0.

Usage guidelines

The logging feature is available for IPv4 or IPv6 ACL rules that have the **logging** keyword.

You can configure the ACL module to generate log entries for packet filtering and output them to the information center at the output interval. When the first packet of a flow matches an ACL rule, the output interval starts. At the end of the interval, the device outputs a log entry to record the number of

matching packets and the matched ACL rule during the interval. For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Configure the device to generate and output packet filtering log entries every 10 minutes.

```
<Sysname> system-view
[Sysname] acl logging interval 10
```

Related commands

rule (IPv4 advanced ACL view)

rule (IPv4 basic ACL view)

rule (IPv6 advanced ACL view)

rule (IPv6 basic ACL view)

acl trap interval

Use **acl trap interval** to enable SNMP notifications for packet filtering and set the interval.

Use **undo acl interval** to restore the default.

Syntax

acl trap interval *interval*

undo acl trap interval

Default

The interval is 0. The device does not generate SNMP notifications for packet filtering.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the interval at which SNMP notifications are generated and output. It must be a multiple of 5, in the range of 0 to 1440 minutes. To disable SNMP notifications, set the value to 0.

Usage guidelines

The SNMP notifications feature is available for IPv4 or IPv6 ACL rules that have the **logging** keyword.

You can configure the ACL module to generate SNMP notifications for packet filtering and output them to the SNMP module at the output interval. When the first packet of a flow matches an ACL rule, the output interval starts. At the end of the interval, the device outputs an SNMP notification to record the number of matching packets and the matched ACL rule during the interval.For more information about SNMP, see *Network Management and Monitoring Configuration Guide*.

Examples

Configure the device to generate and output packet filtering SNMP notifications every 10 minutes.

```
<Sysname> system-view
[Sysname] acl trap interval 10
```

Related commands

rule (IPv4 advanced ACL view)

rule (IPv4 basic ACL view)

rule (IPv6 advanced ACL view)

rule (IPv6 basic ACL view)

description

Use **description** to configure a description for an ACL.

Use **undo description** to delete an ACL description.

Syntax

description *text*

undo description

Default

An ACL does not have a description.

Views

IPv4 basic/advanced ACL view

IPv6 basic/advanced ACL view

Layer 2 ACL view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 127 characters.

Examples

Configure a description for IPv4 basic ACL 2000.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] description This is an IPv4 basic ACL.
```

Related commands

display acl

display acl

Use **display acl** to display ACL configuration and match statistics.

Syntax

display acl [**ipv6** | **mac**] { *acl-number* | **all** | **name** *acl-name* }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number. The following are available value ranges:

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

all: Specifies all ACLs of the specified type.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

Usage guidelines

This command displays ACL rules in **config** or **auto** order, whichever is configured.

To specify the IPv4 ACL type, do not specify the **ipv6** or **mac** keyword.

Examples

Display configuration and match statistics for IPv4 basic ACL 2001.

```
<Sysname> display acl 2001
Basic IPv4 ACL 2001, 1 rule, match-order is auto,
This is an IPv4 basic ACL.
ACL's step is 5, start ID is 0
 rule 5 permit source 1.1.1.1 0
 rule 5 comment This rule is used on Ten-GigabitEthernet1/0/1.
```

Table 1 Command output

Field	Description
Basic IPv4 ACL 2001	Type and number of the ACL. The following field information is about IPv4 basic ACL 2001.
1 rule	The ACL contains one rule.
match-order is auto	The match order for the ACL is **auto**, which sorts ACL rules in depth-first order. This field is not displayed when the match order is **config**.
This is an IPv4 basic ACL.	Description of the ACL.
ACL's step is 5	The rule numbering step is 5.
start ID is 0	The start rule ID is 0.
rule 5 permit source 1.1.1.1 0	Content of rule 5. The rule permits packets sourced from the IP address 1.1.1.1.
rule 5 comment This rule is used on Ten-GigabitEthernet1/0/1.	Comment of rule 5.

display packet-filter

Use **display packet-filter** to display ACL application information for packet filtering.

Syntax

display packet-filter interface [*interface-type interface-number*] [**inbound** | **outbound**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface [*interface-type interface-number*]: Specifies an interface by its type and number. If you do not specify an interface, this command displays ACL application information for packet filtering on all interfaces. If you specify an Ethernet interface, you do not need to specify the **slot** *slot-number* option.

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays ACL application information for packet filtering for the master device.

Usage guidelines

If neither the **inbound** keyword nor the **outbound** keyword is specified, this command displays ACL application information for packet filtering in both directions.

Examples

Display ACL application information for inbound packet filtering on interface Ten-GigabitEthernet 1/0/1.

```
<Sysname> display packet-filter interface ten-gigabitethernet 1/0/1 inbound
Interface: Ten-GigabitEthernet1/0/1
 Inbound policy:
  IPv4 ACL 2001r
  IPv6 ACL 2002 (Failed)
  MAC ACL 4003
```

Table 2 Command output

Field	Description
Interface	Interface to which the ACL applies.
Inbound policy	ACL used for filtering incoming traffic.
Outbound policy	ACL used for filtering outgoing traffic.
IPv4 ACL 2001	IPv4 basic ACL 2001 has been successfully applied.
IPv6 ACL 2002 (Failed)	The device has failed to apply IPv6 basic ACL 2002.
Hardware-count	ACL rule match counting in hardware has been successfully enabled.
Hardware-count (Failed)	The device has failed to enable counting ACL rule matches in hardware.
IPv4 default action	Packet filter default action for packets that do not match any IPv4 ACLs:

Field	Description
	• **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.
IPv6 default action	Packet filter default action for packets that do not match any IPv6 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.
MAC default action	Packet filter default action for packets that do not match any Layer 2 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.

display packet-filter statistics

Use **display packet-filter statistics** to display packet filtering statistics.

Syntax

display packet-filter statistics interface *interface-type interface-number* { **inbound** | **outbound** } [[**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }] [**brief**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number. The following are available value ranges:

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

brief: Displays brief statistics.

Usage guidelines

If *acl-number*, **name** *acl-name*, **ipv6**, or **mac** is not specified, this command displays packet filtering statistics for all ACLs.

To specify the IPv4 ACL type, do not specify the **ipv6** or **mac** keyword.

Examples

Display packet filtering statistics for all ACLs on incoming packets of Ten-GigabitEthernet 1/0/1.

```
<Sysname> display packet-filter statistics interface ten-gigabitethernet 1/0/1 inbound
Interface: Ten-GigabitEthernet1/0/1
 Inbound policy:
  IPv4 ACL 2001, Hardware-count
   From 2011-06-04 10:25:21 to 2011-06-04 10:35:57
   rule 0 permit source 2.2.2.2 0 (2 packets)
   rule 5 permit source 1.1.1.1 0 (Failed)
   Totally 2 packets permitted, 0 packets denied
   Totally 100% permitted, 0% denied

  IPv6 ACL 2000

  MAC ACL 4000
   rule 0 permit
```

Table 3 Command output

Field	Description
Interface	Interface to which the ACL applies.
Inbound policy	ACL used for filtering incoming traffic.
Outbound policy	ACL used for filtering outgoing traffic.
IPv4 ACL 2001	IPv4 basic ACL 2001 has been successfully applied.
IPv4 ACL 2002 (Failed)	The device has failed to apply IPv4 basic ACL 2002.
Hardware-count	ACL rule match counting in hardware has been successfully enabled.
Hardware-count (Failed)	The device has failed to enable counting ACL rule matches in hardware.
From 2011-06-04 10:25:21 to 2011-06-04 10:35:57	Start time and end time of the statistics. The start time is the time when the packet filter was deployed to the member device.
2 packets	Two packets matched the rule. This field is not displayed when no packets matched the rule.
No resource	Resources are not enough for counting matches for the rule. In packet filtering statistics, this field is displayed for a rule when resources are not sufficient for rule match counting.

Field	Description
rule 5 permit source 1.1.1.1 0 (Failed)	The device has failed to apply rule 5.
Totally 2 packets permitted, 0 packets denied	Number of packets permitted and denied by the ACL.
Totally 100% permitted, 0% denied	Ratios of permitted and denied packets to all packets.
IPv4 default action	Packet filter default action for packets that do not match any IPv4 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.
IPv6 default action	Packet filter default action for packets that do not match any IPv6 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.
MAC default action	Packet filter default action for packets that do not match any Layer 2 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.

Related commands

reset packet-filter statistics

display packet-filter statistics sum

Use **display packet-filter statistics sum** to display accumulated packet filtering statistics for an ACL.

Syntax

display packet-filter statistics sum { **inbound** | **outbound** } [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* } [**brief**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number.

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

brief: Displays brief statistics.

Usage guidelines

To specify the IPv4 ACL type, do not specify the **ipv6** or **mac** keyword.

Examples

Display accumulated packet filtering statistics for IPv4 basic ACL 2001 on incoming packets.

```
<Sysname> display packet-filter statistics sum inbound 2001
Sum:
 Inbound policy:
  IPv4 ACL 2001
   rule 0 permit source 2.2.2.2 0 (2 packets)
   rule 5 permit source 1.1.1.1 0
   Totally 2 packets permitted, 0 packets denied
   Totally 100% permitted, 0% denied
```

Display brief accumulated packet filtering statistics for IPv4 basic ACL 2000 on incoming packets.

```
<Sysname> display packet-filter statistics sum inbound 2000 brief
Sum:
 Inbound policy:
  IPv4 ACL 2000
   Totally 2 packets permitted, 0 packets denied
   Totally 100% permitted, 0% denied
```

Table 4 Command output

Field	Description
Sum	Accumulated packet filtering statistics.
Inbound policy	Accumulated packet filtering statistics in the inbound direction.
Outbound policy	Accumulated packet filtering statistics in the outbound direction.
IPv4 ACL 2001	Accumulated packet filtering statistics of IPv4 basic ACL 2001.
2 packets	Two packets matched the rule. This field is not displayed when no packets matched the rule.
Totally 2 packets permitted, 0 packets denied	Number of packets permitted and denied by the ACL.

Field	Description
Totally 100% permitted, 0% denied	Ratios of permitted and denied packets to all packets.

Related commands

reset packet-filter statistics

display packet-filter verbose

Use **display packet-filter verbose** to display ACL application details for packet filtering.

Syntax

display packet-filter verbose interface *interface-type interface-number* { **inbound** | **outbound** } [[**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. The **slot** *slot-number* option is not available for an Ethernet interface.

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number.

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays ACL application details for packet filtering for the master device.

Usage guidelines

If *acl-number*, **name** *acl-name*, **ipv6**, or **mac** is not specified, this command displays application details of all ACLs for packet filtering.

To specify the IPv4 ACL type, do not specify the **ipv6** or **mac** keyword.

Examples

Display application details of all ACLs for inbound packet filtering on Ten-GigabitEthernet 1/0/1.

```
<Sysname> display packet-filter verbose interface ten-gigabitethernet 1/0/1 inbound
Interface: Ten-GigabitEthernet1/0/1
```

```
 Inbound policy:
  IPv4 ACL 2001
   rule 0 permit
   rule 5 permit source 1.1.1.1 0 (Failed)

  IPv6 ACL 2000
   rule 0 permit

  MAC ACL 4000

  IPv4 default action: Deny

  MAC default action: Deny
```

Display application details of all ACLs for inbound packet filtering on all physical interfaces.

```
<Sysname> display packet-filter verbose global inbound
Global:
 Inbound policy:
  IPv4 ACL 2001
   rule 0 permit
   rule 5 permit source 1.1.1.1 0 (Failed)
   rule 10 permit vpn-instance test (Failed)

  IPv4 ACL 2002 (Failed)

  IPv6 ACL 2000, Hardware-count

  MAC ACL 4000, Hardware-count
   rule 0 permit

  IPv4 default action: Deny

  IPv6 default action: Deny

  MAC default action: Deny
```

Table 5 Command output

Field	Description
Interface	Interface to which the ACL applies.
Inbound policy	ACL used for filtering incoming traffic.
Outbound policy	ACL used for filtering outgoing traffic.
IPv4 ACL 2001	IPv4 basic ACL 2001 has been successfully applied.
IPv4 ACL 2002 (Failed)	The device has failed to apply IPv4 basic ACL 2002.
Hardware-count	ACL rule match counting in hardware has been successfully enabled.
Hardware-count (Failed)	The device has failed to enable counting ACL rule matches in hardware.

Field	Description
rule 5 permit source 1.1.1.1 0 (Failed)	The device has failed to apply rule 5.
IPv4 default action	Packet filter default action for packets that do not match any IPv4 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.
IPv6 default action	Packet filter default action for packets that do not match any IPv6 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.
MAC default action	Packet filter default action for packets that do not match any Layer 2 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.

display qos-acl resource

Use **display qos-acl resource** to display QoS and ACL resource usage.

Syntax

display qos-acl resource [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays QoS and ACL resource usage for all member devices.

Usage guidelines

This command does not display any usage data if the specified device does not support counting QoS and ACL resources.

The total number of QoS and ACL resources varies by operating mode. You can use the **switch-mode** command to set the operating mode and the **display qos-acl resource**

command to display the total number of QoS and ACL resources. For more information about the **switch-mode** command, see device management commands in *Fundamentals Command Reference*.

Examples

Display QoS and ACL resource usage.

```
<Sysname> display qos-acl resource
Interfaces: XGE1/0/1 to XGE1/0/48, HGE1/0/49
            HGE1/0/50 (slot 1)
-------------------------------------------------------------------------
 Type             Total      Reserved   Configured Remaining  Usage
-------------------------------------------------------------------------
 TTI ACL          3072       0          2          3070       0%
 IPCL0 ACL        768        9          0          759        1%
 IPCL1 ACL        256        0          0          256        0%
 IPCL2 ACL        256        30         0          226        11%
 IPCL Counter     4096       35         0          4061       0%
 EPCL ACL         256        0          0          256        0%
 EPCL Counter     1024       0          0          1024       0%
 IPCL Meter       4888       0          0          4888       0%
 EPCL Meter       4096       0          0          4096       0%
```

Table 6 Command output

Field	Description
Interfaces	Interface range for the resources.
Type	Resource type: • **TTI ACL**—ACL resources used for tunnel termination and interfaces. • **IPCL ACL**—ACL resources used for inbound policies. • **IPCL Counter**—Accounting resources used for inbound policies. • **EPCL ACL**—ACL resources used for outbound policies. • **EPCL Counter**—Accounting resources used for outbound policies. • **IPCL Meter**—Traffic policing resources used in inbound QoS policies. • **EPCL Meter**—Traffic policing resources used in outbound QoS policies.
Total	Total number of resources.
Reserved	Number of reserved resources.
Configured	Number of resources that has been applied.
Remaining	Number of resources that you can apply.
Usage	Configured and reserved resources as a percentage of total resources. If the percentage is not an integer, this field displays the integer part. For example, if the actual usage is 50.8%, this field displays 50%.

packet-filter

Use **packet-filter** to apply an ACL to an interface to filter packets.

Use **undo packet-filter** to remove an ACL from an interface.

Syntax

packet-filter [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** } [**hardware-count**]

undo packet-filter [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** }

Default

No ACL is applied to an interface to filter packets.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

VLAN interface view

VSI interface view

Predefined user roles

network-admin

Parameters

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number.

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

inbound: Filters incoming packets.

outbound: Filters outgoing packets.

hardware-count: Enables counting ACL rule matches performed in hardware. If you do not specify this keyword, rule matches for the ACL are not counted in hardware.

Usage guidelines

If you use the *acl-number* argument to specify an ACL, follow these guidelines:

- To specify an IPv4 ACL, use the *acl-number* argument directly.
- To specify an IPv6 ACL, specify the **ipv6** keyword, and then the *acl-number* argument.
- To specify a Layer 2 ACL, the **mac** keyword is not a must. You can either specify the **mac** keyword and then the *acl-number* argument or specify only the *acl-number* argument.

If you use the **name** *acl-name* option to specify an ACL, follow these guidelines:

- To specify an IPv4 ACL, use the **name** *acl-name* option.
- To specify an IPv6 or Layer 2 ACL, specify the related keyword and then the **name** *acl-name* option.

The **hardware-count** keyword in this command enables match counting in hardware for all rules in an ACL, and the **counting** keyword in the **rule** command enables match counting specific to rules.

To disable ACL rule match counting in hardware when resources are insufficient, you must execute the **undo packet-filter** command and then reconfigure the **packet-filter** command without specifying the **hardware-count** keyword.

To disable ACL rule match counting in hardware when resources are sufficient, you can directly reconfigure the **packet-filter** command without specifying the **hardware-count** keyword.

To the same direction of an interface, you can apply a maximum of three ACLs: one IPv4 ACL, one IPv6 ACL, and one Layer 2 ACL.

The packet filtering configured on a VLAN interface filters only packets forwarded at Layer 3.

Examples

Apply IPv4 basic ACL 2001 to filter incoming traffic on Ten-GigabitEthernet 1/0/1, and enable counting ACL rule matches performed in hardware.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] packet-filter 2001 inbound hardware-count
```

Related commands

display packet-filter

display packet-filter statistics

display packet-filter verbose

packet-filter default deny

Use **packet-filter default deny** to set the packet filtering default action to **deny**. The packet filter denies packets that do not match any ACL rule.

Use **undo packet-filter default deny** to restore the default.

Syntax

packet-filter default deny

undo packet-filter default deny

Default

The packet filtering default action is **permit**. The packet filter permits packets that do not match any ACL rule.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The packet filter applies the default action to all ACL applications for packet filtering. The default action appears in the **display** command output for packet filtering.

Examples

Set the packet filter default action to **deny**.

```
<Sysname> system-view
[Sysname] packet-filter default deny
```

Related commands

display packet-filter

display packet-filter statistics

display packet-filter verbose

packet-filter filter

Use **packet-filter filter** to specify the applicable scope of packet filtering on a VLAN interface.

Use **undo packet-filter filter** to restore the default.

Syntax

packet-filter filter [**route** | **all**]

undo packet-filter filter

Default

The packet filtering filters all packets.

Views

VLAN interface view

Predefined user roles

network-admin

Parameters

route: Filters packets forwarded at Layer 3 by the VLAN interface.

all: Filters all packets, including packets forwarded at Layer 3 by the VLAN interface and packets forwarded at Layer 2 by the physical ports associated with the VLAN interface.

Examples

Configure the packet filtering on VLAN-interface 2 to filter packets forwarded at Layer 3.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] packet-filter filter route
```

reset acl counter

Use **reset acl counter** to clear statistics for ACLs.

Syntax

reset acl [**ipv6** | **mac**] **counter** { *acl-number* | **all** | **name** *acl-name* }

Views

User view

Predefined user roles

network-admin

Parameters

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number.

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

all: Clears statistics for all ACLs of the specified type.

name *acl-name*: Clears statistics of an ACL specified by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

Usage guidelines

When specifying an ACL by its number, follow these rules:

- To specify an IPv6 ACL, you must specify both its ACL number and the **ipv6** keyword.
- To specify a Layer 2 ACL, you can specify its ACL number without the **mac** keyword.

To specify an IPv6 ACL or Layer 2 ACL by a name, you must specify both the ACL name and the **ipv6** or **mac** keyword.

Examples

Clear statistics for IPv4 basic ACL 2001.

```
<Sysname> reset acl counter 2001
```

Related commands

display acl

reset packet-filter statistics

Use **reset packet-filter statistics** to clear the packet filtering statistics.

Syntax

reset packet-filter statistics interface [*interface-type interface-number*] { **inbound** | **outbound** } [[**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }]

Views

User view

Predefined user roles

network-admin

Parameters

interface [*interface-type interface-number*]: Specifies an interface by its type and number. If you do not specify an interface, this command clears packet filtering statistics for all interfaces.

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number.

- 2000 to 2999 for basic ACLs.

- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

Usage guidelines

If *acl-number*, **name** *acl-name*, **ipv6**, or **mac** is not specified, this command clears the packet filtering statistics for all ACLs.

To specify the IPv4 ACL type, do not specify the **ipv6** or **mac** keyword.

Examples

Clear IPv4 basic ACL 2001 statistics for inbound packet filtering on Ten-GigabitEthernet 1/0/1.

```
<Sysname> reset packet-filter statistics interface ten-gigabitethernet 1/0/1 inbound 2001
```

Related commands

display packet-filter statistics

display packet-filter statistics sum

rule (IPv4 advanced ACL view)

Use **rule** to create or edit an IPv4 advanced ACL rule.

Use **undo rule** to delete an entire IPv4 advanced ACL rule or some attributes in the rule.

Syntax

rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { *dest-address dest-wildcard* | **any** } | **destination-port** *operator port1* [*port2*] | { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* } * } | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **logging** | **source** { *source-address source-wildcard* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name*] *

undo rule *rule-id* [{ { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **established** } | **counting** | **destination** | **destination-port** | { **dscp** | { **precedence** | **tos** } * | **fragment** | **icmp-type** | **logging** | **source** | **source-port** | **time-range**] *

undo rule { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { *dest-address dest-wildcard* | **any** } | **destination-port** *operator port1* [*port2*] | { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* } * | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **logging** | **source** { *source-address source-wildcard* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name*] *

Default

No IPv4 advanced ACL rules exist.

Views

IPv4 advanced ACL view

Predefined user roles

network-admin

Parameters

rule-id: Specifies a rule ID in the range of 0 to 65534. If you do not specify a rule ID when creating an ACL rule, the system automatically assigns it a rule ID. This rule ID is the nearest higher multiple of the numbering step to the current highest rule ID, starting from the start rule ID. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the rule is numbered 30.

deny: Denies matching packets.

permit: Allows matching packets to pass.

protocol: Specifies a protocol carried over IPv4 by its number in the range of 0 to 255 or by its keyword, as shown in Table 7.

Table 7 Protocols carried over IPv4

Number	Keyword	Description
N/A	**ip**	Matches IPv4 packets.
1	**icmp**	Matches ICMP packets.
2	**igmp**	Matches IGMP packets.
4	**ipinip**	Matches IP-in-IP packets.
6	**tcp**	Matches TCP packets.
17	**udp**	Matches UDP packets.
47	**gre**	Matches GRE packets. For information about GRE, see *Layer 3—IP Services Configuration Guide*.
89	**ospf**	Matches OSPF packets.

Table 8 describes the parameters that you can specify, regardless of the value for the *protocol* argument.

Table 8 Match criteria and other rule information for IPv4 advanced ACL rules

Parameters	Function	Description
source { *source-address source-wildcard* | **any** }	Specifies a source address.	The *source-address source-wildcard* arguments specify a source IP address and a wildcard mask in dotted decimal notation. An all-zero wildcard represents a host address. The **any** keyword specifies any source IP address.
destination { *dest-address dest-wildcard* | **any** }	Specifies a destination address.	The *dest-address dest-wildcard* arguments specify a destination IP address and a wildcard mask in dotted decimal notation. An all-zero wildcard mask represents a host address. The **any** keyword represents any destination IP address.
counting	Enables rule match counting in software.	The **counting** keyword enables match counting specific to rules, and the **hardware-count** keyword in the **packet-filter** command enables match counting in hardware for all rules in

Parameters	Function	Description
		an ACL. If the **counting** keyword is not specified, matches for the rule are not counted in software.
precedence *precedence*	Specifies an IP precedence value.	The *precedence* argument can be a number in the range of 0 to 7, or in words: **routine** (0), **priority** (1), **immediate** (2), **flash** (3), **flash-override** (4), **critical** (5), **internet** (6), or **network** (7).
tos *tos*	Specifies a ToS preference.	The *tos* argument can be a number in the range of 0 to 15, or in words: **max-reliability** (2), **max-throughput** (4), **min-delay** (8), **min-monetary-cost** (1), or **normal** (0).
dscp *dscp*	Specifies a DSCP priority.	The *dscp* argument can be a number in the range of 0 to 63, or in words: **af11** (10), **af12** (12), **af13** (14), **af21** (18), **af22** (20), **af23** (22), **af31** (26), **af32** (28), **af33** (30), **af41** (34), **af42** (36), **af43** (38), **cs1** (8), **cs2** (16), **cs3** (24), **cs4** (32), **cs5** (40), **cs6** (48), **cs7** (56), **default** (0), or **ef** (46).
fragment	Applies the rule only to fragments.	If you do not specify this keyword, the rule applies to all fragments and non-fragments.
logging	Logs the number of matching packets.	This feature requires that the module (for example, packet filtering) that uses the ACL supports logging.
time-range *time-range-name*	Specifies a time range for the rule.	The *time-range-name* argument is a case-insensitive string of 1 to 32 characters. It must start with an English letter. If the time range is not configured, the system creates the rule. However, the rule using the time range can take effect only after you configure the time range. For more information about time range, see *ACL and QoS Configuration Guide*.

If the *protocol* argument is **tcp** (6) or **udp** (17), set the parameters shown in Table 9.

Table 9 TCP/UDP-specific parameters for IPv4 advanced ACL rules

Parameters	Function	Description
source-port *operator port1* [*port2*]	Specifies one or more UDP or TCP source ports.	The *operator* argument can be **lt** (lower than), **gt** (greater than), **eq** (equal to), or **range** (inclusive range). The *port1* and *port2* arguments are TCP or UDP port numbers in the range of 0 to 65535. The *port2* argument is needed only when the *operator* argument is **range**. TCP port numbers can be represented as: **chargen** (19), **bgp** (179), **cmd** (514), **daytime** (13), **discard** (9), **dns** (53), **domain** (53), **echo** (7), **exec** (512), **finger** (79), **ftp** (21), **ftp-data** (20), **gopher** (70), **hostname**
destination-port *operator port1* [*port2*]	Specifies one or more UDP or TCP destination ports.	

Parameters	Function	Description
		(101), **irc** (194), **klogin** (543), **kshell** (544), **login** (513), **lpd** (515), **nntp** (119), **pop2** (109), **pop3** (110), **smtp** (25), **sunrpc** (111), **tacacs** (49), **talk** (517), **telnet** (23), **time** (37), **uucp** (540), **whois** (43), and **www** (80). UDP port numbers can be represented as: **biff** (512), **bootpc** (68), **bootps** (67), **discard** (9), **dns** (53), **dnsix** (90), **echo** (7), **mobilip-ag** (434), **mobilip-mn** (435), **nameserver** (42), **netbios-dgm** (138), **netbios-ns** (137), **netbios-ssn** (139), **ntp** (123), **rip** (520), **snmp** (161), **snmptrap** (162), **sunrpc** (111), **syslog** (514), **tacacs-ds** (65), **talk** (517), **tftp** (69), **time** (37), **who** (513), and **xdmcp** (177).
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } *	Specifies one or more TCP flags including ACK, FIN, PSH, RST, SYN, and URG.	Parameters specific to TCP. The value for each argument can be 0 (flag bit not set) or 1 (flag bit set). The TCP flags in a rule are ANDed. For example, a rule configured with **ack** 0 **psh** 1 matches packets that have the ACK flag bit not set and the PSH flag bit set.
established	Specifies the flags for indicating the established status of a TCP connection.	Parameter specific to TCP. The rule matches TCP connection packets with the ACK or RST flag bit set.

If the *protocol* argument is **icmp** (1), set the parameters shown in Table 10.

Table 10 ICMP-specific parameters for IPv4 advanced ACL rules

Parameters	Function	Description
icmp-type { *icmp-type* *icmp-code* | *icmp-message* }	Specifies the ICMP message type and code.	The *icmp-type* argument is in the range of 0 to 255. The *icmp-code* argument is in the range of 0 to 255. The *icmp-message* argument specifies a message name. Supported ICMP message names and their corresponding type and code values are listed in Table 11.

Table 11 ICMP message names supported in IPv4 advanced ACL rules

ICMP message name	ICMP message type	ICMP message code
echo	8	0
echo-reply	0	0
fragmentneed-DFset	3	4
host-redirect	5	1
host-tos-redirect	5	3
host-unreachable	3	1
information-reply	16	0
information-request	15	0
net-redirect	5	0

ICMP message name	ICMP message type	ICMP message code
net-tos-redirect	5	2
net-unreachable	3	0
parameter-problem	12	0
port-unreachable	3	3
protocol-unreachable	3	2
reassembly-timeout	11	1
source-quench	4	0
source-route-failed	3	5
timestamp-reply	14	0
timestamp-request	13	0
ttl-exceeded	11	0

Usage guidelines

Within an ACL, the permit or deny statement of each rule must be unique. If the rule you are creating or editing has the same deny or permit statement as another rule in the ACL, the rule will not be created or changed.

You can edit ACL rules only when the match order is **config**.

If an IPv4 advanced ACL is used for QoS traffic classification or packet filtering in a VXLAN network, the ACL matches packets as follows:

- On a VTEP, the ACL can only match the incoming packets of Ethernet service instances.
- On an intermediate transport device, the ACL can match both incoming packets and outgoing packets.

To view the existing IPv4 basic and advanced ACL rules, use the **display acl all** command.

The **undo rule** *rule-id* command without any optional parameters deletes an entire rule. If you specify optional parameters, the **undo rule** *rule-id* command deletes the specified attributes for the rule.

The **undo rule** { **deny** | **permit** } command can only be used to delete an entire rule. You must specify all the attributes of the rule for the command.

Examples

Create an IPv4 advanced ACL rule to permit TCP packets with the destination port 80 from 129.9.0.0/16 to 202.38.160.0/24.

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule permit tcp source 129.9.0.0 0.0.255.255 destination
202.38.160.0 0.0.0.255 destination-port eq 80
```

Create IPv4 advanced ACL rules to permit all IP packets but the ICMP packets destined for 192.168.1.0/24.

```
<Sysname> system-view
[Sysname] acl advanced 3001
[Sysname-acl-ipv4-adv-3001] rule deny icmp destination 192.168.1.0 0.0.0.255
[Sysname-acl-ipv4-adv-3001] rule permit ip
```

Create IPv4 advanced ACL rules to permit inbound and outbound FTP packets.

```
<Sysname> system-view
[Sysname] acl advanced 3002
[Sysname-acl-ipv4-adv-3002] rule permit tcp source-port eq ftp
[Sysname-acl-ipv4-adv-3002] rule permit tcp source-port eq ftp-data
[Sysname-acl-ipv4-adv-3002] rule permit tcp destination-port eq ftp
[Sysname-acl-ipv4-adv-3002] rule permit tcp destination-port eq ftp-data
```

Create IPv4 advanced ACL rules to permit inbound and outbound SNMP and SNMP trap packets.

```
<Sysname> system-view
[Sysname] acl advanced 3003
[Sysname-acl-ipv4-adv-3003] rule permit udp source-port eq snmp
[Sysname-acl-ipv4-adv-3003] rule permit udp source-port eq snmptrap
[Sysname-acl-ipv4-adv-3003] rule permit udp destination-port eq snmp
[Sysname-acl-ipv4-adv-3003] rule permit udp destination-port eq snmptrap
```

Related commands

acl

acl logging interval

display acl

step

time-range

rule (IPv4 basic ACL view)

Use **rule** to create or edit an IPv4 basic ACL rule.

Use **undo rule** to delete an entire IPv4 basic ACL rule or some attributes in the rule.

Syntax

rule [*rule-id*] { **deny** | **permit** } [**counting** | **fragment** | **logging** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-range-name*] *

undo rule *rule-id* [**counting** | **fragment** | **logging** | **source** | **time-range**] *

undo rule { **deny** | **permit** } [**counting** | **fragment** | **logging** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-range-name*] *

Default

No IPv4 basic ACL rules exist.

Views

IPv4 basic ACL view

Predefined user roles

network-admin

Parameters

rule-id: Specifies a rule ID in the range of 0 to 65534. If you do not specify a rule ID when creating an ACL rule, the system automatically assigns it a rule ID. This rule ID is the nearest higher multiple of the numbering step to the current highest rule ID, starting from the start rule ID. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the rule is numbered 30.

deny: Denies matching packets.

permit: Allows matching packets to pass.

counting: Enables rule match counting in software. If you do not specify this keyword, matches for the rule are not counted in software.

fragment: Applies the rule only to fragments. If you do not specify this keyword, the rule applies to both fragments and non-fragments.

logging: Logs the number of matching packets. This feature is available only when the application module (for example, packet filtering) that uses the ACL supports the logging feature.

source { *source-address source-wildcard* | **any** }: Matches a source address. The *source-address* and *source-wildcard* arguments specify a source IP address and a wildcard mask in dotted decimal notation. A wildcard mask of zeros represents a host address. The **any** keyword represents any source IP address.

time-range *time-range-name*: Specifies a time range for the rule. The *time-range-name* argument is a case-insensitive string of 1 to 32 characters. It must start with an English letter. If the time range is not configured, the system creates the rule. However, the rule using the time range can take effect only after you configure the time range. For more information about time range, see *ACL and QoS Configuration Guide*.

Usage guidelines

Within an ACL, the permit or deny statement of each rule must be unique. If the rule you are creating or editing has the same deny or permit statement as another rule in the ACL, the rule will not be created or changed.

You can edit ACL rules only when the match order is **config**.

If an IPv4 basic ACL is used for QoS traffic classification or packet filtering in a VXLAN network, the ACL matches packets as follows:

- On a VTEP, the ACL can only match the incoming packets of Ethernet service instances.
- On an intermediate transport device, the ACL can match both incoming packets and outgoing packets.

The **counting** keyword in this command enables match counting specific to rules, and the **hardware-count** keyword in the **packet-filter** command enables match counting in hardware for all rules in an ACL.

To view the existing IPv4 basic and advanced ACL rules, use the **display acl all** command.

The **undo rule** *rule-id* command without any optional parameters deletes an entire rule. If you specify optional parameters, the **undo rule** *rule-id* command deletes the specified attributes for the rule.

The **undo rule** { **deny** | **permit** } command can only be used to delete an entire rule. You must specify all the attributes of the rule for the command.

Examples

Create a rule in IPv4 basic ACL 2000 to deny the packets from any source IP subnet but 10.0.0.0/8, 172.17.0.0/16, or 192.168.1.0/24.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule permit source 10.0.0.0 0.255.255.255
[Sysname-acl-ipv4-basic-2000] rule permit source 172.17.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Sysname-acl-ipv4-basic-2000] rule deny source any
```

Related commands

acl

acl logging interval

display acl

step

time-range

rule (IPv6 advanced ACL view)

Use **rule** to create or edit an IPv6 advanced ACL rule.

Use **undo rule** to delete an entire IPv6 advanced ACL rule or some attributes in the rule.

Syntax

rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { *dest-address dest-prefix* | *dest-address/dest-prefix* | **any** } | **destination-port** *operator port* | **dscp** *dscp* | **flow-label** *flow-label-value* | **fragment** | **icmp6-type** { *icmp6-type icmp6-code* | *icmp6-message* } | **logging** | **routing** [**type** *routing-type*] | **hop-by-hop** [**type** *hop-type*] | **source** { *source-address source-prefix* | *source-address/source-prefix* | **any** } | **source-port** *operator port* | **time-range** *time-range-name*] *

undo rule *rule-id* [{ { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **established** } | **counting** | **destination** | **destination-port** | **dscp** | **flow-label** | **fragment** | **icmp6-type** | **logging** | **routing** | **hop-by-hop** | **source** | **source-port** | **time-range**] *

undo rule { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { *dest-address dest-prefix* | *dest-address/dest-prefix* | **any** } | **destination-port** *operator port* | **dscp** *dscp*| **flow-label** *flow-label-value* | **fragment** | **icmp6-type** { *icmp6-type icmp6-code* | *icmp6-message* } | **logging** | **routing** [**type** *routing-type*] | **hop-by-hop** [**type** *hop-type*] | **source** { *source-address source-prefix* | *source-address/source-prefix* | **any** } | **source-port** *operator port* | **time-range** *time-range-name*] *

Default

No IPv6 advanced ACL rules exist.

Views

IPv6 advanced ACL view

Predefined user roles

network-admin

Parameters

rule-id: Specifies a rule ID in the range of 0 to 65534. If you do not specify a rule ID when creating an ACL rule, the system automatically assigns it a rule ID. This rule ID is the nearest higher multiple of the numbering step to the current highest rule ID, starting from the start rule ID. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the rule is numbered 30.

deny: Denies matching packets.

permit: Allows matching packets to pass.

protocol: Specifies a protocol carried over IPv6 by its number in the range of 0 to 255 or by its keyword, as shown in Table 12.

Table 12 Protocols carried over IPv6

Number	Keyword	Description
N/A	**ipv6**	Matches IPv6 packets.
1	**icmpv6**	Matches ICMPv6 packets.
2	**igmp**	Matches IGMP packets.
4	**ipinip**	Matches IP-in-IP packets.
6	**tcp**	Matches TCP packets.
17	**udp**	Matches UDP packets.
47	**gre**	Matches GRE packets. For information about GRE, see *Layer 3—IP Services Configuration Guide*.
50	**ipv6-esp**	Matches IPv6-ESP packets.
51	**ipv6-ah**	Matches IPv6-AH packets.
89	**ospf**	Matches OSPF packets.

Table 13 describes the parameters that you can specify, regardless of the value for the *protocol* argument.

Table 13 Match criteria and other rule information for IPv6 advanced ACL rules

Parameters	Function	Description
source { *source-address source-prefix* | *source-address/source-prefix* | **any** }	Specifies a source IPv6 address.	The *source-address* argument specifies an IPv6 source address. The *source-prefix* argument specifies a prefix length in the range of 1 to 128. The **any** keyword represents any IPv6 source address.
destination { *dest-address dest-prefix* | *dest-address/dest-prefix* | **any** }	Specifies a destination IPv6 address.	The *dest-address* argument specifies a destination IPv6 address. The *dest-prefix* argument specifies a prefix length in the range of 1 to 128. The **any** keyword represents any IPv6 destination address.
counting	Enables rule match counting in software.	The **counting** keyword enables match counting specific to rules, and the **hardware-count** keyword in the **packet-filter ipv6** command enables match counting in hardware for all rules in an ACL. If the **counting** keyword is not specified, matches for the rule are not counted in software.
dscp *dscp*	Specifies a DSCP preference.	The *dscp* argument can be a number in the range of 0 to 63, or in words, **af11** (10), **af12** (12), **af13** (14), **af21** (18), **af22** (20), **af23** (22), **af31** (26), **af32** (28), **af33** (30), **af41** (34), **af42** (36), **af43** (38), **cs1** (8), **cs2** (16), **cs3** (24), **cs4** (32), **cs5** (40), **cs6** (48), **cs7** (56), **default** (0), or **ef** (46).

Parameters	Function	Description
flow-label *flow-label-value*	Specifies a flow label value in an IPv6 packet header.	The *flow-label-value* argument is in the range of 0 to 1048575.
fragment	Applies the rule only to fragments.	If you do not specify this keyword, the rule applies to all fragments and non-fragments.
logging	Logs the number of matching packets.	This feature requires that the module (for example, packet filtering) that uses the ACL supports logging.
routing [**type** *routing-type*]	Specifies an IPv6 routing header type.	*routing-type*: Value of the IPv6 routing header type, in the range of 0 to 255. If you specify the **type** *routing-type* option, the rule applies to the specified type of IPv6 routing header. If you do not specify the **type** *routing-type* option, the rule applies to all types of IPv6 routing headers.
hop-by-hop [**type** *hop-type*]	Specifies an IPv6 Hop-by-Hop Options header type.	*hop-type*: Value of the IPv6 Hop-by-Hop Options header type, in the range of 0 to 255. If you specify the **type** *hop-type* option, the rule applies to the specified type of IPv6 Hop-by-Hop Options header. If you do not specify the **type** *hop-type* option, the rule applies to all types of IPv6 Hop-by-Hop Options header.
time-range *time-range-name*	Specifies a time range for the rule.	The *time-range-name* argument is a case-insensitive string of 1 to 32 characters. It must start with an English letter. If the time range is not configured, the system creates the rule. However, the rule using the time range can take effect only after you configure the time range. For more information about time range, see *ACL and QoS Configuration Guide*.

If the *protocol* argument is **tcp** (6) or **udp** (17), set the parameters shown in Table 14.

Table 14 TCP/UDP-specific parameters for IPv6 advanced ACL rules

Parameters	Function	Description
source-port *operator port*	Specifies one or more UDP or TCP source ports.	The *operator* argument can be only **eq** (equal to).. The *port* argument specifies a TCP or UDP port number in the range of 0 to 65535. TCP port numbers can be represented as: **chargen** (19), **bgp** (179), **cmd** (514), **daytime** (13), **discard** (9), **dns** (53), **domain** (53), **echo** (7), **exec** (512), **finger** (79), **ftp** (21), **ftp-data** (20), **gopher** (70), **hostname** (101), **irc** (194), **klogin** (543), **kshell** (544), **login** (513), **lpd** (515), **nntp** (119), **pop2** (109), **pop3** (110), **smtp** (25), **sunrpc** (111), **tacacs** (49), **talk** (517), **telnet** (23), **time** (37), **uucp** (540), **whois** (43), and **www** (80). UDP port numbers can be represented as: **biff** (512), **bootpc** (68), **bootps** (67), **discard** (9), **dns** (53), **dnsix** (90), **echo** (7), **mobilip-ag** (434), **mobilip-mn** (435), **nameserver** (42), **netbios-dgm** (138), **netbios-ns** (137), **netbios-ssn** (139), **ntp** (123), **rip** (520), **snmp** (161), **snmptrap** (162), **sunrpc** (111), **syslog** (514),
destination-port *operator port*	Specifies one or more UDP or TCP destination ports.	

Parameters	Function	Description
		tacacs-ds (65), **talk** (517), **tftp** (69), **time** (37), **who** (513), and **xdmcp** (177).
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* }*	Specifies one or more TCP flags, including ACK, FIN, PSH, RST, SYN, and URG.	Parameters specific to TCP. The value for each argument can be 0 (flag bit not set) or 1 (flag bit set). The TCP flags in a rule are ANDed. For example, a rule configured with **ack** 0 **psh** 1 matches packets that have the ACK flag bit not set and the PSH flag bit set.
established	Specifies the flags for indicating the established status of a TCP connection.	Parameter specific to TCP. The rule matches TCP packets with the ACK or RST flag bit set.

If the *protocol* argument is **icmpv6** (58), set the parameters shown in Table 15.

Table 15 ICMPv6-specific parameters for IPv6 advanced ACL rules

Parameters	Function	Description
icmp6-type { *icmp6-type icmp6-code* | *icmp6-message* }	Specifies the ICMPv6 message type and code.	The *icmp6-type* argument is in the range of 0 to 255. The *icmp6-code* argument is in the range of 0 to 255. The *icmp6-message* argument specifies a message name. Supported ICMP message names and their corresponding type and code values are listed in Table 16.

Table 16 ICMPv6 message names supported in IPv6 advanced ACL rules

ICMPv6 message name	ICMPv6 message type	ICMPv6 message code
echo-reply	129	0
echo-request	128	0
err-Header-field	4	0
frag-time-exceeded	3	1
hop-limit-exceeded	3	0
host-admin-prohib	1	1
host-unreachable	1	3
neighbor-advertisement	136	0
neighbor-solicitation	135	0
network-unreachable	1	0
packet-too-big	2	0
port-unreachable	1	4
redirect	137	0
router-advertisement	134	0
router-solicitation	133	0
unknown-ipv6-opt	4	2

ICMPv6 message name	ICMPv6 message type	ICMPv6 message code
unknown-next-hdr	4	1

Usage guidelines

If an IPv6 advanced ACL is used for QoS traffic classification or packet filtering:

- Do not specify the **fragment** keyword.
- Do not specify the **routing**, **hop-by-hop**, or **flow-label** keyword if the ACL is for outbound application.

Within an ACL, the permit or deny statement of each rule must be unique. If the rule you are creating or editing has the same deny or permit statement as another rule in the ACL, the rule will not be created or changed.

You can edit ACL rules only when the match order is **config**.

To view the existing IPv6 basic and advanced ACL rules, use the **display acl ipv6 all** command.

The **undo rule** *rule-id* command without any optional parameters deletes an entire rule. If you specify optional parameters, the **undo rule** *rule-id* command deletes the specified attributes for a rule.

The **undo rule** { **deny** | **permit** } command can only be used to delete an entire rule. You must specify all the attributes of the rule for the command.

Examples

Create an IPv6 advanced ACL rule to permit TCP packets with the destination port 80 from 2030:5060::/64 to FE80:5060::/96.

```
<Sysname> system-view
[Sysname] acl ipv6 advanced 3000
[Sysname-acl-ipv6-adv-3000] rule permit tcp source 2030:5060::/64 destination
fe80:5060::/96 destination-port eq 80
```

Create IPv6 advanced ACL rules to permit all IPv6 packets but the ICMPv6 packets destined for FE80:5060:1001::/48.

```
<Sysname> system-view
[Sysname] acl ipv6 advanced 3001
[Sysname-acl-ipv6-adv-3001] rule deny icmpv6 destination fe80:5060:1001:: 48
[Sysname-acl-ipv6-adv-3001] rule permit ipv6
```

Create IPv6 advanced ACL rules to permit inbound and outbound FTP packets.

```
<Sysname> system-view
[Sysname] acl ipv6 advanced 3002
[Sysname-acl-ipv6-adv-3002] rule permit tcp source-port eq ftp
[Sysname-acl-ipv6-adv-3002] rule permit tcp source-port eq ftp-data
[Sysname-acl-ipv6-adv-3002] rule permit tcp destination-port eq ftp
[Sysname-acl-ipv6-adv-3002] rule permit tcp destination-port eq ftp-data
```

Create IPv6 advanced ACL rules to permit inbound and outbound SNMP and SNMP trap packets.

```
<Sysname> system-view
[Sysname] acl ipv6 advanced 3003
[Sysname-acl-ipv6-adv-3003] rule permit udp source-port eq snmp
[Sysname-acl-ipv6-adv-3003] rule permit udp source-port eq snmptrap
[Sysname-acl-ipv6-adv-3003] rule permit udp destination-port eq snmp
[Sysname-acl-ipv6-adv-3003] rule permit udp destination-port eq snmptrap
```

Create IPv6 advanced ACL 3004, and configure two rules: one permits packets with the Hop-by-Hop Options header type as 5, and the other one denies packets with other Hop-by-Hop Options header types.

```
<Sysname> system-view
[Sysname] acl ipv6 advanced 3004
[Sysname-acl-ipv6-adv-3004] rule permit ipv6 hop-by-hop type 5
[Sysname-acl-ipv6-adv-3004] rule deny ipv6 hop-by-hop
```

Related commands

acl

acl logging interval

display acl

step

time-range

rule (IPv6 basic ACL view)

Use **rule** to create or edit an IPv6 basic ACL rule.

Use **undo rule** to delete an entire IPv6 basic ACL rule or some attributes in the rule.

Syntax

rule [*rule-id*] { **deny** | **permit** } [**counting** | **fragment** | **logging** | **routing** [**type** *routing-type*] | **source** { *source-address source-prefix* | *source-address*/*source-prefix* | **any** } | **time-range** *time-range-name*] *

undo rule *rule-id* [**counting** | **fragment** | **logging** | **routing** | **source** | **time-range**] *

undo rule { **deny** | **permit** } [**counting** | **fragment** | **logging** | **routing** [**type** *routing-type*] | **source** { *source-address source-prefix* | *source-address*/*source-prefix* | **any** } | **time-range** *time-range-name*] *

Default

No IPv6 basic ACL rules exist.

Views

IPv6 basic ACL view

Predefined user roles

network-admin

Parameters

rule-id: Specifies a rule ID in the range of 0 to 65534. If you do not specify a rule ID when creating an ACL rule, the system automatically assigns it a rule ID. This rule ID is the nearest higher multiple of the numbering step to the current highest rule ID, starting from the start rule ID. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the rule is numbered 30.

deny: Denies matching packets.

permit: Allows matching packets to pass.

counting: Enables rule match counting in software. If you do not specify this keyword, matches for the rule are not counted in software.

fragment: Applies the rule only to fragments. If you do not specify this keyword, the rule applies to both fragments and non-fragments.

logging: Logs the number of matching packets. This feature is available only when the application module (for example, packet filtering) that uses the ACL supports the logging feature.

routing [**type** *routing-type*]: Applies the rule to the specified type of IPv6 routing header or all types of IPv6 routing headers. The *routing-type* argument specifies the value of the IPv6 routing header type, in the range of 0 to 255. If you do not specify the **type** *routing-type* option, the rule applies to all types of IPv6 routing headers.

source { *source-address source-prefix* | *source-address*/*source-prefix* | **any** }: Matches a source IPv6 address. The *source-address* argument specifies a source IPv6 address. The *source-prefix* argument specifies an address prefix length in the range of 1 to 128. The **any** keyword represents any IPv6 source address.

time-range *time-range-name*: Specifies a time range for the rule. The *time-range-name* argument is a case-insensitive string of 1 to 32 characters. It must start with an English letter. If the time range is not configured, the system creates the rule. However, the rule using the time range can take effect only after you configure the time range. For more information about time range, see *ACL and QoS Configuration Guide*.

Usage guidelines

The **fragment** keyword is not supported for a QoS policy or a packet filter.

The **routing** keyword is not supported for an outbound QoS policy or packet filter.

Within an ACL, the permit or deny statement of each rule must be unique. If the rule you are creating or editing has the same deny or permit statement as another rule in the ACL, the rule will not be created or changed.

You can edit ACL rules only when the match order is **config**.

The **counting** keyword in this command enables match counting specific to rules, and the **hardware-count** keyword in the **packet-filter ipv6** command enables match counting in hardware for all rules in an ACL.

To view the existing IPv6 basic and advanced ACL rules, use the **display acl ipv6 all** command.

The **undo rule** *rule-id* command without any optional parameters deletes an entire rule. If you specify optional parameters, the **undo rule** *rule-id* command deletes the specified attributes for a rule.

The **undo rule** { **deny** | **permit** } command can only be used to delete an entire rule. You must specify all the attributes of the rule for the command.

Examples

Create an IPv6 basic ACL rule to deny the packets from any source IP subnet but 1001::/16, 3124:1123::/32, or FE80:5060:1001::/48.

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2000
[Sysname-acl-ipv6-basic-2000] rule permit source 1001:: 16
[Sysname-acl-ipv6-basic-2000] rule permit source 3124:1123:: 32
[Sysname-acl-ipv6-basic-2000] rule permit source fe80:5060:1001:: 48
[Sysname-acl-ipv6-basic-2000] rule deny source any
```

Related commands

acl

acl logging interval

display acl

step

time-range

rule (Layer 2 ACL view)

Use **rule** to create or edit a Layer 2 ACL rule.

Use **undo rule** to delete an entire Layer 2 ACL rule or some attributes in the rule.

Syntax

rule [*rule-id*] { **deny** | **permit** } [**cos** *dot1p* | **counting** | **dest-mac** *dest-address dest-mask* | { **lsap** *lsap-type lsap-type-mask* | **type** *protocol-type protocol-type-mask* } | **source-mac** *source-address source-mask* | **time-range** *time-range-name*] *

undo rule *rule-id* [**counting** | **time-range**] *

undo rule { **deny** | **permit** } [**cos** *dot1p* | **counting** | **dest-mac** *dest-address dest-mask* | { **lsap** *lsap-type lsap-type-mask* | **type** *protocol-type protocol-type-mask* } | **source-mac** *source-address source-mask* | **time-range** *time-range-name*] *

Default

No Layer 2 ACL rules exist.

Views

Layer 2 ACL view

Predefined user roles

network-admin

Parameters

rule-id: Specifies a rule ID in the range of 0 to 65534. If you do not specify a rule ID when creating an ACL rule, the system automatically assigns it a rule ID. This rule ID is the nearest higher multiple of the numbering step to the current highest rule ID, starting from the start rule ID. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the rule is numbered 30.

deny: Denies matching packets.

permit: Allows matching packets to pass.

cos *dot1p:* Matches an 802.1p priority. The 802.1p priority can be specified by one of the following values:

- A priority number in the range of 0 to 7.
- A priority name: **best-effort** (0), **background** (1), **spare** (2), **excellent-effort** (3), **controlled-load** (4), **video** (5), **voice** (6), or **network-management** (7).

counting: Enables rule match counting in software. If you do not specify this keyword, matches for the rule are not counted in software.

dest-mac *dest-address dest-mask:* Matches a destination MAC address range. The *dest-address* and *dest-mask* arguments represent a destination MAC address and mask in the H-H-H format.

lsap *lsap-type lsap-type-mask:* Matches the DSAP and SSAP fields in LLC encapsulation. The *lsap-type* argument is a hexadecimal number that represents the encapsulation format. The value range for the *lsap-type* argument is 0 to ffff. The *lsap-type-mask* argument is a hexadecimal number that represents the LSAP mask. The value range for the *lsap-type-mask* argument is 0 to ffff.

type *protocol-type protocol-type-mask*: Matches one or more protocols in the Layer 2. The *protocol-type* argument is a hexadecimal number that represents a protocol type in Ethernet_II and Ethernet_SNAP frames. The value range for the *protocol-type* argument is 0 to ffff. The *protocol-type-mask* argument is a hexadecimal number that represents a protocol type mask. The value range for the *protocol-type-mask* argument is 0 to ffff.

source-mac *source-address source-mask:* Matches a source MAC address range. The *source-address* argument represents a source MAC address, and the *sour-mask* argument represents a mask in the H-H-H format.

time-range *time-range-name*: Specifies a time range for the rule. The *time-range-name* argument is a case-insensitive string of 1 to 32 characters. It must start with an English letter. If the time range is not configured, the system creates the rule. However, the rule using the time range can take effect only after you configure the time range. For more information about time range, see *ACL and QoS Configuration Guide*.

Usage guidelines

Within an ACL, the permit or deny statement of each rule must be unique. If the rule you are creating or editing has the same deny or permit statement as another rule in the ACL, the rule will not be created or changed.

You can edit ACL rules only when the match order is **config**.

The **counting** keyword in this command enables match counting specific to rules, and the **hardware-count** keyword in the **packet-filter** command enables match counting in hardware for all rules in an ACL.

To view the existing Layer 2 ACL rules, use the **display acl mac all** command.

The **undo rule** *rule-id* command without any optional parameters deletes an entire rule. If you specify optional parameters, the **undo rule** *rule-id* command deletes the specified attributes for the rule.

The **undo rule** { **deny** | **permit** } command can only be used to delete an entire rule. You must specify all the attributes of the rule for the command.

Examples

Create a rule in Layer 2 ACL 4000 to permit ARP packets and deny RARP packets.

```
<Sysname> system-view
[Sysname] acl mac 4000
[Sysname-acl-mac-4000] rule permit type 0806 ffff
[Sysname-acl-mac-4000] rule deny type 8035 ffff
```

Related commands

acl

display acl

step

time-range

rule comment

Use **rule comment** to configure a comment for an ACL rule.

Use **undo rule comment** to delete an ACL rule comment.

Syntax

rule *rule-id* **comment** *text*

undo rule *rule-id* **comment**

Default

A rule does not have a comment.

Views

IPv4 basic/advanced ACL view

IPv6 basic/advanced ACL view

Layer 2 ACL view

Predefined user roles

network-admin

Parameters

rule-id: Specifies an ACL rule ID in the range of 0 to 65534. The ACL rule must already exist.

text: Specifies a comment about the ACL rule, a case-sensitive string of 1 to 127 characters.

Usage guidelines

This command adds a comment to a rule if the rule does not have a comment. It modifies the comment for a rule if the rule already has a comment.

Examples

Create a rule for IPv4 basic ACL 2000, and add a comment about the rule.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule 0 deny source 1.1.1.1 0
[Sysname-acl-ipv4-basic-2000] rule 0 comment This rule is used on ten-gigabitethernet
1/0/1.
```

Related commands

display acl

step

Use **step** to set a rule numbering step for an ACL.

Use **undo step** to restore the default.

Syntax

step *step-value* [**start** *start-value*]

undo step

Default

The rule numbering step is 5, and the start rule ID is 0.

Views

IPv4 basic/advanced ACL view

IPv6 basic/advanced ACL view

Layer 2 ACL view

Predefined user roles

network-admin

Parameters

step-value: Specifies the ACL rule numbering step in the range of 1 to 20.

start *start-value*: Specifies the start rule ID in the range of 0 to 20.

Usage guidelines

The rule numbering step sets the increment by which the system numbers rules automatically. If you do not specify a rule ID when creating an ACL rule, the system automatically assigns it a rule ID. This rule ID is the nearest higher multiple of the numbering step to the current highest rule ID, starting from the start rule ID. For example, if the rule numbering step is 5 and the current highest rule ID is 12, the rule is numbered 15.

The wider the numbering step, the more rules you can insert between two rules. Whenever the step or start rule ID changes, the rules are renumbered, starting from the start rule ID. For example, if there are five rules numbered 0, 5, 9, 10, and 15, changing the step from 5 to 2 causes the rules to be renumbered 0, 2, 4, 6, and 8.

Examples

Set the rule numbering step to 2 for IPv4 basic ACL 2000.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] step 2
```

Related commands

display acl

Contents

QoS policy commands

Traffic class commands

description

Use **description** to configure a description for a traffic class.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

No description is configured for a traffic class.

Views

Traffic class view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 127 characters.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure the description as **classifier** for traffic class **class1**.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] description classifier
```

display traffic classifier

Use **display traffic classifier** to display traffic classes.

Syntax

display traffic classifier user-defined [*classifier-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

user-defined: Specifies user-defined traffic classes.

classifier-name: Specifies a traffic class by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a traffic class, this command displays all traffic classes.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the traffic classes for the master device.

Examples

Display all user-defined traffic classes.

```
<Sysname> display traffic classifier user-defined

  User-defined classifier information:

   Classifier: 1 (ID 100)
     Operator: AND
     Rule(s) :
      If-match acl 2000

   Classifier: 2 (ID 101)
     Operator: AND
     Rule(s) :
      If-match protocol ipv6

   Classifier: 3 (ID 102)
     Operator: AND
     Rule(s) :
      -none-
```

Table 1 Command output

Field	Description
Classifier	Traffic class name and its match criteria.
Operator	Match operator you set for the traffic class. If the operator is AND, the traffic class matches the packets that match all its match criteria. If the operator is OR, the traffic class matches the packets that match any of its match criteria.
Rule(s)	Match criteria.

if-match

Use **if-match** to define a match criterion.

Use **undo if-match** to delete a match criterion.

Syntax

if-match *match-criteria*

undo if-match *match-criteria*

Default

No match criterion is configured.

Views

Traffic class view

Predefined user roles

network-admin

Parameters

match-criteria: Specifies a match criterion. Table 2 shows the available match criteria.

Table 2 Available match criteria

Option	Description
acl [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }	Matches an ACL. The value range for the *acl-number* argument is as follows: • 2000 to 3999 for IPv4 ACLs. • 2000 to 3999 for IPv6 ACLs. • 4000 to 4999 for Layer 2 MAC ACLs. The *acl-name* argument is a case-insensitive string of 1 to 63 characters, which must start with an English letter. To avoid confusion, make sure the argument is not **all**.
any	Matches all packets.
customer-dot1p *dot1p-value*&<1-8>	Matches 802.1p priority values in inner VLAN tags of double-tagged packets. The *dot1p-value*&<1-8> argument specifies a space-separated list of up to eight 802.1p priority values. The value range for the *dot1p-value* argument is 0 to 7.
customer-vlan-id *vlan-id-list*	Matches VLAN IDs in inner VLAN tags of double-tagged packets. The *vlan-id-list* argument specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* **to** *vlan-id2*. The value for *vlan-id2* must be greater than or equal to the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.
destination-mac *mac-address* [*mac-address-mask*]	Matches a destination MAC address. This option takes effect only on Ethernet interfaces.
dscp *dscp-value*&<1-8>	Matches DSCP values. The *dscp-value*&<1-8> argument specifies a space-separated list of up to eight DSCP values. The value range for the *dscp-value* argument is 0 to 63 or keywords shown in Table 4.
ip-precedence *ip-precedence-value*&<1-8>	Matches IP precedence values. The *ip-precedence-value*&<1-8> argument specifies a space-separated list of up to eight IP precedence values. The value range for the *ip-precedence-value* argument is 0 to 7.
protocol *protocol-name*	Matches a protocol. The *protocol-name* argument can be **ip** or **ipv6**.
service-dot1p *dot1p-value*&<1-8>	Matches 802.1p priority values in outer VLAN tags.

Option	Description
	The *dot1p-value*&<1-8> argument specifies a space-separated list of up to eight 802.1p priority values. The value range for the *dot1p-value* argument is 0 to 7.
service-vlan-id *vlan-id-list*	Matches VLAN IDs in outer VLAN tags. The *vlan-id-list* argument specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* **to** *vlan-id2*. The value for *vlan-id2* must be greater than or equal to the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094. You can use this option to match single-tagged packets.
source-mac *mac-address* [*mac-address-mask*]	Matches a source MAC address. This option takes effect only on Ethernet interfaces.
tunnel-id *tunnel-id*	Matches a VXLAN tunnel ID. For the traffic class to take effect, the tunnel must be a VXLAN tunnel.
vxlan { **any** | *vxlan-id* }	Matches a VXLAN ID.

Usage guidelines

In a traffic class with the logical OR operator, you can configure multiple **if-match** commands for any of the available match criteria.

When you configure a match criterion that can have multiple values in one **if-match** command, follow these restrictions and guidelines:

- You can specify up to eight values for any of the following match criteria in one **if-match** command:
  - DSCP.
  - 802.1p priority.
  - IP precedence.
  - VLAN ID.
- If a packet matches one of the specified values, it matches the **if-match** command.
- To delete a criterion that has multiple values, the specified values in the **undo if-match** command must be the same as those specified in the **if-match** command. The order of the values can be different.

When you configure ACL-based match criteria, follow these restrictions and guidelines:

- The ACL must already exist.
- The ACL is used for classification only and the permit/deny actions in ACL rules are ignored. Actions taken on matching packets are defined in traffic behaviors.

You can use both AND and OR operators to define the match relationships between the criteria for a class. For example, you can define relationships among three match criteria in traffic class **classA** as follows:

```
traffic classifier classB operator and
if-match criterion 1
if-match criterion 2
traffic classifier classA operator or
if-match criterion 3
```

If a traffic class in a QoS policy includes the **customer-vlan-id** match criterion, the QoS policy can be applied only to interfaces.

For the **customer-vlan-id** and **service-vlan-id** match criteria, you can configure multiple values in one **if-match** command.

Examples

Define a match criterion for traffic class **class1** to match the packets with a destination MAC address of 0050-ba27-bed3.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match destination-mac 0050-ba27-bed3
```

Define a match criterion for traffic class **class2** to match the packets with a source MAC address of 0050-ba27-bed2.

```
<Sysname> system-view
[Sysname] traffic classifier class2
[Sysname-classifier-class2] if-match source-mac 0050-ba27-bed2
```

Define a match criterion for traffic class **class1** to match the packets with a source MAC address of 0050-ba27-bed3 and a MAC address mask of ffff-ffff-0000.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match destination-mac 0050-ba27-bed3 ffff-ffff-0000
```

Define a match criterion for traffic class **class2** to match the packets with a source MAC address of 0050-ba27-bed2 and a MAC address mask of ffff-ffff-0000.

```
<Sysname> system-view
[Sysname] traffic classifier class2
[Sysname-classifier-class2] if-match source-mac 0050-ba27-bed2 ffff-ffff-0000
```

Define a match criterion for traffic class **class1** to match the double-tagged packets with 802.1p priority 3 in the inner VLAN tag.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match customer-dot1p 3
```

Define a match criterion for traffic class **class1** to match the packets with 802.1p priority 5 in the outer VLAN tag.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match service-dot1p 5
```

Define a match criterion for traffic class **class1** to match advanced ACL 3101.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl 3101
```

Define a match criterion for traffic class **class1** to match the ACL named **flow**.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl name flow
```

Define a match criterion for traffic class **class1** to match advanced IPv6 ACL 3101.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl ipv6 3101
```

Define a match criterion for traffic class **class1** to match the IPv6 ACL named **flow**.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl ipv6 name flow
```

Define a match criterion for traffic class **class1** to match all packets.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match any
```

Define a match criterion for traffic class **class1** to match the packets with a DSCP value of 1, 6, or 9.

```
<Sysname> system-view
[Sysname] traffic classifier class1 operator or
[Sysname-classifier-class1] if-match dscp 1 6 9
```

Define a match criterion for traffic class **class1** to match the packets with an IP precedence value of 1 or 6.

```
<Sysname> system-view
[Sysname] traffic classifier class1 operator or
[Sysname-classifier-class1] if-match ip-precedence 1 6
```

Define a match criterion for traffic class **class1** to match IP packets.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match protocol ip
```

Define a match criterion for traffic class **class1** to match double-tagged packets with VLAN ID 1, 6, or 9 in the inner VLAN tag.

```
<Sysname> system-view
[Sysname] traffic classifier class1 operator or
[Sysname-classifier-class1] if-match customer-vlan-id 1 6 9
```

Define a match criterion for traffic class **class1** to match the packets with VLAN ID 2, 7, or 10 in the outer VLAN tag.

```
<Sysname> system-view
[Sysname] traffic classifier class1 operator or
[Sysname-classifier-class1] if-match service-vlan-id 2 7 10
```

Define a match criterion for traffic class **class1** to match the VXLAN packets with tunnel ID 2.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match tunnel-id 2
```

Define a match criterion for traffic class **class1** to match the packets with VXLAN 10.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match vxlan 10
```

traffic classifier

Use **traffic classifier** to create a traffic class and enter its view, or enter the view of an existing traffic class.

Use **undo traffic classifier** to delete a traffic class.

Syntax

traffic classifier *classifier-name* [**operator** { **and** | **or** }]

undo traffic classifier *classifier-name*

Default

No traffic classes exist.

Views

System view

Predefined user roles

network-admin

Parameters

classifier-name: Specifies a name for the traffic class, a case-sensitive string of 1 to 31 characters.

operator: Sets the operator to logic AND (the default) or OR for the traffic class.

and: Specifies the logic AND operator. The traffic class matches the packets that match all its criteria.

or: Specifies the logic OR operator. The traffic class matches the packets that match any of its criteria.

Examples

Create a traffic class named **class1**.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1]
```

Related commands

display traffic classifier

Traffic behavior commands

accounting

Use **accounting** to configure a traffic accounting action in a traffic behavior.

Use **undo accounting** to restore the default.

Syntax

accounting { **byte** | **packet** }

undo accounting

Default

No traffic accounting action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

byte: Counts traffic in bytes.

packet: Counts traffic in packets.

Examples

Configure a traffic accounting action in traffic behavior **database** to count traffic in bytes.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] accounting byte
```

car

Use **car** to configure a CAR action in absolute value in a traffic behavior.

Use **undo car** to restore the default.

Syntax

car cir *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**green** *action* | **red** *action* | **yellow** *action*] *

car cir *committed-information-rate* [**cbs** *committed-burst-size*] **pir** *peak-information-rate* [**ebs** *excess-burst-size*] [**green** *action* | **red** *action* | **yellow** *action*] *

undo car

Default

No CAR action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

cir *committed-information-rate*: Specifies the committed information rate (CIR) in the range of 1 to 160000000 kbps.

cbs *committed-burst-size*: Specifies the committed burst size (CBS) in bytes. The value range for *committed-burst-size* is 512 to 256000000, in increments of 512. The default value for this argument is the product of 62.5 and the CIR and must be an integral multiple of 512. When the product is not an integral multiple of 512, it is rounded up to the nearest integral multiple of 512 that is greater than the product. A default value greater than 256000000 is converted to 256000000.

ebs *excess-burst-size*: Specifies the excess burst size (EBS) in bytes. The value range for *excess-burst-size* is 0 to 256000000, in increments of 512. If the PIR is configured, the default EBS is the product of 62.5 and the PIR and must be an integral multiple of 512. When the product is not an integral multiple of 512, it is rounded up to the nearest integral multiple of 512. A default value greater than 256000000 is converted to 256000000.

pir *peak-information-rate*: Specifies the peak information rate (PIR) in the range of 1 to 160000000 kbps.

green *action*: Specifies the action to take on packets that conform to the CIR. The default setting is **pass**.

red *action*: Specifies the action to take on packets that conform to neither CIR nor PIR. The default setting is **discard**.

yellow *action*: Specifies the action to take on packets that conform to the PIR but not to the CIR. The default setting is **pass**.

action: Sets the action to take on the packet:

- **discard**: Drops the packet.
- **pass**: Permits the packet to pass through.
- **remark-dot1p-pass** *new-cos*: Sets the 802.1p priority value of the 802.1p packet to *new-cos* and permits the packet to pass through. The *new-cos* argument is in the range of 0 to 7.
- **remark-dscp-pass** *new-dscp*: Sets the DSCP value of the packet to *new-dscp* and permits the packet to pass through. The *new-dscp* argument is in the range of 0 to 63.
- **remark-lp-pass** *new-local-precedence*: Sets the local precedence value of the packet to *new-local-precedence* and permits the packet to pass through. The *new-local-precedence* argument is in the range of 0 to 7.

Usage guidelines

To use two rates for traffic policing, configure the **car** command with the **pir** *peak-information-rate* option. To use one rate for traffic policing, configure the **car** command without the **pir** *peak-information-rate* option.

If you execute the **car** command multiple times in the same traffic behavior, the most recent configuration takes effect.

Examples

Configure a CAR action in traffic behavior **database**:

- Set the CIR to 200 kbps, CBS to 51200 bytes, and EBS to 0.
- Transmit the conforming packets, and mark the excess packets with DSCP value 0 and transmit them.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] car cir 200 cbs 51200 ebs 0 green pass red remark-dscp-pass
0
```

display traffic behavior

Use **display traffic behavior** to display traffic behaviors.

Syntax

display traffic behavior user-defined [*behavior-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

user-defined: Specifies user-defined traffic behaviors.

behavior-name: Specifies a behavior by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a traffic behavior, this command displays all traffic behaviors.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the traffic behaviors for the master device.

Examples

Display all user-defined traffic behaviors.

```
<Sysname> display traffic behavior user-defined

  User-defined behavior information:

    Behavior: 1 (ID 100)
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 112 (kbps), CBS 5120 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard

    Behavior: 2 (ID 101)
      Accounting enable: Packet
      Filter enable: Permit
      Redirecting:
        Redirect to the CPU

    Behavior: 3 (ID 102)
      -none-
```

Table 3 Command output

Field	Description
Behavior	Name and contents of a traffic behavior.
Marking	Information about priority marking.
Remark dscp	Action of setting the DSCP value for packets.
Committed Access Rate	Information about the CAR action.
Green action	Action to take on green packets.
Yellow action	Action to take on yellow packets.
Red action	Action to take on red packets.
Accounting enable	Class-based accounting action.
Filter enable	Traffic filtering action.
Redirecting	Information about traffic redirecting.
Mirroring	Information about traffic mirroring.
none	No other traffic behavior is configured.

filter

Use **filter** to configure a traffic filtering action in a traffic behavior.

Use **undo filter** to restore the default.

Syntax

filter { **deny** | **permit** }

undo filter

Default

No traffic filtering action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

deny: Drops packets.

permit: Transmits packets. The permitted packets can be processed by other class-behavior associations in the same QoS policy.

Examples

Configure a traffic filtering action as **deny** in traffic behavior **database**.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] filter deny
```

nest top-most

Use **nest top-most** to configure an outer VLAN tag adding action in a traffic behavior.

Use **undo nest top-most** to restore the default.

Syntax

nest top-most vlan *vlan-id*

undo nest top-most

Default

No outer VLAN tag adding action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

vlan-id *vlan-id*: Specifies the VLAN ID to be added in the outer VLAN tag, in the range of 1 to 4094.

Usage guidelines

If a QoS policy contains an outer VLAN tag adding action, apply it only to the incoming traffic of an interface.

If you execute the **nest top-most** command multiple times in the same traffic behavior, the most recent configuration takes effect.

An outer VLAN tag adding action takes effect only when the QoS policy is applied to the inbound direction of an interface, VLANs, or globally.

This command does not take effect on packets forwarded by a VXLAN overlay network.

Examples

Configure traffic behavior **b1** to add an outer VLAN tag with VLAN ID 123.

```
<Sysname> system-view
[Sysname] traffic behavior b1
[Sysname-behavior-b1] nest top-most vlan 123
```

redirect

Use **redirect** to configure a traffic redirecting action in a traffic behavior.

Use **undo redirect** to restore the default.

Syntax

redirect { **cpu** | **interface** *interface-type interface-number* }

undo redirect { **cpu** | **interface** *interface-type interface-number* }

Default

No traffic redirecting action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

cpu: Redirects traffic to the CPU.

interface *interface-type interface-number*: Redirects traffic to an interface specified by its type and number.

Usage guidelines

If you execute the **redirect** command multiple times in the same traffic behavior, the most recent configuration takes effect.

A traffic redirecting action takes effect only when the QoS policy is applied to the inbound direction.

If a QoS policy applied to a user profile contains the **redirect interface** action, make sure the redirected-to interface and the incoming interface of packets are in the same VLAN.

Examples

Configure redirecting traffic to Ten-GigabitEthernet 1/0/1 in traffic behavior **database**.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] redirect interface ten-gigabitethernet 1/0/1
```

Related commands

classifier behavior

qos policy

traffic behavior

remark customer-vlan-id

Use **remark customer-vlan-id** to configure a CVLAN marking action in a traffic behavior.

Use **undo remark customer-vlan-id** to restore the default.

Syntax

remark customer-vlan-id *vlan-id*

undo remark customer-vlan-id

Default

No CVLAN marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies a CVLAN ID in the range of 1 to 4094.

Examples

Configure traffic behavior **b1** to mark matching packets with CVLAN 111.

```
<Sysname> system-view
[Sysname] traffic behavior b1
[Sysname-behavior-b1] remark customer-vlan-id 111
```

remark dot1p

Use **remark dot1p** to configure an 802.1p priority marking action or an inner-to-outer tag priority copying action in a traffic behavior.

Use **undo remark dot1p** to restore the default.

Syntax

remark [**green** | **red** | **yellow**] **dot1p** *dot1p-value*

undo remark [**green** | **red** | **yellow**] **dot1p**

remark dot1p customer-dot1p-trust

undo remark dot1p

Default

No 802.1p priority marking action or inner-to-outer tag priority copying action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

green: Specifies green packets.

red: Specifies red packets.

yellow: Specifies yellow packets.

dot1p-value: Specifies the 802.1p priority to be marked for packets, in the range of 0 to 7.

customer-dot1p-trust: Copies the 802.1p priority value in the inner VLAN tag to the outer VLAN tag.

Usage guidelines

The **remark dot1p** and **remark dot1p customer-dot1p-trust** commands override each other in the same traffic behavior. The **remark dot1p customer-dot1p-trust** command does not take effect on single-tagged packets.

If you execute the **remark dot1p** command multiple times for the same color, the most recent configuration takes effect.

An 802.1p priority marking action takes effect only when the QoS policy is applied to the inbound direction.

Examples

Configure traffic behavior **database** to mark matching traffic with 802.1p 2.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark dot1p 2
```

Configure an inner-to-outer tag priority copying action in traffic behavior **database**.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark dot1p customer-dot1p-trust
```

remark drop-precedence

Use **remark drop-precedence** to configure a drop priority marking action in a traffic behavior.

Use **undo remark drop-precedence** to restore the default.

Syntax

remark drop-precedence *drop-precedence-value*

undo remark drop-precedence

Default

No drop priority marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

drop-precedence-value: Specifies the drop priority to be marked for packets, in the range of 0 to 2.

Usage guidelines

A drop priority marking action takes effect only when the QoS policy is applied to the inbound direction.

If you execute the **remark drop-precedence** command multiple times in the same traffic behavior, the most recent configuration takes effect.

Examples

Configure traffic behavior **database** to mark matching traffic with drop priority 2.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark drop-precedence 2
```

remark dscp

Use **remark dscp** to configure a DSCP marking action in a traffic behavior.

Use **undo remark dscp** to restore the default.

Syntax

remark [**green** | **red** | **yellow**] **dscp** *dscp-value*

undo remark [**green** | **red** | **yellow**] **dscp**

Default

No DSCP marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

green: Specifies green packets.

red: Specifies red packets.

yellow: Specifies yellow packets.

dscp-value: Specifies a DSCP value, which can be a number from 0 to 63 or a keyword in Table 4.

Table 4 DSCP keywords and values

Keyword	DSCP value (binary)	DSCP value (decimal)
af11	001010	10
af12	001100	12
af13	001110	14
af21	010010	18
af22	010100	20
af23	010110	22

Keyword	DSCP value (binary)	DSCP value (decimal)
af31	011010	26
af32	011100	28
af33	011110	30
af41	100010	34
af42	100100	36
af43	100110	38
cs1	001000	8
cs2	010000	16
cs3	011000	24
cs4	100000	32
cs5	101000	40
cs6	110000	48
cs7	111000	56
default	000000	0
ef	101110	46

Examples

Configure traffic behavior **database** to mark matching traffic with DSCP 6.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark dscp 6
```

remark local-precedence

Use **remark local-precedence** to configure a local precedence marking action in a traffic behavior.

Use **undo remark local-precedence** to restore the default.

Syntax

remark [**green** | **red** | **yellow**] **local-precedence** *local-precedence-value*

undo remark [**green** | **red** | **yellow**] **local-precedence**

Default

No local precedence marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

green: Specifies green packets.

red: Specifies red packets.

yellow: Specifies yellow packets.

local-precedence-value: Specifies the local precedence to be marked for packets, in the range of 0 to 7.

Usage guidelines

A local precedence marking action takes effect only when the QoS policy is applied to the inbound direction.

Examples

Configure traffic behavior **database** to mark matching traffic with local precedence 2.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark local-precedence 2
```

remark service-vlan-id

Use **remark service-vlan-id** to configure an SVLAN marking action in a traffic behavior.

Use **undo remark service-vlan-id** to restore the default.

Syntax

remark service-vlan-id *vlan-id*

undo remark service-vlan-id

Default

No SVLAN marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies an SVLAN ID in the range of 1 to 4094.

Examples

Configure traffic behavior **b1** to mark matching packets with SVLAN 222.

```
<Sysname> system-view
[Sysname] traffic behavior b1
[Sysname-behavior-b1] remark service-vlan-id 222
```

traffic behavior

Use **traffic behavior** to create a traffic behavior and enter its view, or enter the view of an existing traffic behavior.

Use **undo traffic behavior** to delete a traffic behavior.

Syntax

traffic behavior *behavior-name*

undo traffic behavior *behavior-name*

Default

No traffic behaviors exist.

Views

System view

Predefined user roles

network-admin

Parameters

behavior-name: Specifies a name for the traffic behavior, a case-sensitive string of 1 to 31 characters.

Examples

Create a traffic behavior named **behavior1**.

```
<Sysname> system-view
[Sysname] traffic behavior behavior1
[Sysname-behavior-behavior1]
```

Related commands

display traffic behavior

QoS policy commands

classifier behavior

Use **classifier behavior** to associate a traffic behavior with a traffic class in a QoS policy.

Use **undo classifier** to delete a class-behavior association from a QoS policy.

Syntax

classifier *classifier-name* **behavior** *behavior-name* [**insert-before** *before-classifier-name*]

undo classifier *classifier-name*

Default

No traffic behavior is associated with a traffic class.

Views

QoS policy view

Predefined user roles

network-admin

Parameters

classifier-name: Specifies a traffic class by its name, a case-sensitive string of 1 to 31 characters.

behavior-name: Specifies a traffic behavior by its name, a case-sensitive string of 1 to 31 characters.

insert-before *before-classifier-name*: Inserts the new traffic class before an existing traffic class in the QoS policy. The *before-classifier-name* argument specifies an existing traffic class by its name, a case-sensitive string of 1 to 31 characters. If you do not specify the

insert-before *before-classifier-name* option, the new traffic class is placed at the end of the QoS policy.

Usage guidelines

A traffic class can be associated only with one traffic behavior in a QoS policy.

If the specified traffic class or traffic behavior does not exist, the system defines a null traffic class or traffic behavior.

Examples

Associate traffic class **database** with traffic behavior **test** in QoS policy **user1**.

```
<Sysname> system-view
[Sysname] qos policy user1
[Sysname-qospolicy-user1] classifier database behavior test
```

Associate traffic class **database** with traffic behavior **test** in QoS policy **user1**, and insert traffic class **database** before an existing traffic class named **class-a**.

```
<Sysname> system-view
[Sysname] qos policy user1
[Sysname-qospolicy-user1] classifier database behavior test insert-before class-a
```

Related commands

qos policy

display qos policy

Use **display qos policy** to display QoS policies.

Syntax

display qos policy user-defined [*policy-name* [**classifier** *classifier-name*]] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

user-defined: Specifies user-defined QoS policies.

policy-name: Specifies a QoS policy by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a QoS policy, this command displays all user-defined QoS policies.

classifier *classifier-name*: Specifies a traffic class by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a traffic class, this command displays all traffic classes.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the QoS policies for the master device.

Examples

Display all user-defined QoS policies.

```
<Sysname> display qos policy user-defined

  User-defined QoS policy information:
```

```
Policy: 1 (ID 100)
 Classifier: 1 (ID 100)
   Behavior: 1
    Marking:
      Remark dscp 3
    Committed Access Rate:
      CIR 112 (kbps), CBS 51200 (Bytes), EBS 512 (Bytes)
      Green action  : pass
      Yellow action : pass
      Red action    : discard
 Classifier: 2 (ID 101)
   Behavior: 2
    Accounting enable: Packet
    Filter enable: Permit
    Marking:
      Remark dot1p 4
 Classifier: 3 (ID 102)
   Behavior: 3
    -none-
```

Table 5 Command output

Field	Description
User-defined QoS policy information	Information about a user-defined QoS policy.
System-defined QoS policy information	Information about a system-defined QoS policy.

For the description of other fields, see Table 1 and Table 3.

display qos policy global

Use **display qos policy global** to display QoS policies applied globally.

Syntax

display qos policy global [**slot** *slot-number*] [**inbound** | **outbound**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

inbound: Specifies the QoS policy applied in the inbound direction.

outbound: Specifies the QoS policy applied in the outbound direction.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays global QoS policies for the master device.

Usage guidelines

If you do not specify a direction, this command displays both inbound and outbound global QoS policies.

Examples

Display QoS policies applied globally.

```
<Sysname> display qos policy global
  Direction: Inbound
  Policy: 1
   Classifier: 1
     Operator: AND
     Rule(s) :
      If-match acl 2000
     Behavior: 1
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 112 (kbps), CBS 51200 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets) 0 (Bytes)
        Yellow packets: 0 (Packets) 0 (Bytes)
        Red packets   : 0 (Packets) 0 (Bytes)
   Classifier: 2
     Operator: AND
     Rule(s) :
      If-match protocol ipv6
     Behavior: 2
      Accounting enable:
        0 (Packets)
      Filter enable: Permit
      Marking:
        Remark dscp 3
   Classifier: 3
     Operator: AND
     Rule(s) :
      -none-
     Behavior: 3
      -none-
```

Table 6 Command output

Field	Description
Direction	Direction in which the QoS policy is applied.
Policy	User-defined generic QoS policy name or system-defined QoS policy name.
Green packets	Statistics about green packets.
Yellow packets	Statistics about yellow packets.

Field	Description
Red packets	Statistics about red packets.

For the description of other fields, see Table 1 and Table 3.

display qos policy interface

Use **display qos policy interface** to display the QoS policies applied to interfaces.

Syntax

display qos policy interface [*interface-type interface-number*] [**inbound** | **outbound**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number.

inbound: Specifies the QoS policy applied to incoming traffic.

outbound: Specifies the QoS policy applied to outgoing traffic.

Usage guidelines

If you do not specify a direction, this command displays the QoS policy applied to incoming traffic and the QoS policy applied to outgoing traffic.

Examples

Display the QoS policy applied to the incoming traffic of Ten-GigabitEthernet 1/0/1.

```
<Sysname> display qos policy interface ten-gigabitethernet 1/0/1 inbound
Interface: Ten-GigabitEthernet1/0/1
  Direction: Inbound
  Policy: 1
   Classifier: 1
     Matched : 0 (Packets) 0 (Bytes)
     5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
     Operator: AND
     Rule(s) :
      If-match acl 2000
     Behavior: 1
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 112 (kbps), CBS 51200 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
```

```
      Red action    : discard
      Green packets : 0 (Packets) 0 (Bytes)
      Yellow packets: 0 (Packets) 0 (Bytes)
      Red packets   : 0 (Packets) 0 (Bytes)
  Classifier: 2
    Matched : 0 (Packets) 0 (Bytes)
    5-minute statistics:
     Forwarded: 0/0 (pps/bps)
     Dropped  : 0/0 (pps/bps)
    Operator: AND
    Rule(s) :
     If-match protocol ipv6
    Behavior: 2
     Accounting enable:
       0 (Packets)
     Filter enable: Permit
     Marking:
       Remark dscp 3
  Classifier: 3
    Matched : 0 (Packets) 0 (Bytes)
    5-minute statistics:
     Forwarded: 0/0 (pps/bps)
     Dropped  : 0/0 (pps/bps)
    Operator: AND
    Rule(s) :
     -none-
    Behavior: 3
     -none-
```

Display the QoS policies applied to all interfaces.

```
<Sysname> display qos policy interface
Interface: Ten-GigabitEthernet1/0/1
  Direction: Inbound
  Policy: a
   Classifier: a
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: a
      Mirroring:
        Mirror to the interface: Ten-GigabitEthernet1/0/2
      Committed Access Rate:
        CIR 112 (kbps), CBS 51200 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets)
        Red packets   : 0 (Packets)
```

```
Interface: Ten-GigabitEthernet1/0/3
  Direction: Inbound
  Policy: b
   Classifier: b
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: b
      Committed Access Rate:
        CIR 112 (kbps), CBS 51200 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0(Packets)
        Red packets   : 0 (Packets)

Interface: Ten-GigabitEthernet1/0/4
  Direction: Inbound
  Policy: a
   Classifier: a
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: a
      Mirroring:
        Mirror to the interface: Ten-GigabitEthernet1/0/5
      Committed Access Rate:
        CIR 112 (kbps), CBS 51200 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets)
        Red packets   : 0 (Packets)
```

Table 7 Command output

Field	Description
Direction	Direction in which the QoS policy is applied.
Matched	Number of matching packets.
Forwarded	Average rate of successfully forwarded matching packets in a statistics collection period.
Dropped	Average rate of dropped matching packets in a statistics collection period.
Green packets	Traffic statistics for green packets.
Yellow packets	Traffic statistics for yellow packets.
Red packets	Traffic statistics for red packets.

For the description of other fields, see Table 1 and Table 3.

display qos policy user-profile

Use **display qos policy user-profile** to display QoS policies applied to user profiles.

Syntax

display qos policy user-profile [**name** *profile-name*] [**user-id** *user-id*] [**slot** *slot-number*] [**inbound** | **outbound**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *profile-name*: Specifies a user profile by its name, a case-sensitive string of 1 to 31 characters. Valid characters include English letters, digits, and underscores (_). The name must start with an English letter and must be unique. If you do not specify a user profile, this command displays QoS policies applied to all user profiles.

user-id *user-id*: Specifies an online user by a system-assigned, hexadecimal ID in the range of 0 to ffffffe. If you do not specify an online user, this command displays QoS policies applied to user profiles for all online users.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays QoS policies applied to user profiles for all member devices.

inbound: Specifies QoS policies applied to incoming traffic.

outbound: Specifies QoS policies applied to outgoing traffic.

Usage guidelines

If you do not specify a direction, this command displays QoS policies applied in the inbound direction and QoS policies applied in the outbound direction.

Examples

Display the QoS policy applied to user profile **abc** for a global user.

```
<Sysname> display qos policy user-profile name abc user-id 30000000 inbound
User-Profile: abc
  User ID: 0x30000000(global)
    Direction: Inbound
    Policy: p1
     Classifier: default-class
       Matched : 0 (Packets) 0 (Bytes)
       Operator: AND
       Rule(s) :
        If-match any
       Behavior: be
        -none-
```

Display the QoS policy applied to user profile **abc** for a local user.

```
<Sysname> display qos policy user-profile name abc user-id 30000001 inbound
User-Profile: abc
  slot 2:
```

```
User ID: 0x30000001(local)
  Direction: Inbound
  Policy: p1
   Classifier: default-class
     Matched : 0 (Packets) 0 (Bytes)
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: be
      -none-
```

Table 8 Command output

Field	Description
global	Indicates a global user, who comes online from a global interface such as an aggregate interface.
local	Indicates a local user, who comes online from a physical interface.
Matched	Number of packets that meet match criteria.
Direction	Direction in which the QoS policy is applied.
Green packets	Statistics about green packets.
Yellow packets	Statistics about yellow packets.
Red packets	Statistics about red packets.

For the description of other fields, see Table 1 and Table 3.

display qos vlan-policy

Use **display qos vlan-policy** to display QoS policies applied to VLANs.

Syntax

display qos vlan-policy { **name** *policy-name* | **vlan** [*vlan-id*] } [**slot** *slot-number*] [**inbound** | **outbound**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *policy-name*: Specifies a QoS policy by its name, a case-sensitive string of 1 to 31 characters.

vlan *vlan-id*: Specifies a VLAN by its ID in the range of 1 to 4094.

inbound: Displays QoS policies applied to incoming traffic.

outbound: Displays QoS policies applied to outgoing traffic.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays QoS policies applied to VLANs for the master device.

Usage guidelines

If you do not specify a direction, this command displays QoS policies applied to VLANs in both the inbound and outbound directions.

Examples

Display QoS policies applied to VLAN 2.

```
<Sysname> display qos vlan-policy vlan 2
Vlan 2
  Direction: Inbound
  Policy: 1
   Classifier: 1
     Operator: AND
     Rule(s) :
      If-match acl 2000
     Behavior: 1
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 112 (kbps), CBS 5120 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0(Packets) 0(Bytes)
        Yellow packets: 0(Packets) 0(Bytes)
        Red packets   : 0(Packets) 0(Bytes)
   Classifier: 2
     Operator: AND
     Rule(s) :
      If-match protocol ipv6
     Behavior: 2
      Accounting enable:
        0 (Packets)
      Filter enable: Permit
      Marking:
        Remark dscp 3
   Classifier: 3
     Operator: AND
     Rule(s) :
      -none-
     Behavior: 3
      -none-
```

Table 9 Command output

Field	Description
Direction	Direction in which the QoS policy is applied.
Green packets	Statistics about green packets.
Yellow packets	Statistics about yellow packets.

Field	Description
Red packets	Statistics about red packets.

For the description of other fields, see Table 1 and Table 3.

qos apply policy (interface view)

Use **qos apply policy** to apply a QoS policy to an interface.

Use **undo qos apply policy** to remove an applied QoS policy.

Syntax

qos apply policy *policy-name* { **inbound** | **outbound** }

undo qos apply policy *policy-name* { **inbound** | **outbound** }

Default

No QoS policy is applied.

Views

Interface view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a QoS policy by its name, a case-sensitive string of 1 to 31 characters.

inbound: Applies the QoS policy to incoming traffic.

outbound: Applies the QoS policy to outgoing traffic.

Examples

Apply QoS policy **TEST1** to the outgoing traffic of Ten-GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] qos apply policy TEST1 outbound
```

qos apply policy (user profile view)

Use **qos apply policy** to apply a QoS policy to a user profile.

Use **undo qos apply policy** to remove a QoS policy applied to a user profile.

Syntax

qos apply policy *policy-name* { **inbound** | **outbound** }

undo qos apply policy *policy-name* { **inbound** | **outbound** }

Default

No QoS policy is applied to a user profile.

Views

User profile view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a QoS policy by its name, a case-sensitive string of 1 to 31 characters.

inbound: Applies the QoS policy to the incoming traffic of the device (traffic sent by online users).

outbound: Applies the QoS policy to the outgoing traffic of the device (traffic received by online users).

Usage guidelines

Deleting a user profile also removes the QoS policies applied to the user profile.

For a user profile to be active, the QoS policy applied in user profile view cannot be empty. A user profile supports only the **car** and **accounting** actions in a QoS policy.

Examples

Apply QoS policy **test** to incoming traffic of user profile **user**.

```
<Sysname> system-view
[Sysname] user-profile user
[Sysname-user-profile-user] qos apply policy test outbound
```

qos apply policy global

Use **qos apply policy global** to apply a QoS policy globally.

Use **undo qos apply policy global** to remove a globally applied QoS policy.

Syntax

qos apply policy *policy-name* **global** { **inbound** | **outbound** }

undo qos apply policy *policy-name* **global** { **inbound** | **outbound** }

Default

No QoS policy is applied globally.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a QoS policy by its name, a case-sensitive string of 1 to 31 characters.

inbound: Applies the QoS policy to the incoming packets on all interfaces.

outbound: Applies the QoS policy to the outgoing packets on all interfaces.

Usage guidelines

A global QoS policy takes effect on all incoming or outgoing traffic depending on the direction in which the QoS policy is applied.

Examples

Globally apply QoS policy **user1** to the incoming traffic.

```
<Sysname> system-view
[Sysname] qos apply policy user1 global inbound
```

qos policy

Use **qos policy** to create a QoS policy and enter its view, or enter the view of an existing QoS policy.

Use **undo qos policy** to delete a QoS policy.

Syntax

qos policy *policy-name*

undo qos policy *policy-name*

Default

No QoS policies exist.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a name for the QoS policy, a case-sensitive string of 1 to 31 characters.

Usage guidelines

To delete a QoS policy that has been applied to an object, you must first remove the QoS policy from the object.

Examples

Create a QoS policy named **user1**.

```
<Sysname> system-view
[Sysname] qos policy user1
[Sysname-qospolicy-user1]
```

Related commands

classifier behavior

qos apply policy

qos apply policy global

qos vlan-policy

qos vlan-policy

Use **qos vlan-policy** to apply a QoS policy to the specified VLANs.

Use **undo qos vlan-policy** to remove a QoS policy from the specified VLANs.

Syntax

qos vlan-policy *policy-name* **vlan** *vlan-id-list* { **inbound** | **outbound** }

undo qos vlan-policy *policy-name* **vlan** *vlan-id-list* { **inbound** | **outbound** }

Default

No QoS policy is applied to a VLAN.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a QoS policy by its name, a case-sensitive string of 1 to 31 characters.

vlan *vlan-id-list*: Specifies a space-separated list of up to eight VLAN IDs or a VLAN ID range in the form of *vlan-id1* **to** *vlan-id2*. The value for *vlan-id2* must be greater than or equal to the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

inbound: Applies the QoS policy to incoming packets.

outbound: Applies the QoS policy to outgoing packets.

Examples

Apply QoS policy **test** to the incoming traffic of VLAN 200, VLAN 300, VLAN 400, and VLAN 500.

```
<Sysname> system-view
[Sysname] qos vlan-policy test vlan 200 300 400 500 inbound
```

reset qos policy global

Use **reset qos policy global** to clear statistics for QoS policies applied globally.

Syntax

reset qos policy global [**inbound** | **outbound**]

Views

User view

Predefined user roles

network-admin

Parameters

inbound: Specifies the QoS policy applied to the inbound direction globally.

outbound: Specifies the QoS policy applied to the outbound direction globally.

Usage guidelines

If you do not specify a direction, this command clears statistics for the global QoS policies in both directions.

Examples

Clear statistics for the QoS policy applied to the inbound direction globally.

```
<Sysname> reset qos policy global inbound
```

reset qos vlan-policy

Use **reset qos vlan-policy** to clear the statistics for QoS policies applied to VLANs.

Syntax

reset qos vlan-policy [**vlan** *vlan-id*] [**inbound** | **outbound**]

Views

User view

Predefined user roles

network-admin

Parameters

vlan *vlan-id*: Specifies a VLAN ID in the range of 1 to 4094.

inbound: Specifies the QoS policy applied to incoming traffic.

outbound: Specifies the QoS policy applied to outgoing traffic.

Usage guidelines

If you do not specify a direction, this command clears the statistics of the QoS policies in both directions of the VLAN.

Examples

Clear the statistics of QoS policies applied to VLAN 2.

```
<Sysname> reset qos vlan-policy vlan 2
```

Priority mapping commands

Priority map commands

display qos map-table

Use **display qos map-table** to display the configuration of priority maps.

Syntax

display qos map-table [**dot1p-dp** | **dot1p-exp** | **dot1p-lp** | **dscp-dot1p** | **dscp-dp** | **dscp-dscp** | **exp-dot1p** | **exp-dp**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

The device provides the following types of priority map.

Table 10 Priority maps

Priority mapping	Description
dot1p-dp	802.1p-drop priority map.
dot1p-exp	802.1p-EXP priority map.
dot1p-lp	802.1p-local priority map.
dscp-dot1p	DSCP-802.1p priority map.
dscp-dp	DSCP-drop priority map.
dscp-dscp	DSCP-DSCP priority map.
exp-dot1p	EXP-802.1p priority map.
exp-dp	EXP-drop priority map.

Usage guidelines

If you do not specify a priority map, this command displays the configuration of all priority maps.

Examples

Display the configuration of the 802.1p-local priority map.

```
<Sysname> display qos map-table dot1p-lp
MAP-TABLE NAME: dot1p-lp   TYPE: pre-define
IMPORT  :  EXPORT
   0    :    2
   1    :    0
   2    :    1
   3    :    3
   4    :    4
```

```
5    :    5
6    :    6
7    :    7
```

Table 11 Command output

Field	Description
MAP-TABLE NAME	Name of the priority map.
TYPE	Type of the priority map.
IMPORT	Input values of the priority map.
EXPORT	Output values of the priority map.

import

Use **import** to configure mappings for a priority map.

Use **undo import** to restore the specified or all mappings to the default for a priority map.

Syntax

import *import-value-list* **export** *export-value*

undo import { *import-value-list* | **all** }

Default

The default priority maps are used. For more information, see *ACL and QoS Configuration Guide*.

Views

Priority map view

Predefined user roles

network-admin

Parameters

import-value-list: Specifies a list of input values.

export-value: Specifies the output value.

all: Restores all mappings in the priority map to the default.

Examples

Configure the 802.1p-local priority map to map 802.1p priority values 4 and 5 to local priority 1.

```
<Sysname> system-view
[Sysname] qos map-table dot1p-lp
[Sysname-maptbl-dot1p-lp] import 4 5 export 1
```

Related commands

display qos map-table

qos map-table

Use **qos map-table** to enter the specified priority map view.

Syntax

qos map-table { **dot1p-dp** | **dot1p-exp** | **dot1p-lp** | **dscp-dot1p** | **dscp-dp** | **dscp-dscp** | **exp-dot1p** | **exp-dp** }

Views

System view

Predefined user roles

network-admin

Parameters

For the description of the keywords, see Table 10.

Examples

Enter 802.1p-local priority map view.

```
<Sysname> system-view
[Sysname] qos map-table dot1p-lp
[Sysname-maptbl-dot1p-lp]
```

Related commands

display qos map-table

import

Priority trust mode commands

display qos trust interface

Use **display qos trust interface** to display the priority trust mode and port priorities of an interface.

Syntax

display qos trust interface [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays the priority trust mode and port priorities of all interfaces.

Examples

Display the priority trust mode and port priority of Ten-GigabitEthernet 1/0/1.

```
<Sysname> display qos trust interface ten-gigabitethernet 1/0/1
Interface: Ten-GigabitEthernet1/0/1
 Port priority trust information
  Port priority:4
  Port priority trust type: dscp
```

Table 12 Command output

Field	Description
Interface	Interface type and interface number.
Port priority	Port priority set for the interface.
Port priority trust type	Priority trust mode on the interface: • **dot1p**—Uses the 802.1p priority of received packets for mapping. • **dscp**—Uses the DSCP precedence of received IP packets for mapping. • **none**—Trusts no packet priority.

qos trust

Use **qos trust** to configure the priority trust mode for an interface.

Use **undo qos trust** to restore the default.

Syntax

qos trust { **dot1p** | **dscp** }

undo qos trust

Default

An interface does not trust any packet priority and uses the port priority as the 802.1p priority for mapping.

Views

Layer 2/Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

dot1p: Uses the 802.1p priority in incoming packets for priority mapping.

dscp: Uses the DSCP value in incoming packets for priority mapping.

Examples

Set the priority trust mode to 802.1p priority on Ten-GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] qos trust dot1p
```

Related commands

display qos trust interface

Port priority commands

qos priority

Use **qos priority** to change the port priority of an interface.

Use **undo qos priority** to restore the default.

Syntax

qos priority *priority-value*

undo qos priority

Default

The port priority is 0.

Views

Layer 2/Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

priority-value: Specifies a port priority value in the range of 0 to 7.

Examples

Set the port priority of Ten-GigabitEthernet 1/0/1 to 2.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] qos priority 2
```

Related commands

display qos trust interface

Traffic policing, GTS, and rate limit commands

Traffic policing commands

qos car any

Use **qos car any** to configure a CAR policy for all packets of a user profile.

Use **undo qos car** to delete a CAR policy from a user profile.

Syntax

qos car { **inbound** | **outbound** } **any cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]]

qos car { **inbound** | **outbound** } **any cir** *committed-information-rate* [**cbs** *committed-burst-size*] **pir** *peak-information-rate* [**ebs** *excess-burst-size*]

undo qos car { **inbound** | **outbound** }

Default

No CAR policy is configured.

Views

User profile view

Predefined user roles

network-admin

Parameters

inbound: Performs CAR for incoming traffic.

outbound: Performs CAR for outgoing traffic.

cir *committed-information-rate*: Specifies the CIR in kbps. The value range for *committed-information-rate* is 8 to 160000000.

cbs *committed-burst-size*: Specifies the committed burst size (CBS) in bytes. The value range for *committed-burst-size* is 512 to 256000000, in increments of 512. The default value for this argument is the product of 62.5 and the CIR and must be an integral multiple of 512. When the product is not an integral multiple of 512, it is rounded up to the nearest integral multiple of 512 that is greater than the product. A default value greater than 256000000 is converted to 256000000.

ebs *excess-burst-size*: Specifies the EBS in bytes. The default value for *excess-burst-size* is 0 bytes. The value range for *excess-burst-size* is 0 to 256000000.

pir *peak-information-rate*: Specifies the PIR in kbps. The value range for *peak-information-rate* is 1 to 160000000.

Usage guidelines

To use two rates for traffic policing, configure the **qos car** command with the **pir** *peak-information-rate* option. To use one rate for traffic policing, configure the **qos car** command without the **pir** *peak-information-rate* option.

The conforming traffic is permitted to pass through, and the excess traffic is dropped.

If you execute the **qos car** command multiple times for the same user profile, the most recent configuration takes effect.

Examples

Perform CAR for packets received by user profile **user**. The CAR parameters are as follows:

- The CIR is 200 kbps.
- The CBS is 51200 bytes.

```
<Sysname> system-view
[Sysname] user-profile user
[Sysname-user-profile-user] qos car outbound any cir 200 cbs 51200
```

GTS commands

display qos gts interface

Use **display qos gts interface** to display the GTS configuration for interfaces.

Syntax

display qos gts interface [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays the GTS configuration for all interfaces.

Examples

Display the GTS configuration for all interfaces.

```
<Sysname> display qos gts interface
Interface: Ten-GigabitEthernet1/0/1
 Rule: If-match queue 1
  CIR 512 (kbps), CBS 51200 (Bytes)
```

Table 13 Command output

Field	Description
Interface	Interface name, including the interface type and interface number.
Rule	Match criteria.
CIR	CIR in kbps.
CBS	CBS in bytes.

qos gts

Use **qos gts** to set GTS parameters on an interface.

Use **undo qos gts** to delete the GTS configuration on an interface.

Syntax

qos gts queue *queue-id* **cir** *committed-information-rate* [**cbs** *committed-burst-size*]

undo qos gts queue *queue-id*

Default

No GTS parameters are configured.

Views

Layer 2/Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

queue *queue-id*: Shapes the packets in a queue specified by its ID. The value range for *queue-id* is 0 to 7.

cir *committed-information-rate*: Specifies the CIR in kbps. The value range for *committed-information-rate* is 1000 to 10485760 for 10-GE interfaces, 1000 to 41943040 for 40-GE interfaces, and 1000 to 104857600 for 100-GE interfaces.

cbs *committed-burst-size*: Specifies the CBS in bytes. The value range for *committed-burst-size* is 512 to 16777216, in increments of 512. The default value for this argument is the product of 62.5 and the CIR and must be a multiple of 512. When the product is not a multiple of 512, it is rounded up to the nearest integral multiple of 512 that is greater than the product. A default value greater than 16777216 is converted to 16777216.

Examples

Shape the packets of queue 1 on Ten-GigabitEthernet 1/0/1. The GTS parameters are as follows:

- The CIR is 6400 kbps.
- The CBS is 51200 bytes.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos gts queue 1 cir 6400 cbs 51200
```

Rate limit commands

display qos lr interface

Use **display qos lr interface** to display the rate limit configuration for interfaces.

Syntax

display qos lr interface [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays the rate limit configuration for all interfaces.

Examples

Display the rate limit configuration for all interfaces.

```
<Sysname> display qos lr interface
Interface: Ten-GigabitEthernet1/0/1
 Direction: Outbound
  CIR 2000 (kbps), CBS 20480 (Bytes)
```

Table 14 Command output

Field	Description
Interface	Interface name, including the interface type and interface number.
Direction	Direction in which the rate limit configuration is applied.
CIR	CIR in kbps.
CBS	CBS in bytes.

qos lr

Use **qos lr** to configure rate limiting on an interface.

Use **undo qos lr** to delete the rate limit configuration on an interface.

Syntax

qos lr { **inbound** | **outbound** } **cir** *committed-information-rate* [**cbs** *committed-burst-size*]

undo qos lr { **inbound** | **outbound** }

Default

No rate limit is configured.

Views

Layer 2/Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

inbound: Limits the rate of incoming packets.

outbound: Limits the rate of outgoing packets.

cir *committed-information-rate*: Specifies the CIR in kbps. The value range for *committed-information-rate* is 1000 to 10485760 for 10-GE interfaces, 1000 to 41943040 for 40-GE interfaces, and 1000 to 104857600 for 100-GE interfaces.

cbs *committed-burst-size*: Specifies the CBS in bytes. The value range for *committed-burst-size* is 512 to 134217728, in increments of 512. The default value for this argument is the product of 62.5 and the CIR and must be a multiple of 512. When the product is not a multiple of 512, it is rounded up to the nearest integral multiple of 512 that is greater than the product. A default value greater than 134217728 is converted to 134217728.

Examples

Limit the rate of outgoing packets on Ten-GigabitEthernet 1/0/1, with CIR 256 kbps and CBS 51200 bytes.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] qos lr outbound cir 256 cbs 51200
```

Congestion management commands

Common commands

display qos queue interface

Use **display qos queue interface** to display the queuing information for interfaces.

Syntax

display qos queue interface [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays the queuing information for all interfaces.

Examples

Display the queuing information for all interfaces.

```
<Sysname> display qos queue interface
Interface: Ten-GigabitEthernet1/0/1
Output queue: Weighted Round Robin queuing
 Queue ID     Queue name     Group     Byte count
 -------------------------------------------------
 0            be             1         1
 1            af1            1         2
 2            af2            1         3
 3            af3            1         4
 4            af4            1         5
 5            ef             1         9
 6            cs6            1         13
 7            cs7            1         15
Interface: Ten-GigabitEthernet1/0/2
Output queue: Weighted Round Robin queuing
 Queue ID     Queue name     Group     Byte count
 -------------------------------------------------
 0            be             1         1
 1            af1            1         2
 2            af2            1         3
 3            af3            1         4
 4            af4            1         5
 5            ef             1         9
 6            cs6            1         13
```

```
 7             cs7             1          15
...
```

Table 15 Command output

Field	Description
Interface	Interface name, including the interface type and interface number.
Output queue	Type of the current output queue.
Group	Number of the group that holds the queue.
Weight	Packet-count scheduling weight of the queue. N/A is displayed for a queue that uses the SP scheduling algorithm.

SP commands

display qos queue sp interface

Use **display qos queue sp interface** to display the SP queuing configuration of an interface.

Syntax

display qos queue sp interface [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays the SP queuing configuration of all interfaces.

Examples

Display the SP queuing configuration of Ten-GigabitEthernet 1/0/1.

```
<Sysname> display qos queue sp interface ten-gigabitethernet 1/0/1
Interface: Ten-GigabitEthernet1/0/1
 Output queue: Strict Priority queuing
```

Table 16 Command output

Field	Description
Interface	Interface type and interface number.
Output queue	Type of the current output queue.

qos sp

Use **qos sp** to enable SP queuing on an interface.

Use **undo qos sp** to restore the default.

Syntax

qos sp

undo qos sp

Default

An interface uses packet-count WRR queuing.

Views

Layer 2/Layer 3 Ethernet interface view

Predefined user roles

network-admin

Examples

Enable SP queuing on Ten-GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] qos sp
```

Related commands

display qos queue sp interface

WRR commands

display qos queue wrr interface

Use **display qos queue wrr interface** to display the WRR queuing configuration of an interface.

Syntax

display qos queue wrr interface [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays the WRR queuing configuration of all interfaces.

Examples

Display the WRR queuing configuration of Ten-GigabitEthernet 1/0/1.

```
<Sysname> display qos queue wrr interface ten-gigabitethernet 1/0/1
Interface: Ten-GigabitEthernet1/0/1
 Output queue: Weighted Round Robin queuing
 Queue ID        Queue name      Group           Weight
 ------------------------------------------------------
 0               be              1               1
 1               af1             1               1
```

```
2               af2             1               1
3               af3             1               1
4               af4             1               1
5               ef              1               1
6               cs6             1               1
7               cs7             sp              N/A
```

Table 17 Command output

Field	Description
Interface	Interface type and interface number.
Output queue	Type of the current output queue.
Group	ID of the group a queue is assigned to.
Weight	Packet-count queue scheduling weight of a queue. N/A is displayed for a queue that uses the SP scheduling algorithm.

qos wrr

Use **qos wrr** to enable WRR queuing on an interface.

Use **undo qos wrr** to restore the default.

Syntax

qos wrr weight

undo qos wrr weight

Default

An interface uses packet-count WRR queuing.

Views

Layer 2/Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

weight: Allocates bandwidth to queues in packets.

Usage guidelines

You must use the **qos wrr** command to enable WRR queuing before you can configure WRR queuing parameters for a queue on an interface.

Examples

Enable packet-count WRR queuing on Ten-GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] qos wrr weight
```

Related commands

display qos queue wrr interface

qos wrr weight

Use **qos wrr weight** to configure the WRR queuing parameters for a queue on an interface.

Use **undo qos wrr** to restore the default.

Syntax

qos wrr *queue-id* **group 1 weight** *schedule-value*

undo qos wrr *queue-id*

Default

All queues on a WRR-enabled interface are in WRR group 1, and queues 0 through 7 have a weight of 1, 2, 3, 4, 5, 9, 13, and 15, respectively.

Views

Layer 2/Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

queue-id: Specifies a queue by its ID. The value range for this argument is 0 to 7 or keywords in Table 18.

Table 18 The number-keyword map for the *queue-id* argument

Number	Keyword
0	be
1	af1
2	af2
3	af3
4	af4
5	ef
6	cs6
7	cs7

group 1: Specifies WRR group 1. Only WRR group 1 is supported in the current software version.

weight: Allocates bandwidth to queues in packets.

schedule-value: Specifies a scheduling weight. The value range for this argument is 1 to 15.

Usage guidelines

You must use the **qos wrr** command to enable WRR queuing before you can configure WRR queuing parameters for a queue on an interface.

Examples

Enable packet-based WRR queuing on Ten-GigabitEthernet 1/0/1, assign queue 0 to WRR group 1, and specify scheduling weight 10 for queue 0.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] qos wrr weight
```

```
[Sysname-Ten-GigabitEthernet1/0/1] qos wrr 0 group 1 weight 10
```

Related commands

display qos queue wrr interface

qos wrr

qos wrr group sp

Use **qos wrr group sp** to assign a queue to the SP group.

Use **undo qos wrr group sp** to remove a queue from the SP group.

Syntax

qos wrr *queue-id* **group sp**

undo qos wrr *queue-id*

Default

All queues on a WRR-enabled interface are in WRR group 1.

Views

Layer 2/Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

queue-id: Specifies a queue by its ID. The value range for this argument is 0 to 7 or keywords in Table 18.

Usage guidelines

This command is available only on a WRR-enabled interface. Queues in the SP group are scheduled with SP. The SP group has higher scheduling priority than the WRR groups.

You must use the **qos wrr** command to enable WRR queuing before you can configure this command on an interface.

Examples

Enable WRR queuing on Ten-GigabitEthernet 1/0/1, and assign queue 0 to the SP group.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] qos wrr weight
[Sysname-Ten-GigabitEthernet1/0/1] qos wrr 0 group sp
```

Related commands

display qos queue wrr interface

qos wrr

Queue scheduling profile commands

display qos qmprofile configuration

Use **display qos qmprofile configuration** to display the queue scheduling profile configuration.

Syntax

display qos qmprofile configuration [*profile-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

profile-name: Specifies a queue scheduling profile by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a queue scheduling profile, this command displays the configuration of all queue scheduling profiles.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the queue scheduling profile configuration for the master device.

Examples

Display the configuration of queue scheduling profile **myprofile**.

```
<Sysname> display qos qmprofile configuration myprofile
Queue management profile: myprofile (ID 1)
Queue ID  Type  Group   Schedule   Schedule  Min         Max
                        unit       value     bandwidth   bandwidth
-------------------------------------------------------------------
be        SP    N/A     N/A        N/A       N/A         N/A
af1       SP    N/A     N/A        N/A       N/A         N/A
af2       SP    N/A     N/A        N/A       N/A         N/A
af3       SP    N/A     N/A        N/A       N/A         N/A
af4       SP    N/A     N/A        N/A       N/A         N/A
ef        SP    N/A     N/A        N/A       N/A         N/A
cs6       SP    N/A     N/A        N/A       N/A         N/A
cs7       SP    N/A     N/A        N/A       N/A         N/A
```

Table 19 Command output

Field	Description
Queue management profile	Queue scheduling profile name.
Type	Queue scheduling type: • SP. • WRR.
Group	Priority group to which the queue belongs. The value can only be 1. **N/A** indicates this field is ignored.
Schedule unit	Scheduling unit, which can only be **weight**. **N/A** indicates that this field is ignored.
Schedule value	This field indicates the number of packets scheduled each time. **N/A** indicates that this field is ignored.
Min bandwidth	Minimum guaranteed bandwidth for the queue. **N/A** indicates that this field is ignored.

Field	Description
Max bandwidth	This field is not supported in the current software version. Maximum allowed bandwidth for the queue. **N/A** indicates that this field is ignored.

display qos qmprofile interface

Use **display qos qmprofile interface** to display the queue scheduling profile applied to an interface.

Syntax

display qos qmprofile interface [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays the queue scheduling profiles applied to all interfaces.

Examples

Display the queue scheduling profile applied to Ten-GigabitEthernet 1/0/1.

```
<Sysname> display qos qmprofile interface ten-gigabitethernet 1/0/1
Interface: Ten-GigabitEthernet1/0/1
Direction: Outbound
 Queue management profile: myprofile
```

Table 20 Command output

Field	Description
Direction	Direction in which the queue scheduling profile is applied.
Queue management profile	Name of the queue scheduling profile applied to the interface.

qos apply qmprofile

Use **qos apply qmprofile** to apply a queue scheduling profile to the outbound direction of an interface.

Use **undo qos apply qmprofile** to restore the default.

Syntax

qos apply qmprofile *profile-name*

undo qos apply qmprofile

Default

No queue scheduling profile is applied to an interface.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

profile-name: Specifies a queue scheduling profile by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

You can apply only one queue scheduling profile to an interface.

Examples

Apply queue scheduling profile **myprofile** to the outbound direction of Ten-GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] qos apply qmprofile myprofile
```

Related commands

display qos qmprofile interface

qos qmprofile

Use **qos qmprofile** to create a queue scheduling profile and enter its view, or enter the view of an existing queue scheduling profile.

Use **undo qos qmprofile** to delete a queue scheduling profile.

Syntax

qos qmprofile *profile-name*

undo qos qmprofile *profile-name*

Default

No user-created queue scheduling profiles exist.

Views

System view

Predefined user roles

network-admin

Parameters

profile-name: Specifies a name for the queue scheduling profile, a case-sensitive string of 1 to 31 characters.

Usage guidelines

To delete a queue scheduling profile already applied to an object, first remove it from the object.

Examples

Create a queue scheduling profile named **myprofile** and enter queue scheduling profile view.

```
<Sysname> system-view
[Sysname] qos qmprofile myprofile
[Sysname-qmprofile-myprofile]
```

Related commands

display qos qmprofile interface

queue

queue

Use **queue** to configure queue scheduling parameters.

Use **undo queue** to delete queue scheduling parameter settings.

Syntax

queue *queue-id* { **sp** | **wrr group** *group-id* **weight** *schedule-value* }

undo queue *queue-id*

Default

All queues in a queue scheduling profile are SP queues.

Views

Queue scheduling profile view

Predefined user roles

network-admin

Parameters

queue-id: Specifies a queue by its ID. The value range for this argument is 0 to 7 or keywords in Table 18.

sp: Enables SP for the queue.

wrr: Enables WRR for the queue.

group *group-id*: Specifies a WRR group by its ID. The group ID can only be 1.

weight: Allocates bandwidth to queues in packets.

schedule-value: Specifies the scheduling weight. The value range for this argument is 1 to 15.

Examples

Create a queue scheduling profile named **myprofile**, and configure queue 0 to use SP.

```
<Sysname> system-view
[Sysname] qos qmprofile myprofile
[Sysname-qmprofile-myprofile] queue 0 sp
```

Create a queue scheduling profile named **myprofile**. Configure queue 1 to meet the following requirements:

- The WRR queuing is used.
- The WRR group is group 1.
- The scheduling weight is 10.

```
<Sysname> system-view
[Sysname] qos qmprofile myprofile
[Sysname-qmprofile-myprofile] queue 1 wrr group 1 weight 10
```

Related commands

display qos qmprofile interface

qos qmprofile

Global CAR commands

car name

Use **car name** to use an aggregate CAR action in a traffic behavior.

Use **undo car** to restore the default.

Syntax

car name *car-name*

undo car

Default

No aggregate CAR action is configured in a traffic behavior.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

car-name: Specifies the name of an aggregate CAR action. This argument must start with a letter, and is a case-sensitive string of 1 to 31 characters.

Examples

Use aggregate CAR action **aggcar-1** in traffic behavior **be1**.

```
<Sysname> system-view
[Sysname] traffic behavior be1
[Sysname-behavior-be1] car name aggcar-1
```

Related commands

display qos car name

display traffic behavior user-defined

display qos car name

Use **display qos car name** to display information about aggregate CAR actions.

Syntax

display qos car name [*car-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

car-name: Specifies an aggregate CAR action by its name. This argument must start with a letter, and is a case-sensitive string of 1 to 31 characters. If you do not specify an aggregate CAR action, this command displays information about all aggregate CAR actions.

Examples

Display information about all aggregate CAR actions.

```
<Sysname> display qos car name
 Name: a
  Mode: aggregative
   CIR 32 (kbps) CBS: 2048 (Bytes) PIR: 888 (kbps) EBS: 0 (Bytes)
   Green action  : pass
   Yellow action : pass
   Red action    : discard
  Slot 0:
   Green packets : 0 (Packets), 0 (Bytes)
   Yellow packets: 0 (Packets), 0 (Bytes)
   Red packets   : 0 (Packets), 0 (Bytes)
  Slot 1:
   Green packets : 0 (Packets), 0 (Bytes)
   Yellow packets: 0 (Packets), 0 (Bytes)
   Red packets   : 0 (Packets), 0 (Bytes)
  Slot 2:
   Apply failed
```

Table 21 Command output

Field	Description
Name	Name of the aggregate CAR action.
Mode	Type of the CAR action, which can be **aggregative**.
CIR CBS PIR EBS	Parameters for the CAR action.
Green action	Action to take on green packets: • **discard**—Drops the packets. • **pass**—Permits the packets to pass through.
Yellow action	Action to take on yellow packets: • **discard**—Drops the packets. • **pass**—Permits the packets to pass through.
Red action	Action to take on red packets: • **discard**—Drops the packets. • **pass**—Permits the packets to pass through.
Green packets	Statistics about green packets.
Yellow packets	Statistics about yellow packets.
Red packets	Statistics about red packets.

qos car

Use **qos car aggregative** to configure an aggregate CAR action.

Use **undo qos car** to delete an aggregate CAR action.

Syntax

qos car *car-name* **aggregative cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**green** *action* | **red** *action* | **yellow** *action*] *

qos car *car-name* **aggregative cir** *committed-information-rate* [**cbs** *committed-burst-size*] **pir** *peak-information-rate* [**ebs** *excess-burst-size*] [**green** *action* | **red** *action* | **yellow** *action*] *

undo qos car *car-name*

Default

No aggregate CAR action is configured.

Views

System view

Predefined user roles

network-admin

Parameters

car-name: Specifies the name of the aggregate CAR action. This argument must start with a letter, and is a case-sensitive string of 1 to 31 characters.

cir *committed-information-rate*: Specifies the CIR in kbps, which is an average traffic rate. The value range for *committed-information-rate* is 8 to 160000000.

cbs *committed-burst-size*: Specifies the CBS in bytes. The value range for *committed-burst-size* is 512 to 256000000, in increments of 512. The default value for this argument is the product of 62.5 and the CIR and must be an integral multiple of 512. When the product is not an integral multiple of 512, it is rounded up to the nearest integral multiple of 512 that is greater than the product. A default value greater than 256000000 is converted to 256000000.

ebs *excess-burst-size*: Specifies the EBS in bytes. The value range for *excess-burst-size* is 0 to 256000000, in increments of 512. If the PIR is configured, the default EBS is the product of 62.5 and the PIR and must be an integral multiple of 512. When the product is not an integral multiple of 512, it is rounded up to the nearest integral multiple of 512. A default value greater than 256000000 is converted to 256000000.

pir *peak-information-rate*: Specifies the PIR in kbps. The value range for *peak-information-rate* is 8 to 160000000.

green *action*: Specifies the action to take on packets that conform to CIR. The default setting is **pass**.

red *action*: Specifies the action to take on the packet that conforms to neither CIR nor PIR. The default setting is **discard**.

yellow *action*: Specifies the action to take on packets that conform to PIR but not to CIR. The default setting is **pass**.

action: Specifies the action to take on packets:

- **discard**: Drops the packet.
- **pass**: Permits the packet to pass through.
- **remark-dot1p-pass** *new-cos*: Sets the 802.1p priority value of the 802.1p packet to *new-cos* and permits the packet to pass through. The *new-cos* argument is in the range of 0 to 7.

- **remark-dscp-pass** *new-dscp*: Remarks the packet with a new DSCP value and permits the packet to pass through. The *new-dscp* argument is in the range of 0 to 63. Alternatively, you can specify the *new-dscp* argument with **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, **default**, or **ef**.

Usage guidelines

To use two rates for aggregate CAR, configure the **qos car** command with the **pir** *peak-information-rate* option. To use one rate for aggregate CAR, configure the **qos car** command without the **pir** *peak-information-rate* option.

An aggregate CAR action takes effect only after it is used in a QoS policy.

Examples

Configure aggregate CAR action **aggcar-1**, where CIR is 25600, CBS is 512000, and red packets are dropped.

```
<Sysname> system-view
[Sysname] qos car aggcar-1 aggregative cir 25600 cbs 512000 red discard
```

Related commands

display qos car name

reset qos car name

Use **reset qos car name** to clear the statistics about aggregate CAR actions.

Syntax

reset qos car name [*car-name*]

Views

User view

Predefined user roles

network-admin

Parameters

car-name: Specifies an aggregate CAR action by its name. This argument must start with a letter, and is a case-sensitive string of 1 to 31 characters. If you do not specify an aggregate CAR action, this command clears statistics for all aggregate CAR actions.

Examples

Clear the statistics about aggregate CAR action **aggcar-1**.

```
<Sysname> reset qos car name aggcar-1
```

Queue-based accounting commands

display qos queue-statistics interface outbound

Use **display qos queue-statistics interface outbound** to display outgoing traffic statistics collected for interfaces on a per-queue basis.

Syntax

display qos queue-statistics interface [*interface-type interface-number*] **outbound**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays the outgoing traffic statistics for all interfaces.

Examples

Display queue-based outgoing traffic statistics of GigabitEthernet 1/0/1.

```
<Sysname> display qos queue-statistics interface gigabitethernet 1/0/1 outbound
Interface: GigabitEthernet1/0/1
 Direction: outbound
Queue 0
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
  Green dropped: 0 packets, 0 bytes
…
Queue 7
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
```

Table 22 Command output

Field	Description
Interface	Interface for which queue-based traffic statistics are displayed.
Direction	Direction of traffic for which statistics are collected.
Forwarded	Counts forwarded traffic in both packets and bytes.
Dropped	Counts dropped traffic in both packets and bytes.
Current queue length	Current number of packets in a queue.

Related commands

`reset counters interface` (*Interface Command Reference*)

Contents

Data buffer commands

Inappropriate data buffer changes can cause system problems. Before manually changing data buffer settings, make sure you understand its impact on your device. As a best practice, use the **burst-mode enable** command if the system requires large buffer spaces. The **burst-mode enable** command and the **buffer apply** command are mutually exclusive. If you have configured the data buffer by using one command, you must execute the **undo** form of the command before using the other command.

buffer apply

Use **buffer apply** to apply manually configured data buffer settings.

Use **undo buffer apply** to restore the default.

Syntax

buffer apply

undo buffer apply

Views

System view

Predefined user roles

network-admin

Usage guidelines

For data buffer settings to take effect, you must execute this command after configuring data buffer settings.

After applying manually configured data buffer settings, you cannot directly modify the applied settings. To modify them, you must cancel the application, reconfigure data buffer settings, and reapply the new settings.

Examples

Apply manually configured data buffer settings.

```
<Sysname> system-view
[Sysname] buffer apply
```

buffer queue guaranteed

Use **buffer queue guaranteed** to set the fixed-area space for a queue.

Use **undo buffer queue guaranteed** to delete the fixed-area space setting of a queue.

Syntax

buffer egress [**slot** *slot-number*] **cell queue** *queue-id* **guaranteed ratio** *ratio*

undo buffer egress [**slot** *slot-number*] **cell queue** *queue-id* **guaranteed**

Default

The fixed-area ratio for a queue is 12%.

Views

System view

Predefined user roles

network-admin

Parameters

egress: Specifies the egress buffer.

slot *slot-number*: Specifies an IRF member device by its member ID (slot number). If you do not specify an IRF member device, this command applies to all IRF member devices.

cell: Specifies cell resources.

queue-id: Specifies a queue by its ID in the range of 0 to 7.

ratio *ratio*: Specifies the fixed-area space ratio, in percentage. The value range for *ratio* is 1 to 100.

Usage guidelines

By default, all queues have an equal share of the fixed area. You can set the fixed-area ratio for a queue. The other queues equally share the remaining part.

The fixed-area space for a queue cannot be used by other queues. Therefore, it is also called the minimum guaranteed buffer for the queue. The sum of fixed-area space configured for all queues cannot exceed the total fixed-area space. Otherwise, the configuration fails.

Examples

Configure queue 0 to use 20% fixed-area space of cell resources in the egress buffer.

```
<Sysname> system-view
[Sysname] buffer egress cell queue 0 guaranteed ratio 20
```

buffer shared

Use **buffer shared** to set the maximum shared-area ratio for each port or a queue.

Use **undo buffer shared** to delete the maximum shared-area ratio setting of each port or a queue.

Syntax

buffer egress [**slot** *slot-number*] **cell** [**queue** *queue-id*] **shared ratio** *ratio*

undo buffer egress [**slot** *slot-number*] **cell** [**queue** *queue-id*] **shared**

Default

The maximum shared-area ratio for a queue is 33%.

Views

System view

Predefined user roles

network-admin

Parameters

egress: Specifies the egress buffer.

slot *slot-number*: Specifies an IRF member device by its member ID (slot number). If you do not specify an IRF member device, this command applies to all IRF member devices.

cell: Specifies cell resources.

queue-id: Specifies a queue by its ID in the range of 0 to 7.

ratio *ratio*: Specifies the maximum shared-area space ratio, in percentage. The value range for *ratio* is 0 to 100.

Usage guidelines

By default, all ports or queueshave an equal share of the shared area. You can set the shared-area ratio for each port or a queue. The unconfigured queues use the default setting. The shared-area space for each port or queue is finally determined by the chip based on your configuration and the number of packets to be received and sent.

Examples

Configure queue 0 to use up to 10% shared-area space of cell resources in the egress buffer.

```
<Sysname> system-view
[Sysname] buffer egress cell queue 0 shared ratio 10
```

buffer total-shared

Use **buffer total-shared** to set the total shared-area ratio.

Use **undo buffer total-shared** to delete the total shared-area ratio setting.

Syntax

buffer egress [**slot** *slot-number*] **cell total-shared ratio** *ratio*

undo buffer egress [**slot** *slot-number*] **cell total-shared**

Default

The default for this command can be displayed by using the **display buffer** command.

Views

System view

Predefined user roles

network-admin

Parameters

egress: Specifies the egress buffer.

slot *slot-number*: Specifies an IRF member device by its member ID (slot number). If you do not specify an IRF member device, this command applies to all IRF member devices.

cell: Specifies cell resources.

ratio *ratio*: Specifies the ratio of the shared area, in percentage. The value range for *ratio* is 0 to 100.

Usage guidelines

After you set the shared-area ratio, the remaining buffer space is automatically assigned to the fixed area.

This command is not supported on a multichassis IRF fabric.

Examples

Configure the shared area to use 50% space of cell resources in the egress buffer.

```
<Sysname> system-view
[Sysname] buffer egress cell total-shared ratio 50
```

burst-mode enable

Use **burst-mode enable** to enable the Burst feature.

Use **undo burst-mode enable** to disable the Burst feature.

Syntax

burst-mode enable

undo burst-mode enable

Default

The Burst feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The Burst feature is especially useful for reducing packet losses under the following circumstances:

- Broadcast or multicast traffic is intensive, resulting in bursts of traffic.
- Traffic enters a device from a high-speed interface and goes out of a low-speed interface.
- Traffic enters a device from multiple same-rate interfaces and goes out of an interface with the same rate.

The default data buffer settings will be changed after the Burst feature is enabled. You can display the data buffer settings by using the **display buffer** command.

Examples

Enable the Burst feature.

```
<Sysname> system-view
[Sysname] burst-mode enable
```

display buffer

Use **display buffer** to display buffer size settings.

Syntax

display buffer [**slot** *slot-number*][**queue** [*queue-id*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID (slot number). If you do not specify an IRF member device, this command displays buffer size settings for all IRF member devices.

queue *queue-id*: Specifies a queue by its number in the range of 0 to 7. If you specify a queue, this command displays the fixed-area ratio and shared-area ratio for the specified queue. If you specify the **queue** keyword without the *queue-id* argument, this command displays the fixed-area ratio and shared-area ratio for each queue. If you do not specify the **queue** keyword, this command displays the total shared-area ratio.

Examples

Display buffer size settings.

```
<Sysname> display buffer
Slot  Type    Eg(Total-shared , Shared)
1     cell    79 , 33

          Eg: Size of the sending buffer
Total-shared: Size of the shared buffer for all ports
      Shared: Size of the maximum shared buffer per port
        Unit: Ratio
```

Display the fixed-area ratio and shared-area ratio for the queues.

```
<Sysname> display buffer queue
Slot  Queue        Type    Eg(Guaranteed , Shared)
1     0-7          cell    12 , 33

          Eg: Size of the sending buffer
  Guaranteed: Size of the minimum guaranteed buffer per queue
      Shared: Size of the maximum shared buffer per queue
        Unit: Ratio
```

Table 1 Command output

Field	Description
Type	Resource type.
Queue	Queue ID in the range of 0 to 7.
Eg	Egress buffer.
(Total-shared , Shared)	Total-shared indicates the total shared-area ratio. Shared indicates the shared-area ratio of a port.
(Guaranteed , Shared)	• **Guaranteed** indicates the fixed-area ratio of a queue. • **Shared** indicates the shared-area ratio of a queue.

display buffer usage

Use **display buffer usage** to display buffer usage.

Syntax

display buffer usage [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID (slot number). If you do not specify an IRF member device, this command displays buffer usage for all IRF member devices.

Examples

Display buffer usage.

```
<Sysname> display buffer usage
Egress total-shared cell buffer usage on slot 1 :
Total-shared:    2395 KB
Used-shared:       0 KB
Free-shared:    2395 KB
                                  5sec    1min    5min
-------------------------------------------------------------------
Block 1                             0%      0%      0%
Ten-GigabitEthernet1/0/1            0%      0%      0%
Ten-GigabitEthernet1/0/2            0%      0%      0%
Ten-GigabitEthernet1/0/3            0%      0%      0%
Ten-GigabitEthernet1/0/4            0%      0%      0%
Ten-GigabitEthernet1/0/5            0%      0%      0%
Ten-GigabitEthernet1/0/6            0%      0%      0%
Ten-GigabitEthernet1/0/7            0%      0%      0%
Ten-GigabitEthernet1/0/8            0%      0%      0%
Ten-GigabitEthernet1/0/9            0%      0%      0%
Ten-GigabitEthernet1/0/10           0%      0%      0%
Ten-GigabitEthernet1/0/11           0%      0%      0%
Ten-GigabitEthernet1/0/12           0%      0%      0%
Ten-GigabitEthernet1/0/13           0%      0%      0%
Ten-GigabitEthernet1/0/14           0%      0%      0%
Ten-GigabitEthernet1/0/15           0%      0%      0%
Ten-GigabitEthernet1/0/16           0%      0%      0%
Ten-GigabitEthernet1/0/17           0%      0%      0%
Ten-GigabitEthernet1/0/18           0%      0%      0%
Ten-GigabitEthernet1/0/19           0%      0%      0%
Ten-GigabitEthernet1/0/20           0%      0%      0%
Ten-GigabitEthernet1/0/21           0%      0%      0%
Ten-GigabitEthernet1/0/22           0%      0%      0%
Ten-GigabitEthernet1/0/23           0%      0%      0%
Ten-GigabitEthernet1/0/24           0%      0%      0%
```

Table 2 Command output

Field	Description
Egress total-shared cell buffer usage on slot	Usage of cell resources in the shared area on an IRF member device.
Unit	Chip number.

Field	Description
Block	Block where the port resides. The block where the ports on the front panel of the device reside is fixed to Block 1.
Total	Total size of the data buffer.
Used	Size of used data buffer.
Free	Size of free data buffer.
5sec	Percentage of the buffer that the port uses for the last 5 seconds.
1min	Percentage of the buffer that the port uses for the last 1 minute.
5min	Percentage of the buffer that the port uses for the last 5 minutes.

Contents

Time range commands

display time-range

Use **display time-range** to display time range configuration and status.

Syntax

display time-range { *time-range-name* | **all** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

time-range-name: Specifies a time range name, a case-insensitive string of 1 to 32 characters. It must start with an English letter.

all: Displays the configuration and status of all existing time ranges.

Examples

Display the configuration and status of time range **t4**.

```
<Sysname> display time-range t4
Current time is 17:12:34 11/23/2010 Tuesday

Time-range : t4 (Inactive)
 10:00 to 12:00 Mon
 14:00 to 16:00 Wed
 from 00:00 1/1/2011 to 00:00 1/1/2012
 from 00:00 6/1/2011 to 00:00 7/1/2011
```

Table 1 Command output

Field	Description
Current time	Current system time.
Time-range	Configuration and status of the time range, including its name, status (active or inactive), and start time and end time.

time-range

Use **time-range** to create or edit a time range.

Use **undo time-range** to delete a time range or a statement in the time range.

Syntax

time-range *time-range-name* { *start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2* }

undo time-range *time-range-name* [*start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2*]

Default

No time ranges exist.

Views

System view

Predefined user roles

network-admin

Parameters

time-range-name: Specifies a time range name. The name is a case-insensitive string of 1 to 32 characters. It must start with an English letter. To avoid confusion, it cannot be **all**.

start-time **to** *end-time*: Specifies a periodic statement. Both *start-time* and *end-time* are in hh:mm format (24-hour clock). The value is in the range of 00:00 to 23:59 for the start time, and 00:00 to 24:00 for the end time. The end time must be later than the start time.

days: Specifies the day or days of the week (in words or digits) on which the periodic statement is valid. If you specify multiple values, separate each value with a space, and make sure they do not overlap. These values can take one of the following forms:

- A digit in the range of 0 to 6, for Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday.
- A day of a week in abbreviated words: **Sun**, **Mon**, **Tue**, **Wed**, **Thu**, **Fri**, and **Sat**.
- **working-day** for Monday through Friday.
- **off-day** for Saturday and Sunday.
- **daily** for the whole week.

from *time1 date1*: Specifies the start time and date of an absolute statement. The *time1* argument specifies the time of the day in hh:mm format (24-hour clock). Its value is in the range of 00:00 to 23:59. The *date1* argument specifies a date in MM/DD/YYYY or YYYY/MM/DD format, where MM is the month of the year in the range of 1 to 12, DD is the day of the month with the range varying by MM, and YYYY is the year in the calendar in the range of 1970 to 2100. If you do not specify this option, the start time is 01/01/1970 00:00 AM, the earliest time available in the system.

to *time2 date2*: Specifies the end time and date of the absolute time statement. The *time2* argument has the same format as the *time1* argument, but its value is in the range of 00:00 to 24:00. The *date2* argument has the same format and value range as the *date1* argument. The end time must be later than the start time. If you do not specify this option, the end time is 12/31/2100 24:00 PM, the maximum time available in the system.

Usage guidelines

If an existing time range name is provided, this command adds a statement to the time range.

You can create multiple statements in a time range. Each time statement can take one of the following forms:

- Periodic statement in the *start-time* **to** *end-time days* format. A periodic statement recurs periodically on a day or days of the week.
- Absolute statement in the **from** *time1 date1* **to** *time2 date2* format. An absolute statement does not recur.
- Compound statement in the *start-time* **to** *end-time days* **from** *time1 date1* **to** *time2 date2* format. A compound statement recurs on a day or days of the week only within the specified period. For example, to create a time range that is active from 08:00 to 12:00 on

Monday between January 1, 2015, 00:00 and December 31, 2015, 23:59, use the **time-range test 08:00 to 12:00 Mon from 00:00 01/01/2015 to 23:59 12/31/2015** command.

You can create a maximum of 1024 time ranges, each with a maximum of 32 periodic statements and 12 absolute statements. The active period of a time range is calculated as follows:

1. Combining all periodic statements.
2. Combining all absolute statements.
3. Taking the intersection of the two statement sets as the active period of the time range.

Examples

Create a periodic time range **t1**, setting it to be active between 8:00 to 18:00 during working days.

```
<Sysname> system-view
[Sysname] time-range t1 08:00 to 18:00 working-day
```

Create an absolute time range **t2**, setting it to be active in the whole year of 2011.

```
<Sysname> system-view
[Sysname] time-range t2 from 00:00 1/1/2011 to 24:00 12/31/2011
```

Create a compound time range **t3**, setting it to be active from 08:00 to 12:00 on Saturdays and Sundays of the year 2011.

```
<Sysname> system-view
[Sysname] time-range t3 08:00 to 12:00 off-day from 00:00 1/1/2011 to 24:00 12/31/2011
```

Create a compound time range **t4**, setting it to be active from 10:00 to 12:00 on Mondays and from 14:00 to 16:00 on Wednesdays in January and June of the year 2011.

```
<Sysname> system-view
[Sysname] time-range t4 10:00 to 12:00 1 from 00:00 1/1/2011 to 24:00 1/31/2011
[Sysname] time-range t4 14:00 to 16:00 3 from 00:00 6/1/2011 to 24:00 6/30/2011
```

Related commands

display time-range