H3C WA Series WLAN Access Points

ACL and QoS Command Reference

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

Document Version: 6W100-20100910

Preface

The H3C WA documentation set includes 10 command references, which describe the commands and command syntax options available for the H3C WA series WLAN access points.

The *ACL and QoS Command Reference* describes ACL and QoS configuration commands.

This preface includes:

Audience

This documentation is intended for:

- Network planners
- Field technical support and servicing engineers
- Network administrators working with the WA series

Conventions

This section describes the conventions used in this documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select at least one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you may select 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**	Means reader be extremely careful. Improper operation may cause bodily injury.
 **Caution**	Means reader be careful. Improper operation may cause data loss or damage to equipment.
 **Highlight**	Means an action or information that needs special attention to ensure successful configuration or good performance.
 **Note**	Means a complementary description.
 **Tip**	Means techniques helpful for you to make configuration with ease.

About the H3C WA Documentation Set

The H3C WA documentation set includes:

Category	Documents	Purposes
Product description and specifications	Marketing brochures	Describe product specifications and benefits.
	Technology white papers	Provide an in-depth description of software features and technologies.
Hardware specifications and installation	Compliance and safety manual	Provides regulatory information and the safety instructions that must be followed during installation.
	Quick start	Guides you through initial installation and setup procedures to help you quickly set up and use your AP with the minimum configuration.
	Installation guide	Guides you through hardware specifications and installation methods to help you install your AP.
Software configuration	Getting started guide	Guides you through the main functions of your AP, and describes how to install and log in to your AP, perform basic configurations, maintain software, and troubleshoot your AP.
	Configuration guides	Describe software features and configuration procedures.
	Command references	Provide a quick reference to all available commands.
Operations and maintenance	User FAQ	Provides answers to some of the most frequently asked questions on how to troubleshoot your AP.
	Release notes	Provide information about the product release, including the version history, hardware and software compatibility matrix, version upgrade information, technical support information, and software upgrading.

Obtaining Documentation

You can access the most up-to-date H3C product documentation on the World Wide Web at http://www.h3c.com.

Click the links on the top navigation bar to obtain different categories of product documentation:

[Technical Support & Documents > Technical Documents] – Provides hardware installation, software upgrading, getting started, and software feature configuration and maintenance documentation.

[Products & Solutions] – Provides information about products and technologies, as well as solutions.

[Technical Support & Documents > Software Download] – Provides the documentation released with the software version.

Documentation Feedback

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

We appreciate your comments.

Table of Contents

Note

- The models listed in this document are not applicable to all regions. Please consult your local sales office for the models applicable to your region.
- Read this chapter before using an H3C WA series WLAN access point.

1 Applicable Models and Software Versions

H3C WA series WLAN access points include the WA2200 series and WA2600 series. Table 1-1 shows the applicable models and software versions.

Table 1-1 Applicable models and software versions

Series		Model	Software version
WA2200 series	WA2200 series access points (indoors)	WA2210-AG	R 1115
		WA2220-AG	
	WA2200 series access points (outdoors)	WA2210X-G	
		WA2220X-AG	
WA2600 series	WA2600 series access points (indoors)	WA2610-AGN	R 1106
		WA2612-AGN	
		WA2620-AGN	
	WA2600 series access points (enhanced)	WA2610E-AGN	R 1109
		WA2620E-AGN	

2 Feature Matrix

Caution

- Support of the H3C WA series WLAN access points for features, commands and parameters may vary by device model. See this document for more information.
- For information about feature support, see Table 2-1. For information about command and parameter support, see Table 3-1.
- The term *AP* in this document refers to common APs, wireless bridges, or mesh APs.

Table 2-1 Feature matrix

Document	Feature	WA2200 series	WA2600 series
Fundamentals Configuration Guide	HTTPS	Not supported	Supported
WLAN Configuration Guide	802.11n radio mode	Not supported	Supported
	802.11n bandwidth mode	Not supported	Supported
	802.11n rate configuration	Not supported	Supported
Layer 2 – LAN Switching Configuration Guide	Optical Ethernet interface	Supported on WA2210X-G/WA2220X-AG only	Not supported
	GE interface	Not supported	Supported
Layer 3 – IP Services Configuration Guide	DHCP server configuration	Not supported	Supported
	DHCPv6 configuration	Not supported	Supported
IP Multicast Configuration Guide	IGMP snooping configuration	Not supported	Supported
	MLD snooping configuration	Not supported	Supported
Security Configuration Guide	SSH2.0	Not supported	Supported

3 Command/Parameter Matrix

Table 3-1 Command/Parameter matrix

Document	Module	Command/Parameter	WA2200 series	WA2600 series
Fundamentals Command Reference	HTTP commands	**display ip https**	Not supported	Supported
		ip https acl	Not supported	Supported
		ip https certificate access-control-policy	Not supported	Supported
		ip https enable	Not supported	Supported
WLAN Command Reference	WLAN service commands	**a-mpdu enable**	Not supported	Supported
		a-msdu enable	Not supported	Supported
		channel band-width	Not supported	Supported
		client dot11n-only	Not supported	Supported
		preamble { **long** | **short** }	Only APs that support the 802.11b/g radio mode support this command.	Only APs that support the 802.11b/g radio mode support this command.
		radio-type	Keywords **dot11an** and **dot11gn** not supported	Supported
		short-gi enable	Not supported	Supported
	WLAN RRM commands	**dot11a** { **disabled-rate | mandatory-rate | supported-rate** } *rate-value*	Only APs that support 802.11a radio mode support this command.	Only APs that support 802.11a radio mode support this command.
		dot11n mandatory maximum-mcs	Not supported	Supported
		dot11n support maximum-mcs	Not supported	Supported
		power-constraint *power-constraint*	Only APs that support the 802.11a radio mode support this command.	Only APs that support the 802.11a radio mode support this command.

Document	Module	Command/Parameter	WA2200 series	WA2600 series
Layer 2 – LAN Switching Command Reference	The maximum number of broadcast packets that can be forwarded on an Ethernet interface per second	**broadcast-suppression** { *ratio* | **pps** *max-pps* }	**pps** *max-pps* ranges from 1 to 148810.	**pps** *max-pps* ranges from 1 to 1488100.
	The maximum number of multicast packets allowed on an Ethernet interface per second	**multicast-suppression** { *ratio* | **pps** *max-pps* }	**pps** *max-pps* ranges from 1 to 148810.	**pps** *max-pps* ranges from 1 to 1488100.
	The maximum number of unknown unicast packets allowed on an Ethernet interface per second	**unicast-suppression** { *ratio* | **pps** *max-pps* }	**pps** *max-pps* ranges from 1 to 148810.	**pps** *max-pps* ranges from 1 to 1488100.
Layer 3 - IP Services Command Reference	DHCP commands	DHCP server configuration commands	Not supported	Supported
	DHCPv6 commands	**display ipv6 dhcp client** [**interface** *interface-type interface-number*]	Not supported	Supported
		display ipv6 dhcp client statistics [**interface** *interface-type interface-number*]	Not supported	Supported
		display ipv6 dhcp duid	Not supported	Supported
		reset ipv6 dhcp client statistics [**interface** *interface-type interface-number*]	Not supported	Supported

Note

- The models listed in this document are not applicable to all regions. Please consult your local sales office for the models applicable to your region.
- Support of the H3C WA series WLAN access points (APs) for commands may vary by AP model. For more information, see *Feature Matrix*.
- The interface types and the number of interfaces vary by AP model.

4 ACL Configuration Commands

ACL Configuration Commands

acl

Syntax

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

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

View

System view

Default Level

2: System level

Parameters

number *acl-number*: Specifies the number of an IPv4 access control list (ACL):

- 100 to 199 for WLAN ACLs
- 2000 to 2999 for IPv4 basic ACLs
- 3000 to 3999 for IPv4 advanced ACLs
- 4000 to 4999 for Ethernet frame header ACLs

name *acl-name*: Assigns a name for the IPv4 ACL for the ease of identification. The *acl-name* argument takes a case insensitive string of 1 to 32 characters. It must start with an English letter, and to avoid confusion, cannot be **all**.

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

- **auto**: Compares ACL rules in depth-first order. The depth-first order differs with ACL categories. See *ACL* in the *ACL and QoS Configuration Guide* for more information.
- **config**: Compares ACL rules in ascending order of rule ID. The rule with a smaller ID has higher priority. If no match order is specified, the config order applies by default.

all: Deletes all IPv4 ACLs.

Description

Use the **acl** command to create an IPv4 ACL and enter its view. If the ACL has been created, you enter its view directly.

Use the **undo acl** command to delete the specified or all IPv4 ACLs.

By default, no ACL exists.

You can assign a name for an IPv4 ACL only when you create it. After creating an ACL, you can neither rename it nor remove its name, if any.

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

The **match-order** keyword is not available for WLAN ACLs. They always use the config order. In addition, for WLAN ACLs, the **name** is not available.

To display any ACLs you have created, use the **display acl** command.

Examples

Create IPv4 basic ACL 2000, and enter its view.

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

Create IPv4 basic ACL 2001, named **flow**, and enter its view.

```
<Sysname> system-view
[Sysname] acl number 2001 name flow
[Sysname-acl-basic-2001-flow]
```

acl copy

Syntax

acl copy { *source-acl-number* | **name** *source-acl-name* } **to** { *dest-acl-number* | **name** *dest-acl-name* }

View

System view

Default Level

2: System level

Parameters

source-acl-number: Specifies a source IPv4 ACL that already exists by its number:

- 100 to 199 for WLAN ACLs
- 2000 to 2999 for IPv4 basic ACLs
- 3000 to 3999 for IPv4 advanced ACLs
- 4000 to 4999 for Ethernet frame header ACLs

name *source-acl-name*: Specifies a source IPv4 ACL that already exists by its name. The *source-acl-name* argument takes a case insensitive string of 1 to 32 characters.

dest-acl-number: Assigns a unique number for the IPv4 ACL you are creating. This number must be from the same ACL category as the source ACL. Available value ranges include:

- 100 to 199 for WLAN ACLs
- 2000 to 2999 for IPv4 basic ACLs
- 3000 to 3999 for IPv4 advanced ACLs

- 4000 to 4999 for Ethernet frame header ACLs

name *dest-acl-name*: Assigns a unique name for the IPv4 ACL you are creating. The *dest-acl-name* takes a case insensitive string of 1 to 32 characters. It must start with an English letter and to avoid confusion, cannot be **all**. For this ACL, the system automatically picks the smallest number from all available numbers in the same ACL category as the source ACL.

Description

Use the **acl copy** command to create an IPv4 ACL by copying an IPv4 ACL that already exists. Except the number and name (if any), the new ACL has the same configuration as the source ACL.

You can assign a name for an IPv4 ACL only when you create it. After it is created, you can neither rename it nor remove its name, if any.

The **name** keyword and argument combinations are not available for WLAN ACLs.

Examples

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

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

acl ipv6

Syntax

acl ipv6 number *acl6-number* [**name** *acl6-name*] [**match-order** { **auto** | **config** }]

undo acl ipv6 { **all** | **name** *acl6-name* | **number** *acl6-number* }

View

System view

Default Level

2: System level

Parameters

number *acl6-number*: Specifies the number of an IPv6 ACL:

- 2000 to 2999 for IPv6 basic ACLs
- 3000 to 3999 for IPv6 advanced ACLs

name *acl6-name*: Assigns a name for the IPv6 ACL for the ease of identification. The *acl6-name* argument takes a case insensitive string of 1 to 32 characters. It must start with an English letter, and to avoid confusion, cannot be **all**.

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

- **auto**: Compares ACL rules in depth-first order. The depth-first order differs with ACL categories. See *ACL* in the *ACL and QoS Configuration Guide* for more information.
- **config**: Compares ACL rules in ascending order of rule ID. The rule with a smaller ID has higher priority. If no match order is specified, the config order applies by default.

all: Delete all IPv6 ACLs.

Description

Use the **acl ipv6** command to create an IPv6 ACL and enter its ACL view. If the ACL has been created, you enter its view directly.

Use the **undo acl ipv6** command to delete the specified IPv6 ACL or all IPv6 ACLs.

By default, no ACL exists.

You can assign a name for an IPv6 ACL only when you create it. After creating an ACL, you can neither rename it, nor remove its name.

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

To display any ACLs you have created, use the **display acl ipv6** command.

Examples

Create IPv6 ACL 2000 and enter its view.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000]
```

Create IPv6 basic ACL 2001, named **flow**, and enter its view.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2001 name flow
[Sysname-acl6-basic-2001-flow]
```

acl ipv6 copy

Syntax

acl ipv6 copy { *source-acl6-number* | **name** *source-acl6-name* } **to** { *dest-acl6-number* | **name** *dest-acl6-name* }

View

System view

Default Level

2: System level

Parameters

source-acl6-number: Specifies a source IPv6 ACL that already exists by its number:

- 2000 to 2999 for IPv6 basic ACLs,
- 3000 to 3999 for IPv6 advanced ACLs.

name *source-acl6-name*: Specifies a source IPv6 ACL that already exists by its name. The *source-acl6-name* argument takes a case insensitive string of 1 to 32 characters.

dest-acl6-number: Assigns a unique number for the IPv6 ACL you are creating. This number must be from the same ACL category as the source ACL. Available value ranges include:

- 2000 to 2999 for IPv6 basic ACLs
- 3000 to 3999 for IPv6 advanced ACLs

name *dest-acl6-name*: Assigns a unique name for the IPv6 ACL you are creating. The *dest-acl6-name* takes a case insensitive string of 1 to 32 characters. It must start with an English letter and to avoid confusion, cannot be **all**. For this ACL, the system automatically picks the smallest number from all available numbers in the same ACL category as the source ACL.

Description

Use the **acl ipv6 copy** command to create an IPv6 ACL by copying an IPv6 ACL that already exists. Except the number and name (if any), the new ACL has the same configuration as the source ACL.

You can assign a name for an IPv6 ACL only when you create it. After it is created, you can neither rename it nor remove its name, if any.

Examples

Create IPv6 basic ACL 2002 by copying IPv6 basic ACL 2001.

```
<Sysname> system-view
[Sysname] acl ipv6 copy 2001 to 2002
```

acl ipv6 name

Syntax

acl ipv6 name *acl6-name*

View

System view

Default Level

2: System level

Parameters

acl6-name: Specifies the name of an existing IPv6 ACL, a case insensitive string of 1 to 32 characters. It must start with an English letter.

Description

Use the **acl ipv6 name** command to enter the view of an existing IPv6 ACL by specifying its name.

Related commands: **acl ipv6**.

Examples

Enter the view of IPv6 ACL **flow**.

```
<Sysname> system-view
[Sysname] acl ipv6 name flow
[Sysname-acl6-basic-2001-flow]
```

acl name

Syntax

acl name *acl-name*

View

System view

Default Level

2: System level

Parameters

acl-name: Specifies the name of an existing IPv4 ACL, which is a case insensitive string of 1 to 32 characters. It must start with an English letter.

Description

Use the **acl name** command to enter the view of an existing IPv4 ACL by specifying its name.

Related commands: **acl**.

Examples

Enter the view of IPv4 ACL **flow**.

```
<Sysname> system-view
[Sysname] acl name flow
[Sysname-acl-basic-2001-flow]
```

description

Syntax

description *text*

undo description

View

WLAN ACL view, IPv4 basic/advanced ACL view, IPv6 basic/advanced ACL view, Ethernet frame header ACL view

Default Level

2: System level

Parameters

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

Description

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

Use the **undo description** command to remove the ACL description.

By default, an ACL has no ACL description.

Related commands: **display acl** and **display acl ipv6**.

Examples

Configure a description for IPv4 basic ACL 2000.

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

Configure a description for IPv6 basic ACL 2000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] description This is an IPv6 basic ACL.
```

display acl

Syntax

display acl { *acl-number* | **all** | **name** *acl-name* }

View

Any view

Default Level

1: Monitor level

Parameters

acl-number: Specifies an IPv4 ACL by its number:

- 100 to 199 for WLAN ACLs
- 2000 to 2999 for basic ACLs
- 3000 to 3999 for advanced ACLs
- 4000 to 4999 for Ethernet frame header ACLs

all: Displays information for all IPv4 ACLs.

name *acl-name*: Specifies an IPv4 ACL by its name. The *acl-name* argument takes a case insensitive string of 1 to 32 characters. It must start with an English letter.

Description

Use the **display acl** command to display configuration and match statistics for the specified or all IPv4 ACLs.

This command displays ACL rules in config or depth-first order, whichever is configured.

Examples

Display the configuration and match statistics for all IPv4 ACLs.

```
<Sysname> display acl all
Basic ACL  2000, named flow, 3 rules,
ACL's step is 5
 rule 0 permit
 rule 5 permit source 1.1.1.1 0 (2 times matched)
Basic ACL  2001, named -none-, 3 rules, match-order is auto,
ACL's step is 5
 rule 5 permit source 2.2.2.2 0
 rule 0 permit
```

Table 4-1 display acl command output description

Field	Description
Basic ACL 2000	Category and number of the ACL. The following field information is about IPv4 basic ACL 2000.
named flow	The name of the ACL is flow. "-none-" means the ACL is not named. This field is not present for a WLAN ACL.
3 rules	The ACL contains three rules.
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.
ACL's step is 5	The rule numbering step is 5.
rule 0 permit	Content of rule 0
5 times matched	There have been five matches for the rule. The statistic counts only ACL matches performed by software. This field is not displayed when no packets have matched the rule.
No statistics resource	Resources are not enough for counting matches for the IPv4 rules.
Uncompleted	Applying the rule to hardware failed.

display acl ipv6

Syntax

display acl ipv6 { *acl6-number* | **all** | **name** *acl6-name* }

View

Any view

Default Level

1: Monitor level

Parameters

acl6-number: Specifies an IPv6 ACL by its number:

- 2000 to 2999 for IPv6 basic ACLs
- 3000 to 3999 for IPv6 advanced ACLs

all: Displays information for all IPv6 ACLs.

name *acl6-name*: Specifies an IPv6 ACL by its name. The *acl6-name* argument takes a case insensitive string of 1 to 32 characters. It must start with an English letter.

Description

Use the **display acl ipv6** command to display the configuration and match statistics for the specified or all IPv6 ACLs.

This command displays ACL rules in config or depth-first order, whichever is configured.

Examples

Display the configuration and match statistics for all IPv6 ACLs.

```
<Sysname> display acl ipv6 all
 Basic IPv6 ACL  2000, named flow, 3 rules,
 ACL's step is 5
 rule 0 permit
 rule 5 permit source 1::/64
 rule 10 permit source 1::1/128 (2 times matched)
 Basic IPv6 ACL  2001, named -none-, 3 rules, match-order is auto,
 ACL's step is 5
 rule 10 permit source 1::1/128
 rule 10 comment This rule is used on Ethernet 1/0/1.
 rule 5 permit source 1::/64
 rule 0 permit
```

Table 4-2 display acl ipv6 command output description

Field	Description
Basic IPv6 ACL 2000	Category and number of the ACL. The following field information is about this IPv6 basic ACL 2000.
named flow	The name of the ACL is flow. "-none-" means the ACL is not named.
3 rules	The ACL contains three rules.
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.
ACL's step is 5	The rule numbering step is 5.

Field	Description
rule 0 permit	Content of rule 0
5 times matched	There have been five matches for the rule. The statistic counts only IPv6 ACL matches performed by software. This field is not displayed when no packets have matched the rule.
No statistics resource	Resources are not enough for counting matches for the IPv6 ACL rules.
Uncompleted	Apply the rule to hardware failed.
rule 10 comment This rule is used on Ethernet 1/0/1.	The description of ACL rule 10 is "This rule is used on Ethernet 1/0/1."

display time-range

Syntax

display time-range { *time-range-name* | **all** }

View

Any view

Default Level

1: Monitor level

Parameters

time-range-name: Specifies a time range name, which is 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.

Description

Use the **display time-range** command to display the configuration and status of the specified or all time ranges.

Examples

Display the configuration and status of time range **t4**.

```
<Sysname> display time-range t4
Current time is 17:12:34 4/13/2010 Tuesday

Time-range : t4 ( Inactive )
 10:00 to 12:00 Mon
 14:00 to 16:00 Wed
 from 00:00 1/1/2010 to 23:59 1/31/2010
 from 00:00 6/1/2010 to 23:59 6/30/2010
```

Table 4-3 display time-range command output description

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.

reset acl counter

Syntax

reset acl counter { *acl-number* | **all** | **name** *acl-name* }

View

User view

Default Level

2: System level

Parameters

acl-number: Specifies an IPv4 ACL by its number:

- 100 to 199 for WLAN ACLs
- 2000 to 2999 for IPv4 basic ACLs
- 3000 to 3999 for IPv4 advanced ACLs
- 4000 to 4999 for Ethernet frame header ACLs

all: Clears statistics for all IPv4 ACLs.

name *acl-name*: Specifies an IPv4 ACL by its name. The *acl-name* argument takes a case insensitive string of 1 to 32 characters. It must start with an English letter.

Description

Use the **reset acl counter** command to clear statistics for the specified or all IPv4 ACLs.

Related commands: **display acl**.

Examples

Clear statistics for IPv4 basic ACL 2001.

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

Clear statistics for IPv4 ACL **flow**.

```
<Sysname> reset acl counter name flow
```

reset acl ipv6 counter

Syntax

reset acl ipv6 counter { *acl6-number* | **all** | **name** *acl6-name* }

View

User view

Default Level

2: System level

Parameters

acl6-number: Specifies an IPv6 ACL by its number:

- 2000 to 2999 for IPv6 basic ACLs
- 3000 to 3999 for IPv6 advanced ACLs

all: Clears statistics for all IPV6 basic and advanced ACLs.

name *acl6-name*: Specifies an IPv6 ACL by its name. The *acl6-name* argument takes a case insensitive string of 1 to 32 characters. It must start with an English letter.

Description

Use the **reset acl ipv6 counter** command to clear statistics for the specified or all IPv6 basic and IPv6 advanced ACLs.

Related commands: **display acl ipv6**.

Examples

Clear statistics for IPv6 basic ACL 2001.

```
<Sysname> reset acl ipv6 counter 2001
```

Clear statistics for IPv6 ACL **flow**.

```
<Sysname> reset acl ipv6 counter name flow
```

rule (Ethernet frame header ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } [**cos** *vlan-pri* | **dest-mac** *dest-addr dest-mask* | { **lsap** *lsap-type lsap-type-mask* | **type** *protocol-type protocol-type-mask* } | **source-mac** *sour-addr source-mask* | **time-range** *time-range-name*] *

undo rule *rule-id* **time-range**

View

Ethernet frame header ACL view

Default Level

2: System level

Parameters

rule-id: Specifies a rule ID, which ranges from 0 to 65534. If no rule ID is provided when you create an ACL rule, the system automatically assigns it a rule ID. This rule ID takes 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 *vlan-pri* argument can be a number in the range 0 to 7, or in words, **best-effort** (0), **background** (1), **spare** (2), **excellent-effort** (3), **controlled-load** (4), **video** (5), **voice** (6), or **network-management** (7).

dest-mac *dest-addr dest-mask:* Matches a destination MAC address range. The *dest-addr* and *dest-mask* arguments represent a destination MAC address and mask in 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 Ethernet frame header. 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 *sour-addr source-mask:* Matches a source MAC address range. The *sour-addr* argument represents a source MAC address, and the *sour-mask* argument represents a mask in 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.

Description

Use the **rule** command to create or edit an Ethernet frame header ACL rule. You can edit ACL rules only when the match order is config.

Use the **undo rule** command to delete an Ethernet frame header ACL rule or some attributes in the rule. If no optional keywords are provided, you delete the entire rule. If optional keywords or arguments are provided, you delete the specific attributes.

By default, an Ethernet frame header ACL does not contain any rule.

Within an ACL, the permit or deny statement of each rule must be unique. If the ACL rule you are creating or editing has the same deny or permit statement as another rule in the ACL, your creation or editing attempt will fail.

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

Related commands: **acl**, **display acl**, and **step**.

Examples

Create a rule in ACL 4000 to deny packets with the 802.1p priority of 3.

```
<Sysname> system-view
[Sysname] acl number 4000
[Sysname-acl-ethernetframe-4000] rule deny cos 3
```

rule (IPv4 advanced ACL view)

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** } | **destination** { *dest-addr dest-wildcard* | **any** } | **destination-port** *operator port1* [*port2*] | **dscp** *dscp* | **fragment** | **icmp-type** { *icmp-type icmp-code* | *icmp-message* } | **logging** | **precedence** *precedence* | **reflective** | **source** { *sour-addr sour-wildcard* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name* | **tos** *tos*] *

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

View

IPv4 advanced ACL view

Default Level

2: System level

Parameters

rule-id: Specifies a rule ID, which ranges from 0 to 65534. If no rule ID is provided when you create an ACL rule, the system automatically assigns it a rule ID. This rule ID takes 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: Protocol carried by IPv4. It can be a number in the range 0 to 255, or in words, **gre** (47), **icmp** (1), **igmp** (2), **ip**, **ipinip** (4), **ospf** (89), **tcp** (6), or **udp** (17). Table 4-4 describes the parameters that can be specified after the *protocol* argument.

Table 4-4 Match criteria and other rule information for IPv4 advanced ACL rules

Parameters	Function	Description
source { *sour-addr sour-wildcard* | **any** }	Specifies a source address	The *sour-addr sour-wildcard* arguments represent a source IP address and wildcard mask in dotted decimal notation. An all-zero wildcard specifies a host address. The **any** keyword specifies any source IP address.
destination { *dest-addr dest-wildcard* | **any** }	Specifies a destination address	The *dest-addr dest-wildcard* arguments represent a destination IP address and wildcard mask in dotted decimal notation. An all-zero wildcard specifies a host address. The **any** keyword represents any destination IP address.
precedence *precedence*	Specifies an IP precedence value	The *precedence* argument can be a number in the range 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 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 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).
logging	Logs matching packets	This function requires that the module that uses the ACL supports logging.
reflective	Specifies that the rule be reflective	A rule with the **reflective** keyword can be defined only for TCP, UDP, or ICMP packets and can only be a permit statement.
fragment	Applies the rule to only non-first fragments	Without this keyword, the rule applies to all fragments and non-fragments.
time-range *time-range-name*	Specifies a time range for the rule	The *time-range-name* argument takes a case insensitive string of 1 to 32 characters. It must start with an English letter.

Note

If you provide the **precedence** or **tos** keyword in addition to the **dscp** keyword, only the **dscp** keyword takes effect.

Setting the *protocol* argument to **tcp** (6) or **udp** (7), you may set the parameters shown in Table 4-5.

Table 4-5 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 0 to 65535. *port2* is needed only when the *operator* argument is **range**. TCP port numbers can be represented in these words: **chargen** (19), **bgp** (179), **cmd** (514), **daytime** (13), **discard** (9), **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 in these words: **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 relationship between the TCP flags in a rule is AND.
established	Specifies the flags for indicating the established status of a TCP connection	Parameter specific to TCP.

Setting the *protocol* argument to **icmp** (1), you may set the parameters shown in Table 4-6.

Table 4-6 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 ranges from 0 to 255. The *icmp-code* argument ranges from 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 4-7.

Table 4-7 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

ICMP message name	ICMP message type	ICMP message code
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

Description

Use the **rule** command to create or edit an IPv4 advanced ACL rule. You can edit ACL rules only when the match order is config.

Use the **undo rule** command to delete an entire IPv4 advanced ACL rule or some attributes in the rule. If no optional keywords are provided, you delete the entire rule. If optional keywords or arguments are provided, you delete the specific attributes.

By default, an IPv4 advanced ACL does not contain any rule.

Within an ACL, the permit or deny statement of each rule must be unique. If the ACL rule you are creating or editing has the same deny or permit statement as another rule in the ACL, your creation or editing attempt will fail.

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

Related commands: **acl**, **display acl**, and **step**.

Examples

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

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-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
```

rule (IPv4 basic ACL view)

Syntax

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

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

View

IPv4 basic ACL view

Default Level

2: System level

Parameters

rule-id: Specifies a rule ID, which ranges from 0 to 65534. If no rule ID is provided when you create an ACL rule, the system automatically assigns it a rule ID. This rule ID takes 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.

fragment: Applies the rule only to non-first fragments. A rule without this keyword applies to both fragments and non-fragments.

logging: Logs matching packets. This function is available only when the application module that uses the ACL supports the logging function.

source { *sour-addr sour-wildcard* | **any** }: Matches a source address. The *sour-addr sour-wildcard* arguments represent a source IP address and wildcard mask in dotted decimal notation. A wildcard mask of zeros specifies 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.

vpn-instance *vpn-instance-name*: Applies the rule to packets in a VPN instance. The *vpn-instance-name* argument takes a case sensitive string of 1 to 31 characters. If no VPN instance is specified, the rule applies only to non-VPN packets.

Description

Use the **rule** command to create or edit an IPv4 basic ACL rule. You can edit ACL rules only when the match order is config.

Use the **undo rule** command to delete an entire IPv4 basic ACL rule or some attributes in the rule. If no optional keywords are provided, you delete the entire rule. If optional keywords or arguments are provided, you delete the specific attributes.

By default, an IPv4 basic ACL does not contain any rule.

Within an ACL, the permit or deny statement of each rule must be unique. If the ACL rule you are creating or editing has the same deny or permit statement as another rule in the ACL, your creation or editing attempt will fail.

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

Related commands: **acl**, **display acl**, and **step**.

Examples

Create a rule in IPv4 basic ACL 2000 to deny packets sourced from 1.1.1.1/32.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule deny source 1.1.1.1 0
```

rule (IPv6 advanced ACL view)

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** } | **destination** { *dest dest-prefix* | *dest/dest-prefix* | **any** } | **destination-port** *operator port1* [*port2*] | **dscp** *dscp* | **fragment** | **icmp6-type** { *icmp6-type icmp6-code* | *icmp6-message* } | **logging** | **source** { *source source-prefix* | *source/source-prefix* **| any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name*] *

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

View

IPv6 advanced ACL view

Default Level

2: System level

Parameters

rule-id: Specifies a rule ID, which ranges from 0 to 65534. If no rule ID is provided when you create an ACL rule, the system automatically assigns it a rule ID. This rule ID takes 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: Matches protocol carried over IPv6. It can be a number in the range 0 to 255, or in words, **gre** (47), **icmpv6** (58), **ipv6**, **ipv6-ah** (51), **ipv6-esp** (50), **ospf** (89), **tcp** (6), or **udp** (17). Table 4-8 describes the parameters that can be specified after the *protocol* argument.

Table 4-8 Match criteria and other rule information for IPv6 advanced ACL rules

Parameters	Function	Description
source { *source source-prefix* | *source/source-prefix* | **any** }	Specifies a source IPv6 address	The *source* and *source-prefix* arguments represent an IPv6 source address, and prefix length that ranges from 1 to 128. The **any** keyword represents any IPv6 source address.
destination { *dest dest-prefix* | *dest/dest-prefix* | **any** }	Specifies a destination IPv6 address	The *dest* and *dest-prefix* arguments represent a destination IPv6 address, and prefix length that ranges from 1 to 128. The **any** keyword specifies any IPv6 destination address.

Parameters	Function	Description
dscp *dscp*	Specifies a DSCP preference	The *dscp* argument can be a number in the range 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).
logging	Logs matching packets	This function requires that the module that uses the ACL supports logging.
fragment	Applies the rule to only non-first fragments	Without this keyword, the rule applies to all fragments and non-fragments.
time-range *time-range-name*	Specifies a time range for the rule	The *time-range-name* argument takes a case insensitive string of 1 to 32 characters. It must start with an English letter.

Setting the *protocol* argument to **tcp** (6) or **udp** (17), you may set the parameters shown in Table 4-9.

Table 4-9 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). The *port1* and *port2* arguments are TCP or UDP port numbers in the range 0 to 65535. *port2* is needed only when the *operator* argument is **range**. TCP port numbers can be represented in these words: **chargen** (19), **bgp** (179), **cmd** (514), **daytime** (13), **discard** (9), **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 in these words: **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 relationship between the TCP flags in a rule is AND.
established	Specifies the flags for indicating the established status of a TCP connection	Parameter specific to TCP.

Setting the *protocol* argument to **icmpv6** (58), you may set the parameters shown in Table 4-10.

Table 4-10 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 ranges from 0 to 255. The *icmp6-code* argument ranges from 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 4-11.

Table 4-11 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

Description

Use the **rule** command to create or edit an IPv6 advanced ACL rule. You can edit ACL rules only when the match order is config.

Use the **undo rule** command to delete an entire IPv6 advanced ACL rule or some attributes in the rule. If no optional keywords are provided, you delete the entire rule. If optional keywords or arguments are provided, you delete the specific attributes.

By default, an IPv6 advanced ACL does not contain any rule.

Within an ACL, the permit or deny statement of each rule must be unique. If the ACL rule you are creating or editing has the same deny or permit statement as another rule in the ACL, your creation or editing attempt will fail.

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

Related commands: **acl ipv6**, **display ipv6 acl**, and **step**.

Examples

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

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] rule permit tcp source 2030:5060::/64 destination fe80:5060::/96
destination-port eq 80
```

rule (IPv6 basic ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } [**fragment** | **logging** | **source** { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* **| any** } | **time-range** *time-range-name*] *

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

View

IPv6 basic ACL view

Default Level

2: System level

Parameters

rule-id: Specifies a rule ID, which ranges from 0 to 65534. If no rule ID is provided when you create an ACL rule, the system automatically assigns it a rule ID. This rule ID takes 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.

fragment: Applies the rule only to non-first fragments. A rule without this keyword applies to both fragments and non-fragments.

logging: Logs matching packets. This function requires that the module that uses the ACL supports logging.

source { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* | **any** }: Matches a source IP address. The *ipv6-address* and *prefix-length* arguments represent a source IPv6 address and address prefix length in the range 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 takes a case insensitive string of 1 to 32 characters. It must start with an English letter.

Description

Use the **rule** command to create or edit an IPv6 basic ACL rule. You can edit ACL rules only when the match order is config.

Use the **undo rule** command to delete an entire IPv6 basic ACL rule or some attributes in the rule. If no optional keywords are provided, you delete the entire rule. If optional keywords or arguments are provided, you delete the specific attributes.

By default, an IPv6 basic ACL does not contain any rule.

Within an ACL, the permit or deny statement of each rule must be unique. If the ACL rule you are creating or editing has the same deny or permit statement as another rule in the ACL, your creation or editing attempt will fail.

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

Related commands: **acl ipv6**, **display ipv6 acl**, and **step**.

Examples

Create an IPv6 basic ACL rule to deny packets sourced from FE80:5060::101/128.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule deny source fe80:5060::101/128
```

rule (WLAN ACL view)

Syntax

rule [*rule-id*] { **permit** | **deny** } [**ssid** *ssid-name*]

undo rule *rule-id*

View

WLAN ACL view

Default Level

2: system level

Parameters

rule-id: Specifies a rule ID, which ranges from 0 to 65534. If no rule ID is provided when you create an ACL rule, the system automatically assigns it a rule ID. This rule ID takes 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.

ssid-name: Specifies an SSID name, which is a case sensitive string of 1 to 32 alphanumeric characters. Spaces are allowed.

Description

Use the **rule** command to create or edit a WLAN ACL rule.

Use the **undo rule** command to delete an entire WLAN ACL rule.

By default, a WLAN ACL does not contain any rule.

Within an ACL, the permit or deny statement of each rule must be unique. If the ACL rule you are creating or editing has the same deny or permit statement as another rule in the ACL, your creation or editing attempt will fail.

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

Related commands: **acl**, **display acl**, and **step**.

Examples

Create a rule for WLAN ACL 100 to permit packets with the SSID name of **user1** and apply this ACL to user interface VTY 0 to restrict user access.

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

```
[Sysname] acl number 100
[Sysname-acl-wlan-100] rule permit ssid user1
[Sysname-acl-wlan-100] quit
[Sysname] user-interface vty 0
[Sysname-ui-vty0] acl 100 inbound
```

rule comment

Syntax

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

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

View

WLAN ACL view, IPv4 basic/advanced ACL view, IPv6 basic/advanced ACL view, Ethernet frame header ACL view

Default Level

2: System level

Parameters

rule-id: Specifies the ID of an existing ACL rule. The ID ranges from 0 to 65534.

text: Provides a description for the ACL rule, a case sensitive string of 1 to 127 characters.

Description

Use the **rule comment** command to configure a description for an existing ACL rule or edit its description for the ease of identification.

Use the **undo rule comment** command to delete the ACL rule description.

By default, an IPv4 ACL rule has no rule description.

Related commands: **display acl** and **display acl ipv6**.

Examples

Create a rule in IPv4 basic ACL 2000 and configure a description for this rule.

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

Create a rule in IPv6 basic ACL 2000 and configure a description for this rule.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule 0 permit source 1001::1 128
[Sysname-acl6-basic-2000] rule 0 comment This rule is used on Ethernet 1/0/1.
```

step

Syntax

step *step-value*

undo step

View

WLAN ACL view, IPv4 basic/advanced ACL view, IPv6 basic/advanced ACL view, Ethernet frame header ACL view

Default Level

2: System level

Parameters

step-value: ACL rule numbering step, which ranges from 1 to 20.

Description

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

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

The default rule numbering step is 5. After you restore the default numbering step by the **undo step** command, the rules are renumbered in the step of 5.

Related commands: **display acl** and **display acl ipv6**.

Examples

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

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

Set the rule numbering step to 2 for IPv6 basic ACL 2000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] step 2
```

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*]

View

System view

Default Level

2: System level

Parameters

time-range-name: Assigns a name for a time range. The name is a case insensitive string of 1 to 32 characters. It must start with an English letter and to avoid confusion, cannot be **all**.

start-time **to** *end-time*: Specifies a periodic time range. Both *start-time* and *end-time* are in hh:mm format (24-hour clock), and each value ranges from 00:00 to 23:59. The end time must be greater than the start time.

days: Specifies the day or days of the week on which the periodic time range is valid. You may specify multiple values, in words or in digits, separated by spaces, but make sure that they do not overlap. The values are ANDed. These values can take one of the following forms:

- A digit in the range 0 to 6, respectively for Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday.
- A day of a week in 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 time range. The *time1* argument specifies the time of the day in hh:mm format (24-hour clock). Its value ranges from 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 1 to 12, DD is the day of the month with the range depending on MM, and YYYY is the year in the usual Gregorian calendar in the range 1970 to 2100. If not specified, the start time is the earliest time available in the system, 01/01/1970 00:00 AM.

to *time2 date2*: Specifies the end time and date of the absolute time range. The *time2* argument is in the same format as that of the *time1* argument, but its value ranges from 00:00 to 24:00. The format and value range of the *date2* argument are the same as those of the *date1* argument. The end time must be greater than the start time. If not specified, the end time is the maximum time available in the system, 12/31/2100 24:00 PM.

Description

Use the **time-range** command to create a time range.

Use the **undo time-range** command to delete a time range.

By default, no time range exists.

You can create a time range as follows:

- Create a periodic time range in the *start-time* **to** *end-time days* format. A periodic time range recurs periodically on a day or days of the week.
- Create an absolute time range in the **from** *time1 date1* **to** *time2 date2* format. Unlike a periodic time range, an absolute time range does not recur.
- Create a compound time range in the *start-time* **to** *end-time days* **from** *time1 date1* **to** *time2 date2* format. A compound time range 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, 2010 00:00 and December 31, 2010 23:59, use the **time-range test 08:00 to 12:00 mon from 00:00 01/01/2010 to 23:59 12/31/2010** command.

You may create individual time ranges identified with the same name. They are regarded as one time range whose active period is the result of ORing periodic ones, ORing absolute ones, and ANDing periodic and absolute ones.

You may create a maximum of 256 uniquely named time ranges, each with 32 periodic time ranges at most and 12 absolute time ranges at most.

Related commands: **display 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 8:0 to 18:0 working-day
```

Create an absolute time range **t2**, setting it to be active in the whole year of 2010.

```
<Sysname> system-view
[Sysname] time-range t2 from 0:0 1/1/2010 to 23:59 12/31/2010
```

Create a compound time range **t3**, setting it to be active from 08:00 to 12:00 on Saturdays and Sundays of the year 2010.

```
<Sysname> system-view
[Sysname] time-range t3 8:0 to 12:0 off-day from 0:0 1/1/2010 to 23:59 12/31/2010
```

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 the period of January through June of the year 2010.

```
<Sysname> system-view
[Sysname] time-range t4 10:0 to 12:0 1 from 0:0 1/1/2010 to 23:59 1/31/2010
[Sysname] time-range t4 14:0 to 16:0 3 from 0:0 6/1/2010 to 23:59 6/30/2010
```

Note

- The models listed in this document are not applicable to all regions. Please consult your local sales office for the models applicable to your region.
- Support of the H3C WA series WLAN access points (APs) for commands may vary by AP model. For more information, see *Feature Matrix.*
- The interface types and the number of interfaces vary by AP model.
- The term *AP* in this document refers to common APs, wireless bridges, and mesh APs.

5 QoS Policy Configuration Commands

Class Configuration Commands

display traffic classifier user-defined

Syntax

display traffic classifier user-defined [*tcl-name*]

View

Any view

Default Level

1: Monitor level

Parameters

user-defined: Displays user-defined classes.

tcl-name: Name of a class.

Description

Use the **display traffic classifier** command to display information about user-defined classes.

If no class name is specified, the command displays information about all user-defined classes.

Examples

Display information about all user-defined classes.

```
<Sysname> display traffic classifier user-defined
User Defined Classifier Information:
 Classifier: USER1
  Operator: AND
  Rule(s) : if-match ip-precedence 5

 Classifier: database
  Operator: AND
  Rule(s) : if-match acl 3131
```

```
if-match inbound-interface Ethernet1/0/1
```

Table 5-1 display traffic classifier user-defined command output description

Field	Description
User Defined Classifier Information	User-defined class information
Classifier	Class name and its match criteria
Operator	Logical relationship between match criteria
Rule(s)	Match criteria

if-match

Syntax

if-match *match-criteria*

undo if-match *match-criteria*

undo if-match acl { *acl-number* | **name** *acl-name* } [**update acl** { *acl-number* | **name** *acl-name* }]

View

Class view

Default Level

2: System level

Parameters

match-criteria: Match criterion. Table 5-2 shows the available criteria.

acl { *acl-number* | **name** *acl-name* }: Specifies an ACL currently referenced in the class by the ACL name or ACL number.

update acl { *acl-number* | **name** *acl-name* }: Specifies a new ACL to replace the specified current ACL by the number or name of the new ACL.

Table 5-2 The range of the *match-criteria* argument

Value	Description
acl { *acl-number* | **name** *acl-name* }	Matches an ACL The *acl-number* argument ranges from 2000 to 4999 for an IPv4 ACL. The *acl-name* argument is a case-insensitive string of 1 to 32 characters, which must start with an English letter from a to z or A to Z and cannot be **all** to avoid confusion.
any	Matches all packets
dscp *dscp-list*	Matches DSCP values. The *dscp-list* argument is a list of up to 8 DSCP values. A DSCP value ranges from 0 to 63.
destination-mac *mac-address*	Matches a destination MAC address
customer-dot1p *8021p-list*	Matches the 802.1p priority of the customer network. The *8021p-list* argument is a list of up to eight 802.1p priority values. An 802.1p priority ranges from 0 to 7.

Value	Description
ip-precedence *ip-precedence-list*	Matches IP precedence. The *ip-precedence-list* argument is a list of up to 8 IP precedence values. An IP precedence ranges from 0 to 7.
protocol *protocol-name*	Matches a protocol. The *protocol-name* argument can be IP or IPv6.
source-mac *mac-address*	Matches a source MAC address
customer-vlan-id { *vlan-id-list* | *vlan-id1* **to** *vlan-id2* }	Matches the VLAN IDs of customer networks. The *vlan-id-list* argument is a list of up to 8 VLAN IDs. *vlan-id1* **to** *vlan-id2* specifies a VLAN ID range, where *vlan-id1* must be smaller than *vlan-id2*. A VLAN ID ranges from 1 to 4094.

Description

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

Use the **undo if-match** command to delete the match criterion.

When defining match criteria, use the usage guidelines described in these subsections:

- Define an ACL-based match criterion
- Define a criterion to match a destination MAC address
- Define a criterion to match a source MAC address
- Define a criterion to match DSCP values
- Define a criterion to match the 802.1p priority values of the customer network
- Define a criterion to match the IP precedence values
- Define a criterion to match customer network VLAN IDs

Define an ACL-based match criterion

- If the ACL referenced in the **if-match** command does not exist, the class cannot be applied to hardware.
- For a class, you can reference an ACL twice by its name and number respectively with the if-match command.

Define a criterion to match a destination MAC address

- You can configure multiple destination MAC address match criteria for a class.
- A criterion to match a destination MAC address is significant only to Ethernet interfaces.

Define a criterion to match a source MAC address

- You can configure multiple source MAC address match criteria for a class.
- A criterion to match an source MAC address is significant only to Ethernet interfaces.

Define a criterion to match DSCP values

- You can configure multiple DSCP match criteria for a class. All the defined DSCP values are automatically arranged in ascending order.
- You can configure up to eight DSCP values in one command line. If multiple identical DSCP values are specified, the system considers them as one. If a packet matches one of the defined DSCP values, it matches the **if-match** clause.
- To delete a criterion matching DSCP values, the specified DSCP values must be identical with those defined in the rule (the sequence may be different).

Define a criterion to match the 802.1p priority values of the customer network

- You can configure multiple 802.1p priority match criteria for a class. All the defined 802.1p values are automatically arranged in ascending order.
- You can configure up to eight 802.1p priority values in one command line. If the same 802.1p priority value is specified multiple times, the system considers them as one. If a packet matches one of the defined 802.1p priority values, it matches the **if-match** clause.
- To delete a criterion matching 802.1p priority values, the specified 802.1p priority values in the command must be identical with those defined in the criterion (the sequence may be different).
- The match criterion takes effect only on incoming traffic.

Define a criterion to match the IP precedence values

- You can configure multiple IP precedence match criteria for a class. The defined IP precedence values are automatically arranged in ascending order.
- You can configure up to eight IP precedence values in one command line. If the same IP precedence is specified multiple times, the system considers them as one. If a packet matches one of the defined IP precedence values, it matches the **if-match** clause.
- To delete a criterion that matches IP precedence values, the specified IP precedence values in the command must be identical with those defined in the criterion (the sequence may be different).

Define a criterion to match customer network VLAN IDs

- You can configure multiple VLAN ID match criteria for a class. The defined VLAN IDs are automatically arranged in ascending order.
- You can configure multiple VLAN IDs in one command line. If the same VLAN ID is specified multiple times, the system considers them as one. If a packet matches one of the defined VLAN IDs, it matches the **if-match** clause.
- To delete a criterion that matches VLAN IDs, the specified VLAN IDs in the command must be identical with those defined in the criterion (the sequence may be different).
- The match criterion takes effect only on incoming traffic.

Related commands: **traffic classifier**.

Note

Support for the augments and keywords of the **if-match** command varies by AP model.

Examples

Define a criterion to match IP packets.

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

Define a match criterion for class **class1** to match the packets with the destination MAC address 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 class **class2** to match the packets with the source MAC address 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 class **class1** to match ACL 3101.

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

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

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

Define a match criterion for class **class1** to match the packets with IP precedence 5. Reference class **class1** to define a match criterion for class **class2**.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match ip-precedence 5
```

Define match criteria for class **class1** to match the packets that have the destination MAC address 0050-BA27-BED3.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match destination-address mac 0050-BA27-BED3
```

Define a match criterion for class **class1** to match the packets with a DSCP precedence 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 class **class1** to match the packets with an IP precedence 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 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 class **class1** to match the packets with customer network VLAN ID 1, 6, or 9.

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

traffic classifier

Syntax

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

undo traffic classifier *tcl-name*

View

System view

Default Level

2: System level

Parameters

tcl-name: Specifies a class name.

operator: Sets the operator to logic AND or OR for the class.

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

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

Description

Use the **traffic classifier** command to define a class and enter class view.

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

If no match operator is specified, the default AND operator applies.

Related commands: **qos policy**, **qos apply policy**, and **classifier behavior**.

Examples

Create a class named **class1**.

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

Traffic Behavior Configuration Commands

car

Syntax

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

undo car

View

Traffic behavior view

Default Level

2: System level

Parameters

cir *committed-information-rate*: Committed information rate (CIR) in kbps, which is the average traffic rate.

cbs *committed-burst-size*: Committed burst size (CBS). By default, CBS is traffic transmitted in 500 ms at the rate of CIR.

ebs *excess-burst-size*: Excess burst size (EBS) in bytes. The default is 0.

pir *peak information rate*: Peak information rate (PIR) in kbps.

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

action: Sets the action to take on packets:

- **discard**: Drops packets.
- **pass**: Permits packets to pass through.

Description

Use the **car** command to configure a CAR action in the traffic behavior.

Use the **undo car** command to delete a CAR action from the traffic behavior.

You can apply a QoS policy that references the behavior to either the incoming or outgoing traffic of an interface.

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

Related commands: **qos policy**, **traffic behavior**, and **classifier behavior**.

Examples

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

- Set the CIR to 200 kbps, CBS to 50000 bytes, and EBS to 0.
- Allow the conforming packets to pass, and drop the excess packets.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] car cir 200 cbs 50000 ebs 0 red discard
```

display traffic behavior user-defined

Syntax

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

View

Any view

Default Level

1: Monitor level

Parameters

user-defined: Displays user-defined traffic behaviors.

behavior-name: Behavior name. If no traffic behavior is specified, this command displays the information of all the user-defined behaviors.

Description

Use the **display traffic behavior** command to display user-defined traffic behavior information.

Examples

Display user-defined traffic behaviors.

```
<Sysname> display traffic behavior user-defined
User Defined Behavior Information:
    Behavior: ipv4
      Filter enable : permit
      Committed Access Rate:
        CIR 9999 (kbps), CBS 624937 (byte), EBS 0 (byte)
        Green Action: pass
```

```
  Red Action: discard
Marking:
  Remark local precedence 4
```

Table 5-3 display traffic behavior user-defined command output description

Field	Description
User Defined Behavior Information	User-defined behavior information
Behavior	Name of a behavior
Marking	Information about traffic marking
Committed Access Rate	Information about the CAR action

filter

Syntax

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

undo filter

View

Traffic behavior view

Default Level

2: System level

Parameters

deny: Drops packets.

permit: Permits packets to pass through.

Description

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

Use the **undo filter** command to delete the traffic filtering action.

If you configure a deny filtering action, the traffic behavior drops all matching packets. If you configure a permit filtering action, the traffic behavior permits all matching packets to pass through.

Examples

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

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

remark dot1p

Syntax

remark dot1p *8021p*

undo remark dot1p

View

Traffic behavior view

Default Level

2: System level

Parameters

8021p: 802.1p priority to be marked for packets, which ranges from 0 to 7.

Description

Use the **remark dot1p** command to configure an 802.1p priority marking action.

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

Related commands: **qos policy**, **traffic behavior**, and **classifier behavior**.

Examples

Set the 802.1p priority to 2 for packets.

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

remark local-precedence

Syntax

remark local-precedence *local-precedence*

undo remark local-precedence

View

Traffic behavior view

Default Level

2: System level

Parameters

local-precedence: Sets the local precedence value to be marked for packets, which ranges from 0 to 7.

Description

Use the **remark local-precedence** command to configure a local precedence marking action.

Use the **undo remark local-precedence** command to delete the action.

Related commands: **qos policy**, **traffic behavior**, and **classifier behavior**.

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
```

traffic behavior

Syntax

traffic behavior *behavior-name*

undo traffic behavior *behavior-name*

View

System view

Default Level

2: System level

Parameters

behavior-name: Sets a behavior name.

Description

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

Use the **undo traffic classifier** command to delete a traffic behavior.

A traffic behavior is a set of actions, such as priority marking, dropping, rate limiting, and accounting. You provide QoS for a class of traffic by associating a traffic behavior with the class of traffic.

Related commands: **qos policy**, **qos apply policy**, and **classifier behavior**.

Examples

Create a traffic behavior named **behavior1**.

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

QoS Policy Configuration and Application Commands

classifier behavior

Syntax

classifier *tcl-name* **behavior** *behavior-name*

undo classifier *tcl-name*

View

Policy view

Default Level

2: System level

Parameters

tcl-name: Class name.

behavior-name: Behavior name.

Description

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

Use the **undo classifier** command to remove a class from the policy. You cannot remove a default class.

You can perform a set of QoS actions on a traffic class by associating a traffic behavior with the traffic class.

You can assign multiple classes to a QoS policy, and each class can associate with only one traffic behavior. You can associate a class with only one behavior.

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

Related commands: **qos policy**.

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
[Sysname-qospolicy-user1]
```

display qos policy user-defined

Syntax

display qos policy user-defined [*policy-name* [**classifier** *tcl-name*]]

View

Any view

Default Level

1: Monitor level

Parameters

user-defined: Displays user-defined QoS policies.

policy-name: QoS policy name, a string of 1 to 31 characters. If no policy is specified, this command displays configuration information of all the policies.

tcl-name: Class name.

Description

Use the **display qos policy user-defined** command to display user-defined QoS policy configuration information.

Examples

Display the configuration information of user-defined QoS policies.

```
<Sysname> display qos policy user-defined
User Defined QoS Policy Information:

  Policy: ipv4
   Classifier: ipv4
     Behavior: ipv4
      Filter enable : permit
      Committed Access Rate:
        CIR 9999 (kbps), CBS 624937 (byte), EBS 0 (byte)
        Green Action: pass
        Red Action: discard
      Marking:
        Remark local precedence 4
```

Table 5-4 display qos policy command output description

Field	Description
Policy	Policy name

Field	Description
Classifier	Class name A policy can contain multiple classes, and each class is associated with a traffic behavior. A class can be configured with multiple match criteria. For more information, see the **traffic classifier** command.
Behavior	Behavior associated with the class. A behavior is associated with a class. It can be configured with multiple actions. For more information, see the **traffic behavior** command.

display qos policy interface

Syntax

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

View

Any view

Default Level

1: Monitor level

Parameters

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

Description

Use the **display qos policy interface** command to display information about the QoS policy or policies applied to an interface or all interfaces.

Examples

Display information about the QoS policy applied to port Ethernet1/0/1.

```
<Sysname> display qos policy interface ethernet 1/0/1
  Interface: Ethernet1/0/1
  Direction: Inbound
  Policy: test
   Classifier: test
     Matched : 0(Packets) 0(Bytes)
     Operator: AND
     Rule(s) : If-match acl 3000
     Behavior: test
      Committed Access Rate:
        CIR 1000 (kbps), CBS 62500 (byte), EBS 0 (byte)
        Green Action: pass
        Red Action: discard
        Green : 0(Packets) 0(Bytes)
        Red   : 0(Packets) 0(Bytes)
```

Table 5-5 display qos policy interface command output description

Field	Description
Interface	Interface type and interface number

Field	Description
Direction	The direction in which the policy is applied to the interface
Policy	Name of the policy applied to the interface
Classifier	Class name and corresponding configuration information
Matched	Number of packets satisfying the match criteria
Operator	Logical relationship between match criteria in the class
Rule(s)	Match criteria in the class
Behavior	Behavior name and corresponding configuration information

qos apply policy

Syntax

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

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

View

Interface view

Default Level

2: System level

Parameters

inbound: Inbound direction.

outbound: Outbound direction.

policy *policy-name*: Specifies a policy by its name.

Description

Use the **qos apply policy** command to apply a QoS policy to the interface.

Use the **undo qos apply policy** command to remove the QoS policy.

To successfully apply a policy to an interface, make sure that the total bandwidth assigned to AF and EF in the policy is smaller than the available bandwidth of the interface. If the available bandwidth of an interface is modified to a value smaller the total bandwidth for AF and EF, the applied policy is removed.

Examples

Apply policy **USER1** to the outgoing traffic of Ethernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0/1
[Sysname-Ethernet1/0/1] qos apply policy USER1 outbound
```

qos policy

Syntax

qos policy *policy-name*

undo qos policy *policy-name*

View

System view

Default Level

2: System level

Parameters

policy *policy-name*: Policy name, a string of 1 to 31 characters.

Description

Use the **qos policy** command to create a policy and enter policy view.

Use the **undo qos policy** command to delete a policy.

To use the **undo qos policy** command to delete a policy that has been applied to an interface, you must first remove it from the interface.

Related commands: **classifier behavior** and **qos apply policy**.

Examples

Define a policy named **user1**.

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

6 Priority Mapping Configuration Commands

Priority Mapping Table Configuration Commands

display qos map-table

Syntax

display qos map-table [**dot11e-lp** | **dot1p-lp** | **dscp-lp** | **lp-dot11e** | **lp-dot1p** | **lp-dscp**]

View

Any view

Default Level

1: Monitor level

Parameters

dot11e-lp: 802.11e-to-local priority mapping table.

dot1p-lp: 802.1p-to-local priority mapping table.

dscp-lp: DSCP-to-local priority mapping table.

lp-dot11e: Local-to-802.11e priority mapping table.

lp-dot1p: Local-to-802.1p priority mapping table.

lp-dscp: Local-to-DSCP priority mapping table.

Description

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

If no priority mapping table is specified, this command displays the configuration information of all priority mapping tables. If no direction is specified, this command displays the priority mapping tables in any direction.

Related commands: **qos map-table**.

Examples

Display the configuration information of the 802.1p-to-local priority mapping table.

```
<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 6-1 display qos map-table command output description

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

import

Syntax

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

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

View

Priority mapping table view

Default Level

2: System level

Parameters

import-value-list: List of input values.

export-value: Output value.

all: Deletes all the mappings in the priority mapping table.

Description

Use the **import** command to configure a mapping from one or multiple input values to an output value.

Use the **undo import** command to restore the specified or all mappings to the default mappings.

Related commands: **display qos map-table**.

Examples

Configure the 802.1p-to-local priority mapping table to map 802.1p priority values 4 and 5 to local precedence value 1.

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

qos map-table

Syntax

qos map-table { **dot11e-lp** | **dot1p-lp** | **dscp-lp** | **lp-dot11e** | **lp-dot1p** | **lp-dscp** }

View

System view

Default Level

2: System level

Parameters

dot11e-lp: 802.11e-to-local priority mapping table.

dot1p-lp: 802.1p-to-local priority mapping table.

dscp-lp: DSCP-to-local priority mapping table.

lp-dot11e: Local-to-802.11e priority mapping table.

lp-dot1p: Local-to-802.1p priority mapping table.

lp-dscp: Local-to-DSCP priority mapping table.

Description

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

Related commands: **display qos map-table**.

Examples

Enter 802.1p-to-local priority mapping table view.

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

Port Priority Configuration Commands

qos priority

Syntax

qos priority *priority-value*

undo qos priority

View

Interface view

Default Level

2: System level

Parameters

priority-value: Port priority value, which ranges from 0 to 7.

Description

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

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

By default, the port priority of an interface is 0.

If a WLAN-BSS interface is in use, you cannot modify the port priority of the WLAN-BSS interface. To do so, you must stop the service the interface provides (in other words, make the current users on the interface offline) and then modify the port priority.

Examples

Set the port priority of interface Ethernet 1/0/1 to 2.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0/1
[Sysname-Ethernet1/0/1] qos priority 2
```

Set the port priority of interface WLAN-BSS 1 to 2.

```
<Sysname> system-view
[Sysname] interface WLAN-BSS 1
[Sysname-WLAN-BSS1] qos priority 2
```

Priority Trust Mode Configuration Commands

display qos trust interface

Syntax

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

View

Any view

Default Level

1: Monitor level

Parameters

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

Description

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

If no interface is specified, the command displays priority trust mode and port priority information for all interfaces.

Examples

Display the priority trust mode and port priority information of Ethernet 1/0/1.

```
<Sysname> display qos trust interface ethernet 1/0/1
Interface: Ethernet1/0/1
 Port priority information
  Port priority :0
  Port priority trust type : dot1p
```

Table 6-2 display qos trust interface command output description

Field	Description
Interface	Interface type and interface number
Port priority trust information	Priority trust mode and port priority information
Port priority trust type	Priority trust mode on the interface, which can be **dot11e**, **dot1p**, or **dscp**

qos trust

Syntax

qos trust { **dot11e** | **dot1p** | **dscp** }

undo qos trust

View

Interface view

Default Level

2: System level

Parameters

dot11e: Uses the 802.11e priority in incoming packets for priority mapping. This keyword is applicable to only WLAN-ESS interfaces.

dot1p: Uses the 802.1p priority in incoming packets for priority mapping. This keyword is applicable to only Ethernet interfaces.

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

Description

Use the **qos trust** command to configure an interface to use a particular priority field carried in packets for priority mapping.

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

By default, QoS is disabled.

When packets enter the AP, the AP assigns a series of parameters (including 802.11e priority, 802.1p priority, DSCP value, and local precedence value) to the packets as configured.

A local precedence value is locally significant and corresponds to an output queue.

If a WLAN-BSS interface is in use, you cannot modify the priority trust mode of the WLAN-BSS interface. To do so, stop the service the interface provides (in other words, make the current users on the interface offline) first.

Examples

Configure Ethernet 1/0/1 to use the 802.1p priority in incoming packets for priority mapping.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0/1
[Sysname-Ethernet1/0/1] qos trust dot1p
```

Configure WLAN-BSS 1 to use the 802.11e priority in incoming packets for priority mapping.

```
<Sysname> system-view
[Sysname] interface wlan-bss 1
[Sysname-WLAN-BSS 1] qos trust dot11e
```

7 Index