Hewlett Packard Enterprise

HPE FlexNetwork MSR Router Series

Comware 7 ACL and QoS Command Reference

Part number: 5998-6932
Software version: CMW710-R0403L02
Document version: 6PW200-20160226

Acknowledgments

Contents

ACL commands

Commands and descriptions for centralized devices apply to the following routers:

- MSR1002-4/1003-8S.
- MSR2003.
- MSR2004-24/2004-48.
- MSR3012/3024/3044/3064.
- MSR954(JH296A/JH297A/JH298A/JH299A)

Commands and descriptions for distributed devices apply to MSR4060 and MSR4080 routers.

accelerate

Use **accelerate** to enable ACL acceleration for an ACL.

Use **undo accelerate** to disable ACL acceleration.

Syntax

accelerate

undo accelerate

Default

ACL acceleration is disabled.

Views

IPv4 basic/advanced ACL view

IPv6 basic/advanced ACL view

Layer 2 ACL view

Predefined user roles

network-admin

Usage guidelines

This command does not take effect if the hardware resources are insufficient. When the hardware resources become sufficient, the following operations will make ACL acceleration take effect:

- Execute the **accelerate** command again.
- Modify, add, or delete rules for the ACL.

You can modify, add, or delete rules for an accelerated ACL. The rule adding or modification operation fails if the hardware resources are insufficient. The failure does not affect the accelerated ACL.

Examples

Enable ACL acceleration for ACL 2000.

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

Related commands

display acl accelerate

acl

Use **acl** to create an ACL, and enter its view. If the ACL has already been created, the command only places you in the ACL view.

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

Syntax

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 ACL exists.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6: Specifies the IPv6 ACL type. To specify the IPv4 ACL type, do not provide 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.

- 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. The depth-first order varies by ACL type. For more information, see *ACL and QoS Configuration Guide*.
- **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

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

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 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 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.

- 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 ACL you are creating. This number must be from the same ACL type as the source ACL. Available value ranges include:

- 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 ACL you are creating. 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 has the same properties and content as the source ACL, but uses a different number or name than the source ACL.

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

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 interval

Use **acl** { **logging** | **trap** } **interval** to enable logging or SNMP notifications for packet filtering, and set the interval.

Use **undo acl** { **logging** | **trap** } **interval** to restore the default.

Syntax

acl { **logging** | **trap** } **interval** *interval*

undo acl { **logging** | **trap** } **interval**

Default

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

Views

System view

Predefined user roles

network-admin

Parameters

logging: Enables logging and sends the log entries to the information center. For information about the information center, see *Network Management and Monitoring Configuration Guide*.

trap: Enables SNMP notifications and sends the traps to the SNMP module. For information about SNMP, see *Network Management and Monitoring Configuration Guide*.

interval *interval*: Sets the interval in minutes. It must be a multiple of 5, in the range of 0 to 1440. To disable the logging or notification, set the value to 0.

Usage guidelines

The logging or SNMP notifications is available for IPv4, IPv6, and Layer 2 ACL rules that have the **logging** keyword.

The device generates log entries or SNMP traps for packet filtering and outputs them at the configured interval. If an ACL is matched for the first time, the device immediately outputs a log entry or trap instead of waiting for the next output time.

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)
- **rule** (Layer 2 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 has no description.

Views

IPv4 basic/advanced ACL view

IPv6 basic/advanced ACL view

Layer 2 ACL view

Predefined user roles

network-admin

Parameters

text: Configures a description for the ACL, 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.

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

all: Displays information about 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 rules, match-order is auto,
This is an IPv4 basic ACL.
ACL's step is 5
ACL accelerated
 rule 5 permit source 1.1.1.1 0 (5 times matched)
 rule 5 comment This rule is used on GigabitEthernet 2/0/1.
```

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 rules	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 present when the match order is **config**.
This is an IPv4 basic ACL.	Description of this ACL.
ACL's step is 5	The rule numbering step is 5.
ACL accelerated	ACL acceleration is enabled for the ACL.
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.
5 times matched	There have been five matches for the rule. The statistic counts only ACL matches performed in software. This field is not displayed when no packets matched the rule.

rule 5 comment This rule is used on GigabitEthernet 2/0/1.	Comment of ACL rule 5.

display acl accelerate

Use **display acl accelerate** to display ACL acceleration status.

Syntax

Centralized devices in standalone mode:

display acl accelerate { **summary** [**ipv6** | **mac**] | **verbose** [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* } }

Distributed devices in standalone mode/centralized devices in IRF mode:

display acl accelerate { **summary** [**ipv6** | **mac**] | **verbose** [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* } **slot** *slot-number* }

Distributed devices in IRF mode:

display acl accelerate { **summary** [**ipv6** | **mac**] | **verbose** [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* } **chassis** *chassis-number* **slot** *slot-number* }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

summary: Displays summary information about ACL acceleration status.

verbose: Displays detailed information about ACL acceleration status.

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 a card by its slot number. The specified card must be the card where the acceleration chip resides. (Distributed devices in standalone mode.)

slot *slot-number*: Specifies an IRF member device. The *slot-number* argument represents the ID of the IRF member device. The specified device must be the device where the acceleration chip resides. (Centralized devices in IRF mode.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on an IRF member device. The *chassis-number* argument represents the ID of the IRF member device. The *slot-number* argument represents the number of the slot that holds the card. The specified card must be the card where the acceleration chip resides. (Distributed devices in IRF mode.)

Usage guidelines

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

Examples

Display summary information about ACL acceleration status.

```
<Sysname> display acl accelerate summary
Basic IPv4 ACL 2000
ACL named acl.
```

Display detailed information about ACL acceleration status.

```
<Sysname> display acl accelerate verbose 2000
Basic IPv4 ACL 2000.
 rule 0 permit
 rule 1 deny (failed)
```

Table 2 Command output

Field	Description
failed	ACL acceleration for the rule failed, and the rule is not effective.

display packet-filter

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

Syntax

Centralized devices in standalone mode:

display packet-filter { **interface** [*interface-type interface-number*] [**inbound** | **outbound**] | **zone-pair security** [**source** *source-zone-name* **destination** *destination-zone-name*] }

Distributed devices in standalone mode/centralized devices in IRF mode:

display packet-filter { **interface** [*interface-type interface-number*] [**inbound** | **outbound**] | **zone-pair security** [**source** *source-zone-name* **destination** *destination-zone-name*] [**slot** *slot-number*] }

Distributed devices in IRF mode:

display packet-filter { **interface** [*interface-type interface-number*] [**inbound** | **outbound**] | **zone-pair security** [**source** *source-zone-name* **destination** *destination-zone-name*] [**chassis** *chassis-number* **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.

zone-pair security [**source** *source-zone-name* **destination** *destination-zone-name*]: Specifies a zone pair. The *source-zone-name* argument specifies a source security zone by its name. The *destination-zone-name* argument specifies a destination security zone by its name. A security zone name is a case-insensitive string of 1 to 31 characters.

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command displays ACL application information for packet filtering for the active MPU. (Distributed devices in standalone mode.)

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. (Centralized devices in IRF mode.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. If you do not specify a card, this command displays ACL application information for packet filtering for the global active MPU. (Distributed devices in IRF mode.)

Usage guidelines

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

If no source and destination security zones are specified, this command displays ACL application information about all zone pairs.

Examples

Display ACL application information for inbound packet filtering on interface GigabitEthernet 2/0/1.

```
<Sysname> display packet-filter interface gigabitethernet 2/0/1 inbound
Interface: GigabitEthernet2/0/1
 In-bound policy:
  IPv4 ACL 2001
  IPv6 ACL 2002 (Failed)
  MAC ACL 4003 (Failed)
  IPv4 ACL 2004
  IPv4 default action: Deny, Hardware-count
```

Display ACL application information for packet filtering from source security zone **office** to destination security zone **library**.

```
<Sysname> display packet-filter zone-pair security source office destination library
Zone-pair: source office destination library
  IPv4 ACL 2001
  IPv4 ACL 2002
```

Table 3 Command output

Field	Description
Interface	Interface to which the ACL applies.
Zone-pair	Zone pair to which the ACL applies.
In-bound policy	ACL used for filtering incoming traffic.
Out-bound 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.

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. • **Hardware-count**—The **hardware-count** feature has been successfully applied for the default action for packet filtering. • **Hardware-count (Failed)**—The device has failed to apply the **hardware-count** feature for the packet filtering default action.
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. • **Hardware-count**—The **hardware-count** feature has been successfully applied for the default action for packet filtering. • **Hardware-count (Failed)**—The device has failed to apply the **hardware-count** feature for the packet filtering default action.
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. • **Hardware-count**—The **hardware-count** feature has been successfully applied for the default action for packet filtering. • **Hardware-count (Failed)**—The device has failed to apply the **hardware-count** feature for the packet filtering default action.

display packet-filter statistics

Use **display packet-filter statistics** to display packet filtering statistics and default action statistics.

Syntax

display packet-filter statistics { **interface** *interface-type interface-number* { **inbound** | **outbound** } [**default** | [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }] | **zone-pair security source** *source-zone-name* **destination** *destination-zone-name* [[**ipv6**] { *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.

zone-pair security source *source-zone-name* **destination** *destination-zone-name*: Specifies a zone pair. The *source-zone-name* argument specifies a source security zone by its name. The *destination-zone-name* argument specifies a destination security zone by its name. A security zone name is a case-insensitive string of 1 to 31 characters.

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

default: Displays the default action statistics for packet filtering.

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.

When **default**, *acl-number*, **name** *acl-name*, **ipv6**, and **mac** are not specified, this command displays packet filtering statistics for all ACLs and default action statistics.

Examples

Display packet filtering statistics for all ACLs and default action statistics on incoming packets of GigabitEthernet 2/0/1.

```
<Sysname> display packet-filter statistics interface gigabitethernet 2/0/1 inbound
Interface: GigabitEthernet2/0/1
 In-bound policy:
  IPv4 ACL 2001
   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)
   rule 10 permit vpn-instance test
   Totally 2 packets permitted, 0 packets denied
   Totally 100% permitted, 0% denied

  IPv4 ACL 2002 (Failed)

  MAC ACL 4000
   From 2011-06-04 10:25:34 to 2011-06-04 10:35:57
   rule 0 permit
```

```
IPv6 ACL 2000

IPv4 default action: Deny, Hardware-count
 From 2011-06-04 10:25:21 to 2011-06-04 10:35:57
 Totally 7 packets

IPv6 default action: Deny, Hardware-count
 From 2011-06-04 10:25:41 to 2011-06-04 10:35:57
 Totally 0 packets

MAC default action: Deny, Hardware-count
 From 2011-06-04 10:25:34 to 2011-06-04 10:35:57
 Totally 0 packets
```

Display packet filtering statistics for IPv4 advanced ACL 3001 on packets from source security zone **office** to destination security zone **library**.

```
<Sysname> display packet-filter statistics zone-pair security source office destination library 3001
Zone-pair: source office destination library
IPv4 ACL 3001
   rule 0 permit source 2.2.2.2 0
   rule 5 permit source 1.1.1.1 0 counting (2 packets)
   rule 10 permit vpn-instance test (Failed)
   Totally 2 packets permitted, 0 packets denied
   Totally 100% permitted, 0% denied
```

Table 4 Command output

Field	Description
Interface	Interface to which the ACL applies.
Zone-pair	Zone pair to which the ACL applies.
In-bound policy	ACL used for filtering incoming traffic.
Out-bound 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.
From 2011-06-04 10:25:21 to 2011-06-04 10:35:57	Start time and end time of the statistics.
2 packets	Two packets matched the rule. This field is not displayed when no packets matched the rule.
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. • **Hardware-count**—The **hardware-count** feature has been successfully applied for the default action for packet filtering. • **Hardware-count (Failed)**—The device has failed to apply the **hardware-count** feature for the packet filtering default action.
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. • **Hardware-count**—The **hardware-count** feature has been successfully applied for the default action for packet filtering. • **Hardware-count (Failed)**—The device has failed to apply the **hardware-count** feature for the packet filtering default action.
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. • **Hardware-count**—The **hardware-count** feature has been successfully applied for the default action for packet filtering. • **Hardware-count (Failed)**—The device has failed to apply the **hardware-count** feature for the packet filtering default action.
Totally 7 packets	The default action has been executed on seven packets.

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:
 In-bound policy:
  IPv4 ACL 2001
   rule 0 permit source 2.2.2.2 0 (2 packets)
   rule 5 permit source 1.1.1.1 0
   rule 10 permit vpn-instance test
   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 5 Command output

Field	Description
Sum	Accumulated packet filtering ACL statistics.
In-bound policy	Accumulated ACL statistics used for filtering incoming traffic.
Out-bound policy	Accumulated ACL statistics used for filtering outgoing traffic.
IPv4 ACL 2001	Accumulated ACL statistics used for 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.

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

Centralized devices in standalone mode:

display packet-filter verbose { **interface** *interface-type interface-number* { **inbound** | **outbound** } [[**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }] | **zone-pair security source** *source-zone-name* **destination** *destination-zone-name* [[**ipv6**] { *acl-number* | **name** *acl-name* }] }

Distributed devices in standalone mode/centralized devices in IRF mode:

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

Distributed devices in IRF mode:

display packet-filter verbose { **interface** *interface-type interface-number* { **inbound** | **outbound** } [[**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }] | **zone-pair security source** *source-zone-name* **destination** *destination-zone-name* [[**ipv6**] { *acl-number* | **name** *acl-name* }] } [**chassis** *chassis-number* **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.

zone-pair security source *source-zone-name* **destination** *destination-zone-name*: Specifies a zone pair. The *source-zone-name* argument specifies a source security zone by its name. The *destination-zone-name* argument specifies a destination security zone by its name. A security zone name is a case-insensitive string of 1 to 31 characters.

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 a card by its slot number. If you do not specify a card, this command displays ACL application details for packet filtering for the active MPU. (Distributed devices in standalone mode.)

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. (Centralized devices in IRF mode.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. If you do not specify a card, this command displays ACL application details for packet filtering for the global active MPU. (Distributed devices in IRF mode.)

Usage guidelines

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

When *acl-number*, **name** *acl-name*, **ipv6**, and **mac** are not specified, this command displays application details of all ACLs for packet filtering.

Examples

Display application details of all ACLs for inbound packet filtering on GigabitEthernet 2/0/1.

```
<Sysname> display packet-filter verbose interface gigabitethernet 2/0/1 inbound
Interface: GigabitEthernet2/0/1
 In-bound 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
   rule 0 permit

  MAC ACL 4000

  IPv4 default action: Deny, Hardware-count (Failed)

  IPv6 default action: Deny, Hardware-count (Failed)

  MAC default action: Deny, Hardware-count (Failed)
```

Display application details of all ACLs for packet filtering from source security zone **office** to destination security zone **library**.

```
<Sysname> display packet-filter verbose zone-pair security source office destination
library
Zone-pair: source office destination library
  IPv4 ACL 2001
   rule 0 permit
   rule 5 permit source 1.1.1.1 0
   rule 10 permit vpn-instance test
```

Table 6 Command output

Field	Description
Interface	Interface to which the ACL applies.
Zone-pair	Zone pair to which the ACL applies.
In-bound policy	ACL used for filtering incoming traffic.
Out-bound 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.
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. • **Hardware-count**—The **hardware-count** feature has been successfully applied for the default action for packet filtering. • **Hardware-count (Failed)**—The device has failed to apply the **hardware-count** feature for the packet filtering default action.
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. • **Hardware-count**—The **hardware-count** feature has been successfully applied for the default action for packet filtering. • **Hardware-count (Failed)**—The device has failed to apply the **hardware-count** feature for the packet filtering default action.
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. • **Hardware-count**—The **hardware-count** feature has been successfully applied for the default action for packet filtering. • **Hardware-count (Failed)**—The device has failed to apply the **hardware-count** feature for the packet filtering default action.

packet-filter (interface view)

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

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

Syntax

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

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

Default

An interface does not filter packets.

Views

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.

Usage guidelines

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

Examples

Apply IPv4 basic ACL 2001 to filter incoming traffic on GigabitEthernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] packet-filter 2001 inbound
```

Related commands

- **display packet-filter**
- **display packet-filter statistics**
- **display packet-filter verbose**

packet-filter (zone pair view)

Use **packet-filter** to apply an ACL to a zone pair to filter packets.

Use **undo packet-filter** to remove an ACL application from a zone pair.

Syntax

packet-filter [**ipv6**] { *acl-number* | **name** *acl-name* }

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

Default

A zone pair does not filter packets.

Views

Zone pair view

Predefined user roles

network-admin

Parameters

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

acl-number: Specifies an ACL by its number:

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

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

Examples

Apply IPv4 basic ACL 2002 to filter traffic from source security zone **office** to destination security zone **library**.

```
<Sysname> system-view
[Sysname] zone-pair security source office destination library
[Sysname-zone-pair-security-office-library] packet-filter 2002
```

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 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 default hardware-count

Use **packet-filter default hardware-count** to enable hardware-count for the packet filtering default action.

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

Syntax

packet-filter default { **inbound** | **outbound** } **hardware-count**

undo packet-filter default { **inbound** | **outbound** } **hardware-count**

Default

Hardware-count is disabled for the packet filtering default action.

Views

Interface view

Predefined user roles

network-admin

Parameters

inbound: Specifies the incoming packets.

outbound: Specifies the outgoing packets.

Usage guidelines

To enable hardware-count for the packet filtering default action on an interface, make sure you have applied ACLs to the interface for packet filtering.

Examples

Set the packet filtering default action to **deny** globally. Apply IPv4 basic ACL 2001 to GigabitEthernet 2/0/1 for filtering incoming packets, and enable hardware-count for the packet filtering default action on GigabitEthernet 2/0/1.

```
<Sysname> system-view
[Sysname] packet-filter default deny
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] packet-filter 2001 inbound
[Sysname-GigabitEthernet2/0/1] packet-filter default inbound hardware-count
```

Related commands

- **packet-filter**
- **packet-filter default deny**
- **display packet-filter**
- **display packet-filter statistics**

reset acl counter

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

Syntax

reset acl counter [**ipv6** | **mac**] { *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

To specify the IPv4 ACL type, do not specify 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 (including the accumulated statistics) for an ACL and the default action statistics.

Syntax

reset packet-filter statistics { **interface** [*interface-type interface-number*] { **inbound** | **outbound** } [**default** | [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }] | **zone-pair security** [**source** *source-zone-name* **destination** *destination-zone-name*] [**ipv6**] { *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.

zone-pair security [**source** *source-zone-name* **destination** *destination-zone-name*]: Specifies a zone pair. The *source-zone-name* argument specifies a source security zone by its name. The *destination-zone-name* argument specifies a destination security zone by its name. A security zone name is a case-insensitive string of 1 to 31 characters.

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

default: Clears the default action statistics for packet filtering.

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

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

When **default**, *acl-number*, **name** *acl-name*, **ipv6**, and **mac** are not specified, this command clears the packet filtering statistics for all ACLs and the default action statistics.

If no source and destination security zones are specified, this command clears statistics of packet filtering ACLs on all zone pairs.

Examples

Clear IPv4 basic ACL 2001 statistics for inbound packet filtering on GigabitEthernet 2/0/1.

```
<Sysname> reset packet-filter statistics interface gigabitethernet 2/0/1 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* | **vpn-instance** *vpn-instance-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** | **vpn-instance**] *

Default

An IPv4 advanced ACL does not contain any rule.

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 0. 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 one of the following values:

- A protocol number in the range of 0 to 255.
- A protocol by its name: **gre** (47), **icmp** (1), **igmp** (2), **ip**, **ipinip** (4), **ospf** (89), **tcp** (6), or **udp** (17). The **ip** keyword specifies all protocols.

Table 7 describes the parameters that you can specify regardless of the value for the *protocol* argument.

Table 7 Match criteria and other rule information for IPv4 advanced ACL rules

Parameters	Function	Description
source { *source-address source-wildcard* | **any** }	Specifies source addresses.	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 destination addresses.	The *dest-address dest-wildcard* arguments specify a destination IP address and a wildcard mask in dotted decimal notation. An all-zero wildcard represents a host address. The **any** keyword represents any destination IP address.
counting	Counts the times that the rule is matched.	If the **counting** keyword is not specified, matches for the rule are not counted.
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 non-first fragments.	If you do not specify this keyword, the rule applies to all fragments and non-fragments.
logging	Logs matching packets.	This function 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*.
vpn-instance *vpn-instance-name*	Applies the rule to a VPN instance.	The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the rule applies only to non-VPN packets.

If the *protocol* argument is **tcp** (6) or **udp** (7), set the parameters shown in Table 8.

Table 8 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), **neq** (not 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** (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).
destination-port *operator port1* [*port2*]	Specifies one or more UDP or TCP destination ports.	
{ **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 ORed. For example, a rule configured with **ack** 0 **psh** 1 matches both packets that have the ACK flag bit not set and packets that have the PSH flag bit set.
established	Specifies the flags for indicating the established status of a TCP	Parameter specific to TCP. The rule matches TCP connection packets with the ACK or RST flag bit set.

	connection.	

If the *protocol* argument is **icmp** (1), set the parameters shown in Table 9.

Table 9 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 10.

Table 10 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
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 you do not specify any optional keywords, the **undo rule** command deletes the entire rule.
- If you specify optional keywords or arguments, the **undo rule** command deletes the specified attributes.

To view rules in an ACL and their rule IDs, use the **display acl all** 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* | **vpn-instance** *vpn-instance-name*] *

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

Default

An IPv4 basic ACL does not contain any rule.

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 0. 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: Counts the times that the rule is matched. If the **counting** keyword is not specified, matches for the rule are not counted.

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

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

source { *source-address source-wildcard* | **any** }: Matches source addresses. The *source-address* and *source-wildcard* arguments specify a source IP address and a wildcard mask in dotted decimal notation. An all-zero wildcard mask 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*.

vpn-instance *vpn-instance-name*: Applies the rule to a VPN instance. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the rule applies only to non-VPN packets.

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 you do not specify any optional keywords, the **undo rule** command deletes the entire rule.
- If you specify optional keywords or arguments, the **undo rule** command deletes the specified attributes.

To view rules in an ACL and their rule IDs, use the **display acl all** command.

Examples

Create a rule in IPv4 basic ACL 2000 to deny the packets from any source IP segment 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 port1* [*port2*] | **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 port1* [*port2*] | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-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** | **vpn-instance**] *

Default

An IPv6 advanced ACL does not contain any rule.

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 0. 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 one of the following values:

- A protocol number in the range of 0 to 255.
- A protocol name: **gre** (47), **icmpv6** (58), **ipv6**, **ipv6-ah** (51), **ipv6-esp** (50), **ospf** (89), **tcp** (6), or **udp** (17). The **ipv6** keyword specifies all protocols.

Table 11 describes the parameters that you can specify regardless of the value for the *protocol* argument.

Table 11 Match criteria and other rule information for IPv6 advanced ACL rules

Parameters	Function	Description
source	Specifies source IPv6	The *source-address* argument specifies an IPv6 source

{ *source-address source-prefix* | *source-address/source-prefix* | **any** }	addresses.	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 destination IPv6 addresses.	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	Counts the times that the rule is matched.	If the **counting** keyword is not specified, matches for the rule are not counted.
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).
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 non-first fragments.	If you do not specify this keyword, the rule applies to all fragments and non-fragments.
logging	Logs matching packets.	This function 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 do not specify the **type** *routing-type* option, the rule applies to all types of IPv6 routing header.
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. Otherwise, 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*.
vpn-instance *vpn-instance-name*	Applies the rule to a VPN instance.	The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the rule applies only to non-VPN packets.

If the *protocol* argument is **tcp** (6) or **udp** (17), set the parameters shown in Table 12.

Table 12 TCP/UDP-specific parameters for IPv6 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), **neq** (not equal to), or **range** (inclusive range).

destination-port *operator port1* [*port2*]	Specifies one or more UDP or TCP destination ports.	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** (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 ORed. For example, a rule configured with **ack** 0 **psh** 1 matches both packets that have the ACK flag bit not set and packets that have 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 **icmpv6** (58), set the parameters shown in Table 13.

Table 13 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 14.

Table 14 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
unknown-next-hdr	4	1

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 you do not specify any optional keywords, the **undo rule** command deletes the entire rule.
- If you specify optional keywords or arguments, the **undo rule** command deletes the specified attributes.

To view rules in an ACL and their rule IDs, use the **display acl ipv6 all** 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* | **vpn-instance** *vpn-instance-name*] *

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

Default

An IPv6 basic ACL does not contain any rule.

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 0. 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: Counts the times that the rule is matched. If the **counting** keyword is not specified, matches for the rule are not counted.

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

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

routing [**type** *routing-type*]: Applies the rule to the specified type of routing header or all types of routing header. The *routing-type* argument specifies the value of the 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 routing header.

source { *source-address source-prefix* | *source-address*/*source-prefix* | **any** }: Matches source IPv6 addresses. 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*.

vpn-instance *vpn-instance-name*: Applies the rule to a VPN instance. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the rule applies only to non-VPN packets.

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 you do not specify any optional keywords, the **undo rule** command deletes the entire rule.
- If you specify optional keywords or arguments, the **undo rule** command deletes the specified attributes.

To view rules in an ACL and their rule IDs, use the **display acl ipv6 all** command.

Examples

Create an IPv6 basic ACL rule to deny the packets from any source IP segment 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 a Layer 2 ACL rule or some attributes in the rule.

Syntax

rule [*rule-id*] { **deny** | **permit** } [**cos** *vlan-pri* | **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**] *

Default

A Layer 2 ACL does not contain any rule.

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 0. 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 *vlan-pri:* 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: Counts the times that the rule is matched. If the **counting** keyword is not specified, matches for the rule are not counted.

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 16-bit hexadecimal number that represents the encapsulation format. The *lsap-type-mask* argument is a 16-bit hexadecimal number that represents the LSAP mask.

type *protocol-type protocol-type-mask*: Matches one or more protocols in the Layer 2. The *protocol-type* argument is a 16-bit hexadecimal number that represents a protocol type in Ethernet_II and Ethernet_SNAP frames. The *protocol-type-mask* argument is a 16-bit hexadecimal number that represents a protocol type mask.

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**.

- If you do not specify any optional keywords, the **undo rule** command deletes the entire rule.
- If you specify optional keywords or arguments, the **undo rule** command deletes the specified attributes.

To view rules in an ACL and their rule IDs, use the **display acl all** 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 add a comment about an existing ACL rule or edit its comment to make the rule easy to understand.

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.

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 GigabitEthernet 2/0/1.
```

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*

undo step

Default

The rule numbering step is five.

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.

Usage guidelines

The rule numbering step sets the increment by which the system numbers rules automatically. For example, the default ACL rule numbering step is 5. If you do not assign IDs to rules you are creating, they are numbered 0, 5, 10, 15, and so on.

The wider the numbering step, the more rules you can insert between two rules. Whenever the step changes, the rules are renumbered, starting from 0. For example, if there are five rules numbered 5, 10, 13, 15, and 20, 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

QoS policy commands

Commands and descriptions for centralized devices apply to the following routers:

- MSR1002-4/1003-8S.
- MSR2003.
- MSR2004-24/2004-48.
- MSR3012/3024/3044/3064.
- MSR954(JH296A/JH297A/JH298A/JH299A)

Commands and descriptions for distributed devices apply to MSR4060 and MSR4080 routers.

Traffic class commands

display traffic classifier

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

Syntax

Centralized devices in standalone mode:

display traffic classifier { **system-defined** | **user-defined** } [*classifier-name*]

Distributed devices in standalone mode/centralized devices in IRF mode:

display traffic classifier { **system-defined** | **user-defined** } [*classifier-name*] [**slot** *slot-number*]

Distributed devices in IRF mode:

display traffic classifier { **system-defined** | **user-defined** } [*classifier-name*] [**chassis** *chassis-number* **slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

system-defined: Specifies system-defined traffic classes.

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 a card by its slot number. If you do not specify a card, this command displays the traffic classes for the active MPU. (Distributed devices in standalone mode.)

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. (Centralized devices in IRF mode.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. If you do not specify this option, the command displays the traffic classes for the global active MPU. (Distributed devices in IRF mode.)

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 not protocol ipv6

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

Display the system-defined traffic class **default-class**.

```
<Sysname> display traffic classifier system-defined default-class

  System-defined classifier information:

   Classifier: default-class (ID 0)
     Operator: AND
     Rule(s) :
      If-match any
```

Table 15 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 [**not**] *match-criteria*

undo if-match [**not**] *match-criteria*

Default

No match criterion is configured.

Views

Traffic class view

Predefined user roles

network-admin

Parameters

not: Matches packets that do not conform to the specified criterion.

match-criteria: Specifies a match criterion. Table 16 shows the available match criteria.

Table 16 Available match criteria

Option	Description
acl [**ipv6**] { *acl-number* | **name** *acl-name* }	Matches an ACL. The value range for the *acl-number* argument is 2000 to 3999 for IPv4 ACLs and 2000 to 3999 for IPv6 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**.
app-group *group-name*	Matches an application group. The *group-name* argument specifies a system-defined application group by its name.
application *app-name*	Matches an application. The *app-name* argument specifies a system-defined application by its name.
any	Matches all packets.
classifier *classifier-name*	Matches a class. The *classifier-name* argument specifies a class by its name.
control-plane protocol *protocol-name*&<1-8>	Matches control plane protocols. The *protocol-name*&<1-8> argument specifies a space-separated list of up to eight system-defined control plane protocols. For available system-defined control plane protocols, see Table 17.
control-plane protocol-group *protocol-group-name*	Matches a control plane protocol group. The *protocol-group-name* argument can be **critical**, **important**, **management**, **monitor**, or **normal**.
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*	Matches a destination MAC address.

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 19.
inbound-interface *interface-type interface-number*	Matches an input interface specified by its type and number.
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.
local-precedence *local-precedence-value*&<1-8>	Matches local precedence values. The *local-precedence-value*&<1-8> argument specifies a space-separated list of up to eight local precedence values. The value range for the *local-precedence-value* argument is 0 to 7.
mpls-exp *exp-value*&<1-8>	Matches MPLS EXP values. The *exp-value*&<1-8> argument specifies a space-separated list of up to eight EXP values. The value range for the *exp-value* argument is 0 to 7.
packet-length { **min** *min-value* | **max** *max-value* } *	Matches the packet length. The *min-value* argument specifies the minimum packet length in bytes. The *max-value* argument specifies the maximum packet length in bytes.
protocol *protocol-name*	Matches a protocol. The *protocol-name* argument can be **arp**, **ip**, or **ipv6**.
qos-local-id *local-id-value*	Matches a local QoS ID in the range of 1 to 4095.
rtp start-port *start-port-number* **end-port** *end-port-number*	Matches RTP protocol ports. The value ranges for the *start-port-number* and *end-port-number* arguments are both 2000 to 65535. This criterion matches RTP packets with an even UDP destination port number in the specified RTP port number range.
source-mac *mac-address*	Matches a source MAC address.

Table 17 Available system-defined control plane protocols

Protocol	Description
default	Protocol packets other than the following packet types
arp	ARP packets
bgp	BGP packets
bgp4+	IPv6 BGP packets
ftp	FTP packets
http	HTTP packets
https	HTTPS packets
icmp	ICMP packets
icmpv6	ICMPv6 packets
igmp	IGMP packets
isis	IS-IS packets
ldp	LDP packets

ldp6	IPv6 LDP packets
msdp	MSDP packets
ntp	NTP packets
ospf-multicast	OSPF multicast packets
ospf-unicast	OSPF unicast packets
ospf3-multicast	OSPFv3 multicast packets
ospf3-unicast	OSPFv3 unicast packets
pim-multicast	PIM multicast packets
pim-unicast	PIM unicast packets
pim6-multicast	IPv6 PIM multicast packets
pim6-unicast	IPv6 PIM unicast packets
radius	RADIUS packets
rip	RIP packets
ripng	RIPng packets
rsvp	RSVP packets
snmp	SNMP packets
ssh	SSH packets
tacacs	TACACS packets
telnet	Telnet packets
tftp	TFTP packets
vrrp	VRRP packets
vrrp6	IPv6 VRRP packets

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

- If the ACL used as a match criterion does not exist, the traffic class cannot be applied to hardware.
- In a traffic class, you can add two **if-match** statements that use the same ACL as the match criterion. In one statement, specify the ACL by its name. In the other statement, specify the ACL by its number.
- If the ACL contains deny rules, the **if-match** command is ignored and the matching process continues.

The source MAC address and destination MAC address match criteria are applicable only to Ethernet interfaces.

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-match classifier classB
```

When you configure the packet length match criterion, follow these restrictions and guidelines:

- If you configure only the **min** *min-value* option, the match criterion matches packets longer than *min-value*.
- If you configure only the **max** *max-value* option, the match criterion matches packets shorter than *max-value*.
- If you configure both **min** *min-value* and **max** *max-value* (*max-value* must be greater than *min-value*), the match criterion matches packets longer than *min-value* and shorter than *max-value*.

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:
  - Control plane protocol.
  - 802.1p priority.
  - DSCP.
  - IP precedence.
  - Local precedence.
  - MPLS EXP.
  - 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 identical with those specified in the **if-match** command. The order of values can be different.

When you configure the MPLS EXP match criterion, follow these additional restrictions and guidelines:

- The MPLS EXP match criterion takes effect only on MPLS packets.
- For software forwarding QoS, MPLS packets do not support IP-related match criteria.

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 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 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 the 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
[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
[Sysname-classifier-class1] if-match ip-precedence 1 6
```

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

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match local-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 the RTP packets with even UDP destination port numbers in the range of 16384 to 32767.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match rtp start-port 16384 end-port 32767
```

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
```

```
[Sysname-classifier-class1] if-match customer-vlan-id 1 6 9
```

Define a match criterion for traffic class **class1** to match the packets with a local QoS ID of 3.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match qos-local-id 3
```

Define a match criterion for traffic class **class1** to match the packets of the application group **multimedia**.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match app-group multimedia
```

Define a match criterion for traffic class **class1** to match the packets of the application **3link**.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match app-name 3link
```

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

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match control-plane protocol arp
```

Define a match criterion for traffic class **class1** to match packets of the protocols in protocol group **normal**.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match control-plane protocol-group normal
```

Define a match criterion for traffic class **class1** to match packets with the length in the range of 100 to 200 bytes.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match packet-length min 100 max 200
```

traffic classifier

Use **traffic classifier** to create a traffic class and enter traffic class view.

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 class exists.

Views

System view

Predefined user roles

network-admin

Parameters

classifier-name: Specifies the name of the traffic class to be created, 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 **class1**.

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

Related commands

display traffic classifier

Traffic behavior commands

car

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

Use **undo car** to delete the action.

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 8 to 10000000 kbps.

cbs *committed-burst-size*: Specifies the committed burst size (CBS) in the range of 1000 to 1000000000 bytes. The default is the amount of traffic transmitted at the rate of CIR over 500 milliseconds.

ebs *excess-burst-size*: Specifies the excess burst size (EBS) in the range of 0 to 1000000000 bytes. The default is 0.

pir *peak-information-rate*: Specifies the peak information rate (PIR) in the range of 8 to 10000000 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-mpls-exp-pass** *new-exp*: Sets the EXP field value of the MPLS packet to *new-exp* and permits the packet to pass through. The *new-exp* argument is in the range of 0 to 7.
- **remark-prec-pass** *new-precedence*: Sets the IP precedence of the packet to *new-precedence* and permits the packet to pass through. The *new-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.

A QoS policy that uses a traffic behavior configured with CAR can be applied in either the inbound direction or outbound direction of an interface.

If you configure 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 50000 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 50000 ebs 0 green pass red remark-dscp-pass
0
```

car percent

Use **car percent** to configure a CAR action in percentage in a traffic behavior.

Use **undo car** to delete the action.

Syntax

car cir percent *cir-percent* [**cbs** *cbs-time* [**ebs** *ebs-time*]] [**green** *action* | **red** *action* | **yellow** *action*] *

car cir percent *cir-percent* [**cbs** *cbs-time*] **pir percent** *pir-percent* [**ebs** *ebs-time*] [**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 percent *cir-percent*: Specifies the CIR in percentage, in the range of 1 to 100.

cbs *cbs-time*: Specifies the CBS in milliseconds. The actual CBS value is *cbs-time* × the actual CIR value.

ebs e*bs-time*: Specifies the EBS in milliseconds. The actual EBS value is *ebs-time* × the actual CIR value.

pir percent *pir-percent*: Specifies the PIR in percentage, in the range of 1 to 100. The PIR value must be equal to or greater than the CIR value.

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

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

yellow *action*: Specifies the action to take on packets that conform to the PIR but not to the CIR. The default 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 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. 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**.
- **remark-mpls-exp-pass** *new-exp*: Sets the EXP field value of the MPLS packet to *new-exp* and permits the packet to pass through. The *new-exp* argument is in the range of 0 to 7.
- **remark-prec-pass** *new-precedence*: Sets the IP precedence of the packet to *new-precedence* and permits the packet to pass through. The *new-precedence* argument is in the range of 0 to 7.

Usage guidelines

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

A QoS policy that uses a traffic behavior configured with CAR can be applied in the inbound or outbound direction of an interface.

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

A QoS policy that uses a behavior configured with CAR in percentage can be applied only to interfaces.

The actual CIR value is *cir-percent* × bandwidth. The actual PIR value is *pir-percent* × bandwidth. In the policy nesting case, the bandwidth used for the CIR and PIR calculations is determined following these rules:

- The top policy uses the interface bandwidth.
- A child policy uses the CIR value in GTS configured in the behavior of the child policy.
- If the CIR value is not available in the behavior, the child policy uses the CIR value in GTS configured in the behavior of the higher-level policy.
- If the CIR value is not available in the behavior of the higher-level policy, the child policy uses the interface bandwidth.

Examples

Configure a CAR action in percentage in traffic behavior **database** with the following parameters:

- The CIR is 20%.
- The CBS is 100 milliseconds.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] car cir percent 20 cbs 100
```

display traffic behavior

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

Syntax

Centralized devices in standalone mode:

display traffic behavior { **system-defined** | **user-defined** } [*behavior-name*]

Distributed devices in standalone mode/centralized devices in IRF mode:

display traffic behavior { **system-defined** | **user-defined** } [*behavior-name*] [**slot** *slot-number*]

Distributed devices in IRF mode:

display traffic behavior { **system-defined** | **user-defined** } [*behavior-name*] [**chassis** *chassis-number* **slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

system-defined: Specifies system-defined traffic behaviors.

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 a card by its slot number. If you do not specify a card, this command displays traffic behaviors for the active MPU. (Distributed devices in standalone mode.)

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. (Centralized devices in IRF mode.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. If you do not specify this option, the command displays the traffic behaviors for the global active MPU. (Distributed devices in IRF mode.)

Examples

Display all user-defined traffic behaviors.

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

  User-defined behavior information:

    Behavior: 0 (ID 100)
      Expedited Forwarding:
        Bandwidth 200 (kbps) CBS 5000 (Bytes)

    Behavior: 1 (ID 101)
      Committed Access Rate:
        CIR 200 (kbps), CBS 50000 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : remark dscp default and pass
      Assured Forwarding:
        Bandwidth 200 (kbps)
        Discard Method: Tail

    Behavior: 2 (ID 102)
      Marking:
        Remark dscp af11

    Behavior: 3 (ID 103)
      -none-

    Behavior: 4 (ID 104)
      Flow based Weighted Fair Queue:
        Max number of hashed queues: 256
        Discard Method: DSCP based WRED
        Exponential Weight: 9
        DSCP Low   High  Dis-prob
        -------------------------
        0    10    30    10
        1    10    30    10
        2    10    30    10
        3    10    30    10
        4    10    30    10
        5    10    30    10
        6    10    30    10
        7    10    30    10
        8    10    30    10
        9    10    30    10
```

10	10	30	10
11	10	30	10
12	10	30	10
13	10	30	10
14	10	30	10
15	10	30	10
16	10	30	10
17	10	30	10
18	10	30	10
19	10	30	10
20	10	30	10
21	10	30	10
22	10	30	10
23	10	30	10
24	10	30	10
25	10	30	10
26	10	30	10
27	10	30	10
28	10	30	10
29	10	30	10
30	10	30	10
31	10	30	10
32	10	30	10
33	10	30	10
34	10	30	10
35	10	30	10
36	10	30	10
37	10	30	10
38	10	30	10
39	10	30	10
40	10	30	10
41	10	30	10
42	10	30	10
43	10	30	10
44	10	30	10
45	10	30	10
46	10	30	10
47	10	30	10
48	10	30	10
49	10	30	10
50	10	30	10
51	10	30	10
52	10	30	10
53	10	30	10
54	10	30	10
55	10	30	10
56	10	30	10
57	10	30	10

```
        58   10    30    10
        59   10    30    10
        60   10    30    10
        61   10    30    10
        62   10    30    10
        63   10    30    10
```

Display all system-defined traffic behaviors.

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

System-defined behavior information:

    Behavior: be (ID 0)
      -none-

    Behavior: af (ID 1)
      Assured Forwarding:
        Bandwidth 20 (%)
        Discard Method: Tail

    Behavior: ef (ID 2)
      Expedited Forwarding:
        Bandwidth 20 (%) Cbs-ratio 25

    Behavior: be-flow-based (ID 3)
      Flow based Weighted Fair Queue:
        Max number of hashed queues: 256
        Discard Method: IP Precedence based WRED
        Exponential Weight: 9
        Pre  Low   High  Dis-prob
        ------------------------
        0    10    30    10
        1    10    30    10
        2    10    30    10
        3    10    30    10
        4    10    30    10
        5    10    30    10
        6    10    30    10
        7    10    30    10
```

Table 18 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.
Assured Forwarding	Assure forwarding (AF) information.
Bandwidth	Bandwidth of the queue.
Filter enable	Traffic filtering action.
Remark mpls-exp	Action of setting the MPLS EXP value for packets.
Expedited Forwarding	Expedited forwarding (EF) information.
none	No other traffic behavior is configured.
Exponential Weight	Exponent for average queue size calculation
Pre	IP precedence.
Low	Lower threshold of the queue.
High	Upper threshold of the queue.
Dis-prob	Denominator for drop probability calculation.

filter

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

Use **undo filter** to delete the action.

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.

Examples

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

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

gts

Use **gts** to configure a GTS action in absolute value in a traffic behavior.

Use **undo gts** to delete the action.

Syntax

gts cir *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**queue-length** *queue-length*]

gts cir *committed-information-rate* [**cbs** *committed-burst-size*] **pir** *peak-information-rate* [**ebs** *excess-burst-size*] [**queue-length** *queue-length*]

undo gts

Default

No GTS action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

cir *committed-information-rate*: Sets the CIR in kbps, which specifies the average traffic rate.

cbs *committed-burst-size*: Sets the CBS in bytes, which specifies the size of bursty traffic when the actual average rate is not greater than CIR.

ebs *excess-burst-size*: Sets the EBS in the range of 0 to 1000000000 bytes. The default is 0.

pir *peak-information-rate*: Sets the PIR in kbps. The PIR cannot be smaller than the CIR.

queue-length *queue-length*: Sets the maximum queue length. The default is 50.

Usage guidelines

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

A QoS policy that uses a behavior configured with GTS can be applied only to the outbound direction of an interface.

A QoS policy that uses a behavior configured with GTS overwrites the **qos gts** command on the interface, if both are configured.

If this command is configured for the same traffic behavior multiple times, the most recent configuration takes effect.

Examples

Configure a GTS action in absolute value in traffic behavior **database**. The GTS parameters are as follows: CIR is 200 kbps, CBS is 50000 bytes, EBS is 0, and the maximum queue length is 100.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] gts cir 200 cbs 50000 ebs 0 queue-length 100
```

Related commands

gts percent

gts percent

Use **gts percent** to configure a GTS action in percentage in a traffic behavior.

Use **undo gts** to delete the action.

Syntax

gts percent cir *cir-percent* [**cbs** *cbs-time* [**ebs** *ebs-time*]] [**queue-length** *queue-length*]

undo gts

Default

No GTS action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

cir *cir-percent*: Specifies the CIR in percentage, in the range of 1 to 100. The actual CIR value is *cir-percent* × interface bandwidth.

cbs *cbs-time*: Specifies the CBS in milliseconds. The default *cbs-time* is 500 milliseconds. The actual CBS value is *cbs-time* × the actual CIR value.

ebs e*bs-time*: Specifies the EBS in milliseconds. The default *ebs-time* is 0 milliseconds. The actual EBS value is *ebs-time* × the actual CIR value.

queue-length *queue-length*: Specifies the maximum queue length. The default is 50.

Usage guidelines

A QoS policy that uses a behavior configured with GTS can be applied only to the outbound direction of an interface.

A QoS policy that uses a behavior configured with GTS overwrites the **qos gts** command on the interface, if both configured.

If this command is configured for the same traffic behavior multiple times, the most recent configuration takes effect.

Examples

Configure a GTS action in percentage in traffic behavior **database**. The GTS parameters are as follows: CIR is 50 and CBS is 200 ms.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] gts percent cir 50 cbs 200
```

Related commands

gts

redirect

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

Use **undo redirect** to delete the action.

Syntax

redirect interface *interface-type interface-number*

undo redirect interface *interface-type interface-number*

Default

No traffic redirecting action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Redirects traffic to an interface specified by its type and number. To redirect traffic to a tunnel interface, set the interface type to **tunnel**. To redirect traffic to a Layer 2 aggregate interface, set the interface type to **bridge-aggregation**. To redirect traffic to a Layer 3 aggregate interface, set the interface type to **route-aggregation**.

Examples

Configure redirecting traffic to GigabitEthernet 2/1/1 in the traffic behavior **database**.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] redirect interface gigabitethernet 2/1/1
```

Usage guidelines

This command is supported only on the following ports:

- Layer 2 Ethernet ports on Ethernet switching modules.
- Fixed Layer 2 Ethernet ports of the following routers:
  - MSR954(JH296A/JH297A/JH298A/JH299A).
  - MSR1002-4/1003-8S.
  - MSR2004-24/2004-48.

Related commands

- **classifier behavior**
- **qos policy**
- **traffic behavior**

remark dot1p

Use **remark dot1p** to configure an 802.1p priority marking action in a traffic behavior.

Use **undo remark dot1p** to delete the action.

Syntax

remark dot1p *dot1p-value*

undo remark dot1p

Default

No 802.1p priority marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

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

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
```

remark dscp

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

Use **undo remark dscp** to delete the action.

Syntax

remark dscp *dscp-value*

undo remark dscp

Default

No DSCP marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value, which can be a number from 0 to 63 or a keyword in Table 19.

Table 19 DSCP keywords and values

Keyword	DSCP value (binary)	DSCP value (decimal)
default	000000	0
af11	001010	10
af12	001100	12
af13	001110	14
af21	010010	18
af22	010100	20
af23	010110	22
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
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 ip-precedence

Use **remark ip-precedence** to configure an IP precedence marking action in a traffic behavior.

Use **undo remark ip-precedence** to delete the action.

Syntax

remark ip-precedence *ip-precedence-value*

undo remark ip-precedence

Default

No IP precedence marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

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

Examples

Set the IP precedence to 6 for packets.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark ip-precedence 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 delete the action.

Syntax

remark local-precedence *local-precedence-value*

undo remark local-precedence

Default

No local precedence marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

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

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 qos-local-id

Use **remark qos-local-id** to configure a local QoS ID marking action in a traffic behavior.

Use **undo remark qos-local-id** to delete the action.

Syntax

remark qos-local-id *local-id-value*

undo remark qos-local-id

Default

No local QoS ID marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

local-id-value: Specifies the local QoS ID to be marked for packets. The value range for this argument is 1 to 4095.

Examples

Configure the action of marking packet with local QoS ID 2.

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

traffic behavior

Use **traffic behavior** to create a traffic behavior and enter traffic behavior view.

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

Syntax

traffic behavior *behavior-name*

undo traffic behavior *behavior-name*

Default

No traffic behavior exists.

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

traffic-policy

Use **traffic-policy** to nest a policy in a traffic behavior.

Use **undo traffic-policy** to remove child policies from a traffic behavior.

Syntax

traffic-policy *policy-name*

undo traffic-policy

Default

Policy nesting is not configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a policy by its name, a string of 1 to 31 characters. If the policy does not exist, it is automatically created.

Usage guidelines

After you nest a child policy in a behavior of a parent policy, the system performs the following operations:

- Performs the associated behavior defined in the parent policy for a class of traffic.

- Uses the child policy to further classify the class of traffic and performs the behaviors defined in the child policy.

When you nest QoS policies, follow these guidelines:

- A parent policy can nest up to two layers of child policies. This child policy cannot be the parent policy itself.
- You can nest only one child policy at one layer of a behavior.
- To configure CBQ in the child policy successfully, configure GTS in the parent policy. Make sure the configured GTS bandwidth is greater than CBQ bandwidth configured in the child policy.
- If GTS bandwidth is set in percentage in the parent policy, you must set CBQ bandwidth in percentage in the child policy. If GTS bandwidth is set as an absolute value in the parent policy, you can set CBQ bandwidth in either format in the child policy.
- A child policy cannot contain GTS actions.
- Policy nesting is available for IPv4 and IPv6 packets.
- To delete the child policy after you apply the parent policy to an interface, first remove the child policy from the parent policy.

Examples

Nest the child policy **child** in traffic behavior **database** of the parent policy.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] traffic-policy child
```

Related commands

- **traffic behavior**
- **traffic classifier**

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*

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.

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.

The **undo classifier default-class** command performs the following tasks:

- Removes the existing class-behavior association for the system-defined class **default-class**.
- Associates the system-defined class **default-class** with the system-defined behavior **be**.

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
```

Related commands

qos policy

control-plane

Use **control-plane** to enter control plane view.

Syntax

Centralized devices in standalone mode:

control-plane

Distributed devices in standalone mode/centralized devices in IRF mode:

control-plane slot *slot-number*

Distributed devices in IRF mode:

control-plane chassis *chassis-number* **slot** *slot-number*

Views

System view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies a card by its slot number. (Distributed devices in standalone mode.)

slot *slot-number*: Specifies an IRF member device by its member ID. (Centralized devices in IRF mode.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. (Distributed devices in IRF mode.)

Examples

(Centralized devices in standalone mode.) Enter control plane view.

```
<Sysname> system-view
[Sysname] control-plane
[Sysname-cp]
```

(Distributed devices in standalone mode.) Enter the control plane view of card 3.

```
<Sysname> system-view
[Sysname] control-plane slot 3
[Sysname-cp-slot3]
```

(Centralized devices in IRF mode.) Enter the control plane view of IRF member device 3.

```
<Sysname> system-view
[Sysname] control-plane slot 3
[Sysname-cp-slot3]
```

(Distributed devices in IRF mode.) Enter the control plane view of card 3 on IRF member 1.

```
<Sysname> system-view
[Sysname] control-plane chassis 1 slot 3
[Sysname-cp-chassis1-slot3]
```

control-plane management

Use **control-plane management** to enter management interface control plane view.

Syntax

control-plane management

Views

System view

Predefined user roles

network-admin

Usage guidelines

The following matrix shows the command and hardware compatibility:

Hardware	Command compatibility
MSR954(JH296A/JH297A/ JH298A/JH299A)	Yes
MSR1002-4/1003-8S	No
MSR2003	No
MSR2004-24/2004-48	No
MSR3012/3024/3044/3064	No
MSR4060/4080	Yes

The commands executed in management interface control plane view apply to packets sent from the management interface to the control plane.

Examples

Enter management interface control plane view.

```
<Sysname> system-view
[Sysname] control-plane management
[Sysname-cp-management]
```

display qos policy

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

Syntax

Centralized devices in standalone mode:

display qos policy { **system-defined** | **user-defined** } [*policy-name* [**classifier** *classifier-name*]]

Distributed devices in standalone mode/centralized devices in IRF mode:

display qos policy { **system-defined** | **user-defined** } [*policy-name* [**classifier** *classifier-name*]] [**slot** *slot-number*]

Distributed devices in IRF mode:

display qos policy { **system-defined** | **user-defined** } [*policy-name* [**classifier** *classifier-name*]] [**chassis** *chassis-number* **slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

system-defined: Displays system-defined QoS policies.

user-defined: Displays 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 a card by its slot number. If you do not specify a card, this command displays the QoS policies for the active MPU. (Distributed devices in standalone mode.)

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. (Centralized devices in IRF mode.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. If you do not specify this option, the command displays the QoS policies for the global active MPU. (Distributed devices in IRF mode.)

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 7000 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
```

```
      Red action    : discard
  Classifier: 2 (ID 101)
    Behavior: 2
     Filter enable: Permit
     Marking:
       Remark mpls-exp 4
  Classifier: 3 (ID 102)
    Behavior: 3
     -none-
```

Display the system-defined QoS policy.

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

  System-defined QoS policy information:

  Policy: default (ID 0)
   Classifier: default-class (ID 0)
     Behavior: be
      -none-
   Classifier: ef (ID 1)
     Behavior: ef
      Expedited Forwarding:
        Bandwidth 20 (%) Cbs-ratio 25
   Classifier: af1 (ID 2)
     Behavior: af
      Assured Forwarding:
        Bandwidth 20 (%)
        Discard Method: Tail
   Classifier: af2 (ID 3)
     Behavior: af
      Assured Forwarding:
        Bandwidth 20 (%)
        Discard Method: Tail
   Classifier: af3 (ID 4)
     Behavior: af
      Assured Forwarding:
        Bandwidth 20 (%)
        Discard Method: Tail
   Classifier: af4 (ID 5)
     Behavior: af
      Assured Forwarding:
        Bandwidth 20 (%)
        Discard Method: Tail
```

For the output description, see Table 15 and Table 18.

display qos policy control-plane

Use **display qos policy control-plane** to display QoS policies applied to a control plane.

Syntax

Centralized devices in standalone mode:

display qos policy control-plane

Distributed devices in standalone mode/centralized devices in IRF mode:

display qos policy control-plane slot *slot-number*

Distributed devices in IRF mode:

display qos policy control-plane chassis *chassis-number* **slot** *slot-number*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies a card by its slot number. (Distributed devices in standalone mode.)

slot *slot-number*: Specifies an IRF member device by its member ID. (Centralized devices in IRF mode.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. (Distributed devices in IRF mode.)

Examples

(Centralized devices in standalone mode.) Display the QoS policy applied to the control plane.

```
<Sysname> display qos policy control-plane inbound

Control plane

  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 7000 (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 not protocol ipv6
  Behavior: 2
   Filter enable: Permit
   Marking:
     Remark mpls-exp 4
Classifier: 3
  Operator: AND
  Rule(s) :
   -none-
  Behavior: 3
   -none-
```

Table 20 Command output

Field	Description
Direction	Inbound direction on the control plane.
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 15 and Table 18.

display qos policy control-plane management

Use **display qos policy control-plane management** to display the QoS policies applied to the management interface control plane.

Syntax

display qos policy control-plane management

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

The following matrix shows the command and hardware compatibility:

Hardware	Command compatibility
MSR954(JH296A/JH297A/JH298A/JH299A)	Yes
MSR1002-4/1003-8S	No
MSR2003	No
MSR2004-24/2004-48	No
MSR3012/3024/3044/3064	No
MSR4060/4080	Yes

A QoS policy applied to the management interface control plane takes effect on the packets sent from the management interface to the control plane.

Examples

Display the QoS policy applied to the management interface control plane.

```
<Sysname> display qos policy control-plane management

Control plane management

  Direction: Inbound

  Policy: a
   Classifier: default-class
     Matched : 0 (Packets) 0 (Bytes)
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: be
      -none-
   Classifier: a
     Matched : 3 (Packets) 180 (Bytes)
     Operator: OR
     Rule(s) :
      If-match control-plane protocol arp
      If-match control-plane protocol rip
      If-match control-plane protocol-group critical
      If-match acl 3001
      If-match control-plane protocol bgp
      If-match control-plane protocol bgp4+
      If-match control-plane protocol ftp
      If-match control-plane protocol http https icmp icmp6 ripng snmp
     Behavior: a
      Committed Access Rate:
        CIR 128 (kbps), CBS 8000 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 3 (Packets) 180 (Bytes)
        Yellow packets: 0 (Packets) 0 (Bytes)
        Red packets   : 0 (Packets) 0 (Bytes)
```

Table 21 Command output

Field	Description
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 15 and Table 18.

display qos policy control-plane management pre-defined

Use **display qos policy control-plane management pre-defined** to display the predefined QoS policy applied to the management interface control plane.

Syntax

display qos policy control-plane management pre-defined

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

The following matrix shows the command and hardware compatibility:

Hardware	Command compatibility
MSR954(JH296A/JH297A/JH298A/JH299A)	Yes
MSR1002-4/1003-8S	No
MSR2003	No
MSR2004-24/2004-48	No
MSR3012/3024/3044/3064	No
MSR4060/4080	Yes

Examples

Display the predefined QoS policy applied to the management interface control plane.

```
<Sysname> display qos policy control-plane management pre-defined
Pre-defined policy information
  Protocol          Priority   Bandwidth (kbps)   Group
  Default           N/A        100000             N/A
  ARP               N/A        100000             normal
  BGP               N/A        100000             critical
  BGPv6             N/A        100000             critical
  HTTP              N/A        100000             management
  HTTPS             N/A        100000             management
  ICMP              N/A        100000             monitor
  ICMPv6            N/A        100000             monitor
  IGMP              N/A        100000             important
  IS-IS             N/A        100000             critical
  LDP               N/A        100000             critical
  LDPv6             N/A        100000             critical
  MSDP              N/A        100000             critical
  NTP               N/A        100000             important
  OSPF Multicast    N/A        100000             critical
  OSPF Unicast      N/A        100000             critical
  OSPFv3 Multicast  N/A        100000             critical
```

```
OSPFv3 Unicast    N/A        100000            critical
PIM Multicast     N/A        100000            critical
PIM Unicast       N/A        100000            critical
PIMv6 Multicast   N/A        100000            critical
PIMv6 Unicast     N/A        100000            critical
RADIUS            N/A        100000            management
RIP               N/A        100000            critical
RIPng             N/A        100000            critical
RSVP              N/A        100000            critical
SNMP              N/A        100000            management
TACACS            N/A        100000            management
VRRP              N/A        100000            important
VRRPv6            N/A        100000            important
SSH               N/A        100000            management
TELNET            N/A        100000            management
FTP               N/A        100000            management
TFTP              N/A        100000            management
```

Table 22 Command output

Field	Description
Pre-defined control plane policy management	Predefined QoS policy applied to the management interface control plane.
Protocol	System-defined protocol packet type.
Group	Protocol group to which the protocol belongs.

display qos policy control-plane pre-defined

Use **display qos policy control-plane pre-defined** to display predefined control plane QoS policies of cards.

Syntax

Centralized devices in standalone mode:

display qos policy control-plane pre-defined

Distributed devices in standalone mode/centralized devices in IRF mode:

display qos policy control-plane pre-defined [**slot** *slot-number*]

Distributed devices in IRF mode:

display qos policy control-plane pre-defined [**chassis** *chassis-number* **slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command displays the predefined control plane QoS policies for all cards. (Distributed devices in standalone mode.)

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays predefined control plane QoS policies for all member devices. (Centralized devices in IRF mode.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. If you do not specify this option, the command displays predefined control plane QoS policies for all cards. (Distributed devices in IRF mode.)

Examples

(Distributed devices in standalone mode.) Display the predefined control plane QoS policy of slot 3.

```
<Sysname> display qos policy control-plane pre-defined slot 1
Pre-defined control plane policy slot 1
  Protocol          Priority   Bandwidth (kbps)   Group
  Default           N/A        100000             N/A
  ARP               N/A        100000             normal
  BGP               N/A        100000             critical
  BGPv6             N/A        100000             critical
  HTTP              N/A        100000             management
  HTTPS             N/A        100000             management
  ICMP              N/A        100000             monitor
  ICMPv6            N/A        100000             monitor
  IGMP              N/A        100000             important
  IS-IS             N/A        100000             critical
  LDP               N/A        100000             critical
  LDPv6             N/A        100000             critical
  MSDP              N/A        100000             critical
  NTP               N/A        100000             important
  OSPF Multicast    N/A        100000             critical
  OSPF Unicast      N/A        100000             critical
  OSPFv3 Multicast  N/A        100000             critical
  OSPFv3 Unicast    N/A        100000             critical
  PIM Multicast     N/A        100000             critical
  PIM Unicast       N/A        100000             critical
  PIMv6 Multicast   N/A        100000             critical
  PIMv6 Unicast     N/A        100000             critical
  RADIUS            N/A        100000             management
  RIP               N/A        100000             critical
  RIPng             N/A        100000             critical
  RSVP              N/A        100000             critical
  SNMP              N/A        100000             management
  TACACS            N/A        100000             management
  VRRP              N/A        100000             important
  VRRPv6            N/A        100000             important
  SSH               N/A        100000             management
  TELNET            N/A        100000             management
```

```
FTP                 N/A         100000              management
TFTP                N/A         100000              management
```

Table 23 Command output

Field	Description
Pre-defined control plane policy	Contents of the predefined control plane QoS policy.

display qos policy interface

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

Syntax

Centralized devices in standalone mode:

display qos policy interface [*interface-type interface-number* [**pvc** { *pvc-name* | *vpi/vci* }]] [**inbound** | **outbound**]

Distributed devices in standalone mode/centralized devices in IRF mode:

display qos policy interface [*interface-type interface-number* [**pvc** { *pvc-name* | *vpi/vci* }]] [**slot** *slot-number*] [**inbound** | **outbound**]

Distributed devices in IRF mode:

display qos policy interface [*interface-type interface-number* [**pvc** { *pvc-name* | *vpi/vci* }]] [**chassis** *chassis-number* **slot** *slot-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.

pvc { *pvc-name* | *vpi/vci* }: Specifies a PVC by its name or VPI/VCI value. You can specify a PVC only for an ATM interface. When you specify an ATM interface but do not specify a PVC, this command applies to all PVCs on the ATM interface. When you specify a PVC, you cannot specify the **inbound** or **outbound** keyword.

slot *slot-number*: Specifies a card by its slot number. Only virtual interfaces such as VLAN interfaces and aggregate interfaces support this option. (Distributed devices in standalone mode.)

slot *slot-number*: Specifies an IRF member device by its member ID. Only virtual interfaces such as VLAN interfaces and aggregate interfaces support this option. (Centralized devices in IRF mode.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. Only virtual interfaces such as VLAN interfaces and aggregate interfaces support this option. (Distributed devices in IRF mode.)

inbound: Displays the QoS policy applied to the incoming traffic of the specified interface.

outbound: Displays the QoS policy applied to the outgoing traffic of the specified interface.

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.

If you specify a VT interface, this command displays the QoS policies applied to each VA interface of the VT interface. It does not display QoS information about the VT interface.

Examples

Display the QoS policy applied to the incoming traffic of GigabitEthernet 2/1/1.

```
<Sysname> display qos policy interface gigabitethernet 2/1/1 inbound
Interface: GigabitEthernet2/1/1
  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 7000 (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 not protocol ipv6
     Behavior: 2
      Filter enable: Permit
      Marking:
        Remark mpls-exp 4
   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-
```

Table 24 Command output

Field	Description
Direction	Direction in which the QoS policy is applied to the interface.
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 15 and Table 18.

display qos policy l2vpn-pw

Use **display qos policy l2vpn-pw** to display the QoS policies applied to PWs.

Syntax

display qos policy l2vpn-pw [**peer** *ip-address* **pw-id** *pw-id*] [**outbound**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

peer *ip-address* **pw-id** *pw-id*: Specifies a PW by its peer PE LSR ID and its PW ID. The *ip-address* argument represents the LSR ID of the peer PE of the PW. The value range for the *pw-id* argument is 1 to 4294967295. If you do not specify a PW, this command displays the rate limit information for all PWs.

outbound: Displays the QoS policies applied to the outgoing traffic of PWs.

Usage guidelines

The specified LSR ID and PW ID uniquely identify the PW.

If you do not specify a direction, this command displays the QoS policies applied to outgoing traffic of PWs.

Examples

Display the QoS policy applied to the outgoing traffic of PW 1 with peer PE IP address 1.1.1.1.

```
<Sysname> display qos policy l2vpn-pw peer 1.1.1.1 pw-id 1 outbound

L2VPN-PW: peer 1.1.1.1, pw-id 1

  Direction: Outbound
```

```
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 7000 (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 not protocol ipv6
   Behavior: 2
    Filter enable: Permit
    Marking:
      Remark mpls-exp 4
 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-
```

Table 25 Command output

Field	Description
L2VPN-PW	A PW is uniquely identified by a combination of the peer PE IP address and PW ID.
Direction	Direction to which the QoS policy is applied on the PW.

Matched	Number of matching packets.
5-minute statistics	Traffic statistics in the last 5 minutes.
Forwarded	Average rate of successfully forwarded matching packets during a statistics collection period.
Dropped	Average rate of dropped matching packets during 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 15 and Table 18.

qos apply policy (interface view, PVC view, control plane view, management interface control plane view, PW view)

Use **qos apply policy** to apply a QoS policy to an interface, PVC, control plane, or PW.

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 to an interface, PVC, control plane, or PW.

Views

Control plane view/management interface control plane view

Cross-connect PW view/VSI LDP PW view/VSI static PW view

Interface view

PVC 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 an interface, PVC, control plane, or management interface control plane. This keyword is not supported in PW view.

outbound: Applies the QoS policy to the outgoing traffic of an interface, PVC, or PW. This keyword is not supported in control plane view or management interface control plane view.

Usage guidelines

When you apply a QoS policy to an interface, PVC, or PW, follow these rules:

- The bandwidth assigned to AF and EF queues in the QoS policy must be smaller than the available bandwidth of the interface, PVC, or PW. Otherwise, the QoS policy cannot be successfully applied to the interface or PVC.
- If you modify the available bandwidth of the interface, PVC, or PW to be smaller than the bandwidth for AF and EF queues, the applied QoS policy is removed.

- An inbound QoS policy cannot contain a GTS action or any of these queuing actions: **queue ef**, **queue af**, or **queue wfq**.

A QoS policy applied to the management interface control plane takes effect on the packets sent from the management interface to the control plane.

A QoS policy configured with CBQ is not supported in control plane view or management interface control plane view.

Examples

Apply QoS policy **USER1** to the outgoing traffic of GigabitEthernet 2/1/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/1/1
[Sysname-GigabitEthernet2/1/1] qos apply policy USER1 outbound
```

Apply QoS policy **aaa** to the incoming traffic of the control plane of slot 3.

```
<Sysname> system-view
[Sysname] control-plane slot 3
[Sysname-cp-slot3] qos apply policy aaa inbound
```

Apply QoS policy **bbb** to the incoming traffic of the management interface control plane.

```
<Sysname> system-view
[Sysname] control-plane management
[Sysname-cp-management] qos apply policy bbb inbound
```

Apply a QoS policy to the outgoing traffic of PW 1 with peer PE IP address 1.1.1.1.

```
<Sysname> system-view
[Sysname] xconnect-group a
[Sysname-xcg-a] connection a
[Sysname-xcg-a-a] peer 1.1.1.1 pw-id 1
[Sysname-xcg-a-a-1.1.1.1-1] qos apply policy 1 outbound
```

qos policy

Use **qos policy** to create a QoS policy and enter QoS policy view.

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

Syntax

qos policy *policy-name*

undo qos policy *policy-name*

Default

No QoS policy is configured.

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.

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

Define QoS policy **user1**.

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

Related commands

- **classifier behavior**
- **qos apply policy**

reset qos policy control-plane

Use **reset qos policy control-plane** to clear the statistics of the QoS policy applied to a control plane.

Syntax

Centralized devices in standalone mode:

reset qos policy control-plane

Distributed devices in standalone mode/centralized devices in IRF mode:

reset qos policy control-plane slot *slot-number*

Distributed devices in IRF mode:

reset qos policy control-plane chassis *chassis-number* **slot** *slot-number*

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies a card by its slot number. (Distributed devices in standalone mode.)

slot *slot-number*: Specifies an IRF member device by its member ID. (Centralized devices in IRF mode.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. (Distributed devices in IRF mode.)

Examples

(Centralized devices in standalone mode.) Clear the statistics of the QoS policy applied to the control plane.

```
<Sysname> reset qos policy control-plane
```

(Distributed devices in standalone mode.) Clear the statistics of the QoS policy applied to the control plane of card 3.

```
<Sysname> reset qos policy control-plane slot 3
```

(Centralized devices in IRF mode.) Clear the statistics of the QoS policy applied to the control plane of member device 3.

```
<Sysname> reset qos policy control-plane slot 3
```

(Distributed devices in IRF mode.) Clear the statistics of the QoS policy applied to the control plane of card 3 on IRF member 1.

```
<Sysname> reset qos policy control-plane chassis 1 slot 3
```

reset qos policy control-plane management

Use **reset qos policy control-plane management** to clear the statistics of the QoS policy applied to the management interface control plane.

Syntax

reset qos policy control-plane management

Views

User view

Predefined user roles

network-admin

Usage guidelines

The following matrix shows the command and hardware compatibility:

Hardware	Command compatibility
MSR954(JH296A/JH297A/JH298A/JH299A)	Yes
MSR1002-4/1003-8S	No
MSR2003	No
MSR2004-24/2004-48	No
MSR3012/3024/3044/3064	No
MSR4060/4080	Yes

Examples

Clear the statistics of the QoS policy applied to the management interface control plane.

```
<Sysname> reset qos policy control-plane management
```

QoS policy-based traffic rate statistics collection period commands

qos flow-interval

Use **qos flow-interval** to set the QoS policy-based traffic rate statistics collection period for an interface.

Use **undo qos flow-interval** to restore the default.

Syntax

qos flow-interval *interval*

undo qos flow-interval

Default

The QoS policy-based traffic rate statistics collection period is 5 minutes on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

interval: Sets the QoS policy-based traffic rate statistics collection period in the range of 1 to 10 minutes.

Usage guidelines

You can enable collection of per-class traffic statistics over a period of time, including the average forwarding rate and drop rate. For example, if you set the statistics collection period to 10 minutes, the system performs the following tasks:

- Collects traffic statistics for the most recent 10 minutes.
- Refreshes the statistics every 10/5 minutes, 2 minutes.

The traffic rate statistics collection period of a subinterface is the same as the period configured on the main interface.

Examples

Set the QoS policy-based traffic rate statistics collection period to 10 minutes on GigabitEthernet 2/1/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/1/1
[Sysname-GigabitEthernet2/1/1] qos flow-interval 10
```

Related commands

display qos policy interface

Priority mapping commands

Priority map commands

display qos map-table

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

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

dot1p-lp: Specifies the 802.1p-local priority map.

dscp-lp: Specifies the DSCP-local 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 26 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-lp** | **dscp-lp** }

Views

System view

Predefined user roles

network-admin

Parameters

dot1p-lp: Specifies the 802.1p-local priority map.

dscp-lp: Specifies the DSCP-local priority map.

Examples

Enter the 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**

Port priority commands

This feature is supported only on the following ports:

- Layer 2 Ethernet ports on Ethernet switching modules.
- Fixed Layer 2 Ethernet ports of the following routers:
  - MSR954(JH296A/JH297A/JH298A/JH299A).
  - MSR1002-4/1003-8S.
  - MSR2004-24/2004-48.

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 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 to 2 for interface GigabitEthernet 2/1/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/1/1
[Sysname-GigabitEthernet2/1/1] qos priority 2
```

Related commands

display qos trust interface

Priority trust mode commands

This feature is supported only on the following ports:

- Layer 2 Ethernet ports on Ethernet switching modules.

- Fixed Layer 2 Ethernet ports of the following routers:
  - MSR954(JH296A/JH297A/JH298A/JH299A).
  - MSR1002-4/1003-8S.
  - MSR2004-24/2004-48.

display qos trust interface

Use **display qos trust interface** to display the priority trust mode and port priorities of a Layer 2 Ethernet 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 GigabitEthernet 2/1/1.

```
<Sysname> display qos trust interface gigabitethernet 2/1/1
Interface: GigabitEthernet2/1/1
 Port priority trust information
  Port priority:4
  Port priority trust type: dot1p
```

Table 27 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** or **dscp**.

qos trust

Use **qos trust** to configure the priority trust mode for a Layer 2 Ethernet interface.

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

Syntax

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

undo qos trust

Default

The port priority is trusted.

Views

Layer 2 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. This keyword is supported only on the following ports:

- Layer 2 Ethernet ports on the following modules:
  - HMIM-24GSW.
  - HMIM-24GSWP.
  - HMIM-8GSW.
  - SIC-4GSW.
  - SIC-4GSWP.
- Fixed Layer 2 Ethernet ports of the following routers:
  - MSR954(JH296A/JH297A/JH298A/JH299A).
  - MSR1002-4/1003-8S.
  - MSR2004-24/2004-48.

Examples

Set the priority trust mode to 802.1p priority on GigabitEthernet 2/1/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/1/1
[Sysname-GigabitEthernet2/1/1] qos trust dot1p
```

Related commands

display qos trust interface

Traffic policing, GTS, and rate limit commands

Commands and descriptions for centralized devices apply to the following routers:

- MSR1002-4/1003-8S.
- MSR2003.
- MSR2004-24/2004-48.
- MSR3012/3024/3044/3064.
- MSR954(JH296A/JH297A/JH298A/JH299A)

Commands and descriptions for distributed devices apply to MSR4060 and MSR4080 routers.

Traffic policing commands

display qos car interface

Use **display qos car interface** to display the CAR information on an interface.

Syntax

display qos car 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 CAR information on all interfaces.

Examples

Display the CAR information on GigabitEthernet 2/0/1.

```
<Sysname> display qos car interface gigabitethernet 2/0/1
Interface: GigabitEthernet2/0/1
 Direction: inbound
  Rule: If-match any
   CIR 128 (kbps), CBS 8000 (Bytes), PIR 128 (kbps), 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)
```

Table 28 Command output

Field	Description
Interface	Interface name, including interface type and interface number.
Direction	Direction in which traffic policing is applied.
Rule	Match criteria.
Green action	Action to take on green packets.
Yellow action	Action to take on yellow packets.
Red action	Action to take on red packets.

display qos carl

Use **display qos carl** to display CAR lists.

Syntax

Centralized devices in standalone mode:

display qos carl [*carl-index*]

Distributed devices in standalone mode/centralized devices in IRF mode:

display qos carl [*carl-index*] [**slot** *slot-number*]

Distributed devices in IRF mode:

display qos carl [*carl-index*] [**chassis** *chassis-number* **slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

carl-index: Specifies a CAR list by its number in the range of 1 to 199. If you do not specify a CAR list, this command displays all CAR lists.

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command displays the CAR lists for the active MPU. (Distributed devices in standalone mode.)

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the CAR lists for the master device. (Centralized devices in IRF mode.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. If you do not specify this option, the command displays the CAR lists for the global active MPU. (Distributed devices in IRF mode.)

Examples

Display all CAR lists.

```
<Sysname> display qos carl
List  Rules
1     destination-ip-address range 1.1.1.1 to 1.1.1.2 per-address shared-bandwidth
2     destination-ip-address subnet 1.1.1.1 22 per-address shared-bandwidth
```

```
4     dscp 1 2 3 4 5 6 7 cs1
5     mac 0000-0000-0000
6     mpls-exp 0 1 2
9     precedence 0 1 2 3 4 5 6 7
10    source-ip-address range 1.1.1.1 to 1.1.1.2
11    source-ip-address subnet 1.1.1.1 31
```

qos car

Use **qos car** to configure a CAR policy on an interface.

Use **undo qos car** to remove a CAR policy from an interface.

Syntax

qos car { **inbound** | **outbound** } { **any** | **acl** [**ipv6**] *acl-numbe*r | **carl** *carl-index* } **cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**green** *action* | **red** *action* | **yellow** *action*] *

qos car { **inbound** | **outbound** } { **any** | **acl** [**ipv6**] *acl-numbe*r | **carl** *carl-index* } **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 { **inbound** | **outbound** } { **any** | **acl** [**ipv6**] *acl-number* | **carl** *carl-index* }

Default

No CAR policy is configured on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

inbound: Performs CAR for incoming packets on the interface.

outbound: Performs CAR for outgoing packets on the interface.

any: Performs CAR for all IP data packets in the specified direction.

acl [**ipv6**] *acl-number*: Performs CAR for packets matching an ACL specified by its number in the range of 2000 to 3999. If you do not specify **ipv6**, this option specifies an IPv4 ACL. If you specify **ipv6**, this option specifies an IPv6 ACL.

carl *carl-index*: Performs CAR for packets matching a CAR list specified by its number in the range of 1 to 199.

cir *committed-information-rate*: Specifies CIR in kbps.

cbs *committed-burst-size*: CBS in bytes, which specifies the size of bursty traffic when the actual average rate is not greater than CIR.

ebs *excess-burst-size*: Specifies the EBS in bytes.

pir *peak-information-rate*: Specifies the PIR in kbps.

green: Specifies the action to take on packets when the traffic rate conforms to CIR. The default is **pass**.

red: Specifies the action to take on packets when the traffic rate conforms to neither CIR nor PIR. The default is **discard**.

yellow: Specifies the action to take on packets when the traffic rate exceeds CIR but conforms to PIR. The default is **pass**.

action: Specifies the action to take on packets:

- **continue**: Continues to process the packet by using the next CAR policy.
- **discard**: Drops the packet.
- **pass**: Permits the packet to pass through.
- **remark-dot1p-continue** *new-cos*: Sets the 802.1p priority value of the 802.1p packet to *new-cos* and continues to process the packet by using the next CAR policy. The *new-cos* argument is in the range of 0 to 7.
- **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-continue** *new-dscp*: Remarks the packet with a new DSCP value and continues to process the packet by using the next CAR policy. 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**.
- **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**.
- **remark-mpls-exp-continue** *new-exp*: Sets the EXP field value of the MPLS packet to *new-exp* and continues to process the packet by using the next CAR policy. The *new-exp* argument is in the range of 0 to 7.
- **remark-mpls-exp-pass** *new-exp*: Sets the EXP field value of the MPLS packet to *new-exp* and permits the packet to pass through. The *new-exp* argument is in the range of 0 to 7.
- **remark-prec-continue** *new-precedence*: Remarks the packet with a new IP precedence and continues to process the packet by using the next CAR policy. The *new-precedence* argument is in the range of 0 to 7.
- **remark-prec-pass** *new-precedence*: Remarks the packet with a new IP precedence and permits the packet to pass through. The *new-precedence* argument is in the range of 0 to 7.

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.

You can configure a **qos car** command multiple times to define multiple CAR policies on an interface. The CAR policies are applied in the order they are configured.

Examples

Perform CAR for all packets in the outbound direction of GigabitEthernet 2/0/1. The CAR parameters are as follows:

- CIR is 200 kbps.
- CBS is 50000 bytes.
- EBS is 0.
- Conforming packets are transmitted.
- Excess packets are set with an IP precedence of 0 and transmitted.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] qos car outbound any cir 200 cbs 5000 ebs 0 green pass red
remark-prec-pass 0
```

Related commands

- **display qos car interface**
- **qos carl**

qos car percent

Use **qos car percent** to configure a CAR policy in percentage on an interface.

Use **undo qos car** to remove a CAR policy from an interface.

Syntax

qos car { **inbound** | **outbound** } { **any** | **acl** [**ipv6**] *acl-numbe*r | **carl** *carl-index* } **percent cir** *cir-percent* [**cbs** *cbs-time* [**ebs** *ebs-time*]] [**green** *action* | **red** *action* | **yellow** *action*] *

qos car { **inbound** | **outbound** } { **any** | **acl** [**ipv6**] *acl-numbe*r | **carl** *carl-index* } **percent cir** *cir-percent* [**cbs** *cbs-time*] **pir** *pir-percent* [**ebs** *ebs-time*] [**green** *action* | **red** *action* | **yellow** *action*] *

undo qos car { **inbound** | **outbound** } { **any** | **acl** [**ipv6**] *acl-number* | **carl** *carl-index* }

Default

No CAR policy is configured in percentage on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

inbound: Performs CAR for incoming packets on the interface.

outbound: Performs CAR for outgoing packets on the interface.

any: Performs CAR for all IP data packets in the specified direction.

acl [**ipv6**] *acl-number*: Performs CAR for packets matching an ACL specified by its number in the range of 2000 to 3999. If you do not specify **ipv6**, this option specifies an IPv4 ACL. If you specify **ipv6**, this option specifies an IPv6 ACL.

carl *carl-index*: Performs CAR for packets matching a CAR list specified by its number in the range of 1 to 199.

percent cir *cir-percent*: Specifies the CIR in percentage, in the range of 1 to 100. The actual CIR value is *cir-percent* × interface bandwidth.

cbs *cbs-time*: Specifies the CBS in milliseconds. The actual CBS value is *cbs-time* × the actual CIR value.

ebs *ebs-time*: Specifies the EBS in milliseconds. The actual EBS value is *ebs-time* × the actual CIR value.

pir *pir-percent*: Specifies the PIR in percentage, in the range of 1 to 100. The value for the *pir-percent* argument must be greater than or equal to the value for the *cir-percent* argument.

green: Specifies the action to take on packets when the traffic rate conforms to CIR. The default is **pass**.

red: Specifies the action to take on packets when the traffic rate conforms to neither CIR nor PIR. The default is **discard**.

yellow: Specifies the action to take on packets when the traffic rate exceeds CIR but conforms to PIR. The default is **pass**.

action: Specifies the action to take on packets:

- **continue**: Continues to process the packet by using the next CAR policy.
- **discard**: Drops the packet.
- **pass**: Permits the packet to pass through.
- **remark-dot1p-continue** *new-cos*: Sets the 802.1p priority value of the packet to *new-cos* and continues to process the packet by using the next CAR policy. The *new-cos* argument is in the range of 0 to 7.
- **remark-dot1p-pass** *new-cos*: Sets the 802.1p priority value of the 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-continue** *new-dscp*: Sets the DSCP value of the packet and continues to process the packet by using the next CAR policy. 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**.
- **remark-dscp-pass** *new-dscp*: Sets the DSCP value of the packet 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**.
- **remark-mpls-exp-continue** *new-exp*: Sets the EXP field value of the MPLS packet to *new-exp* and continues to process the packet by using the next CAR policy. The *new-exp* argument is in the range of 0 to 7.
- **remark-mpls-exp-pass** *new-exp*: Sets the EXP field value of the MPLS packet to *new-exp* and permits the packet to pass through. The *new-exp* argument is in the range of 0 to 7.
- **remark-prec-continue** *new-precedence*: Sets the IP precedence of the packet and continues to process the packet by using the next CAR policy. The *new-precedence* argument is in the range of 0 to 7.
- **remark-prec-pass** *new-precedence*: Sets the IP precedence of the packet and permits the packet to pass through. The *new-precedence* argument is in the range of 0 to 7.

Usage guidelines

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

You can configure a **qos car percent** command multiple times to define multiple CAR policies on an interface. These CAR policies are executed in their configuration order.

Examples

Perform CAR for all outgoing packets on GigabitEthernet 2/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] qos car outbound any percent cir 50 cbs 1000
```

qos carl

Use **qos carl** to create or modify a CAR list.

Use **undo qos carl** to delete a CAR list.

Syntax

qos carl *carl-index* { **dscp** *dscp-list* | **mac** *mac-address* | **mpls-exp** *mpls-exp-value* | **precedence** *precedence-value* | { **destination-ip-address** | **source-ip-address** } { **range** *start-ip-address* **to** *end-ip-address* | **subnet** *ip-address mask-length* } [**per-address** [**shared-bandwidth**]] }

undo qos carl *carl-index*

Default

No CAR list is configured.

Views

System view

Predefined user roles

network-admin

Parameters

carl-index: Specifies a CAR list by its number in the range of 1 to 199.

dscp *dscp-list*: Specifies a list of DSCP values. A DSCP value can be a number from 0 to 63 or any of the following keywords **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, **default**, or **ef**. You can configure up to eight DSCP values in one command line. If the same DSCP value is specified multiple times, the system considers the values to be one value. If a packet matches one of the defined DSCP values, it matches the **if-match** clause.

mac *mac-address*: Specifies a MAC address in hexadecimal format.

mpls-exp *mpls-exp-value*: Specifies an MPLS EXP value in the range of 0 to 7. You can configure up to eight MPLS EXP values in one command line. If the same MPLS EXP value is specified multiple times, the system considers the values to be one value. If a packet matches one of the defined MPLS EXP values, it matches the **if-match** clause.

precedence *precedence*: Specifies a precedence value in the range of 0 to 7. You can configure up to eight IP precedence values in one command line. If the same IP precedence value is specified multiple times, the system considers the values to be one value. If a packet matches one of the defined IP precedence values, it matches the **if-match** clause.

destination-ip-address: Configures a destination IP address-based CAR list.

source-ip-address: Configures a source IP address-based CAR list.

range *start-ip-address* **to** *end-ip-address*: Specifies an IP address range by the start address and end address. *end-ip-address* must be greater than *start-ip-address*. The maximum number of IP addresses that an IP address range can accommodate is 1024.

subnet *ip-address mask-length*: Specifies a subnet by the IP subnet address and IP subnet address mask length. The value range for *mask-length* is 22 to 31.

per-address: Performs per-IP address rate limiting within the network segment. When this keyword is specified, the CIR is dedicated bandwidth for each IP address and is not shared by any other IP address. If you do not specify this keyword, the following events occur:

- Rate limiting is performed for the entire network segment.
- All of the CIR is allocated among all IP addresses in proportion to the traffic load of each IP address.

shared-bandwidth: Specifies that traffic of all IP addresses within the network segment shares the remaining bandwidth. If you specify this keyword, all of the CIR is allocated evenly among all IP addresses with traffic load.

Usage guidelines

You can create a CAR list based on IP precedence, MAC address, MPLS EXP, DSCP, or IP network segment.

Using the command repeatedly with different CAR list numbers creates multiple CAR lists. Using the command repeatedly with the same *carl-index* modifies the parameters for the CAR list.

To perform rate limiting for a single IP address, use the **qos car acl** command in interface view.

Examples

Apply CAR list 1 to the outbound direction of GigabitEthernet 2/0/1 to meet the following requirements:

- The rate of each host on the subnet 1.1.1.0/24 is limited to 100 kbps.
- Traffic of IP addresses in the subnet does not share the remaining bandwidth.

```
<Sysname> system-view
[Sysname] qos carl 1 source-ip-address subnet 1.1.1.0 24 per-address
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] qos car outbound carl 1 cir 100 cbs 6250 ebs 0 green pass red discard
```

Apply CAR list 2 to the outbound direction of GigabitEthernet 2/0/1 to meet the following requirements:

- The rate of each host in the IP address range of 1.1.2.100 to 1.1.2.199 is limited to 5 Mbps.
- Traffic of IP addresses in the subnet shares the remaining bandwidth.

```
<Sysname> system-view
[Sysname] qos carl 2 source-ip-address range 1.1.2.100 to 1.1.2.199 per-address shared-bandwidth
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] qos car outbound carl 2 cir 5000 cbs 3125 ebs 31250 green pass red discard
```

Related commands

- **display qos carl**
- **qos car**

GTS commands

display qos gts interface

Use **display qos gts interface** to display GTS information on 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 information on all interfaces.

Examples

Display the GTS information on all interfaces.

```
<Sysname> display qos gts interface
Interface: GigabitEthernet2/0/1
 Rule: If-match acl 2001
```

```
CIR 200 (kbps), CBS 50000 (Bytes), EBS 0 (Bytes)
Queue Length: 100 (Packets)
Queue Size: 70 (Packets)
Passed   : 0 (Packets) 0 (Bytes)
Discarded: 0 (Packets) 0 (Bytes)
Delayed  : 0 (Packets) 0 (Bytes)
```

Table 29 Command output

Field	Description
Interface	Interface name, including the interface type and interface number.
Rule	Match criteria.
Queue Length	Number of packets that the buffer can hold.
Queue Size	Number of packets in the buffer.
Passed	Number and bytes of packets that have been forwarded.
Discarded	Number and bytes of dropped packets.
Delayed	Number and bytes of delayed packets.

qos gts

Use **qos gts acl** to set GTS parameters for the traffic matching an ACL. Using the command multiple times with different ACLs sets GTS parameters for different traffic flows.

Use **qos gts any** to set GTS parameters for all traffic on an interface.

Use **undo qos gts** to remove GTS parameters for traffic of a traffic class or all traffic on an interface.

Syntax

qos gts { **any** | **acl** [**ipv6**] *acl-number* } **cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**queue-length** *queue-length*]

undo qos gts { **any** | **acl** [**ipv6**] *acl-number* }

Default

No GTS parameters are configured on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

any: Shapes all packets.

acl [**ipv6**] *acl-number*: Performs GTS for packets matching an ACL specified by its number in the range of 2000 to 3999. If you do not specify **ipv6**, this option specifies an IPv4 ACL. If you specify **ipv6**, this option specifies an IPv6 ACL.

cir *committed-information-rate*: Specifies the CIR in kbps.

cbs *committed-burst-size*: Specifies the CBS in bytes.

ebs *excess-burst-size*: Specifies the EBS in bytes, which is the traffic exceeding CBS when two token buckets are used.

queue-length *queue-length*: Specifies the maximum queue length in the range of 1 to 1024 packets. The default is 50 packets.

Examples

Shape the packets matching ACL 2001 on GigabitEthernet 2/0/1. The GTS parameters are as follows:

- The CIR is 200 kbps.
- The CBS is 50000 bytes.
- The EBS is 0.
- The maximum buffer queue length is 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] qos gts acl 2001 cir 200 cbs 50000 ebs 0 queue-length 100
```

Rate limit commands

display qos lr

Use **display qos lr** to display the rate limit information for interfaces or PWs.

Syntax

display qos lr { **interface** [*interface-type interface-number*] | **l2vpn-pw** [**peer** *ip-address* **pw-id** *pw-id*] }

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 information for all interfaces.

peer *ip-address* **pw-id** *pw-id*: Specifies a PW by its peer PE LSR ID and its PW ID. The *ip-address* argument represents the LSR ID of the peer PE of the PW. The value range for the *pw-id* argument is 1 to 4294967295. If you do not specify a PW, this command displays the rate limit information for all PWs.

Examples

Display the rate limit information for all interfaces.

```
<Sysname> display qos lr interface
Interface: GigabitEthernet2/0/1
 Direction: Inbound
  CIR 2000 (kbps), CBS 20000 (Bytes), EBS 0 (Bytes)
  Passed   : 1000 (Packets) 1000 (Bytes)
  Discarded: 1000 (Packets) 1000 (Bytes)
  Delayed  : 1000 (Packets) 1000 (Bytes)
  Active shaping: No
```

Display the rate limit information for all PWs.

```
<Sysname> display qos lr l2vpn-pw
L2VPN-PW: peer 1.2.3.4, pw-id 1
  Direction: Outbound
   CIR 1024 (kbps), CBS 64000 (Bytes), EBS 0 (Bytes)
   Passed   : 0 (Packets) 0 (Bytes)
   Delayed  : 0 (Packets) 0 (Bytes)
   Active shaping: No
```

Table 30 Command output

Field	Description
Interface	Interface name, including the interface type and interface number.
L2VPN-PW	A PW is uniquely identified by a combination of the peer PE IP address and PW ID.
Direction	Direction to which the rate limit configuration is applied: inbound or outbound.
Passed	Number and bytes of packets that have passed.
Delayed	Number and bytes of delayed packets.
Active shaping	Indicates whether the rate limit configuration is activated: • **Yes**—Activated. • **No**—Not activated.

qos lr

Use **qos lr** to limit the rate of packets on an interface or PW.

Use **undo qos lr** to remove a rate limit.

Syntax

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

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

Default

No rate limit is configured on an interface or PW.

Views

Cross-connect PW view, VSI LDP PW view, VSI static PW view, interface view

Predefined user roles

network-admin

Parameters

inbound: Limits the rate of incoming packets. This keyword is supported only in interface view.

outbound: Limits the rate of outgoing packets.

cir *committed-information-rate*: Specifies the CIR in kbps.

cbs *committed-burst-size*: Specifies the CBS in bytes.

ebs *excess-burst-size*: Specifies the EBS in bytes, which is the traffic exceeding CBS when two token buckets are used.

Examples

Limit the rate of outgoing packets on GigabitEthernet 2/0/1, with CIR 200 kbps and CBS 50000 bytes.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/0/1
[Sysname-GigabitEthernet2/0/1] qos lr outbound cir 200 cbs 50000
```

Congestion management commands

Commands and descriptions for centralized devices apply to the following routers:

- MSR1002-4/1003-8S.
- MSR2003.
- MSR2004-24/2004-48.
- MSR3012/3024/3044/3064.
- MSR954(JH296A/JH297A/JH298A/JH299A)

Commands and descriptions for distributed devices apply to MSR4060 and MSR4080 routers.

Common commands

display qos queue interface

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

Syntax

display qos queue interface [*interface-type interface-number* [**pvc** { *pvc-name* | *vpi/vci* }]]

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.

pvc { *pvc-name* | *vpi/vci* }: Specifies a PVC by its name or VPI/VCI value. You can specify a PVC only for an ATM interface. When you specify an ATM interface but do not specify a PVC, this command displays the queuing information for all PVCs on the ATM interface.

Examples

Display the queuing information for all interfaces.

```
<Sysname> display qos queue interface
Interface: GigabitEthernet2/1/1
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - Weighted Fair queuing: Size/Length/Discards 0/64/0
  Weight: IP Precedence
  Queues: Active/Max active/Total 0/0/128

Interface: GigabitEthernet2/1/2
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
```

Table 31 Command output

Field	Description
Interface	Interface name, including the interface type and interface number.
Size	Number of packets in the queue.
Length	Queue length.
Discards	Number of packets dropped.
Weight	Weight type: • **IP Precedence**. • **DSCP**.
Active	Number of active WFQ queues.
Max active	Maximum number of active WFQ queues that was reached.
Total	Total number of configured WFQ queues.

display qos queue l2vpn-pw

Use **display qos queue l2vpn-pw** to display the queuing information for PWs.

Syntax

display qos queue l2vpn-pw [**peer** *ip-address* **pw-id** *pw-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

peer *ip-address* **pw-id** *pw-id*: Specifies a PW by its peer PE LSR ID and its PW ID. The *ip-address* argument represents the LSR ID of the peer PE of the PW. The value range for the *pw-id* argument is 1 to 4294967295. If you do not specify a PW, this command displays the queuing information for all PWs.

Examples

Display the queuing information for all PWs.

```
<Sysname> display qos queue l2vpn-pw
L2VPN-PW: peer 1.1.1.1, pw-id 1
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
L2VPN-PW: peer 2.2.2.2 pw-id 2
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - Weighted Fair queuing: Size/Length/Discards 0/64/0
  Weight: IP Precedence
  Queues: Active/Max active/Total 0/0/128
```

Table 32 Command output

Field	Description
L2VPN-PW	A PW is uniquely identified by a combination of the peer PE IP address and PW ID.
Size	Number of packets in the queue.
Length	Queue length.
Discards	Number of packets dropped.
Weight	Weight type: • **IP Precedence**. • **DSCP**.
Active	Number of active WFQ queues.
Max active	Maximum number of active WFQ queues that was reached.
Total	Total number of configured WFQ queues.

reset qos statistics l2vpn-pw

Use **reset qos statistics l2vpn-pw** to clear the QoS statistics for PWs.

Syntax

reset qos statistics l2vpn-pw [**peer** *ip-address* **pw-id** *pw-id*]

Views

User view

Predefined user roles

network-admin

Parameters

peer *ip-address* **pw-id** *pw-id*: Specifies a PW by its peer PE LSR ID and its PW ID. The *ip-address* argument represents the LSR ID of the peer PE of the PW. The value range for the *pw-id* argument is 1 to 4294967295. If you do not specify a PW, this command clears QoS statistics for all PWs.

Examples

Clear the QoS statistics for PW 1 with peer PE IP address 1.1.1.1.

```
<Sysname> reset qos statistics l2vpn-pw peer 1.1.1.1 pw-id 1
```

FIFO queuing commands

display qos queue fifo

Use **display qos queue fifo** to display the FIFO information for interfaces, PVCs or PWs.

Syntax

display qos queue fifo { **interface** [*interface-type interface-number* [**pvc** { *pvc-name* | *vpi/vci* }]] | **l2vpn-pw** [**peer** *ip-address* **pw-id** *pw-id*] }

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 FIFO information for all interfaces.

pvc { *pvc-name* | *vpi/vci* }: Specifies a PVC by its name or VPI/VCI value. You can specify a PVC only for an ATM interface. When you specify an ATM interface but do not specify a PVC, this command displays the FIFO information for all PVCs on the ATM interface.

peer *ip-address* **pw-id** *pw-id*: Specifies a PW by its peer PE LSR ID and its PW ID. The *ip-address* argument represents the LSR ID of the peer PE of the PW. The value range for the *pw-id* argument is 1 to 4294967295. If you do not specify a PW, this command displays the FIFO information for all PWs.

Examples

Display the FIFO information for all interfaces.

```
<Sysname> display qos queue fifo interface
Interface: GigabitEthernet2/1/2
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
```

Display the FIFO information for all PWs.

```
<Sysname> display qos queue fifo l2vpn-pw
L2VPN-PW: peer 1.1.1.1, pw-id 1
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
```

Table 33 Command output

Field	Description
Interface	Interface name, including the interface type and interface number.
L2VPN-PW	A PW is uniquely identified by a combination of the peer PE IP address and PW ID.
Size	Number of packets in the queue.
Length	Queue length.
Discards	Number of packets dropped.

qos fifo queue-length

Use **qos fifo queue-length** to set the FIFO queue length.

Use **undo qos fifo queue-length** to restore the default.

Syntax

qos fifo queue-length *queue-length*

undo qos fifo queue-length

Default

The FIFO queue length is 75.

Views

Cross-connect PW view/VSI LDP PW view/VSI static PW view

Interface view

PVC view

Predefined user roles

network-admin

Parameters

queue-length: Specifies the queue length in the range of 1 to 1024 packets.

Usage guidelines

For the queuing feature to take effect on a subinterface, you must configure the rate limit on the subinterface.

Examples

Set the FIFO queue length to 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/1/1
[Sysname-GigabitEthernet2/1/1] qos fifo queue-length 100
```

Related commands

display qos queue fifo interface

PQ commands

display qos queue pq interface

Use **display qos queue pq interface** to display the PQ information for interfaces or PVCs.

Syntax

display qos queue pq interface [*interface-type interface-number* [**pvc** { *pvc-name* | *vpi/vci* }]]

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 PQ information for all interfaces.

pvc { *pvc-name* | *vpi/vci* }: Specifies a PVC by its name or VPI/VCI value. You can specify a PVC only for an ATM interface. When you specify an ATM interface but do not specify a PVC, this command displays the PQ information for all PVCs on the ATM interface.

Usage guidelines

If you specify a VT interface, this command displays the PQ information for all VA interfaces of the VT interface. A VT interface itself does not have QoS information.

Examples

Display the PQ information for interface GigabitEthernet 2/1/1.

```
<Sysname> display qos queue pq interface gigabitethernet 2/1/1
Interface: GigabitEthernet2/1/1
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - Priority queuing: PQL 1 Size/Length/Discards
Top:  0/20/0    Middle:  0/40/0    Normal:  0/60/0    Bottom:  0/80/0
```

Table 34 Command output

Field	Description
Priority queuing: PQL 1	PQL 1 indicates the PQ list in use.
Size	Number of packets in a queue.
Length	Queue length, which specifies the maximum number of packets that a queue can hold.
Discards	Number of dropped packets.
Top	Top priority queue.
Middle	Middle priority queue.
Normal	Normal priority queue.
Bottom	Bottom priority queue.

display qos pql

Use **display qos pql** to display the PQ list configuration.

Syntax

Centralized devices in standalone mode:

display qos pql [*pql-index*]

Distributed devices in standalone mode/centralized devices in IRF mode:

display qos pql [*pql-index*] [**slot** *slot-number*]

Distributed devices in IRF mode:

display qos pql [*pql-index*] [**chassis** *chassis-number* **slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pql-index: Specifies a PQ list by its number in the range of 1 to 16.

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command displays the PQ list configuration for the active MPU. (Distributed devices in standalone mode.)

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the PQ list configuration for the master device. (Centralized devices in IRF mode.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. If you do not specify this option, the command displays the PQ list configuration for the global active MPU. (Distributed devices in IRF mode.)

Examples

Display the configuration of all PQ lists.

```
<Sysname> display qos pql
Current PQL configuration:
List  Queue   Parameters
-------------------------------------------------------
1     Top     Protocol ip less-than 1000
2     Normal  Length 80
2     Bottom  Length 40
3     Middle  Inbound-interface GigabitEthernet2/1/1
4     Top     Local-precedence  7
```

qos pq

Use **qos pq** to apply a PQ list to an interface or PVC.

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

Syntax

qos pq pql *pql-index*

undo qos pq

Default

FIFO queuing is used on an interface.

Views

Interface view, PVC view

Predefined user roles

network-admin

Parameters

pql *pql-index*: Specifies a PQ list by its number in the range of 1 to 16.

Usage guidelines

If you apply multiple PQ lists to an interface or PVC, the PQ list last applied takes effect.

Multiple match criteria can be configured for a PQ list. When a packet arrives, it is examined against match criteria in their configuration order.

- When a match is found, the packet is assigned to the corresponding queue, and the matching process ends.
- If no match is found, the packet is assigned to the default queue.

Examples

Apply PQ list 12 to GigabitEthernet 2/1/1.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 2/1/1
[Sysname-GigabitEthernet2/1/1] qos pq pql 12
```

qos pql default-queue

Use **qos pql default-queue** to specify a priority queue as the default queue for a PQ list.

Use **undo qos pql default-queue** to restore the default.

Syntax

qos pql *pql-index* **default-queue** { **bottom** | **middle** | **normal** | **top** }

undo qos pql *pql-index* **default-queue**

Default

The normal queue is the default queue.

Views

System view

Predefined user roles

network-admin

Parameters

pql-index: Specifies a PQ list by its number in the range of 1 to 16.

top, **middle**, **normal**, **bottom**: Specifies a priority queue. The four queues are in descending priority order.

Usage guidelines

If a packet does not match any criteria in a PQ list, the packet is assigned to the default queue of the PQ list.

If this command is executed multiple times for the same PQ list, the new configuration overrides the previous one.

Examples

Specify the bottom queue as the default queue for PQ list 12.

```
<Sysname> system-view
[Sysname] qos pql 12 default-queue bottom
```

qos pql inbound-interface

Use **qos pql inbound-interface** to configure an assignment rule for a PQ list to assign packets received on the specified interface to a priority queue.

Use **undo qos pql inbound-interface** to delete an assignment rule based on the specified input interface from a PQ list.

Syntax

qos pql *pql-index* **inbound-interface** *interface-type interface-number* **queue** { **bottom** | **middle** | **normal** | **top** }

undo qos pql *pql-index* **inbound-interface** *interface-type interface-number*

Default

No assignment rule is configured for a PQ list.

Views

System view

Predefined user roles

network-admin

Parameters

pql-index: Specifies a PQ list by its number in the range of 1 to 16.

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

top, **middle**, **normal**, **bottom**: Specifies a priority queue. The four queues are in descending priority order.

Usage guidelines

You can configure this command multiple times for the same PQ list to establish multiple assignment rules based on input interfaces.

Examples

In PQ list 12, assign packets received on GigabitEthernet 2/1/1 to the middle queue.

```
<Sysname> system-view
[Sysname] qos pql 12 inbound-interface gigabitethernet 2/1/1 queue middle
```

qos pql local-precedence

Use **qos pql local-precedence** to configure an assignment rule for a PQ list to assign packets with any of the specified local precedence values to a priority queue.

Use **undo qos pql local-precedence** to delete an assignment rule based on the specified local precedence values from a PQ list.

Syntax

qos pql *pql-index* **local-precedence** *local-precedence-list* **queue** { **bottom** | **middle** | **normal** | **top** }

undo qos pql *pql-index* **local-precedence** *local-precedence-list*

Default

No assignment rule is configured for a PQ list.

Views

System view

Predefined user roles

network-admin

Parameters

pql-index: Specifies a PQ list by its number in the range of 1 to 16.

local-precedence-list: Specifies a space-separated list of up to eight local precedence values. The value range is 0 to 7.

top, **middle**, **normal**, **bottom**: Specifies a priority queue. The four queues are in descending priority order.

Usage guidelines

You can configure this command multiple times for the same PQ list to establish multiple assignment rules based on local precedence values.

Examples

In PQ list 12, assign packets with local precedence 3 to the middle queue.

```
<Sysname> system-view
[Sysname] qos pql 12 local-precedence 3 queue middle
```

qos pql protocol

Use **qos pql protocol** to configure an assignment rule for a PQ list to assign packets of the specified protocol type to a priority queue.

Use **undo qos pql protocol** to delete an assignment rule based on the specified protocol type from a PQ list.

Syntax

qos pql *pql-index* **protocol** { **ip** | **ipv6** } [*queue-key key-value*] **queue** { **bottom** | **middle** | **normal** | **top** }

undo qos pql *pql-index* **protocol** { **ip** | **ipv6** } [*queue-key key-value*]

Default

No assignment rule is configured for a PQ list.

Views

System view

Predefined user roles

network-admin

Parameters

pql-index: Specifies a PQ list by its number in the range of 1 to 16.

top, **middle**, **normal**, **bottom**: Specifies a priority queue. The four queues are in descending priority order.

queue-key key-value: Matches specific IP or IPv6 packets. If you specify neither the *queue-key* argument nor the *key-value* argument, all IP or IPv6 packets are matched.

Table 35 Values of the *queue-key* argument and the *key-value* argument

queue-key	key-value	Description
acl	ACL number in the range of 2000 to 3999	Packets matching a specific ACL are enqueued.
fragments	N/A	Fragmented packets are enqueued.
greater-than	Length in the range of 0 to 65535	Packets greater than a specific size are enqueued.
less-than	Length in the range of 0 to 65535	Packets smaller than a specific size are enqueued.
tcp	Port number in the range of 0 to 65535 or port name	Packets with a specific source or destination TCP port number are enqueued.
udp	Port number in the range of 0 to 65535 or port name	Packets with a specific source or destination UDP port number are enqueued.

Usage guidelines

When classifying a packet, the system matches the packet against match criteria in the order configured. When a match is found, the matching process ends.

You can configure this command multiple times for the same PQ list to establish multiple assignment rules based on protocol types.

Examples

In PQ list 5, assign IP packets matching ACL 3100 to the top queue.

```
<Sysname> system-view
[Sysname] qos pql 5 protocol ip acl 3100 queue top
```

qos pql protocol mpls exp

Use **qos pql protocol mpls exp** to configure an assignment rule for a PQ list to assign packets with any of the specified MPLS EXP values to a priority queue.

Use **undo qos pql protocol mpls exp** to delete an assignment rule based on the specified MPLS EXP values from a PQ list.

Syntax

qos pql *pql-index* **protocol mpls exp** *exp-list* **queue** { **bottom** | **middle** | **normal** | **top** }

undo qos pql *pql-index* **protocol mpls exp** *exp-list*

Default

No assignment rule is configured for a PQ list.

Views

System view

Predefined user roles

network-admin

Parameters

pql-index: Specifies a PQ list by its number in the range of 1 to 16.

exp-list: Specifies a space-separated list of up to eight MPLS EXP values. The value range is 0 to 7.

top, **middle**, **normal**, **bottom**: Specifies a priority queue. The four queues are in descending priority order.

Usage guidelines

You can configure this command multiple times for the same PQ list to establish multiple assignment rules based on MPLS EXP values.

Examples

In PQ list 12, assign packets with MPLS EXP value 2 or 4 to the top queue.

```
<Sysname> system-view
[Sysname] qos pql 12 protocol mpls exp 2 4 queue top
```

qos pql queue

Use **qos pql queue** to specify the length of a priority queue in a PQ list.

Use **undo qos pql queue** to restore the default length for a priority queue in a PQ list.

Syntax

qos pql *pql-index* **queue** { **bottom** | **middle** | **normal** | **top** } **queue-length** *queue-length*

undo qos pql *pql-index* **queue** { **bottom** | **middle** | **normal** | **top** } **queue-length**

Default

The queue length values for top, middle, normal, and bottom queues are 20, 40, 60, and 80, respectively.

Views

System view

Predefined user roles

network-admin

Parameters

pql-index: Specifies a PQ list by its number in the range of 1 to 16.

top, **middle**, **normal**, **bottom**: Specifies a priority queue. The four queues are in descending priority order.

queue-length: Specifies the queue length in the range of 1 to 1024.

Usage guidelines

The priority queue length specifies the maximum number of packets that a priority queue can hold.

If a queue is full, all subsequent packets to this queue are dropped.

Examples

In PQ list 10, set the length of the top queue to 10.

```
<Sysname> system-view
[Sysname] qos pql 10 queue top queue-length 10
```

CQ commands

display qos queue cq interface

Use **display qos queue cq interface** to display the CQ information for interfaces or PVCs.

Syntax

display qos queue cq interface [*interface-type interface-number* [**pvc** { *pvc-name* | *vpi/vci* }]]

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 CQ information for all interfaces.

pvc { *pvc-name* | *vpi/vci* }: Specifies a PVC by its name or VPI/VCI value. You can specify a PVC only for an ATM interface. When you specify an ATM interface but do not specify a PVC, this command displays the CQ information for all PVCs on the ATM interface.

Usage guidelines

If you specify a VT interface, this command displays the CQ information for all VA interfaces of the VT interface. A VT interface itself does not have QoS information.

Examples

Display the CQ information for interface GigabitEthernet 2/1/1.

```
<Sysname>display qos queue cq interface gigabitethernet 2/1/1
Interface: GigabitEthernet2/1/1
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - Custom queuing: CQL 1 Size/Length/Discards
1:   0/20/0          2:   0/20/0          3:   0/20/0
4:   0/20/0          5:   0/20/0          6:   0/20/0
7:   0/20/0          8:   0/20/0          9:   0/20/0
10:   0/20/0         11:   0/20/0         12:   0/20/0
13:   0/20/0         14:   0/20/0         15:   0/20/0
16:   0/20/0
```

Table 36 Command output

Field	Description
Size	Number of packets in a queue.
Length	Queue length, which specifies the maximum number of packets that a queue can hold.
Discards	Number of dropped packets.

display qos cql

Use **display qos cql** to display the CQ list configuration.

Syntax

Centralized devices in standalone mode:

display qos cql [*cql-index*]

Distributed devices in standalone mode/centralized devices in IRF mode:

display qos cql [*cql-index*] [**slot** *slot-number*]

Distributed devices in IRF mode:

display qos cql [*cql-index*] [**chassis** *chassis-number* **slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

cql-index: Specifies a CQ list by its number in the range of 1 to 16. If you do not specify a CQ list, this command displays the configuration of all CQ lists.

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command displays the CQ list configuration for the active MPU. (Distributed devices in standalone mode.)

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the CQ list configuration for the master device. (Centralized devices in IRF mode.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. If you do not specify this option, the command displays the CQ list configuration for the global active MPU. (Distributed devices in IRF mode.)

Examples

Display the configuration of all CQ lists.

```
<Sysname> display qos cql
Current CQL configuration:
List  Queue  Parameters
-----------------------------------------------------
2     3      Protocol ip fragments
3     6      Length 100
3     1      Inbound-interface GigabitEthernet2/1/1
4     5      Local-precedence 7
```

qos cq

Use **qos cq** to apply a CQ list to an interface or PVC.

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

Syntax

qos cq cql *cql-index*

undo qos cq

Default

FIFO queuing is used on an interface.

Views

Interface view, PVC view

Predefined user roles

network-admin

Parameters

cql *cql-index*: Specifies a CQ list by its number in the range of 1 to 16.

Usage guidelines

If you apply multiple CQ lists to an interface or PVC, the CQ list last applied takes effect.

Multiple match criteria can be configured for a CQ list. When a packet arrives, it is examined against match criteria in their configuration order.

- When a match is found, the packet is assigned to the corresponding queue, and the matching process ends.
- If no match is found, the packet is assigned to the default queue.

You must configure the rate limit for the queuing feature to take effect on the following interfaces:

- Tunnel interfaces.
- Subinterfaces.
- Layer 3 aggregate interfaces.
- HDLC link bundle interfaces.
- RPR logical interfaces.

- VT and dialer interfaces configured with PPPoE, PPPoA, or PPPoEoA.

Examples

Apply CQ list 5 to GigabitEthernet 2/1/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/1/1
[Sysname-GigabitEthernet2/1/1] qos cq cql 5
```

qos cql default-queue

Use **qos cql default-queue** to specify a custom queue as the default queue for a CQ list.

Use **undo qos cql default-queue** to restore the default.

Syntax

qos cql *cql-index* **default-queue** *queue-id*

undo qos cql *cql-index* **default-queue**

Default

Queue 1 is the default queue.

Views

System view

Predefined user roles

network-admin

Parameters

cql-index: Specifies a CQ list by its number in the range of 1 to 16.

queue-id: Specifies a custom queue by its ID in the range of 1 to 16.

Usage guidelines

If a packet does not match any criteria in a CQ list, the packet is assigned to the default queue of the CQ list.

Examples

Specify queue 2 as the default queue for CQ list 5.

```
<Sysname> system-view
[Sysname] qos cql 5 default-queue 2
```

qos cql inbound-interface

Use **qos cql inbound-interface** to configure an assignment rule for a CQ list to assign packets received on the specified interface to a custom queue.

Use **undo qos cql inbound-interface** to delete an assignment rule based on the specified input interface from a CQ list.

Syntax

qos cql *cql-index* **inbound-interface** *interface-type interface-number* **queue** *queue-id*

undo qos cql *cql-index* **inbound-interface** *interface-type interface-number*

Default

No assignment rule is configured for a CQ list.

Views

System view

Predefined user roles

network-admin

Parameters

cql-index: Specifies a CQ list by its number in the range of 1 to 16.

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

queue-id: Specifies a custom queue by its ID in the range of 1 to 16.

Usage guidelines

You can configure this command multiple times for the same CQ list to establish multiple assignment rules based on input interfaces.

Examples

In CQ list 5, assign packets received from GigabitEthernet 2/1/1 to custom queue 3.

```
<Sysname> system-view
[Sysname] qos cql 5 inbound-interface gigabitethernet 2/1/1 queue 3
```

qos cql local-precedence

Use **qos cql local-precedence** to configure an assignment rule for a CQ list to assign packets with any of the specified local precedence values to a custom queue.

Use **undo qos cql local-precedence** to delete an assignment rule based on the specified local precedence values from a CQ list.

Syntax

qos cql *cql-index* **local-precedence** *local-precedence-list* **queue** *queue-id*

undo qos cql *cql-index* **local-precedence** *local-precedence-list*

Default

No assignment rule is configured for a CQ list.

Views

System view

Predefined user roles

network-admin

Parameters

cql-index: Specifies a CQ list by its number in the range of 1 to 16.

local-precedence-list: Specifies a space-separated list of up to eight local precedence values. The value range is 0 to 7.

queue-id: Specifies a custom queue by its ID in the range of 1 to 16.

Usage guidelines

You can configure this command multiple times for the same CQ list to establish multiple assignment rules based on local precedence values.

Examples

In CQ list 5, assign packets with local precedence 4 to custom queue 3.

```
<Sysname> system-view
```

```
[Sysname] qos cql 5 local-precedence 4 queue 3
```

qos cql protocol

Use **qos cql protocol** to configure an assignment rule for a CQ list to assign packets of the specified protocol type to a custom queue.

Use **undo qos cql protocol** to delete an assignment rule based on the specified protocol type from a CQ list.

Syntax

qos cql *cql-index* **protocol** { **ip** | **ipv6** } [*queue-key key-value*] **queue** *queue-id*

undo qos cql *cql-index* **protocol** { **ip** | **ipv6** } [*queue-key key-value*]

Default

No assignment rule is configured for a CQ list.

Views

System view

Predefined user roles

network-admin

Parameters

cql-index: Specifies a CQ list by its number in the range of 1 to 16.

queue-id: Specifies a custom queue by its ID in the range of 1 to 16.

queue-key key-value: Matches specific IP or IPv6 packets. If you specify neither the *queue-key* argument nor the *key-value* argument, all IP or IPv6 packets are matched.

Table 37 Values of the *queue-key* argument and the *key-value* argument

queue-key	key-value	Description
acl	ACL number in the range of 2000 to 3999	Packets matching a specific ACL are enqueued.
fragments	N/A	Fragmented packets are enqueued.
greater-than	Length in the range of 0 to 65535	Packets greater than a specific size are enqueued.
less-than	Length in the range of 0 to 65535	Packets smaller than a specific size are enqueued.
tcp	Port number in the range of 0 to 65535 or port name	Packets with a specific source or destination TCP port number are enqueued.
udp	Port number in the range of 0 to 65535 or port name	Packets with a specific source or destination UDP port number are enqueued.

Usage guidelines

When classifying a packet, the system matches the packet against match criteria in their configuration order. When a match is found, the matching process ends.

You can configure this command multiple times for the same CQ list to establish multiple assignment rules based on protocol types.

Examples

In CQ list 5, assign IP packets matching ACL 3100 to custom queue 3.

```
<Sysname> system-view
[Sysname] qos cql 5 protocol ip acl 3100 queue 3
```

qos cql protocol mpls exp

Use **qos cql protocol mpls exp** to configure an assignment rule for a CQ list to assign packets with any of the specified MPLS EXP values to a custom queue.

Use **undo qos cql protocol mpls exp** to delete an assignment rule based on the specified MPLS EXP values from a CQ list.

Syntax

qos cql *cql-index* **protocol mpls exp** *exp-list* **queue** *queue-id*

undo qos cql *cql-index* **protocol mpls exp** *exp-list*

Default

No assignment rule is configured for a CQ list.

Views

System view

Predefined user roles

network-admin

Parameters

cql-index: Specifies a CQ list by its number in the range of 1 to 16.

exp-list: Specifies a space-separated list of up to eight MPLS EXP values. The value range is 0 to 7.

queue-id: Specifies a custom queue by its ID in the range of 1 to 16.

Usage guidelines

You can configure this command multiple times for the same CQ list to establish multiple assignment rules based on MPLS EXP values.

Examples

In CQ list 5, assign packets with MPLS EXP value 2 or 4 to custom queue 3.

```
<Sysname> system-view
[Sysname] qos cql 5 protocol mpls exp 2 4 queue 3
```

qos cql queue

Use **qos cql queue** to specify the length of a custom queue in a CQ list.

Use **undo qos cql queue** to restore the default length for a custom queue in a CQ list.

Syntax

qos cql *cql-index* **queue** *queue-id* **queue-length** *queue-length*

undo qos cql *cql-index* **queue** *queue-id* **queue-length**

Default

The queue length is 20 for each queue.

Views

System view

Predefined user roles

network-admin

Parameters

cql-index: Specifies a CQ list by its number in the range of 1 to 16.

queue-id: Specifies a custom queue by its ID in the range of 1 to 16.

queue-length: Specifies the queue length in the range of 1 to 1024.

Usage guidelines

The custom queue length specifies the maximum number of packets that a custom queue can hold.

If a queue is full, all subsequent packets to this queue are dropped.

Examples

In CQ list 5, set the length of custom queue 4 to 40.

```
<Sysname> system-view
[Sysname] qos cql 5 queue 4 queue-length 40
```

qos cql queue serving

Use **qos cql queue serving** to specify the number of bytes forwarded from a queue during a cycle.

Use **undo qos cql queue serving** to restore the default.

Syntax

qos cql *cql-index* **queue** *queue-id* **serving** *byte-count*

undo qos cql *cql-index* **queue** *queue-id* **serving**

Default

The number of bytes forwarded from a queue during a cycle is 1500 bytes.

Views

System view

Predefined user roles

network-admin

Parameters

cql-index: Specifies a CQ list by its number in the range of 1 to 16.

queue-id: Specifies a custom queue by its ID in the range of 1 to 16.

byte-count: Specifies the number of bytes forwarded from a queue during a cycle of queue scheduling. The value range for the *byte-count* argument is 1 to 16777215 bytes.

Examples

In CQ list 5, set the byte count to 1400 for queue 2.

```
<Sysname> system-view
[Sysname] qos cql 5 queue 2 serving 1400
```

WFQ commands

display qos queue wfq

Use **display qos queue wfq** to display the WFQ information for interfaces, PVCs, or PWs.

Syntax

display qos queue wfq { **interface** [*interface-type interface-number* [**pvc** { *pvc-name* | *vpi/vci* }]] | **l2vpn-pw** [**peer** *ip-address* **pw-id** *pw-id*] }

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 WFQ information for all interfaces.

pvc { *pvc-name* | *vpi/vci* }: Specifies a PVC by its name or VPI/VCI value. You can specify a PVC only for an ATM interface. When you specify an ATM interface but do not specify a PVC, this command displays the WFQ information for all PVCs on the ATM interface.

peer *ip-address* **pw-id** *pw-id*: Specifies a PW by its peer PE LSR ID and its PW ID. The *ip-address* argument represents the LSR ID of the peer PE of the PW. The value range for the *pw-id* argument is 1 to 4294967295. If you do not specify a PW, this command displays the WFQ information for all PWs.

Examples

Display the WFQ information for GigabitEthernet 2/1/1.

```
<Sysname> display qos queue wfq interface gigabitethernet 2/1/1
Interface: GigabitEthernet2/1/1
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - Weighted Fair queuing: Size/Length/Discards 0/64/0
  Weight: IP Precedence
  Queues: Active/Max active/Total 0/0/128
```

Display the WFQ information for all PWs.

```
<Sysname> display qos queue wfq l2vpn-pw
L2VPN-PW: peer 1.1.1.1, pw-id 1
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - Weighted Fair queuing: Size/Length/Discards 0/64/0
  Weight: IP Precedence
  Queues: Active/Max active/Total 0/0/128
```

Table 38 Command output

Field	Description
Interface	Interface name, including the interface type and interface number.

L2VPN-PW	A PW is uniquely identified by a combination of the peer PE IP address and PW ID.
Size	Number of packets in the queue.
Length	Queue length.
Discards	Number of dropped packets.
Weight	Weight type: • **IP Precedence**. • **DSCP**.
Active	Number of active WFQ queues.
Max active	Maximum number of active WFQ queues that was reached.
Total	Total number of configured WFQ queues.

qos wfq

Use **qos wfq** to apply WFQ to an interface, PVC, or PW. You can also use this command to modify WFQ parameters.

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

Syntax

qos wfq [**dscp** | **precedence**] [**queue-number** *total-queue-number* | **queue-length** *max-queue-length*] *

undo qos wfq

Default

FIFO is used.

Views

Cross-connect PW view/VSI LDP PW view/VSI static PW view

Interface view

PVC view

Predefined user roles

network-admin

Parameters

dscp: Specifies a DSCP weight.

precedence: Specifies an IP precedence weight.

queue-length *max-queue-length*: Specifies the maximum number of packets a queue can hold. The value range for the *max-queue-length* argument is 1 to 1024, and the default is 64.

queue-number *total-queue-number*: Specifies the total number of queues, which can be 16, 32, 64, 128, 256, 512, 1024, 2048, or 4096. The default is 256.

Usage guidelines

If you do not specify a weight type, the default weight type is IP precedence.

For the queuing feature to take effect on a subinterface, you must configure the rate limit on the subinterface.

Examples

Apply WFQ to GigabitEthernet 2/1/1, and set the maximum queue length to 100 and the total number of queues to 512.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/1/1
[Sysname-GigabitEthernet2/1/1] qos wfq queue-length 100 queue-number 512
```

Related commands

display qos queue wfq interface

RTPQ commands

display qos queue rtpq interface

Use **display qos queue rtpq interface** to display the RTPQ information for interfaces or PVCs.

Syntax

display qos queue rtpq interface [*interface-type interface-number* [**pvc** { *pvc-name* | *vpi/vci* }]]

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 RTPQ information for all interfaces.

pvc { *pvc-name* | *vpi/vci* }: Specifies a PVC by its name or VPI/VCI value. You can specify a PVC only for an ATM interface. When you specify an ATM interface but do not specify a PVC, this command displays the RTPQ information for all PVCs on the ATM interface.

Usage guidelines

If you specify a VT interface, this command displays the RTPQ information for all VA interfaces of the VT interface. A VT interface itself does not have QoS information.

Examples

Display the RTPQ information for interface GigabitEthernet 2/1/1.

```
<Sysname> display qos queue rtpq interface
Interface: GigabitEthernet2/1/1
Output queue - RTP queuing: Size/Max/Outputs/Discards 0/0/0/0
```

Table 39 Command output

Field	Description
Size	Number of packets in a queue.
Max	Historical maximum number of packets in the queue.
Outputs	Number of sent packets.
Discards	Number of dropped packets.

qos rtpq

Use **qos rtpq** to enable RTPQ on an interface or PVC for RTP packets to specific UDP ports.

Use **undo qos rtpq** to disable RTPQ on an interface or PVC.

Syntax

qos rtpq start-port *first-rtp-port-number* **end-port** *last-rtp-port-number* **bandwidth** *bandwidth* [**cbs** *committed-burst-size*]

undo qos rtpq

Default

RTPQ is disabled an interface or PVC.

Views

Interface view, PVC view

Predefined user roles

network-admin

Parameters

start-port *first-rtp-port-numbe*r: Specifies the start UDP port number in the range of 2000 to 65535.

end-port *last-rtp-port-numbe*r: Specifies the end UDP port number in the range of 2000 to 65535.

bandwidth *bandwidth*: Specifies the maximum bandwidth allowed for the RTP priority queue, in the range of 8 to 1000000 kbps.

cbs *committed-burst-size*: Specifies the CBS in the range of 1500 to 2000000 bytes.

Usage guidelines

This command provides preferential service for delay-sensitive applications, such as real-time voice traffic transmission.

Set the *bandwidth* argument to a value greater than the required bandwidth for real-time applications to allow bursts of traffic.

Examples

Enable RTPQ on GigabitEthernet 2/1/1 for RTP packets with a destination UDP port number in the range of 16384 to 32767.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/1/1
[Sysname-GigabitEthernet2/1/1] qos rtpq start-port 16384 end-port 32767 bandwidth 64
```

CBQ commands

display qos queue cbq

Use **display qos queue cbq** to display the CBQ information for interfaces PVCs, or PWs.

Syntax

display qos queue cbq { **interface** [*interface-type interface-number* [**pvc** { *pvc-name* | *vpi/vci* }]] | **l2vpn-pw** [**peer** *ip-address* **pw-id** *pw-id*] }

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 the CBQ information for all interfaces.

pvc { *pvc-name* | *vpi/vci* }: Specifies a PVC by its name or VPI/VCI value. You can specify a PVC only for an ATM interface. When you specify an ATM interface but do not specify a PVC, this command the CBQ information for all PVCs on the ATM interface.

peer *ip-address* **pw-id** *pw-id*: Specifies a PW by its peer PE LSR ID and its PW ID. The *ip-address* argument represents the LSR ID of the peer PE of the PW. The value range for the *pw-id* argument is 1 to 4294967295. If you do not specify a PW, this command displays the CBQ information for all PWs.

Examples

Display the CBQ information for all interfaces.

```
<Sysname> display qos queue cbq interface
Interface: GigabitEthernet2/1/1
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - Class Based Queuing: Size/Discards 0/0
Queue Size: EF/AF/BE 0/0/0
  BE Queues: Active/Max active/Total 0/0/256
  AF Queues: Allocated 1
  Bandwidth(kbps): Available/Max reserve 74992/75000
```

Display the CBQ information for all PWs.

```
<Sysname> display qos queue cbq l2vpn-pw
L2VPN-PW: peer 1.1.1.1, pw-id 1
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - Class Based Queuing: Size/Discards 0/0
Queue Size: EF/AF/BE 0/0/0
  BE Queues: Active/Max active/Total 0/0/256
  AF Queues: Allocated 1
  Bandwidth(kbps): Available/Max reserve 74992/75000
```

Table 40 Command output

Field	Description
Interface	Interface name, including the interface type and interface number.
L2VPN-PW	A PW is uniquely identified by a combination of the peer PE IP address and PW ID.
Size	Number of packets in the queue.
Length	Queue length.
Discards	Number of dropped packets.
EF	EF queue.
AF	AF queue.

BE	BE queue.
Active	Number of active BE queues.
Max active	Maximum number of active BE queues allowed.
Total	Total number of BE queues.
Available	Available bandwidth for CBQ.
Max reserve	Maximum reserved bandwidth for CBQ.

qos reserved-bandwidth

Use **qos reserved-bandwidth** to set the maximum reserved bandwidth as a percentage of available bandwidth of the interface.

Use **undo qos reserved-bandwidth** to restore the default.

Syntax

qos reserved-bandwidth pct *percent*

undo qos reserved-bandwidth

Default

The maximum reserved bandwidth is 80% of available bandwidth of the interface

Views

Interface view, PVC view

Predefined user roles

network-admin

Parameters

percent: Specifies the percentage of available bandwidth to be reserved. The value range for this argument is 1 to 100.

Usage guidelines

The maximum reserved bandwidth is set on a per-interface basis. It decides the maximum bandwidth assignable for the QoS queues on an interface. It is typically set no greater than 80% of available bandwidth, considering the bandwidth for control traffic and Layer 2 frame headers.

Use the default maximum reserved bandwidth setting in most situations. If you adjust the setting, make sure the Layer 2 frame header plus the data traffic is under the maximum available bandwidth of the interface.

The maximum available bandwidth of an interface can be set by using the **bandwidth** command. For more information about this command, see *Interface Command Reference*.

Examples

Set the maximum reserved bandwidth to 70% of available bandwidth on interface GigabitEthernet 2/1/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/1/1
[Sysname-GigabitEthernet2/1/1] qos reserved-bandwidth 70
```

queue af

Use **queue af** to enable assured-forwarding (AF) and set its minimum guaranteed bandwidth.

Use **undo queue af** to delete the action.

Syntax

queue af bandwidth { *bandwidth* | **pct** *percentage* | **remaining-pct** *remaining-percentage* }

undo queue af

Default

AF is not configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

bandwidth: Specifies the bandwidth in the range of 8 to 10000000 kbps.

pct *percentage*: Specifies the percentage of the available bandwidth, in the range of 1 to 100.

remaining-pct *remaining-percentage*: Specifies the percentage of the remaining bandwidth, in the range of 1 to 100.

Usage guidelines

To associate the traffic behavior configured with the **queue af** command with a class in a policy, you must follow these requirements:

- The total bandwidth assigned to AF and EF queues in a policy cannot exceed the maximum available bandwidth of the interface where the policy is applied.
- The total percentage of bandwidth assigned to AF and EF in a policy cannot exceed 100.
- The bandwidth assigned to AF and EF in a policy must use the same form, either as an absolute bandwidth value or as a percentage.

Examples

Configure AF in traffic behavior **database** and assign the minimum guaranteed bandwidth 200 kbps to it.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] queue af bandwidth 200
```

Related commands

- **display qos queue cbq interface**
- **traffic behavior**

queue ef

Use **queue ef** to configure expedited forwarding (EF) and assign its maximum bandwidth.

Use **undo queue ef** to delete the action.

Syntax

queue ef bandwidth { *bandwidth* [**cbs** *burst*] | **pct** *percentage* [**cbs-ratio** *ratio*] }

undo queue ef

Default

EF is not configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

bandwidth: Specifies the bandwidth in the range of 8 to 10000000 kbps.

cbs *burst*: Sets the CBS in the range of 32 to 1000000000 bytes. The default is *bandwidth* × 25.

pct *percentage*: Specifies the percentage of the available bandwidth, in the range of 1 to 100.

cbs-ratio *ratio*: Sets the allowed burst ratio in the range of 25 to 500. This default is 25.

Usage guidelines

You cannot use the command in conjunction with the **queue af** command or the **queue-length** command.

In a policy, the default class cannot be associated with the traffic behavior that has the **queue ef** command.

The total bandwidth assigned to AF and EF in a policy cannot exceed the maximum available bandwidth of the interface where the policy is applied.

The total percentage of the maximum available bandwidth assigned to AF and EF in a policy cannot exceed 100.

The bandwidths assigned to AF and EF in a policy must have the same type, bandwidth or percentage.

After the **queue ef bandwidth pct** *percentage* [**cbs-ratio** *ratio*] command is used, CBS equals (Interface available bandwidth × *percentage* × *ratio*)/100/1000.

After the **queue ef bandwidth** *bandwidth* [**cbs** *burst*] command is used, CBS equals *burst*. If the *burst* argument is not specified, CBS equals *bandwidth* × 25.

Examples

Configure EF in traffic behavior **database**, with the maximum bandwidth as 200 kbps and CBS as 5000 bytes.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] queue ef bandwidth 200 cbs 5000
```

Related commands

- **display qos queue cbq interface**
- **traffic behavior**

queue wfq

Use **queue wfq** to configure WFQ for the default class.

Use **undo queue wfq** to delete the action.

Syntax

queue wfq [**queue-number** *total-queue-number*]

undo queue wfq

Default

WFQ is not configured for the default class.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

queue-number *total-queue-number*: Specifies the number of fair queues, which can be 16, 32, 64, 128, 256, 512, 1024, 2048, or 4096. The default is 256.

Usage guidelines

The traffic behavior configured with this command can only be associated with the default class. This command can be used in conjunction with the **queue-length** or **wred** command.

Examples

Configure the default class to use WFQ with 16 queues.

```
<Sysname> system-view
[Sysname] traffic behavior test
[Sysname-behavior-test] queue wfq queue-number 16
[Sysname] qos policy user1
[Sysname-qospolicy-user1] classifier default-class behavior test
```

Related commands

- **display qos queue cbq interface**
- **traffic behavior**

queue-length

Use **queue-length** to set the maximum queue length and use tail drop.

Use **undo queue-length** to delete the action.

Syntax

queue-length *queue-length*

undo queue-length

Default

Tail drop is used, and the queue length is 64 packets.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

queue-length: Specifies the maximum queue length in the range of 1 to 1024 packets.

Usage guidelines

Before configuring this command, make sure the **queue af** command or the **queue wfq** command has been configured.

The **undo queue af** or **undo queue wfq** command deletes the queue length configured by using the **queue-length** command.

Examples

Set the maximum queue length to 16 and specify tail drop for AF.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] queue af bandwidth 200
[Sysname-behavior-database] queue-length 16
```

Related commands

- **queue af**
- **queue wfq**

wred

Use **wred** to enable WRED.

Use **undo wred** to disable WRED.

Syntax

wred [**dscp** | **ip-precedence**]

undo wred

Default

WRED is not enabled.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

dscp: Uses the DSCP value for calculating the drop probability for a packet.

ip-precedence: Uses the IP precedence value for calculating the drop probability for a packet. This keyword is used by default.

Usage guidelines

You can configure this command only after you have configured the **queue af** or **queue wfq** command.

This command and the **queue-length** command are mutually exclusive.

When WRED is disabled, other WRED configurations are deleted.

Examples

Enable WRED in traffic behavior **database** and calculate the drop probabilities based on IP precedence values.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] queue wfq
[Sysname-behavior-database] wred
```

Related commands

- **queue af**
- **queue wfq**

wred dscp

Use **wred dscp** to set the lower limit, upper limit, and drop probability for packets with a DSCP value.

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

Syntax

wred dscp *dscp-value* **low-limit** *low-limit* **high-limit** *high-limit* [**discard-probability** *discard-prob*]

undo wred dscp *dscp-value*

Default

The lower limit is 10, the upper limit is 30, and the drop probability is 1/10.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63. This argument can also be represented by using one of the keywords listed in Table 19.

low limit *low-limit*: Specifies the lower WRED limit (in packets) in the range of 1 to 1024.

high-limit *high-limit*: Specifies the upper WRED limit (in packets) in the range of 1 to 1024.

discard-probability *discard-prob*: Specifies the drop probability in the range of 1 to 255.

Usage guidelines

Before configuring this command, make sure DSCP-based WRED is enabled by using the **wred** command.

Disabling WRED also removes the **wred dscp** command configuration.

Removing the **queue af** or **queue wfq** command configuration also removes the WRED-related parameters.

Examples

Set the following parameters for packets with DSCP value 3: lower limit 20, upper limit 40, and drop probability 1/15.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] queue wfq
[Sysname-behavior-database] wred dscp
[Sysname-behavior-database] wred dscp 3 low-limit 20 high-limit 40 discard-probability
15
```

Related commands

- **queue af**
- **queue wfq**
- **wred**

wred ip-precedence

Use **wred ip-precedence** to set the lower limit, upper limit, and drop probability for packets with an IP precedence value.

Use **undo wred ip-precedence** to restore the default.

Syntax

wred ip-precedence *precedence* **low-limit** *low-limit* **high-limit** *high-limit* [**discard-probability** *discard-prob*]

undo wred ip-precedence *precedence*

Default

The lower limit is 10, the upper limit is 30, and the drop probability is 1/10.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

precedence: Specifies an IP precedence value in the range of 0 to 7.

low limit *low-limit*: Specifies the lower WRED limit (in packets) in the range of 1 to 1024.

high-limit *high-limit*: Specifies the upper WRED limit (in packets) in the range of 1 to 1024.

discard-probability *discard-prob*: Specifies the drop probability in the range of 1 to 255.

Usage guidelines

Before configuring this command, make sure IP precedence-based WRED is enabled by using the **wred** command.

Disabling WRED also removes the **wred ip-precedence** command configuration.

Removing the **queue af** or **queue wfq** command configuration also removes the WRED-related parameters.

Examples

Configure the following parameters for packets with IP precedence value 3: lower limit 20, upper limit 40, and drop probability 1/15.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] queue wfq
[Sysname-behavior-database] wred ip-precedence
[Sysname-behavior-database] wred ip-precedence 3 low-limit 20 high-limit 40
discard-probability 15
```

Related commands

- **queue af**
- **queue wfq**
- **wred**

wred weighting-constant

Use **wred weighting-constant** to set the exponent for WRED to calculate the average queue size.

Use **undo wred weighting-constant** to restore the default.

Syntax

wred weighting-constant *exponent*

undo wred weighting-constant

Default

The exponent for WRED to calculate the average queue size is 9.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

exponent: Specifies the exponent in the range of 1 to 16.

Usage guidelines

Before configuring this command, make sure the **queue af** or **queue wfq** command is configured and WRED is enabled by using the **wred** command.

Disabling WRED also removes the **wred weighting-constant** command configuration.

Examples

Set the WRED exponent to calculate the average queue size to 6.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] queue af bandwidth 200
[Sysname-behavior-database] wred ip-precedence
[Sysname-behavior-database] wred weighting-constant 6
```

Related commands

- **queue af**
- **queue wfq**
- **wred**

Packet information pre-extraction commands

qos pre-classify

Use **qos pre-classify** to enable packet information pre-extraction on an interface.

Use **undo qos pre-classify** to disable packet information pre-extraction on an interface.

Syntax

qos pre-classify

undo qos pre-classify

Default

Packet information pre-extraction is disabled.

Views

Tunnel interface view

Predefined user roles

network-admin

Examples

Enable packet information pre-extraction on interface Tunnel 1.

```
<Sysname> system-view
[Sysname] interface tunnel 1
[Sysname-Tunnel1] qos pre-classify
```

Token sending commands

qos qmtoken

Use **qos qmtoken** to configure the token sending feature.

Use **undo qos qmtoken** to disable the token sending feature.

Syntax

qos qmtoken *token-number*

undo qos qmtoken

Default

The token sending feature is disabled.

Views

Interface view

Predefined user roles

network-admin

Parameters

token-number: Specifies the number of QoS tokens sent to the low-layer queue at a time, in the range of 1 to 256.

Usage guidelines

This feature is a lower-layer flow control mechanism that controls the number of packets sent to the low-layer queue based on the set number of tokens.

This feature can reduce the delay of the EF queue in CBQ when the interface is congested.

This feature can also help prevent QoS queuing from failing to work in FTP transfers where TCP provides flow control.

As a best practice, do not use this feature for upper layer protocols that do not provide flow control (for example, UDP).

To make the token sending feature take effect on an interface, you must re-enable the interface by executing the **shutdown** and **undo shutdown** commands.

Only serial interfaces support this feature.

Examples

Set the number of QoS tokens sent at a time to 1 for interface Serial 2/2/1.

```
<Sysname> system-view
[Sysname] interface serial 2/2/1
[Sysname-Serial2/2/1] qos qmtoken 1
[Sysname-Serial2/2/1] shutdown
[Sysname-Serial2/2/1] undo shutdown
```

Congestion avoidance commands

WRED commands

display qos wred interface

Use **display qos wred interface** to display the WRED information for interfaces or PVCs.

Syntax

display qos wred interface [*interface-type interface-number* [**pvc** { *pvc-name* | *vpi/vci* }]]

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 WRED information for all interfaces.

pvc { *pvc-name* | *vpi/vci* }: Specifies a PVC by its name or VPI/VCI value. You can specify a PVC only for an ATM interface. When you specify an ATM interface but do not specify a PVC, this command displays the WRED information for all PVCs on the ATM interface.

Examples

Display the WRED information for GigabitEthernet 2/1/4.

```
<Sysname> display qos wred interface
Interface: GigabitEthernet2/1/4
 Current WRED configuration:
 Exponent: 9 (1/512)
 Pre  Low   High  Dis-prob Random-discard  Tail-discard
-----------------------------------------------------
0    10    30    10       0               0
1    10    30    10       0               0
2    10    30    10       0               0
3    10    30    10       0               0
4    10    30    10       0               0
5    10    30    10       0               0
6    10    30    10       0               0
7    10    30    10       0               0
```

Table 41 Command output

Field	Description
Interface	Interface type and interface number.
Pre	IP precedence of packets.
Low	Lower limit for a queue.

High	Upper limit for a queue.
Dis-prob	Drop probability.
Random-discard	Number of packets dropped by WRED.
Tail-discard	Number of packets dropped by tail drop.

qos wred enable

Use **qos wred enable** to enable WRED on an interface or PVC.

Use **undo qos wred enable** to disable WRED.

Syntax

qos wred [**dscp** | **ip-precedence**] **enable**

undo qos wred [**dscp** | **ip-precedence**] **enable**

Default

Tail drop is used.

Views

Interface view, PVC view

Predefined user roles

network-admin

Parameters

dscp: Uses the DSCP values for calculating the drop probability.

ip-precedence: Uses the IP precedence for calculating the drop probability. This keyword is used by default.

Usage guidelines

You must enable WFQ on an interface before configuring the **qos wred enable** command.

Examples

Enable WRED on GigabitEthernet 2/1/1, and use the IP precedence for drop probability calculation.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/1/1
[Sysname-GigabitEthernet2/1/1] qos wfq queue-length 100 queue-number 512
[Sysname-GigabitEthernet2/1/1] qos wred ip-precedence enable
```

Related commands

display qos wred interface

qos wred dscp

Use **qos wred dscp** to set the lower limit, upper limit, and drop probability for a DSCP value.

Use **undo qos wred dscp** to restore the default.

Syntax

qos wred dscp *dscp-value* **low-limit** *low-limit* **high-limit** *high-limit* **discard-probability** *discard-prob*

undo qos wred dscp *dscp-value*

Default

The lower limit is 10, the upper limit is 30, and the drop probability is 1/10.

Views

Interface view, PVC view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63. This argument can also be represented by using one of the keywords listed in Table 19.

low limit *low-limit*: Specifies the lower WRED limit (in packets) in the range of 1 to 1024.

high-limit *high-limit*: Specifies the upper WRED limit (in packets) in the range of 1 to 1024.

discard-probability *discard-prob*: Specifies the drop probability in the range of 1 to 255.

Usage guidelines

Before configuring this command, enable DSCP-based WRED on the interface or PVC with the **qos wred dscp enable** command. The upper and lower limits restrict the average queue length.

Examples

Configure the following parameters for packets with DSCP value 63 on GigabitEthernet 2/1/1: lower limit 20, upper limit 40, and drop probability 1/15.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/1/1
[Sysname-GigabitEthernet2/1/1] qos wfq queue-length 100 queue-number 512
[Sysname-GigabitEthernet2/1/1] qos wred dscp enable
[Sysname-GigabitEthernet2/1/1] qos wred dscp 63 low-limit 20 high-limit 40
discard-probability 15
```

Related commands

- **display qos wred interface**
- **qos wred enable**

qos wred ip-precedence

Use **qos wred ip-precedence** to set the lower limit, upper limit, and drop probability for an IP precedence value.

Use **undo qos wred ip-precedence** to restore the default.

Syntax

qos wred ip-precedence *ip-precedence* **low-limit** *low-limit* **high-limit** *high-limit* **discard-probability** *discard-prob*

undo qos wred ip-precedence *ip-precedence*

Default

The lower limit is 10, the upper limit is 30, and the drop probability is 1/10.

Views

Interface view, PVC view

Predefined user roles

network-admin

Parameters

ip-precedence *precedence*: Specifies an IP precedence value in the range of 0 to 7.

low limit *low-limit*: Specifies the lower WRED limit (in packets) in the range of 1 to 1024.

high-limit *high-limit*: Specifies the upper WRED limit (in packets) in the range of 1 to 1024.

discard-probability *discard-prob*: Specifies the drop probability in the range of 1 to 255.

Usage guidelines

Before configuring this command, enable IP precedence-based WRED on the interface or PVC with the **qos wred enable** command.

The upper and lower limits restrict the average queue length.

Examples

Configure the following parameters for packets with IP precedence value 3 on GigabitEthernet 2/1/1: lower limit 20, upper limit 40, and drop probability 1/15.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/1/1
[Sysname-GigabitEthernet2/1/1] qos wfq queue-length 100 queue-number 512
[Sysname-GigabitEthernet2/1/1] qos wred ip-precedence enable
[Sysname-GigabitEthernet2/1/1] qos wred ip-precedence 3 low-limit 20 high-limit 40
discard-probability 15
```

Related commands

- **display qos wred interface**
- **qos wred enable**

qos wred weighting-constant

Use **qos wred weighting-constant** to set the exponent for WRED to calculate the average queue size.

Use **undo qos wred weighting-constant** to restore the default.

Syntax

qos wred weighting-constant *exponent*

undo qos wred weighting-constant

Default

The exponent for WRED to calculate the average queue size is 9.

Views

Interface view, PVC view

Predefined user roles

network-admin

Parameters

exponent: Specifies the exponent for average queue length calculation, in the range of 1 to 16.

Usage guidelines

Before configuring this command, enable WRED on the interface or PVC with the **qos wred enable** command.

Examples

Set the exponent for the average queue size calculation to 6 on GigabitEthernet 2/1/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/1/1
[Sysname-GigabitEthernet2/1/1] qos wfq queue-length 100 queue-number 512
[Sysname-GigabitEthernet2/1/1] qos wred enable
[Sysname-GigabitEthernet2/1/1] qos wred weighting-constant 6
```

Related commands

- **display qos wred interface**
- **qos wred enable**

QPPB commands

bgp-policy

Use **bgp-policy** to enable QPPB, which transmits the **apply ip-precedence** and **apply qos-local-id** configuration through BGP routing policies.

Use **undo bgp-policy** to disable QPPB.

Syntax

bgp-policy { **destination** | **source** } { **ip-prec-map** | **ip-qos-map** } *

undo bgp-policy { **destination** | **source** } [**ip-prec-map** | **ip-qos-map**] *

Default

QPPB is disabled.

Views

Interface view

Predefined user roles

network-admin

Parameters

destination: Searches the routing table by destination IP address.

source: Searches the routing table by source IP address. If the **source** keyword is specified, the source IP address is used as the destination address for inverse lookup.

ip-prec-map: Sets an IP precedence value for matching packets.

ip-qos-map: Sets a local QoS ID for matching packets.

Usage guidelines

The **bgp-policy** command applies only to the incoming traffic.

In an MPLS L3VPN, the **bgp-policy** command is executed after the QoS features are performed in the inbound direction of the PE's public network interface. In any other case, the **bgp-policy** command is executed before the QoS features.

If two **bgp-policy** commands are executed, one with the **source** keyword and the other with the **destination** keyword, the most recent command entered applies.

Examples

Configure interface GigabitEthernet 2/1/1 to get the IP precedence and local QoS ID by looking up routes based on source IP address.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/1/1
[Sysname-GigabitEthernet2/1/1] bgp-policy source ip-prec-map ip-qos-map
```

Related commands

- **apply ip-precedence** (*Layer 3—IP Routing Command Reference*)
- **apply qos-local-id** (*Layer 3—IP Routing Command Reference*)
- **route-policy** (*Layer 3—IP Routing Command Reference*)

MPLS QoS commands

if-match mpls-exp

Use **if-match mpls-exp** to define a criterion to match the EXP field in the first (topmost) MPLS label.

Use **undo if-match mpls-exp** to delete the match criterion.

Syntax

if-match [**not**] **mpls-exp** *exp-value*&<1-8>

undo if-match [**not**] **mpls-exp** *exp-value*&<1-8>

Default

No criterion is defined to match the EXP field in the topmost MPLS label.

Views

Traffic class view

Predefined user roles

network-admin

Parameters

not: Matches packets not conforming to the specified criterion.

exp-value&<1-8>: Specifies a space-separated list of up to eight EXP values. The value range for the *exp-value* argument is 0 to 7. If the same EXP value is specified multiple times, the system considers them as one. If a packet matches one of the defined MPLS EXP values, it matches the **if-match** clause.

Examples

Define a criterion to match packets with EXP value 3 or 4 in the topmost MPLS label.

```
<Sysname> system-view
[Sysname] traffic classifier database
[Sysname-classifier-database] if-match mpls-exp 3 4
```

remark mpls-exp

Use **remark mpls-exp** to configure an EXP value marking action in a traffic behavior.

Use **undo remark mpls-exp** to delete the action.

Syntax

remark mpls-exp *exp-value*

undo remark mpls-exp

Default

No EXP value marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

exp-value: Specifies an EXP value in the range of 0 to 7.

Usage guidelines

If an MPLS packet has multiple labels, this command marks the topmost label.

Examples

Set the EXP value to 0 for MPLS packets.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark mpls-exp 0
```

remark second-mpls-exp

Use **remark second-mpls-exp** to configure an EXP value marking action for the second label in a traffic behavior.

Use **undo remark second-mpls-exp** to delete the action.

Syntax

remark second-mpls-exp *exp-value*

undo remark second-mpls-exp

Default

No EXP value marking action is configured for the second label.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

exp-value: Specifies an EXP value in the range of 0 to 7.

Examples

Configure the traffic behavior **b1** to mark EXP value 1 for the second label of MPLS packets.

```
<Sysname> system-view
[Sysname] traffic behavior b1
[Sysname-behavior-b1] remark second-mpls-exp 1
```

FR QoS commands

The following matrix shows the feature and hardware compatibility:

Hardware	FR QoS compatibility
MSR954(JH296A/JH297A/ JH298A/JH299A)	No
MSR1002-4/1003-8S	Yes
MSR2003	Yes
MSR2004-24/2004-48	Yes
MSR3012/3024/3044/3064	Yes
MSR4060/4080	Yes

cbs

Use **cbs** to set the CBS for an FR class.

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

Syntax

cbs [**inbound** | **outbound**] *committed-burst-size*

undo cbs [**inbound** | **outbound**]

Default

The CBS for an FR class is 56000 bits.

Views

FR class view

Predefined user roles

network-admin

Parameters

inbound: Sets the CBS for incoming packets. The inbound CBS does not take effect for FR traffic shaping (FRTS).

outbound: Sets the CBS for outgoing packets. The outbound CBS does not take effect for FR traffic policing (FRTP).

committed-burst-size: Sets the CBS in the range of 300 to 16000000 bits. The default is 56000 bits.

Usage guidelines

If you do not specify the **inbound** or **outbound** keyword, the set CBS takes effect on both incoming and outgoing packets.

Examples

Set the CBS to 64000 bits for both incoming and outgoing packets of the FR class **test1**.

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] cbs 64000
```

Related commands

- **cir**
- **cir allow**
- **ebs**

cir

Use **cir** to set the CIR for an FR class.

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

Syntax

cir *committed-information-rate*

undo cir

Default

The CIR for an FR class is 56000 bps.

Views

FR class view

Predefined user roles

network-admin

Parameters

committed-information-rate: Sets the CIR in the range of 1000 to 45000000 bps. The default is 56000 bps.

Usage guidelines

The set CIR takes effect on both incoming and outgoing traffic and must be equal to or smaller than the outbound CIR ALLOW.

Examples

Set the CIR to 32000 bps for the FR class **test1**.

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] cir 32000
```

Related commands

- **cbs**
- **cir allow**
- **ebs**

cir allow

Use **cir allow** to set the CIR ALLOW for an FR class.

Use **undo cir allow** to restore the default.

Syntax

cir allow [**inbound** | **outbound**] *committed-information-rate*

undo cir allow [**inbound** | **outbound**]

Default

The CIR ALLOW for an FR class is 56000 bps.

Views

FR class view

Predefined user roles

network-admin

Parameters

inbound: Sets the CIR ALLOW for incoming packets. The inbound CBS ALLOW does not take effect for FRTS.

outbound: Sets the CIR ALLOW for outgoing packets. The outbound CBS ALLOW does not take effect for FRTP.

committed-information-rate: Sets the CIR ALLOW in the range of 1000 to 45000000 bps.

Usage guidelines

The outbound CIR ALLOW must be greater than or equal to the CIR.

If you do not specify the **inbound** or **outbound** keyword, the set CIR ALLOW takes effect on both incoming and outgoing packets.

Examples

Set the CIR ALLOW to 64000 bps for the FR class **test1**.

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] cir allow 64000
```

display fr class-map

Use **display fr class-map** to display the associations between FR classes and interfaces (including subinterfaces and PVCs).

Syntax

display fr class-map [**fr-class** *class-name* | **interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

fr-class *class-name*: Specifies an FR class by its name, a case-sensitive string of 1 to 30 characters.

interface *interface-type interface-number*: Specifies an interface (main interface or subinterface) by its type and number. If you specify a main interface, the command displays the associations between the following elements:

- The FR class and the main interface.
- The FR classes and the subinterfaces on the main interface.
- The FR classes and the PVCs on the main interface.
- The FR classes and the PVCs on each subinterface.

If you specify a subinterface, the command displays the associations between the following elements:

- The FR class and the subinterface.
- The FR classes and the PVCs on the subinterface.

Usage guidelines

If you do not specify an FR class or an interface, the command displays all associations between FR classes and interfaces.

Examples

Display the associations between Serial 2/1/1 and FR classes.

```
<Sysname> display fr class-map interface serial 2/1/1
Serial2/1/1
  fr-class ts1
  fr dlci 100
    fr-class ts
Serial2/1/1.1
  fr-class ts2
  fr dlci 222
    fr-class ts
```

Display the associations between the FR class **ts** and interfaces.

```
<Sysname> display fr class-map fr-class ts
Serial2/1/1
  fr dlci 100
    fr-class ts
Serial2/1/1.1
  fr dlci 222
    fr-class ts
```

Table 42 Command output

Field	Description
Serial2/1/1 fr-class ts1	FR interface and the FR class associated with the FR interface.
fr dlci 100 fr-class ts	PVC on the FR interface and the FR class associated with the PVC.
Serial2/1/1.1 fr-class ts2	FR subinterface and the FR class associated with the FR subinterface.
fr dlci 222 fr-class ts	PVC on the FR subinterface and the FR class associated with the PVC.

ebs

Use **ebs** to set the EBS for an FR class.

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

Syntax

ebs [**inbound** | **outbound**] *excess-burst-size*

undo ebs [**inbound** | **outbound**]

Default

The EBS for an FR class is 0 bits.

Views

FR class view

Predefined user roles

network-admin

Parameters

inbound: Sets the EBS for incoming packets. The inbound EBS does not take effect for FRTS.

outbound: Sets the EBS for outgoing packets. The outbound EBS does not take effect for FRTP.

excess-burst-size: Sets the EBS in the range of 0 to 16000000 bits. The default is 0 bits.

Usage guidelines

If you do not specify the **inbound** or **outbound** keyword, the set EBS takes effect on both incoming and outgoing packets.

Examples

Set the EBS to 32000 bits for the FR class **test1**.

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] ebs 32000
```

Related commands

- **cbs**
- **cir**
- **cir allow**

fifo queue-length

Use **fifo queue-length** to set the FIFO queue length for an FR class.

Use **undo fifo queue-length** to restore the default.

Syntax

fifo queue-length *queue-length*

undo fifo queue-length

Default

The FIFO queue length for an FR class is 75.

Views

FR class view

Predefined user roles

network-admin

Parameters

queue-length: Sets the FIFO queue length in the range of 1 to 1024.

Examples

Set the FIFO queue length to 80 for the FR class **test1**.

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] fifo queue-length 80
```

Related commands

fr class

fragment enable

Use **fragment enable** to enable Frame Relay FRF.12 fragmentation for an FR class.

Use **undo fragment enable** to disable Frame Relay FRF.12 fragmentation for an FR class.

Syntax

fragment enable

undo fragment enable

Default

Frame Relay FRF.12 fragmentation is disabled for an FR class.

Views

FR class view

Predefined user roles

network-admin

mdc-admin

Usage guidelines

This command enables FRF.12 fragmentation on all PVCs associated with an FR class or PVCs of all interfaces associated with an FR class.

FRF.12 fragmentation includes the following types:

- NNI&UNI.
- End-to-end.

Only end-to-end FRF.12 fragmentation is supported in the current software version.

Examples

Enable Frame Relay FRF.12 fragmentation for the FR class **test1**.

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] fragment enable
```

fragment size

Use **fragment size** to set the fragment size allowed for an FR class.

Use **undo fragment size** to restore the default.

Syntax

fragment size *size*

undo fragment size

Default

The fragment size allowed for an FR class is 45 bytes.

Views

FR class view

Predefined user roles

network-admin

mdc-admin

Parameters

size: Specifies the fragment size in the range 16 to 1600 bytes.

Examples

Set the fragment size to 128 bytes for the FR class **test1**.

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] fragment size 128
```

fr class

Use **fr class** to create an FR class and enter FR class view.

Use **undo fr class** to delete an FR class.

Syntax

fr class *class-name*

undo fr class *class-name*

Default

No FR class is created.

Views

System view

Predefined user roles

network-admin

Parameters

class-name: Specifies the name of the FR class, a case-sensitive string of 1 to 30 characters.

Usage guidelines

For the FR class parameters to take effect, associate the FR class with an interface or PVC and enable FR QoS on the interface.

When an FR class is deleted, all associations between this FR class and interfaces are released.

Examples

Create an FR class **test1**.

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1]
```

Related commands

fr-class

fr de del

Use **fr de del** to apply a DE rule list to an FR PVC.

Use **undo fr de del** to remove a DE rule list from an FR PVC.

Syntax

fr de del *list-number* **dlci** *dlci-number*

undo fr de del *list-number* **dlci** *dlci-number*

Default

No DE rule list is applied to FR PVCs.

Views

FR interface view, MFR interface view

Predefined user roles

network-admin

Parameters

list-number: Specifies a DE rule list by its number in the range of 1 to 10.

dlci-number: Specifies a FR PVC by its number in the range of 16 to 1007.

Usage guidelines

If you specify a PVC of a subinterface on the main interface, the DE rule list cannot be applied to the specified PVC.

After a DE rule list is applied to an FR PVC, the DE bits of outgoing packets matching the DE rule list are set to 1.

Examples

Apply DE rule list 3 to DLCI 100 of Serial 2/1/1.

```
<Sysname> system-view
[Sysname] interface Serial 2/1/1
[Sysname-Serial2/1/1] fr dlci 100
[Sysname-Serial2/1/1-fr-dlci-100] quit
[Sysname-Serial2/1/1] fr de del 3 dlci 100
[Sysname-Serial2/0] fr de del 3 dlci 100
```

Related commands

- **fr del inbound-interface**
- **fr del protocol**

fr del inbound-interface

Use **fr del inbound-interface** to create a DE rule list and add an interface-based DE rule.

Use **undo fr del inbound-interface** to delete an interface-based DE rule from a DE rule list.

Syntax

fr del *list-number* **inbound-interface** *interface-type interface-number*

undo fr del *list-number* **inbound-interface** *interface-type interface-number*

Default

No DE rule list exists.

Views

System view

Predefined user roles

network-admin

Parameters

list-number: Specifies a DE rule list number in the range of 1 to 10.

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

Usage guidelines

This command sets the DE bits of packets that are received on the specified interface to 1.

Execute this command multiple times to add new rules to a DE rule list. Up to 100 rules can be configured for a DE rule list. The **undo fr del inbound-interface** command deletes one DE rule at a time. To delete a DE rule list, delete all DE rules in the DE rule list.

Examples

Add a rule to DE rule list 1. The rule sets the DE bits of incoming packets on Serial 2/1/1 to 1.

```
<Sysname> system-view
[Sysname] fr del 1 inbound-interface serial 2/1/1
```

Related commands

- **fr de del**
- **fr del protocol**

fr del protocol

Use **fr del protocol ip** to create a DE rule list and add an IP protocol-based DE rule.

Use **undo fr del protocol ip** to delete an IP protocol-based DE rule from a DE rule list.

Syntax

fr del *list-number* **protocol ip** [**acl** *acl-number* | **fragments** | **greater-than** *min-number* | **less-than** *max-number* | **tcp-port** *tcpport-number* | **udp-port** *udpport-number*]

undo fr del *list-number* **protocol ip** [**fragments** | **acl** *acl-number* | **less-than** *bytes* | **greater-than** *min-number* | **less-than** *max-number* | **tcp-port** *tcpport-number* | **udp-port** *udpport-number*]

Default

No DE rule list exists.

Views

System view

Predefined user roles

network-admin

Parameters

list-number: Specifies a DE rule list number in the range of 1 to 10.

acl *acl-number*: Specifies the IP packets matching the ACL specified by its number in the range of 2000 to 3999.

fragments: Specifies all fragmented IP packets.

greater-than *min-number*: Specifies the IP packets that are greater than the specified number of bytes. The value range for the *min-number* argument is 0 to 65535.

less-than *max-number*: Specifies the IP packets that smaller than the specified number of bytes. The value range for the *max-number* argument is 0 to 65535.

tcp-port *tcpport-number*: Specifies the IP packets with the specified source or destination TCP port number. The value range for the *tcpport-number* argument is 0 to 65535. The *tcpport-number* argument can be either an upper-layer application name or the associated port number.

Table 43 Application names and TCP port numbers

Application name	TCP port number
bgp	179
chargen	19
cmd	514
daytime	13
discard	9
domain	53
echo	7
exec	512
finger	79
ftp	21
ftp-data	20
gopher	70
hostname	101
ident	113
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
www	80

udp-port *udpport-number*: Specifies the IP packets with the specified source or destination UDP port number. The value range for the *udpport-number* argument is 0 to 65535. The *udpport-number* argument can be either an upper-layer application name or the associated port number.

Table 44 Application names and UDP port numbers

Application name	UDP port number
biff	512
bootpc	68
bootps	67
discard	9
dnsix	195
domain	53
echo	7
mobile-ip	434
nameserver	42
netbios-dgm	138
netbios-ns	137
ntp	123
rip	520
snmp	161
snmptrap	162
sunrpc	111
syslog	514
tacacs	49
talk	517
tftp	69
time	37
who	513
xdmcp	177

Usage guidelines

If a packet matches a DE rule, its DE bit is set to 1.

Execute this command multiple times to add new rules to a DE rule list. Up to 100 rules can be configured for a DE rule list. The **undo fr del protocol ip** command deletes one DE rule at a time. To delete a DE rule list, delete all DE rules in the DE rule list.

If you do not specify any parameters, this command sets the DE bits of all IP packets on a PVC to 1.

Examples

Add a rule to DE rule list 1 that sets the DE bits of all IP packets to 1.

```
<Sysname> system-view
[Sysname] fr del 1 protocol ip
```

Related commands

- **fr de del**
- **fr del inbound-interface**

fr traffic-policing

Use **fr traffic-policing** to enable FRTP.

Use **undo fr traffic-policing** to disable FRTP.

Syntax

fr traffic-policing

undo fr traffic-policing

Views

FR interface view, MFR interface view

Predefined user roles

network-admin

Usage guidelines

FRTP is applicable only to the ingress interfaces on the DCE of an FR network.

Examples

Enable FRTP on Serial 2/1/1.

```
<Sysname> system-view
[Sysname] interface Serial 2/1/1
[Sysname-Serial2/1/1] fr traffic-policing
```

Related commands

fr class

fr traffic-shaping

Use **fr traffic-shaping** to enable FRTS.

Use **undo fr traffic-shaping** to disable FRTS.

Syntax

fr traffic-shaping

undo fr traffic-shaping

Default

FRTS is disabled.

Views

FR interface view

Predefined user roles

network-admin

Usage guidelines

FRTS is applied to the outgoing interfaces and is typically used on the DTEs of an FR network.

FRTS cannot be enabled on an FR interface when fragmentation is enabled on the interface.

Examples

Enable FRTS on Serial 2/1/1.

```
<Sysname> system-view
[Sysname] interface serial 2/1/1
[Sysname-Serial2/1/1] fr traffic-shaping
```

fr-class

Use **fr-class** to associate an FR class with an FR interface or FR PVC.

Use **undo fr-class** to cancel the association.

Syntax

fr-class *class-name*

undo fr-class *class-name*

Default

An FR class is not associated with any FR interface or FR PVC.

Views

FR interface (main interface or subinterface) view, FR PVC view

Predefined user roles

network-admin

Parameters

class-name: Specifies an FR class by its name, a case-sensitive string of 1 to 30 characters. The FC class must already exist.

Usage guidelines

For an interface associated with an FR class, all PVCs on the interface inherit the FR QoS parameters in the FR class.

Examples

Associate the FR class **test1** with an FR PVC with DLCI 200.

```
<Sysname> system-view
[Sysname] interface serial 2/1/1
[Sysname-Serial2/1/1] fr dlci 200
[Sysname-Serial2/1/1-fr-dlci-200] fr-class test1
```

Related commands

fr class

traffic-shaping adaptation

Use **traffic-shaping adaptation** to enable FRTS adaptation for an FR class.

Use **undo traffic-shaping adaptation** to disable FRTS adaptation for an FR class.

Syntax

traffic-shaping adaptation { **becn** | **interface-congestion** *number* }

undo traffic-shaping adaptation { **becn** | **interface-congestion** }

Default

FRTS adaptation is disabled.

Views

FR class view

Predefined user roles

network-admin

Parameters

becn: Adjusts the traffic rate in response to BECNs.

interface-congestion *number*: Adjusts the traffic rate in response to the number of packets in the output queue on the interface. The value range for the *number* argument is 1 to 40.

Usage guidelines

For BECN-based adaptation, the router reduces the transmission rates of all FRTS-enabled PVCs associated with the FR class when it receives packets with the BECN bit set. When the router does not receive packets with the BECN bit set within 125 milliseconds, it increases the transmission rates of those PVCs.

For interface congestion-based adaptation, the router reduces the transmission rates of all FRTS-enabled PVCs associated with the FR class when the number of packets in the output queue reaches the set threshold. When the number of packets drops below the set threshold, the router increases the transmission rates of those PVCs.

Examples

Enable FRTS adaptation to adjust the traffic rate in response to BECNs.

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] traffic-shaping adaptation becn
```

Related commands

fr traffic-shaping

traffic-shaping adaptation percentage

Use **traffic-shaping adaptation percentage** to set the rate adjustment percentage for FRTS adaptation.

Use **undo traffic-shaping adaptation percentage** to restore the default.

Syntax

traffic-shaping adaptation percentage *number*

undo traffic-shaping adaptation percentage

Default

The rate adjustment percentage for FRTS adaptation is 25%.

Views

FR class view

Predefined user roles

network-admin

Parameters

number: Specifies the rate adjustment percentage, in the range of 1 to 30.

Usage guidelines

When rate adjustment is triggered, the router reduces or increases the traffic rate by the set percentage of the current rate. The adjusted rate must be between the CIR and the CIR ALLOW. For example, the current rate is 3000 bps, the rate adjustment percentage is 20%, and the CIR is 2500 bps. The rate is reduced to 2400 bps (3000 – 3000 x 20%). Because the adjusted rate cannot be lower than the CIR, the adjusted rate should be 2500 bps.

Examples

Set the rate adjustment percentage to 20%.

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] traffic-shaping adaptation 20
```

Related commands

fr traffic-shaping

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 45 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 range exists.

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 and 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 greater 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, respectively 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 greater 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, 2011, 00:00 and December 31, 2011, 23:59, use the **time-range test 08:00 to 12:00 mon from 00:00 01/01/2011 to 23:59 12/31/2011** 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

Document conventions and icons

Conventions

This section describes the conventions used in the documentation.

Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.

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 at least 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 appears; 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 card, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG card.

Document conventions and icons

Conventions

This section describes the conventions used in the documentation.

Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.

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 at least 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 appears; 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 card, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG card.

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

  www.hpe.com/assistance
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

  www.hpe.com/support/hpesc

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates, go to either of the following:
  - Hewlett Packard Enterprise Support Center **Get connected with updates** page:

    www.hpe.com/support/e-updates
  - Software Depot website:

    www.hpe.com/support/softwaredepot
- To view and update your entitlements, and to link your contracts, Care Packs, and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

  www.hpe.com/support/AccessToSupportMaterials

IMPORTANT:

Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.

Websites

Website	Link
Networking websites	
Hewlett Packard Enterprise Information Library for Networking	www.hpe.com/networking/resourcefinder
Hewlett Packard Enterprise Networking website	www.hpe.com/info/networking
Hewlett Packard Enterprise My Networking website	www.hpe.com/networking/support
Hewlett Packard Enterprise My Networking Portal	www.hpe.com/networking/mynetworking
Hewlett Packard Enterprise Networking Warranty	www.hpe.com/networking/warranty
General websites	
Hewlett Packard Enterprise Information Library	www.hpe.com/info/enterprise/docs
Hewlett Packard Enterprise Support Center	www.hpe.com/support/hpesc
Hewlett Packard Enterprise Support Services Central	ssc.hpe.com/portal/site/ssc/
Contact Hewlett Packard Enterprise Worldwide	www.hpe.com/assistance
Subscription Service/Support Alerts	www.hpe.com/support/e-updates
Software Depot	www.hpe.com/support/softwaredepot
Customer Self Repair (not applicable to all devices)	www.hpe.com/support/selfrepair
Insight Remote Support (not applicable to all devices)	www.hpe.com/info/insightremotesupport/docs

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

www.hpe.com/support/selfrepair

Remote support

Remote support is available with supported devices as part of your warranty, Care Pack Service, or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

For more information and device support details, go to the following website:

www.hpe.com/info/insightremotesupport/docs

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hpe.com). When submitting your feedback, include the document title,

part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

Index