H3C S5120-SI Series Ethernet Switches

ACL and QoS Command Reference

Hangzhou H3C Technologies Co., Ltd.

http://www.h3c.com

Trademarks

H3C, H3C, Aolynk, Aolynk, H^{3}Care, H3care, TOP G, TOPG, IRF, NetPilot, Neocean, NeoVTL, SecPro, SecPoint, SecEngine, SecPath, Comware, Secware, Storware, NQA, VVG, V^{2}G, V^{n}G, PSPT, XGbus, N-Bus, TiGem, InnoVision and HUASAN are trademarks of Hangzhou H3C Technologies Co., Ltd.

All other trademarks that may be mentioned in this manual are the property of their respective owners.

Notice

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied.

Environmental Protection

This product has been designed to comply with the requirements on environmental protection. The storage, use, and disposal of this product must meet the applicable national laws and regulations.

Preface

The H3C S5120-SI documentation set includes 13 configuration guides, which describe the software features for the H3C S5120-SI Series Routing Switches and guide you through the software configuration procedures. These configuration guides also provide configuration examples to help you apply software features to different network scenarios.

This preface includes:

- Audience
- Conventions
- About the H3C S5120-SI Documentation Set
- Obtaining Documentation
- Documentation Feedback

Audience

This documentation is intended for:

Network planners

Field technical support and servicing engineers

Network administrators working with the S5120-SI series

Conventions

This section describes the conventions used in this documentation set.

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
< >	Button names are inside angle brackets. For example, click <OK>.
[ ]	Window names, menu items, data table and field names are inside square brackets. For example, pop up the [New User] window.
/	Multi-level menus are separated by forward slashes. 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.

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.

About the H3C S5120-SI documentation set

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.
	Card datasheets	Describe card specifications, features, and standards.
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 device with the minimum configuration.
	Installation guide	Provides a complete guide to hardware installation and hardware specifications.
	Card manuals	Provide the hardware specifications of cards.
	H3C Cabinet Installation and Remodel Introduction	Guides you through installing and remodeling H3C cabinets.
	H3C Pluggable SFP [SFP+][XFP] Transceiver Modules Installation Guide	Guides you through installing SFP/SFP+/XFP transceiver modules.
	Adjustable Slider Rail Installation Guide	Guides you through installing adjustable slider rails to a rack.
	H3C High-End Network Products Hot-Swappable Module Manual	Describes the hot-swappable modules available for the H3C high-end network products, their external views, and specifications.
Software configuration	Configuration guides	Describe software features and configuration procedures.
	Command references	Provide a quick reference to all available commands.
	Configuration examples	Describe typical network scenarios and provide configuration examples and instructions.
Operations and maintenance	System log messages	Explains the system log messages.
	Trap messages	Explains the trap messages.
	MIB Companion	Describes the MIBs for the software release.
	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.
	Error code reference	Explains the error codes.

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, 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

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 access control list (ACL):

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

name *acl-name*: Assigns a name for the 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 Configuration* 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 ACLs.

Description

Use the **acl** command to create an 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 ACLs.

By default, no ACL exists.

Note that:

- You can assign a name for an ACL only when you create it. After creating an ACL, you can neither rename it nor remove its name, if any.
- The name of an ACL must be unique among ACLs.
- If you specify both an ACL number and an ACL name in one command to enter the view of an existing ACL, be sure that the ACL number and ACL name identify the same ACL.
- You can change match order only for ACLs that do not contain any rules.

Examples

Create basic ACL 2000, and enter its view.

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

Create 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 ACL that already exists by its number:

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

name *source-acl-name*: Specifies a source 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 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 basic ACLs
- 3000 to 3999 for advanced ACLs
- 4000 to 4999 for Ethernet frame header ACLs

name *dest-acl-name*: Assigns a unique name for the 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.

Examples

Create ACL 2002 by copying ACL 2001.

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

acl name

Syntax

acl name *acl-name*

View

System view

Default Level

2: System level

Parameters

acl-name: Specifies the name of an existing 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 ACL by specifying its name.

Related commands: **acl**.

Examples

Enter the view of ACL **flow**.

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

description

Syntax

description *text*

undo description

View

Basic ACL view, 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**.

Examples

Configure a description for basic ACL 2000.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] description This acl is used on GE1/0/1
```

display acl

Syntax

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

View

Any view

Default Level

1: Monitor level

Parameters

acl-number: Specifies an ACL by its number:

- 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 ACLs.

name *acl-name*: Specifies an 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 ACLs.

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

Examples

Display information about ACL 2001.

```
<Sysname> display acl 2001
Basic ACL  2001, named flow, 1 rule,
ACL's step is 5
 rule 5 permit source 1.1.1.1 0 (5 times matched)
 rule 5 comment This rule is used on GE1/0/1
```

Table 1 display acl command output description

Field	Description
Basic ACL 2001	Category and number of the ACL. The following field information is about basic ACL 2001.
named flow	The name of the ACL is flow. "–none-" means the ACL is not named.
1 rule	The ACL contains one rule.
ACL's step is 5	The rule numbering step is 5.
5 times matched	There have been five matches for the rule. Only ACL matches performed by software are counted. This field is not displayed when no packets have matched the rule.
rule 5 comment This rule is used on GE1/0/1	The description of ACL rule 5 is “This rule is used on GE1/0/1.”

display acl resource

Syntax

display acl resource

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display acl resource** command to display the usage of ACL resources on a device.

Examples

Display the ACL resource usage of device.

```
<Sysname> display acl resource
-----------------------------------------------------
 GE1/0/1..GE1/0/24
 GE1/0/49 GE1/0/50
-----------------------------------------------------
  Type        Total    Reserved  Configured  Remaining
-----------------------------------------------------
  ACL         1024     370       0           654
  Meter       256      0         0           256
-----------------------------------------------------
 GE1/0/25..GE1/0/48
 GE1/0/51 GE1/0/52
-----------------------------------------------------
  Type        Total    Reserved  Configured  Remaining
-----------------------------------------------------
  ACL         1024     374       0           650
  Meter       256      0         0           256
```

Table 2 display acl resource command output description

Field	Description
Type	Resource type. Possible values are as follows: • METER for traffic policing resources, • ACL for rule resources,
Total	Total number of ACL rules supported
Reserved	Number of reserved ACL rules
Configured	Number of configured ACL rules
Remaining	Number of remaining ACL rules

display time-range

Syntax

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

View

Any view

Default Level

1: Monitor level

Parameters

time-range-name: 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.

Description

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

A time range is active if the system time falls into its range.

Examples

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

```
<Sysname> display time-range trname
Current time is 10:45:15 4/14/2005 Thursday
Time-range : trname ( Inactive )
from 08:00 12/1/2005 to 23:59 12/31/2100
```

Table 3 display time-range command output description

Field	Description
Current time	Current system time
Time-range	Configuration and status of the time range, including the name of the time range, its status (active or inactive), and its start time and end time.

packet-filter

Syntax

packet-filter { *acl-number* | **name** *acl-name* } **inbound**

undo packet-filter { *acl-number* | **name** *acl-name* } **inbound**

View

Ethernet port view, VLAN interface view

Default Level

2: System level

Parameters

acl-number: Specifies an ACL by its number:

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

name *acl-name*: Specifies an 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.

inbound: Filters incoming packets.

Description

Use the **packet-filter** command to apply an ACL to an interface to filter IPv4 packets or Ethernet frames.

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

By default, an interface does not filter IPv4 packets or Ethernet frames.

If you execute the command repeatedly, the last configuration takes effect.

Examples

Apply basic ACL 2001 to the inbound direction of interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEtherhet1/0/1] packet-filter 2001 inbound
```

Apply Ethernet frame header ACL 4001 to the inbound direction of interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEtherhet1/0/1] packet-filter 4001 inbound
```

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 ACL by its number:

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

all: Clears statistics for all ACLs.

name *acl-name*: Specifies an 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 ACLs.

Related commands: **display acl**.

Examples

Clear statistics on ACL 2001.

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

Clear statistics on ACL **flow**.

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

rule (advanced ACL view)

Syntax

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

View

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: Drops 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 describes the parameters that can be specified after the *protocol* argument.

Table 4 Match criteria and other rule information for 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 in dotted decimal notation. An all-zero wildcard specifies a host address. The **any** keyword specifies any source IP address.
destination { *dest-addr*	Specifies a destination	The *dest-addr dest-wildcard* arguments represent

Parameters	Function	Description
dest-wildcard | **any** }	address.	a destination IP address 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	Specifies to log matched packets.	This function requires that the module using the ACL support logging.
reflective	Specifies that the rule be reflective.	Not supported.
fragment	Indicates that the rule applies 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.

Caution

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

Setting the *protocol* argument to **tcp** or **udp**, you may define the parameters shown in Table 5.

Table 5 TCP/UDP-specific parameters for 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	Parameters specific to TCP. The value for each argument can be 0 or 1. The TCP flags in one rule are ANDed.
established	Specifies the TCP flags ACK and RST	Parameter specific to TCP.

Setting the *protocol* argument to **icmp**, you may define the parameters shown in Table 6.

Table 6 ICMP-specific parameters for 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 7.

Table 7 ICMP message names supported in advanced ACL rules

ICMP message name	Type	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

Description

Use the **rule** command to create or edit an advanced ACL rule.

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

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

If you do not specify optional keywords, the **undo rule** command removes the entire ACL rule; otherwise, the command removes only the specified criteria. Before performing the **undo rule** command, you can use the **display acl** command to view the ID of the rule.

When defining ACL rules, you do not need to assign them IDs; the system can automatically assign rule IDs starting with 0 and increasing based on certain rule numbering steps. A rule ID thus assigned is the smallest multiple of the step that is bigger than the current biggest number. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the next rule will be numbered 30.

You cannot create a rule with, or modify a rule to have the same permit/deny statement as an existing rule in the ACL.

You can only modify the existing rules of an ACL that uses the match order of **config**. When modifying a rule of such an ACL, you may choose to change just some of the settings, in which case the other settings remain the same.

When the ACL match order is **auto**, a newly created rule will be inserted among the existing rules in the depth-first match order. Note that the IDs of the rules still remain the same.

If the ACL match order is **auto**, rules are displayed in the depth-first match order rather than by rule number.

Note

For a basic ACL rule to be referenced by a QoS policy for traffic classification, the **logging** keyword is not supported.

Related commands: **display acl**.

Examples

Create a rule to permit TCP packets with the destination port of 80 from 129.9.0.0 to 202.38.160.0.

```
<Sysname> system-view
[Sysname] acl number 3101
[Sysname-acl-adv-3101] 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 (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

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 specified when you create an ACL rule, the system 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: Drops matching packets.

permit: Allows matching packets to pass.

fragment: Indicates that the rule applies to only non-first fragments. A rule without this keyword applies to all fragments and non-fragments.

logging: Generates log entries for matched packets.

source { *sour-addr sour-wildcard* | **any** }: Matches a source address. The *sour-addr sour-wildcard* arguments represent a source IP address 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.

Description

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

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

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

If you specify no optional keywords, the **undo rule** command removes the entire ACL rule; otherwise, the command removes only the specified criteria. Before performing the **undo rule** command, you can use the **display acl** command to view the ID of the rule.

When defining ACL rules, you do not need to assign them IDs; the system can automatically assign rule IDs starting with 0 and increasing based on certain rule numbering steps. A rule ID thus assigned is the smallest multiple of the step that is bigger than the current biggest number. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the next rule will be numbered 30.

You cannot create a rule with, or modify a rule to have, the same permit/deny statement as an existing rule in the ACL.

You can only modify the existing rules of an ACL that uses the match order of **config**. When modifying a rule of such an ACL, you may choose to change just some of the settings, in which case the other settings remain the same.

When the ACL match order is **auto**, a newly created rule will be inserted among the existing rules in the depth-first match order. Note that the IDs of the rules still remain the same.

Note

For a basic ACL rule to be referenced by a QoS policy for traffic classification, the **logging** keyword is not supported.

Related commands: **display acl**.

Examples

Create a rule in ACL 2000 to deny packets sourced from 1.1.1.1.

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

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 not 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: Drops matching packets.

permit: Allows matching packets to pass.

cos *vlan-pri:* Defines 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.

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.

Use the **undo rule** command to delete an Ethernet frame header ACL rule or some attributes in the rule.

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

When defining ACL rules, you do not need to assign them IDs; the system can automatically assign rule IDs starting with 0 and increasing in certain rule numbering steps. A rule ID thus assigned is the smallest multiple of the step that is bigger than the current biggest number. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the next rule will be numbered 30.

Before performing the **undo rule** command to remove an Ethernet frame header ACL rule, you may use the **display acl** command to view the ID of the rule.

You cannot create a rule with, or modify a rule to have, the same permit/deny statement as an existing rule in the ACL.

You can only modify the existing rules of an ACL that uses the match order of **config**. When modifying a rule of such an ACL, you may choose to change just some of the settings, in which case the other settings remain the same.

When the ACL match order is **auto**, a newly created rule will be inserted among the existing rules in the depth-first match order. Note that the IDs of the rules still remain the same.

If the ACL match order is **auto**, rules are displayed in the depth-first match order rather than by rule number.

Note

For an Ethernet frame header ACL to be referenced by a QoS policy for traffic classification, the **lsap** keyword is not supported.

Related commands: **display acl**.

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 comment

Syntax

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

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

View

Basic ACL view, 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 ACL rule has no rule description.

Related commands: **display acl**.

Examples

Create a rule in 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 GE1/0/1
```

step

Syntax

step *step-value*

undo step

View

Basic ACL view, 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.

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

By default, the rule numbering step is 5.

Related commands: **display acl**.

Examples

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

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

Set the rule numbering step to 2 for advanced ACL 3000.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] step 2
```

Set the rule numbering step to 2 for Ethernet frame header ACL 4000.

```
<Sysname> system-view
[Sysname] acl number 4000
[Sysname-acl-ethernetframe-4000] 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: Assign 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 00:00:00 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 24:00:00 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 may create a maximum of 256 time ranges.

A time range can be one of the following:

- Periodic time range created using the **time-range** *time-range-name start-time* **to** *end-time days* command. A time range thus created recurs periodically on the day or days of the week.
- Absolute time range created using the **time-range** *time-range-name* { **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2* } command. Unlike a periodic time range, a time range thus created does not recur. For example, to create an absolute time range that is active between January 1, 2004 00:00 and December 31, 2004 23:59, you may use the **time-range test from 00:00 01/01/2004 to 23:59 12/31/2004** command.
- Compound time range created using the **time-range** *time-range-name start-time* **to** *end-time days* { **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2* } command. A time range thus created recurs on the day or days of the week only within the specified period. For example, to create a time range that is active from 12:00 to 14:00 on Wednesdays between January 1, 2004 00:00 and December 31, 2004 23:59, you may use the **time-range test 12:00 to 14:00 wednesday from 00:00 01/01/2004 to 23:59 12/31/2004** 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.

Examples

Create a periodic time range **11**, setting it to be active between 8:00 to 18:00 during working days.

```
<Sysname> system-view
[Sysname] time-range test 8:00 to 18:00 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 t1 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
```

QoS policy configuration commands

Class configuration commands

display traffic classifier

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: Class name, a string of 1 to 31 characters.

Description

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

If no class name is specified, information about all user-defined classes is displayed.

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
```

Table 8 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 9shows 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 9 The form of the match-criteria argument

Form	Description
acl { *access-list-number* | **name** *acl-name* }	Specifies to match an IPv4 ACL specified by its number or name. The *access-list-number* argument specifies an ACL by its number, which ranges from 2000 to 4999; the **name** *acl-name* keyword-argument combination specifies an ACL by its name. In a class configured with the operator **and**, the logical relationship between rules defined in the referenced IPv4 ACL is **or**.
any	Specifies to match all packets.
customer-dot1p *8021p-list*	Specifies to match packets by 802.1p precedence of the customer network. The *8021p-list* argument is a list of CoS values, in the range of 0 to 7.
customer-vlan-id *vlan-id-list*	Specifies to match the packets of specified VLANs of user networks. The *vlan-id-list* argument specifies a list of VLAN IDs, in the form of *vlan-id* **to** *vlan-id* or multiple discontinuous VLAN IDs (separated by spaces). You can specify up to eight VLAN IDs for this argument at a time. VLAN ID is in the range 1 to 4094.
destination-mac *mac-address*	Specifies to match the packets with a specified destination MAC address.
dscp *dscp-list*	Specifies to match packets by DSCP precedence. The *dscp-list* argument is a list of DSCP values in the range of 0 to 63.
ip-precedence *ip-precedence-list*	Specifies to match packets by IP precedence. The *ip-precedence-list* argument is a list of IP precedence values in the range of 0 to 7.
protocol *protocol-name*	Specifies to match the packets of a specified protocol. The *protocol-name*

Form	Description
	argument can be IP.
service-vlan-id *vlan-id-list*	Specifies to match the packets of the VLANs of the operator's network. The *vlan-id-list* argument is a list of VLAN IDs, in the form of *vlan-id* **to** *vlan-id* or multiple discontinuous VLAN IDs (separated by space). You can specify up to eight VLAN IDs for this argument at a time. VLAN ID is in the range of 1 to 4094.
source-mac *mac-address*	Specifies to match the packets with a specified source MAC address.

Note

The matching criteria listed below must be unique in a traffic class with the operator being **AND**. Even though you can define multiple **if-match** clauses for these matching criteria or input multiple values for a *list* argument (such as the *8021p-list* argument) listed below in a traffic class, avoid doing so. Otherwise, the QoS policy referencing the class cannot be successfully applied to interfaces.

- **customer-dot1p** *8021p-list*
- **customer-vlan-id** *vlan-id-list*
- **destination-mac** *mac-address*
- **dscp** *dscp-list*
- **ip-precedence** *ip-precedence-list*
- **service-vlan-id** *vlan-id-list*
- **source-mac** *mac-address*

To create multiple if-match clauses or specify multiple values for a list argument for any of the matching criteria listed above, ensure that the operator of the class is **OR**.

Description

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

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

When defining match criteria, note the following:

1. Define an ACL-based match criterion

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

2. Define a criterion to match a destination MAC address or a source MAC address.

- You can configure multiple destination MAC address or source MAC address match criteria in a class.

3. Define a criterion to match DSCP values

- You can configure multiple DSCP match criteria in a class. All the defined DSCP values are arranged in ascending order automatically.
- 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 is considered matching in the if-match clause.
- To delete a criterion matching DSCP values, the specified DSCP values must be identical with those defined in the rule (sequence may be different).

4. Define a criterion to match the 802.1p precedence values of the customer network

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

5. Define a criterion to match IP precedence values

- You can configure multiple IP precedence match criteria in a class. The defined IP precedence values are arranged automatically 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 is considered matching the if-match clause.
- To delete a criterion matching IP precedence values, the specified IP precedence values in the command must be identical with those defined in the criterion (sequence may be different).

6. Define a criterion to match customer network VLAN IDs or service provider network VLAN IDs

- You can configure multiple VLAN ID match criteria in 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 is considered to be matching the if-match clause.
- To delete a criterion matching VLAN IDs, the specified VLAN IDs in the command must be identical with those defined in the criterion (sequence may be different).

Related commands: **traffic classifier**.

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 the ACL named **flow**.

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

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 DSCP values 1, 6 or 9.

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

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

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

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

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

Change the match criterion of class **class1** from ACL 2008 to ACL 2009.

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

```
[Sysname-classifier-class1] undo if-match acl 2008 update acl 2009
```

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: Class name, a string of 1 to 31 characters.

and: Specifies the relationship between the match criteria in the class as a logical AND. That is, the packets that match all the criteria belong to this class.

or: Specifies the relationship between the criteria in the class as a logical OR. That is, the packets that match any of the criteria belong to this class.

Description

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

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

By default, the relationship between match criteria is **and**.

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

Examples

Define a class named **class1**.

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

Traffic behavior configuration commands

display traffic behavior

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, a string of 1 to 31 characters. If no traffic behavior is specified, the information of all the user-defined behaviors is displayed.

Description

Use the **display traffic behavior** command to display traffic behavior information.

Examples

Display user-defined traffic behaviors.

```
User Defined Behavior Information:
  Behavior: 2
    Redirect enable:
      Redirect type: interface
      Redirect destination: GigabitEthernet1/0/4
  Behavior: 1
    Filter enable: deny
```

Table 10 display traffic behavior user-defined command output description

Field	Description
User Defined Behavior Information	User-defined behavior information.
Behavior	Name of a behavior.
Redirect enable	Traffic redirecting configuration information.
Redirect type	Traffic redirecting type, which can be redirecting to an interface.
Redirect destination	Traffic redirecting destination port .
Filter enable	Traffic filtering option: permit or deny.

filter

Syntax

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

undo filter

View

Traffic behavior view

Default Level

2: System level

Parameters

deny: Drops the packets.

permit: Permits the packet to pass through.

Description

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

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

Note

filter deny is mutually exclusive with **redirect.**

Examples

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

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

redirect

Syntax

redirect interface *interface-type interface-number*

undo redirect interface *interface-type interface-number*

View

Traffic behavior view

Default Level

2: System level

Parameters

interface: Redirects traffic to the specified interface.

interface-type interface-number: Interface identified by an interface number and interface type.

Description

Use the **redirect** command to configure a traffic redirect action for the traffic behavior.

Use the **undo redirect** command to remove the traffic redirect action.

Note

filter deny is mutually exclusive with **redirect.**

Examples

Configure the action of redirecting traffic to GigabitEthernet 1/0/1 for traffic behavior **database**.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] redirect interface gigabitethernet1/0/1
```

traffic behavior

Syntax

traffic behavior *behavior-name*

undo traffic behavior *behavior-name*

View

System view

Default Level

2: System level

Parameters

behavior-name: Behavior name, a string of 1 to 31 characters.

Description

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

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

Related commands: **qos policy**, **qos apply policy**, **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, a string of 1 to 31 characters.

behavior-name: Behavior name, a string of 1 to 31 characters.

Description

Use the **classifier behavior** command to specify a behavior for a class in the policy.

Use the **undo classifier** command to remove a class from the policy.

Note that:

- Each class in the policy can be associated with only one behavior.
- If the class and traffic behavior specified for the command do not exist, the system creates a null class and a null 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

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, configuration information of all the policies is displayed.

tcl-name: Class name, a string of 1 to 31 characters.

Description

Use the **display qos policy** 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: 1
   Classifier: 1
     Behavior: 1
      Redirect enable:
        Redirect type: interface
        Redirect destination: GigabitEthernet1/0/7
```

Table 11 display qos policy command output description

Field	Description
Policy	Policy name
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. Refer to the **traffic classifier** command for related information.
Behavior	Behavior associated with the class. A behavior is associated with a class. It can be configured with multiple actions. Refer to the **traffic behavior** command for related information.

display qos policy interface

Syntax

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

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 QoS policy configuration and operational information on an interface or on all interfaces.

Examples

Display the QoS configuration and operational information on GigabitEthernet1/0/1.

```
<Sysname> display qos policy interface gigabitethernet 1/0/1
  Interface: GigabitEthernet1/0/1
  Direction: Inbound
  Policy: 1
   Classifier: 1
     Operator: AND
     Rule(s) : If-match customer-dot1p 1
     Behavior: 1
       Redirect enable:
        Redirect type: interface
        Redirect destination: GigabitEthernet1/0/7
```

Table 12 display qos policy interface command output description

Field	Description
Interface	Interface type and interface number
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
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**

undo qos apply policy inbound

View

Interface view, port group view

Default Level

2: System level

Parameters

inbound: Inbound direction.

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

Description

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

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

Examples

Apply policy **USER1** in the inbound direction of GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] 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-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 remove a policy.

A policy applied to an interface cannot be deleted directly. You need to cancel application of the policy on the interface before deleting the policy with the **undo qos policy** command.

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

Examples

Define a policy named **user1**.

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

Priority mapping configuration commands

Priority mapping table configuration commands

display qos map-table

Syntax

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

View

Any view

Default Level

1: Monitor level

Parameters

dot1p-dot1p: 802.1p-precedence-to-802.1p-precedence mapping table.

dot1p-dscp: 802.1p-precedence-to-DSCP mapping table.

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

dscp-dot1p: DSCP-to-802.1p-precedence mapping table.

dscp-dscp: DSCP-to-DSCP mapping table.

dscp-lp: DSCP-to-local-precedence 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, the configuration information of all priority mapping tables is displayed.

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

Examples

Display the configuration information of the 802.1p-precedence-to-local-precedence 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 13 display qos map-table command output description

Field	Description
MAP-TABLE NAME	Name of the mapping table
TYPE	Type of the mapping table
IMPORT	Input values of the mapping table
EXPORT	Output values of the 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-precedence-to-local-precedence mapping table to map 802.1p precedence values 4 and 5 to local precedence 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 { **dot1p-dot1p** | **dot1p-dscp** | **dot1p-lp** | **dscp-dot1p** | **dscp-dscp** | **dscp-lp** }

View

System view

Default Level

2: System level

Parameters

dot1p-dot1p: 802.1p-precedence-to-802.1p-precedence mapping table.

dot1p-dscp: 802.1p-precedence-to-DSCP mapping table.

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

dscp-dot1p: DSCP-to-802.1p-precedence mapping table.

dscp-dscp: DSCP-to-DSCP mapping table.

dscp-lp: DSCP-to-local-precedence 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 the inbound 802.1p-precedence-to-local-precedence 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, port group view

Default Level

2: System level

Parameters

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

Description

Use the **qos priority** command to configure a priority for the current port.

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

The default port priority is 0.

Examples

Set the priority of GigabitEthernet 1/0/1 to 2

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

Trusted precedence type 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 trusted precedence type and priority of an interface.

If no interface is specified, the trusted precedence types on all interfaces are displayed.

Examples

Display the trusted precedence type and priority of GigabitEthernet 1/0/1.

```
<Sysname> display qos trust interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1
 Port priority information
  Port priority: 0
  Port priority trust type: untrust
```

Table 14 display qos trust interface command output description

Field	Description
Interface	Interface type and interface number
Port priority	Port priority
Port priority trust type	Trusted precedence type, which can be **dot1p**, **dscp**, or **untrust**

qos trust

Syntax

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

undo qos trust

View

Interface view, port group view

Default Level

2: System level

Parameters

dot1p: Trusts the 802.1p precedence and uses this priority for priority mapping.

dscp: Trusts the DSCP values and uses DSCP values for priority mapping.

Description

Use the **qos trust** command to configure the trusted precedence type on an interface.

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

By default, the port priority is trusted.

Examples

Configure GigabitEthernet 1/0/1 to trust the 802.1p precedence.

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

Line rate configuration commands

Line rate configuration commands

display qos lr interface

Syntax

display qos lr 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 lr interface** command to view the line rate configuration information and operational statistics on a specified interface or all the interfaces.

If no interface is specified, the line rate configuration information and operational statistics on all the interfaces are displayed.

Examples

Display the line rate configuration information and operational statistics on all the interfaces.

```
<Sysname> display qos lr interface
Interface: GigabitEthernet1/0/2
Direction: Inbound
 CIR 1280 (kbps)
Direction: Outbound
 CIR 2560 (kbps)
Interface: GigabitEthernet1/0/4
Direction: Inbound
 CIR 1280 (kbps)
Direction: Outbound
 CIR 2560 (kbps)
```

Table 15 display qos lr command output description

Field	Description
Interface	Interface type and interface number
Direction	The direction in which the line rate configuration is applied: inbound or outbound
CIR	Committed information rate (CIR) in kbps

qos lr

Syntax

qos lr { **inbound** | **outbound** } **cir** *committed-information-rate*

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

View

Interface view, port group view

Default Level

2: System level

Parameters

inbound: Limits the rate of incoming packets on the interface.

outbound: Limits the rate of outgoing packets on the interface.

cir *committed-information-rate*: Specifies the committed information rate (CIR) in kbps, which must be a multiple of 64. CIR ranges from 64 to 1000000.

Description

Use the **qos lr** command to limit the rate of incoming packets or outgoing packets on the interface.

Use the **undo qos lr** command to remove the rate limit.

Settings in interface view are effective on the current interface; settings in port group view are effective on all ports in the port group.

Examples

Limit the rate of outgoing packets on GigabitEthernet 1/0/1, with CIR 1280 kbps.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos lr outbound cir 1280
```

Congestion management configuration commands

Congestion management configuration commands

display qos wrr interface

Syntax

display qos wrr 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 wrr interface** command to display the queuing configuration on an interface.

If no interface is specified, the queuing configuration of all the interfaces is displayed.

Related commands: **qos wrr**.

Examples

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

```
<Sysname> display qos wrr interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1
 Output queue: Weighted round robin queue
Queue ID    Group    Weight
-------------------------------------
   0         1        10
   1         sp       N/A
   2         sp       N/A
   3         2        30
```

Table 16 display qos wrr interface command output description

Field	Description
Interface	Interface type and interface number
Output queue	Pattern of the current output queue
Queue ID	ID of a queue
Group	Number of the group a queue is assigned to. By default, all queues belong to group SP.
Weight	Queue weight based on which queues are scheduled. N/A indicates that the queue adopts the SP queue scheduling algorithm.

qos wrr

Syntax

qos wrr *queue-id* **group** { *group-id* **weight** *queue-weight* | **sp** }

undo qos wrr [*queue-id* **group** { *group-id* **weight** | **sp** }]

View

Interface view, port group view

Default Level

2: System level

Parameters

wrr *queue-id*: Queue ID, in the range of 0 to n-3.

group *group-id*: Specifies a group the queue belongs to, group 1 or group 2. An SP queue scheduling algorithm is adopted between each group.

weight *schedule-value*: Configures the scheduling weight for the queue. The *schedule-value* ranges from 8 to 100.

Description

Use the **qos wrr** command to configure WRR or SP+WRR queuing.

Use the **undo qos wrr** command to disable WRR queuing.

The default queuing algorithm on an interface is SP queuing.

A port on an S5120-SI switch supports four output queues. As required, you can configure part of the queues on a port to adopt the SP queue scheduling algorithm and part of the queues to adopt the WRR queue scheduling algorithm. The SP+WRR queue scheduling algorithm is implemented by adding queues on a port to SP scheduling queues and WRR queue scheduling queues respectively. For example, queue 0 and queue 1 are in the SP queue scheduling group, and queue 2 is in the WRR queue scheduling group 1, queue 3 is in WRR queue scheduling group 2. Round robin is first performed in WRR group 1. If no packet is to be sent in WRR group 1, round robin is performed in the WRR group 2. Lastly, packets in the SP queue scheduling group are processed.

Examples

Enable the SP+WRR queue scheduling algorithm on GigabitEthernet1/0/1. Add queue 0 to the SP queue scheduling group; add queue 1 to WRR queue scheduling group 1, with the weight being 20; add queue 2 and queue 3 to WRR queue scheduling group 2, with the weight being 10 and 50 respectively.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wrr 0 group sp
[Sysname-GigabitEthernet1/0/1] qos wrr 1 group 1 weight 20
[Sysname-GigabitEthernet1/0/1] qos wrr 2 group 2 weight 10
[Sysname-GigabitEthernet1/0/1] qos wrr 3 group 2 weight 50
```

Obtaining support for your product

Register your product

Warranty and other service benefits start from the date of purchase, so it is important to register your product quickly to ensure you get full use of the warranty and other service benefits available to you.

Warranty and other service benefits are enabled through product registration. Register your product at **http://www.h3cnetworks.com**, go to **Support**, **Product Registration**. Support services are based on accounts that you create or have authorization to access. First time users must apply for a user name and password that provides access to a number of eSupport features including Product Registration, Repair Services, and Service Request. If you have trouble registering your product, please contact 3Com Global Services for assistance.

Purchase value-added services

To enhance response times or extend warranty benefits, contact 3Com or your authorized reseller. Value-added services like Express[SM] and Guardian[SM] can include 24x7 telephone technical support, software upgrades, onsite assistance or advance hardware replacement. Experienced engineers are available to manage your installation with minimal disruption to your network. Expert assessment and implementation services are offered to fill resource gaps and ensure the success of your networking projects. More information on 3Com maintenance and Professional Services is available at **http://www.h3cnetworks.com**.

Contact your authorized reseller or 3Com for a complete list of the value-added services available in your area.

Troubleshoot online

You will find support tools posted on the web site at **http://www.h3cnetworks.com/** under **Support**, **Knowledgebase**. **The Knowledgebase** helps you troubleshoot H3C products. This query-based interactive tool contains thousands of technical solutions.

Access software downloads

Software Updates are the bug fix / maintenance releases for the version of software initially purchased with the product. In order to access these Software Updates you must first register your product on the web site at **http://www.h3cnetworks.com,** go to **Support**, **Product Registration.**

First time users will need to apply for a user name and password. A link to software downloads can be found at **http://www.h3cnetworks.com**, under **Support, Drivers and downloads**.

Software Upgrades are the software releases that follow the software version included with your original product. In order to access upgrades and related documentation you must first purchase a service contract from 3Com or your reseller.

Telephone technical support and repair

To enable telephone support and other service benefits, you must first register your product at **http://www.h3cnetworks.com/**

Warranty and other service benefits start from the date of purchase, so it is important to register your product quickly to ensure you get full use of the warranty and other service benefits available to you.

When you contact 3Com for assistance, please have the following information ready:

- Product model name, part number, and serial number
- Proof of purchase, if you have not pre-registered your product
- A list of system hardware and software, including revision level
- Diagnostic error messages
- Details about recent configuration changes, if applicable

To send a product directly to 3Com for repair, you must first obtain a return authorization number (RMA). Products sent to 3Com, without authorization numbers clearly marked on the outside of the package, will be returned to the sender unopened, at the sender's expense. If your product is registered and under warranty, you can obtain an RMA number online at **http://www.h3cnetworks.com** under **support, Repair & Replacement Request**. First time users will need to apply for a user name and password.

Contact us

3Com offers telephone, e-mail and internet access to technical support and repair services. To access these services for your region, use the appropriate telephone number, URL or e-mail address.

Find a current directory of contact information posted on the web site at **http://www.h3cnetworks.com** under **Support**, **Technical Support Contact**.

Acronyms

#ABCDEFGHIKLMNOPQRSTUVWXZ

Acronym	Full spelling
#	Return
10GE	Ten-GigabitEthernet
3DES	Triple Data Encryption Standard
A	Return
AAA	Authentication, Authorization and Accounting
ABC	Activity Based Costing
ABR	Area Border Router
AC	Alternating Current
ACK	Acknowledgement
ACL	Access Control List
ACS	Auto-Configuration Server
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
AF	Assured Forwarding
AFI	Address Family Identifier; Authority and Format Identifier
ALG	Application Layer Gateway
AM	Accounting Management
AMB	Active Main Board
ANSI	American National Standard Institute
AP	Access Point
ARP	Address Resolution Protocol
AS	Autonomous System
ASBR	Autonomous System Boundary Router
ASCII	American Standard Code for Information Interchange
ASE	Application Service Element; Autonomous System External
ASIC	Application Specific Integrated Circuit
ASM	Any-Source Multicast
ASN	Auxiliary Signal Network
AT	Advanced Technology
AT	Adjacency Table

Acronym	Full spelling
AT	Apple Talk
ATM	Asynchronous Transfer Mode
AUX	Auxiliary (port)
AVF	Active Virtual Forwarder
B	Return
BAGG	Bridge Aggregation
BAS	Broadband access server
BC	Bearer Control
BDR	Backup Designated Router
BE	Best Effort
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BIMS	Branch Intelligent Management System
BOOTP	Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface
BSMF	Bootstrap Message Fragment
BSR	Bootstrap Router
BT	BitTorrent
BS	BSR State
BT	Burst Tolerance
C	Return
C-BSR	Candidate Bootstrap Router
C-RP	Candidate Rendezvous Point
C-RP-Adv	Candidate Rendezvous Point Advertisement
CA	Call Appearance
CA	Certificate Authority
CAR	Committed Access Rate
CBS	Committed Burst Size
CBT	Core-Based Tree
CBQ	Class Based Queuing
CBR	Constant Bit Rate
CBT	Core-Based Tree
CC	Continuity Check
CCITT	International Telephone and Telegraph Consultative Committee

Acronym	Full spelling
CCM	Continuity Check Message
CDP	Cisco Discovery Protocol
CE	Customer Edge; Customer Edge Device
CF-Card	Compact Flash Card
CFD	Connectivity Fault Detection
CFI	Canonical Format Indicator
CFM	Configuration File Management; Connectivity Fault Management
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common and Internal Spanning Tree
CLI	Command Line Interface
CLV	Code/Length/Value
CLNP	Connectionless Network Protocol
CoS	Class of Service
CPE	Customer Premise Equipment
CPOS	Channelized POS
CPS	Certification Practice Statement
CPU	Central Processing Unit
CQ	Custom Queuing
CR	Carriage Return
CRC	Cyclic Redundancy Check
CRL	Certificate revocation list
CR-LSP	Constraint-based Routing LSP
CR-LDP	Constraint-based Routing LDP
CSMA/CD	Carrier Sense Multiple Access/Collision Detect
CSNP	Complete Sequence Number Packet
CSPF	Constraint Shortest Path First
CST	Common Spanning Tree
CT	Call Transfer
CV	Connectivity Verification
CVLAN	Customer Virtual Local Area Network
D	Return
DAD	Duplicate Address Detection
DAR	Deeper Application Recognition

Acronym	Full spelling
DBA	Dynamic Bandwidth Allocation
DCE	Data Circuit-terminal Equipment
DD	Database Description
DDN	Digital Data Network
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Service
DIS	Designated Intermediate System
DLCI	Data Link Connection Identifier
DLDP	Device Link Detection Protocol
DN	Distinguished name
DNS	Domain Name System
DoD	Downstream on Demand
DoS	Denial of Service
DR	Designated Router
DSA	Digital Signature Algorithm
DSCP	Differentiated Services Code point Priority
DSP	Digital Signal Processor; Domain Specific Part
DSTE	DiffServ Aware TE
DTE	Data Terminal Equipment
DU	Downstream Unsolicited
DUID	DHCP Unique Identifier
DUID-LL	DUID Based Link Layer Address
D-V	Distance Vector Routing Algorithm
DVMRP	Distance Vector Multicast Routing Protocol
DVPN	Dynamic Virtual Private Network
DWDM	Dense Wavelength Division Multiplexing
E	Return
EACL	Enhanced ACL
EAD	Endpoint Admission Defense
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol over LAN
EAPOR	EAP over RADIUS
EBGP	External Border Gateway Protocol
EBS	Excess Burst Size

Acronym	Full spelling
EF	Expedited Forwarding
EGP	Exterior Gateway Protocol
EOAM	Ethernet Operation, Administration, and Maintenance
EPON	Ethernet Passive Optical Network
ES	End System
ES-IS	End System-Intermediate System
F	Return
FCoE	Fabric Channel over Ethernet
FC	Forwarding Class
FCS	Frame Check Sequence
FDB	Forwarding Database
FDDI	Fiber Distributed Data Interface
FDI	Forward Defect Indication
FEC	Forwarding Equivalence Class; Forward Error Correction
FFD	Fast Failure Detection
FF	Fixed filter
FG	Forwarding Group
FIB	Forwarding information base
FIFO	First In First Out
FQDN	Full Qualified Domain Name
FR	Frame Relay
FRR	Fast Reroute
FRTT	Fairness Round Trip Time
FSM	Finite State Machine
FT	Functional Test
FTP	File Transfer Protocol
FTTB	Fiber to the Building
FTTC	Fiber to the Curb
FTTH	Fiber to the Home
G	Return
GARP	Generic Attribute Registration Protocol
GE	Gigabit Ethernet
GR	Graceful Restart
GRE	Generic Routing Encapsulation
GTS	Generic Traffic Shaping

Acronym	Full spelling
GVRP	GARP VLAN Registration Protocol
H	Return
HA	High Availability
HABP	HW Authentication Bypass Protocol
HDLC	High-level Data Link Control
HEC	Header Error Control
HGMP	HW Group Management Protocol
HGMPv2	HW Group Management Protocol version 2
HMAC	Hash-based Message Authentication Code
HO-DSP	High Order Part of Domain Specific Part
HoPE	Hierarchy of PE
HoVPN	Hierarchy of VPN
HQoS	Hierarchical Quality of Service
HSB	Hot Standby
HTTP	Hyper Text Transport Protocol
HTTPS	HTTP Security
H-VPLS	Hierarchy of VPLS
HVRP	Hierarchy VLAN Register Protocol
HWTACACS	HUAWEI Terminal Access Controller Access Control System
I	Return
IA	Incoming Access; Identity Association
IAD	Integrated Access Device
IANA	Internet Assigned Number Authority
IBGP	Internal Border Gateway Protocol
IBM	International Business Machines
ICMP	Internet Control Message Protocol
ICPIF	Calculated Planning Impairment Factor
ICMPv6	Internet Control Message Protocol for IPv6
ID	Identification; Identity
IDI	Initial Domain Identifier
IDP	Initial Domain Part
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGMP-Snooping	Internet Group Management Protocol Snooping

Acronym	Full spelling
IGP	Interior Gateway Protocol
IIH	IS-to-IS Hello Protocol Data Unit
ILM	Incoming Label Map
ILS	Internet Locator Service
iMC	Intelligent Management Center
IN	Intelligent Network
IntServ	Integrated Service
IP	Internet Protocol
IPC	Inter-Process Communication
IPng	IP Next Generation
IPSec	IP Security
IPTN	IP Phone Telephony Network
IPTV	Internet Protocol Television
IPv6	Internet Protocol Version 6
IPX	Internet Packet Exchange
IRDP	ICMP Router Discovery Protocol
IRF	Intelligent Resilient Framework; Intermediate Routing Function
IS	Intermediate System
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
ISDN	Integrated Services Digital Network
IS-IS	Intermediate System-to-Intermediate System intra-domain routing information exchange protocol
ISO	International Organization for Standardization
ISP	Internet Service Provider
ISSU	In Service Software Upgrade
IST	Internal Spanning Tree
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
K	Return
KB	Kilobyte
KEK	Key-encrypting key
L	Return
L2TP	Layer 2 Tunneling Protocol
L2VPN	Layer 2 Virtual Private Network
L3VPN	Layer 3 Virtual Private Network
LACP	Link Aggregation Control Protocol

Acronym	Full spelling
LACPDU	Link Aggregation Control Protocol Data Unit
LAN	Local Area Network
LAPB	Link Access Procedure, Balanced
LB	Loopback
LBM	Loopback Message
LBR	Loopback Reply
LCP	Link Control Protocol
LDAP	Lightweight Directory Access Protocol
LDP	Label Distribution Protocol
LER	Label Edge Router
LFIB	Label Forwarding Information Base
LIB	Label Information Base
LLC	Link Layer Control; Logical Link Control
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Units
LLID	Logical Link Identifier
LLS	Link-Local Signaling
LLSP-CDP	Link Layer Discovery Protocol-Cisco Discovery Protocol
LOC	Loss of Continuity
LOG	Call Logging
LR	Line Rate
LRTT	Loop Round Trip Time
LS	Link State
LSA	Link State Advertisement
LSAck	Link State Acknowledgment
LSDB	Link State Database
LSP	Label Switch Path; Link State Packet
LSPAGENT	Label Switched Path AGENT
LSPDU	Link State Protocol Data Unit
LSPM	Label Switch Path Management
LSR	Link State Request; Label Switching Route
LSR	Label Switch Router
LSR-ID	Label Switch Router Identity
LSU	Link State Update
LT	Linktrace

Acronym	Full spelling
LTM	Lintrace Message
LTR	Linktrace Reply Message
LVF	Listening Virtual Forwarder
M	Return
MA	Maintenance Association
MAC	Media Access Control
MAD	Multi-Active Detection
MAFV	MAC-based Auth-Fail VLAN
MAN	Metropolitan Area Network
MaxBC	Max Bandwidth Constraints
MBGP	Multicast Border Gateway Protocol
MCE	Multi-VPN instance Customer Edge
MD	Multicast Domain; Maintenance Domain
MD5	Message-Digest 5
MDI	Medium Dependent Interface
MDS	Message-Digest Algorithm 5
MDT	Multicast Distribution Tree
MD5	Message-Digest Algorithm 5
MED	Multi-Exit Discriminator; Media Endpoint Discovery
MEP	Maintenance Association End Point
MFF	MAC Forced Forwarding
MGV	Mac-based guest VLAN
MIB	Management Information Base
MIP	Maintenance Association Intermediate Point
MLD	Multicast Listener Discovery Protocol
MLD-Snooping	Multicast Listener Discovery Snooping
MMC	Meet-Me Conference
MODEM	Modulator/Demodulator
MOS	Mean Opinion Scores
MP	Multilink PPP; Maintenance Point
MP-BGP	Multiprotocol extensions for BGP-4
MPE	Middle-level PE
MP-group	Multilink Point to Point Protocol group
MPLS	Multiprotocol Label Switching
MPLSFW	Multi-protocol Label Switch Forward

Acronym	Full spelling
MPM	Multicast Port Management
MSC	Mobile Switching Center
MSDP	Multicast Source Discovery Protocol
MSOH	Multiplex Section Overhead
MST	Multiple Spanning Tree
MSTI	Multi-Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MT	Multicast Tunnel
MTBF	Mean Time Between Failure
MTI	Multicast Tunnel Interface
MTTR	Mean Time To Repair
MTU	Maximum Transmission Unit
MVRF	Multicast VPN Routing and Forwarding
N	Return
NA	Neighbor Advertisement
NAPT	Network Address Port Translation
NAPT-PT	Network Address Port Translation – Protocol Translation
NAS	Network Access Server
NAT	Net Address Translation
NBMA	Non Broadcast Multi-Access
NBT	NetBIOS over TCP/IP
NCP	Network Control Protocol
ND	Neighborhood discovery
NDA	NetStream Data Analyzer
NDC	Network Data Collector
NDP	Neighbor Discovery Protocol
NET	Network Entity Title
NetBIOS	Network Basic Input/Output System
NHLFE	Next Hop Label Forwarding Entry
NLB	Network Load Balancing
NLPID	Network Layer Protocol Identifier
NLRI	Network Layer Reachability Information
NMS	Network Management Station
NPDU	Network Protocol Data Unit
NPE	Network Provider Edge

Acronym	Full spelling
NQA	Network Quality Analyzer
NS	Neighbor Solicitation
NSAP	Network Service Access Point
NSC	NetStream Collector
N-SEL	NSAP Selector
NSR	Non-Stop Routing
NSSA	Not-So-Stubby Area
NTDP	Neighbor Topology Discovery Protocol
NTK	Need to Know
NTP	Network Time Protocol
O	Return
OAA	Open Application Architecture
OAM	Operation Administration and Maintenance
OAMPDU	OAM Protocol Data Units
OAN	Optical Access Network
OAP	Open Application Platform
OC-3	OC-3
ODN	Optical Distribution Network
OID	Object Identifier
OL	Optical Line
OLT	Optical Line Terminal
ONU	Optical Network Unit
OOB	Out of Band
OS	Operating system
OSI	Open Systems Interconnection
ORF	Outbound Route Filter
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
P	Return
P	Provider
P2MP	Point to MultiPoint
P2P	Point To Point
PAP	Password Authentication Protocol
PAFV	Port-based Auth-Fail VLAN
PAGP	Port Aggregation Protocol

Acronym	Full spelling
PBR	Policy-Based Route
PCB	Printed Circuit Board
PCM	Pulse Code Modulation
PD	Powered Device, Prefix Delegation or Pure Data
PDU	Protocol Data Unit
PE	Provider Edge, Provider Edge Device
PGV	Port-based Guest VLAN
PHP	Penultimate Hop Popping
PHY	Physical Layer
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
PIR	Peak Information Rate
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PLR	Point of Local Repair
PMTU	Path MTU
PoE	Power over Ethernet
PON	Passive Optical Network
POP	Point Of Presence
POS	Packet Over SDH; Passive Optical Splitter
PPPoE	Point-to-Point Protocol over Ethernet
PPP	Point-to-Point Protocol
PPTP	Point to Point Tunneling Protocol
PPVPN	Provider-provisioned Virtual Private Network
PQ	Priority Queuing
PRC	Primary Reference Clock
PRI	Primary Rate Interface
PS	Protection Switching
PSE	Power Sourcing Equipment
PSNP	Partial Sequence Number Packet
PTMP or P2MP	Point-to-Multipoint
PTP or P2P	Point-to-Point
PUP	PARC Universal Packet
PVC	Permanent Virtual Channel

Acronym	Full spelling
PVID	Permitted VLAN ID
PVST	Per-VLAN Spanning Tree
PW	Pseudo wires
PXE	Pre-boot Execution Environment
Q	Return
QACL	QoS/ACL
QinQ	802.1Q in 802.1Q
QoS	Quality of Service
QQIC	Querier's Query Interval Code
QRV	Querier's Robustness Variable
R	Return
RA	Registration Authority; Router Advertisement
RADIUS	Remote Authentication Dial in User Service
RAGG	Route Aggregation
RALM	RADIUS Authenticated Login using MAC-address
RAM	Random-Access Memory
RARP	Reverse Address Resolution Protocol
RD	Routing Domain
RD	Router Distinguisher
RED	Random Early Detection
RFC	Request For comments
RIB	Routing Information Base
RID	Router ID
RIP	Routing Information Protocol
RIPng	RIP next generation
RM	Route Management
RMON	Remote Monitoring
ROM	Read Only Memory
RP	Rendezvous Point
RPC	Remote Procedure Call
RPF	Reverse Path Forwarding
RPR	Resilient Packet Ring
RPT	Rendezvous Point Tree
RR	Route Reflector
RRPP	Rapid Ring Protection Protocol

Acronym	Full spelling
RRPPD	Rapid Ring Protection Protocol Data Unit
RS	Router Solicitation
RSA	Revest-Shamir-Adleman Algorithm
RSB	Reservation State Block
RSOH	Regenerator Section Overhead
RSTP	Rapid Spanning Tree Protocol
RSVP	Resource Reservation Protocol
RSVP-TE	Resource Reservation Protocol – Traffic Engineering
RT	Route Target
RTCP	Real-time Transport Control Protocol
RTE	Route Table Entry
RTP	Real-time Transport Protocol
RTP	Real-time Transport Protocol
S	Return
SA	Source Active; Suppress Advertisement
SAFI	Subsequent Address Family Identifier
SAP	Service Access Point
SBM	Sub-network Bandwidth Management
SC	Secure Digital
SCEP	Simple Certificate Enrollment Protocol
SCFF	Single Choke Fairness Frame
SD	Signal Degrade
SDH	Synchronous Digital Hierarchy
SE	Shared explicit
SEL	Selector
SETS	Synchronous Equipment Timing Source
SF	Sampling Frequency
SFM	Source-Filtered Multicast
sFlow	Sampled Flow
SFTP	Secure FTP
SHA1	Secure Hash Algorithm 1
Share-MDT	Share-Multicast Distribution Tree
SIP	Session Initiation Protocol
Site-of-Origin	Site-of-Origin
SLA	Service Level Agreement

Acronym	Full spelling
SMB	Standby Main Board
SMTP	Simple Mail Transfer Protocol
SNAP	Sub Network Access Point
SNMP	Simple Network Management Protocol
SNP	Sequence Number Packet
SNPA	Sub-network Points of Attachment
SOH	Section Overhead
SONET	Synchronous Optical Network
SOO	Site-of-Origin
SP	Strict Priority Queuing
SPE	Superstratum PE; Sevice Provider-end PE
SPF	Shortest Path First
SPT	Shortest Path Tree
SPX	Sequenced Packet Exchange
SRPT	Sub-ring Packet Tunnel
SRPU	Switching and Routing Processing Unit
SSH	Secure Shell
SSM	Synchronization Status Marker
SSM	Source-Specific Multicast
ST	Shared Tree
STelnet	Secure Telnet
STM-1	SDH Transport Module -1
STM-16	SDH Transport Module -16
STM-16c	SDH Transport Module -16c
STM-4c	SDH Transport Module -4c
STP	Spanning Tree Protocol
SVC	Signaling Virtual Connection
SVLAN	Service Provider Virtual Local Area Network
Switch-MDT	Switch-Multicast Distribution Tree
SYN	Synchronize
T	Return
TA	Terminal Adapter
TACACS	Terminal Access Controller Access Control System
TDM	Time Division Multiplexing
TC	Topology Change

Acronym	Full spelling
TCP	Transmission Control Protocol
TCN	Topology Change Notification
TDMA	Time Division Multiple Access
TE	Traffic Engineering
TEDB	Traffic Engineering Database
TFTP	Trivial File Transfer Protocol
TLS	Transparent LAN Service
TLV	Type-Length-Value
ToS	Type of Service
TP	Traffic Policing
TPID	Tag Protocol Identifier
TQ	Time Quantum
TRIP	Trigger RIP
TS	Traffic Shaping
TTL	Time to Live
TTY	True Type Terminal
U	Return
U/L	Universal/Local
UDLD	Unidirectional Link Detection
UDP	User Datagram Protocol
UNI	User Network Interface
UPE	Under-layer PE or User-end PE
URL	Uniform Resource Locators
URPF	Unicast Reverse Path Forwarding
USM	User-Based Security Model
V	Return
VBR	Variable Bit Rate
VCI	Virtual Channel Identifier
VE	Virtual Ethernet
VF	Virtual Forwarder
VFS	Virtual File System
VLAN	Virtual Local Area Network
VLL	Virtual Leased Lines
VOD	Video On Demand
VoIP	Voice over IP

Acronym	Full spelling
VOS	Virtual Operate System
VPDN	Virtual Private Dial-up Network
VPDN	Virtual Private Data Network
VPI	Virtual Path Identifier
VPLS	Virtual Private Local Switch
VPN	Virtual Private Network
VRID	Virtual Router ID
VRRP	Virtual Router Redundancy Protocol
VSI	Virtual Switch Interface
VT	Virtual Tributary
VTP	VLAN Trunking Protocol
VTY	Virtual Type Terminal
W	Return
WAN	Wide Area Network
WDM	Wavelength-Division Multiplexing
WFQ	Weighted Fair Queuing
WINS	Windows Internet Naming Service
WLAN	Wireless Local Area Network
WRED	Weighted Random Early Detection
WRR	Weighted Round Robin
WTR	Wait-to-Restore
WWW	World Wide Web
X	Return
XGE	Ten-GigabitEthernet
Z	Return
ZBR	Zone Border Router