1 ACL Commands

Command	Function
access-list	Create an access control list (ACL) and add a rule.
access-list list-remark	Add a remark to an ACL.
access-list remark	Add a remark to an ACL rule.
clear access-list counters	Clear statistics on matched packets denied by an ACL.
clear counters access-list	Clear statistics on the packets matching an ACL.
deny	Add a rule of deny type to an ACL.
expert access-group	Apply an expert ACL.
expert access-list advanced	Create an expert advanced ACL.
expert access-list counter	Enable the packet matching counting function of a specified expert extended ACL.
expert access-list extended	Create an expert extended ACL.
expert access-list new-fragment-mode	Switch the fragmented packet matching mode of an expert extended ACL from the default matching mode to the new matching mode.
expert access-list resequence	Configure the start value and step of rule sequence numbers in an expert extended ACL.
global access-group	Make a global security ACL take effect on a port.
global access-group disable	Disable the global security ACL function.
global ip access-group	Make a global security ACL of IP type take effect on a port.
ip access-group	Apply an IP standard ACL or IP extended ACL.
ip access-list	Create an IP standard ACL or IP extended ACL.
ip access-list counter	Enable the packet matching counting function of an IP standard ACL or IP extended ACL.
ip access-list log-update interval	Configure the update interval of IPv4 ACL packet matching logs.
ip access-list new-fragment-mode	Configure the fragmented packet matching mode of

	an IP standard ACL or IP extended ACL.
ip access-list resequence	Configure the start value and step of rule sequence numbers in an IP ACL.
ipv6 access-list	Create an IPv6 ACL.
ipv6 access-list counter	Enable the packet matching counting function of an IPv6 ACL.
ipv6 access-list log-update interval	Configure the update interval of IPv6 ACL packet matching logs.
ipv6 access-list resequence	Configure the start value and step of rule sequence numbers in an IPv6 ACL.
ipv6 traffic-filter	Apply an IPv6 ACL.
list-remark	Add a remark to an ACL.
mac access-group	Apply a MAC extended ACL.
mac access-list counter	Enable the packet matching counting function of a MAC extended ACL.
mac access-list extended	Configure a MAC extended ACL.
mac access-list resequence	Configure the start value and step of rule sequence numbers in a MAC extended ACL.
permit	Add a rule of permit type to an ACL.
redirect destination interface	Configure an ACL redirection port.
remark	Add a remark to an ACL rule.
security access-group	Configure a security channel for a port.
security global access-group	Configure a global security channel.
security uplink enable	Configure an excluded port of a global security channel.
show access-group	Display the ACL configuration applied to a port.
show access-lists	Display the configuration of all ACLs or a specified ACL.
show acl res	Display information about all or a specified TCAM.
show acl res detail	Display detailed usage information of all or a specified TCAM.
show expert access-group	Display the configuration of an expert extended ACL

	applied to a port.
show ip access-group	Display the configuration of IP standard and IP extended ACLs applied to a port.
show ipv6 traffic-filter	Display the configuration of the IPv6 ACL applied to a port.
show mac access-group	Display the MAC extended ACL applied to a port.
show redirect	Display the redirect ACL configuration.
show svi router-acls state	Check whether an ACL applied to an SVI takes effect on L2 and L3 packets.
svi router-acls enable	Enable the function of making an ACL applied to an SVI effective only for L3 forwarded packets.

1.1 access-list

Function

Run the **access-list** command to create an access control list (ACL) and add a rule.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No ACL and its rules are configured by default.

Syntax

The commands for creating ACLs of different types are as follows:

- Create an IP standard ACL and add a rule.

  access-list *acl-number* { **deny** | **permit** } { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } [**time-range** *time-range-name*] [**log**]

- Create an IP extended ACL and add a rule.

  access-list *acl-number* { **deny** | **permit** } *protocol* { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**time-range** *time-range-name*] [**log**]

Note

The commands for creating IP extended ACLs that specify some important protocols in the protocol field are as follows:

The Transmission Control Protocol (TCP) field is selected.

access-list *acl-number* { **deny** | **permit** } *protocol* { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] [**match-all** *tcp-flag* | **established**] [**time-range** *time-range-name*] [**log**]

- Create a MAC extended ACL and add a rule.

  access-list *acl-number* { **deny** | **permit** } { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [*ethernet-type*] [**cos** [*cos-value*] [**inner** *cos-value*]] [**time-range** *time-range-name*]

- Create an expert extended ACL and add a rule.

  access-list *acl-number* { **deny** | **permit** } [*protocol* | [*ethernet-type*] [**cos** [*cos-value*] [**inner** *cos-value*]]] [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**time-range** *time-range-name*]

  The Ethernet type field or **cos** field is selected.

access-list *acl-number* { **deny** | **permit** } { *ethernet-type* | **cos** [*cos-value*] [**inner** *cos-value*] } [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [**time-range** *time-range-name*]

The protocol field is selected.

access-list *acl-number* { **deny** | **permit** } *protocol* [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] [**time-range** *time-range-name*]

Note

The commands for creating expert extended ACLs that specify some important protocols in the protocol field are as follows:

The Internet Control Message Protocol (ICMP) field is selected.

access-list *acl-number* { **deny** | **permit** } **icmp** [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**time-range** *time-range-name*]

The Transmission Control Protocol (TCP) field is selected.

access-list *acl-number* { **deny** | **permit** } **tcp** [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag* | **established**]

The User Datagram Protocol (UDP) field is selected.

access-list *acl-number* { **deny** | **permit** } **udp** [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source-*ipv4-*wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] [**time-range** *time-range-name*]

The commands for deleting ACLs of different types are as follows:

no access-list *acl-number*

default access-list *acl-number*

Parameter Description

acl-number: ACL number. The following value ranges are supported:

IP standard ACLs: 1 to 99 or 1300 to 1999; IP extended ACLs: 100 to 199 or 2000 to 2699; MAC extended ACLs: 700 to 799; expert extended ACLs: 2700 to 2899.

deny: Configures the processing action for an ACL rule. If packets match the rule, the packets are denied.

permit: Configures the processing action for an ACL rule. If packets match the rule, the packets are permitted.

source-ipv4-address: Source IP address (host address or network address) for packet matching.

source-ipv4-wildcard: Source IP address wildcard mask, which is used to match the source IP addresses of multiple hosts. The wildcard masks can be discontinuous, for example, 0.255.0.32.

protocol: IP protocol number for matching. The value range is from 0 to 255. Some important protocol names such as *icmp*, *ip*, *ipv6*, *tcp, and udp* are listed separately.

destination-ipv4-address: Destination IP address (host address or network address) for packet matching.

destination-ipv4-wildcard: Destination IP address wildcard mask, which is used to match the destination IP addresses of multiple hosts. The wildcard masks can be discontinuous, for example, 0.255.0.32.

fragment: Matches the non-first fragment in the default fragmented packet matching mode.

precedence *precedence*: Matches the precedence value of packets. The value range is from 0 to 7. Some important precedence values such as *routine*, *priority*, *immediate*, *flash*, *flash-override*, *critical*, *internet*, and *network* are listed separately.

eq *port*: Matches packets with the L4 port ID equal to the specified value. The value range is from 0 to 65535.

gt *port*: Matches packets with the L4 port ID greater than the specified value. The value range is from 0 to 65535.

lt *port*: Matches packets with the L4 port ID less than the specified value. The value range is from 0 to 65535.

neq *port*: Matches packets with the L4 port ID not equal to the specified value. The value range is from 0 to 65535.

range: Matches the range the L4 port IDs of packets.

lower: Lower limit of the L4 port ID range for matching. The value range is from 0 to 65535.

upper: Upper limit of the L4 port ID range for matching. The value range is from 0 to 65535.

time-range *time-range-name*: Configures the name of the time range for packet filtering.

tos *tos*: Matches the type of service (ToS) value of packets. The value range is from 0 to 15. Some important service types such as *max-reliability*, *max-throughput*, *min-delay*, *min-monetary-cost*, and *normal* are listed separately.

dscp *dscp*: Matches the differentiated services code point (DSCP) value of packets. The value range is from 0 to 63. Some important differentiated services such as *default*, *ef*, *af11*, and *cs1* are listed separately.

icmp-type: Message type for matching ICMP packets. The value range is from 0 to 255.

icmp-code: Message type code for matching ICMP packets. The value range is from 0 to 255.

icmp-message: Message type name for matching ICMP packets.

source-mac-address: MAC address of the source host for matching.

source-mac-wildcard: MAC address wildcard of the source host, which is used to match the source MAC addresses of multiple hosts.

destination-mac-address: MAC address of the destination host for matching.

destination-mac-wildcard: MAC address wildcard of the destination host, which is used to match the destination MAC addresses of multiple hosts.

cos *cos-value*: Matches the priority field value in the outer tag in the L2 packets. The value range is from 0 to 7.

inner *cos-value*: Matches the priority field value in the inner tag in the L2 packets. The value range is from 0 to 7.

VID *vlan-id*: Matches the VLAN ID. The value range is from 1 to 4094.

inner *vlan-id*: Matches the inner VLAN ID. The value range is from 1 to 4094.

ethernet-type: Ethernet protocol type for matching. The value range is from 0x0000 to 0xFFFF. Some important Ethernet protocol type names such as *arp*, *aarp*, and *IPX* are listed separately.

match-all *tcp-flag*: Matches all the bits of the TCP flag.

established: Matches only the RST or ACK bit in the TCP flag, not the other bits.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To use an ACL to filter data, you must first run the **access-list** command to define a series of ACL rule statements. You can use different kinds of ACLs according to actual needs:

- An IP standard ACL (with the number from 1 to 99 and 1300 to 1999) controls packets based on the source address only.
- An IP extended ACL (with the number from 100 to 199 and 2000 to 2699) implements complex control based on the source and destination addresses.
- A MAC extended ACL (with the number from 700 to 799) performs matching based on the source and destination MAC addresses and Ethernet type.
- An expert extended ACL (with the number from 2700 to 2899) is a combination of the IP standard ACL, IP extended ACL, and MAC extended ACL. You can configure the above three kinds of ACL rules in an expert extended ACL. In addition, the expert extended ACL can also match and filter packets based on the VLAN ID.

Note

For the L3 routing protocols (including the unicast routing protocol and multicast routing protocol), the following parameters are not supported in ACL rules: **precedence** *precedence* / **tos** *tos* / **fragment** / **range** *lower upper* / **time-range** *time-range-name*.

The TCP flag contains some or all of the following bits:

- URG
- ACK
- PSH

- RST
- SYN
- FIN

The packet precedence names are as follows:

- critical
- flash
- flash-override
- immediate
- internet
- network
- priority
- routine

The service type names are as follows:

- max-reliability
- max-throughput
- min-delay
- min-monetary-cost
- normal

The message type names of ICMP packets are as follows:

- administratively-prohibited
- dod-host-prohibited
- dod-net-prohibited
- echo
- echo-reply
- fragment-time-exceeded
- general-parameter-problem
- host-isolated
- host-precedence-unreachable
- host-redirect
- host-tos-redirect
- host-tos-unreachable
- host-unknown
- host-unreachable
- information-reply
- information-request
- mask-reply
- mask-request

- mobile-redirect
- net-redirect
- net-tos-redirect
- net-tos-unreachable
- net-unreachable
- network-unknown
- no-room-for-option
- option-missing
- packet-too-big
- parameter-problem
- port-unreachable
- precedence-unreachable
- protocol-unreachable
- redirect
- router-advertisement
- router-solicitation
- source-quench
- source-route-failed
- time-exceeded
- timestamp-reply
- timestamp-request
- ttl-exceeded
- unreachable

The following are TCP port names. A port name or port ID can be used to specify a specific TCP port:

- bgp
- chargen
- cmd
- daytime
- discard
- domain
- echo
- exec
- finger
- ftp
- ftp-data
- gopher
- hostname

- ident
- irc
- klogin
- kshell
- login
- nntp
- pim-auto-rp
- pop2
- pop3
- smtp
- sunrpc
- syslog
- tacacs
- talk
- telnet
- time
- uucp
- whois
- www

The following are UDP port names. A port name or port ID can be used to specify a specific UDP port:

- biff
- bootpc
- bootps
- discard
- dnsix
- domain
- echo
- isakmp
- mobile-ip
- nameserver
- netbios-dgm
- netbios-ns
- netbios-ss
- ntp
- pim-auto-rp
- rip
- snmp

- snmptrap
- sunrpc
- syslog
- tacacs
- talk
- tftp
- time
- who
- xdmcp

The options of **Ethernet-type** are as follows:

- aarp
- arp
- appletalk
- decnet-iv
- diagnostic
- etype-6000
- etype-8042
- lat
- lavc-sca
- mop-console
- mop-dump
- mumps
- netbios
- vines-echo
- xns-idp

The available protocol layer fields of the UDF header are as follows:

- l2-head
- l3-head
- l4-head
- l5-head
- l6-head

Note

To delete ACL rules, enter the ACL configuration mode and run the **no** { *sequence-number* | **permit** | **deny** } command.

Examples

The following example creates an IP standard ACL and adds a rule: Permit the packets with a source IP address in the range of 192.168.1.64 to 192.168.1.127 to pass through.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 1 permit 192.168.1.64 0.0.0.63
```

The following example creates an IP extended ACL and adds a rule: Permit the DNS packets and ICMP packets to pass through.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 102 permit tcp any any eq domain log
Hostname(config)# access-list 102 permit udp any any eq domain log
Hostname(config)# access-list 102 permit icmp any any echo log
Hostname(config)# access-list 102 permit icmp any any echo-reply
```

The following example creates a MAC extended ACL and adds a rule: Deny Ethernet frames of the AARP protocol type sent by a source host with the MAC address 00d0.f800.0c0c.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 702 deny host 00d0f8000c0c any aarp
```

The following example creates an expert extended ACL and adds a rule: Deny all the TCP packets with the source IP address 192.168.12.3 and the source MAC address 00d0.f800.0044.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 2702 deny tcp host 192.168.12.3 host 00d0.f800.0044
any any
Hostname(config)# access-list 2702 permit any any any any
```

Notifications

When a duplicate rule is added to the same ACL, the following notification will be displayed:

```
failed, for the entry is existed or the sequence number has been allocated!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 access-list list-remark

Function

Run the **access-list list-remark** command to add a remark to an ACL.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No remark is added to an ACL by default.

Syntax

access-list *acl-number* **list-remark** *text*

no access-list *acl-number* **list-remark**

default access-list *acl-number* **list-remark**

Parameter Description

acl-number: ACL number. The following value ranges are supported:

IP standard ACLs: 1 to 99 or 1300 to 1999; IP extended ACLs: 100 to 199 or 2000 to 2699; MAC extended ACLs: 700 to 799; expert extended ACLs: 2700 to 2899.

list-remark *text*: Configures a remark for an ACL. The value is a case-sensitive string of 1 to 100 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To view the function of an ACL conveniently in the future, run this command to add a remark to the ACL. If no ACL exists, this command creates an ACL first and then adds a remark.

Examples

The following example configures an extended ACL numbered 100 and adds the following remark to the ACL: this acl is to filter the host 192.168.4.12.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 100 list-remark this acl is to filter the host
192.168.4.12
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- ip access-list

1.3 access-list remark

Function

Run the **access-list remark** command to add a remark to an ACL rule.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No remark is added to an ACL rule by default.

Syntax

access-list *acl-number* **remark** *text*

no access-list *acl-number* **remark** *text*

default access-list *acl-number* **remark** *text*

Parameter Description

acl-number: ACL number. The following value ranges are supported:

IP standard ACLs: 1 to 99 or 1300 to 1999; IP extended ACLs: 100 to 199 or 2000 to 2699; MAC extended ACLs: 700 to 799; expert extended ACLs: 2700 to 2899.

remark *text*: Configures a remark for an ACL rule. The value is a case-sensitive string of 1 to 100 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To view the function of an ACL rule conveniently in the future, run this command to add a remark to the ACL rule.

Examples

The following example configures an ACL numbered 102 and its rule, and then configures the following remark for the ACL rule: deny-host-10.1.1.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# access-list 102 deny ip host 10.1.1.1 host 10.1.1.1
Hostname(config)# access-list 102 remark deny-host-10.1.1.1
```

Notifications

When no rules are configured in an ACL and an ACL rule remark is added, the following notification will be displayed:

```
The ACL has no entry.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 clear access-list counters

Function

Run the **clear access-list counters** command to clear statistics on matched packets denied by an ACL.

Syntax

clear access-list counters [*acl-name* | *acl-number*]

Parameter Description

acl-name: ACL name. The value is a case-sensitive string of 1 to 99 characters.

acl-number: ACL number. The following value ranges are supported:

IP standard ACLs: 1 to 99 or 1300 to 1999; IP extended ACLs: 100 to 199 or 2000 to 2699; MAC extended ACLs: 700 to 799; expert extended ACLs: 2700 to 2899.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

To re-collect statistics on matched packets denied by a specified ACL, run this command to clear the statistics on the matched packets denied by the ACL.

Examples

The following example clears statistics on matched packets denied by an ACL numbered 1.

```
Hostname> enable
Hostname# clear access-list counters
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.5 clear counters access-list

Function

Run the **clear counters access-list** command to clear statistics on the packets matching an ACL.

Syntax

clear counters access-list [*acl-name* | *acl-number*]

Parameter Description

acl-name: ACL name. The value is a case-sensitive string of 1 to 99 characters.

acl-number: ACL number. The following value ranges are supported:

IP standard ACLs: 1 to 99 or 1300 to 1999; IP extended ACLs: 100 to 199 or 2000 to 2699; MAC extended ACLs: 700 to 799; expert extended ACLs: 2700 to 2899.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

To re-collect statistics on the packets matching a specified ACL, run this command to clear statistics on packets matching the ACL.

Examples

The following example clears statistics on the packets matching an extended ACL numbered 2700.

```
Hostname> enable
Hostname# clear counters access-list 2700
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.6 deny

Function

Run the **deny** command to add a rule of deny type to an ACL.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

There is a rule of deny type in an ACL by default.

Syntax

The commands for adding/deleting a rule of deny type to/from ACLs of different types are as follows:

- IP standard ACL

  Add a rule of deny type to an IP standard ACL.

  [*sequence-number*] **deny** { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } [**time-range** *time-range-name*] [**log**]

  Delete a rule of deny type from an IP standard ACL.

  no { *sequence-number* | { **deny** { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } [**time-range** *time-range-name*] [**log**] } }

- IP extended ACL

  Add a rule of deny type to an IP extended ACL.

  [*sequence-number*] **deny** *protocol* { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**time-range** *time-range-name*] [**log**]

  Delete a rule of deny type from an IP extended ACL.

  no { *sequence-number* | { **deny** *protocol* { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**time-range** *time-range-name*] [**log**] } }

Note

The commands for adding a rule of deny type to IP extended ACLs that specify some important protocols in the protocol field are as follows:

The ICMP field is selected.

[*sequence-number*] **deny icmp** { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**time-range** *time-range-name*] [**log**]

The TCP field is selected.

[*sequence-number*] **deny tcp** { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] { *destination-ipv4-address destination-*

ipv4-wildcard | **host** *destination-ipv4-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag* | **established**] [**log**]

The UDP field is selected.

[*sequence-number*] **deny udp** { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] [**time-range** *time-range-name*] [**log**]

- MAC extended ACL

  Add a rule of deny type to a MAC extended ACL.

  [*sequence-number*] **deny** { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [*ethernet-type*] [**cos** [*cos-value*] [**inner** *cos-value*]] [**time-range** *time-range-name*]

  Delete a rule of deny type from a MAC extended ACL.

  no { *sequence-number* | { **deny** { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [*ethernet-type*] [**cos** [*cos-value*] [**inner** *cos-value*]] [**time-range** *time-range-name*] } }

- Expert extended ACL

  Add a rule of deny type to an expert extended ACL.

  [*sequence-number*] **deny** [*protocol* | [*ethernet-type*] [**cos** [*cos-value*] [**inner** *cos-value*]]] [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**time-range** *time-range-name*]

  Delete a rule of deny type from an expert extended ACL.

  no { *sequence-number* | { **deny** [*protocol* | [*ethernet-type*] [**cos** [*cos-value*] [**inner** *cos-value*]]] [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**time-range** *time-range-name*] } }

  The Ethernet type field or **cos** field is selected.

  [*sequence-number*] **deny** { [*ethernet-type*] [**cos** [*cos-value*] [**inner** *cos-value*]] } [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [**time-range** *time-range-name*]

Note

The commands for adding a rule of deny type to expert extended ACLs that specify some important protocols in the protocol field are as follows:

The ICMP field is selected.

[*sequence-number*] **deny icmp** [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* **| host** *destination-mac-address* | **any** } [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**time-range** *time-range-name*]

The TCP field is selected.

[*sequence-number*] **deny tcp** [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag* | **established**]

The UDP field is selected.

[*sequence-number*] **deny udp** [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source*-ipv4-*wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] [**time-range** *time-range-name*]

- Expert advanced ACL

  Add a rule of deny type to an expert advanced ACL.

  [sequence-number] **deny** hex hex-mask offset

  Delete a rule of deny type from an expert advanced ACL.

  no { sequence-number | **deny** hex hex-mask offset }

- IPv6 extended ACL

  Add a rule of deny type to an IPv6 extended ACL.

  [*sequence-number*] **deny** [*protocol* { *source-ipv6-prefix* / *prefix-length* | *source-ipv6-address source-ipv6-mask* | **host** *source-ipv6-address* | **any** } { *destination-ipv6-prefix* / *prefix-length* | *destination-ipv6-address destination-ipv6-mask* | **host** *destination-ipv6-address* | **any** }] [**cos** *cos-value* [**inner** *cos-value*]] [{ **any** | **host** *source-mac-address* | *source-mac-address source-mac-wildcard* } { **any** | **host** *destination–mac-address* | *destination-mac-address destination-mac-wildcard* }] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**VID** [*vlan-id*] [**inner** *vlan-id*]] [**time-range** *time-range-name*] [**log**]

  Delete a rule of deny type from an IPv6 extended ACL.

no { *sequence-number* | { **deny** [*protocol* { *source-ipv6-prefix* / *prefix-length* | *source-ipv6-address source-ipv6-mask* | **host** *source-ipv6-address* | **any** } { *destination-ipv6-prefix* / *prefix-length* | *destination-ipv6-address destination-ipv6-mask* | **host** *destination-ipv6-address* | **any** }] [**cos** *cos-value* [**inner** *cos-value*]] [{ **any** | **host** *source-mac-address* | *source-mac-address source-mac-wildcard* } { **any** | **host** *destination–mac-address* | *destination–mac-address destination-mac-wildcard* }] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**VID** [*vlan-id*] [**inner** *vlan-id*]] [**time-range** *time-range-name*] [**log**] } }

Note

The commands for adding a rule of deny type to IPv6 extended ACLs that specify some important protocols in the protocol field are as follows:

The ICMP field is selected.

[*sequence-number*] **deny icmp** { *source-ipv6-prefix* / *prefix-length* | *source-ipv6-address source-ipv6-mask* | **host** *source-ipv6-address* | **any** } { *destination-ipv6-prefix* / *prefix-length* | *destination-ipv6-address destination-ipv6-mask* | **host** *destination-ipv6-address* | **any** } [{ **any** | **host** *source-mac-address* | *source-mac-address source-mac-wildcard* } { **any** | **host** *destination–mac-address* | *destination–mac-address destination-mac-wildcard* }] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**VID** [*vlan-id*] [**inner** *vlan-id*]] [**time-range** *time-range-name*] [**log**]

The TCP field is selected.

[*sequence-number*] **deny tcp** { *source-ipv6-prefix* / *prefix-length* | *source-ipv6-address source-ipv6-mask* | **host** *source-ipv6-address* | **any** } [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] { *destination-ipv6-prefix* / *prefix-length* | *destination-ipv6-address destination-ipv6-mask* | **host** *destination-ipv6-address* | **any** } [{ **any** | **host** *source-mac-address* | *source-mac-address source-mac-wildcard* } { **any** | **host** *destination–mac-address* | *destination–mac-address destination-mac-wildcard* }] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**VID** [*vlan-id*] [**inner** *vlan-id*]] [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag* | **established**] [**log**]

The UDP field is selected.

[*sequence-number*] **deny udp** { *source-ipv6-prefix* / *prefix-length* | *source-ipv6-address source-ipv6-mask* | **host** *source-ipv6-address* | **any** } [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] { *destination-ipv6-prefix* / *prefix-length* | *destination-ipv6-address destination-ipv6-mask* | **host** *destination-ipv6-address* | **any** } [{ **any** | **host** *source-mac-address* | *source-mac-address source-mac-wildcard* } { **any** | **host** *destination–mac-address* | *destination–mac-address destination-mac-wildcard* }] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**VID** [*vlan-id*] [**inner** *vlan-id*]] [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] [**time-range** *time-range-name*] [**log**]

Parameter Description

sequence-number: Sequence number of an ACL rule. The value range is from 1 to 2147483647.

deny: Configures the processing action for an ACL rule. If packets match this rule, the packets are denied.

source-ipv4-address: Source IP address (host address or network address) for packet matching.

source-ipv4-wildcard: Source IP address wildcard mask, which is used to match the source IP addresses of multiple hosts. The wildcard masks can be discontinuous, for example, 0.255.0.32.

protocol: IP protocol number for matching. The value range is from 0 to 255. Some important protocol names such as *icmp*, *ip*, *ipv6*, *tcp, and udp* are listed separately.0

destination-ipv4-address: Destination IP address (host address or network address) for packet matching.

destination-ipv4-wildcard: Destination IP address wildcard mask, which is used to match the destination IP addresses of multiple hosts. The wildcard masks can be discontinuous, for example, 0.255.0.32.

fragment: Matches the non-first fragment in the default fragmented packet matching mode.

precedence *precedence*: Matches the precedence value of packets. The value range is from 0 to 7. Some important precedence names such as *routine*, *priority*, *immediate*, *flash*, *flash-override*, *critical*, *internet*, and *network* are listed separately.

eq *port*: Matches packets with the L4 port ID equal to the specified value. The value range is from 0 to 65535.

gt *port*: Matches packets with the L4 port ID greater than the specified value. The value range is from 0 to 65535.

lt *port*: Matches packets with the L4 port ID less than the specified value. The value range is from 0 to 65535.

neq *port*: Matches packets with the L4 port ID not equal to the specified value. The value range is from 0 to 65535.

range: Matches the range of L4 port IDs of packets.

lower: Lower limit of the L4 port ID range for matching. The value range is from 0 to 65535.

upper: Upper limit of the L4 port ID range for matching. The value range is from 0 to 65535.

time-range *time-range-name*: Configures the name of the time range for packet filtering.

tos *tos*: Matches the ToS value of packets. The value range is from 0 to 15. Some important service type names such as *max-reliability*, *max-throughput*, *min-delay*, *min-monetary-cost*, and *normal* are listed separately.

dscp *dscp*: Matches the DSCP value of packets. The value range is from 0 to 63. Some important differentiated service names such as *default*, *ef*, *af11*, and *cs1* are listed separately.

icmp-type: Message type for matching ICMP packets. The value range is from 0 to 255.

icmp-code: Message type code for matching ICMP packets. The value range is from 0 to 255.

icmp-message: Message type name for matching ICMP packets.

source-mac-address: MAC address of the source host for matching.

source-mac-wildcard: MAC address wildcard of the source host, which is used to match the source MAC addresses of multiple hosts.

destination-mac-address: MAC address of the destination host for matching.

destination-mac-wildcard: MAC address wildcard of the destination host, which is used to match the destination MAC addresses of multiple hosts.

cos *cos-value*: Matches the priority field value in the outer tag in the L2 packets. The value range is from 0 to 7.

inner *cos-value*: Matches the priority field value in the inner tag in the L2 packets. The value range is from 0 to 7.

VID *vlan-id*: Matches the VLAN ID. The value range is from 1 to 4094.

inner *vlan-id*: Matches the inner VLAN ID. The value range is from 1 to 4094.

ethernet-type: Ethernet protocol type for matching. The value range is from 0x0000 to 0xFFFF. Some important Ethernet protocol type names such as *arp*, *aarp*, and *IPX* are listed separately.

match-all *tcp-flag*: Matches all the bits of the TCP flag.

established: Matches only the RST or ACK bit in the TCP flag, not the other bits.

source-ipv6-prefix: Source IPv6 network address or network type for matching.

destination-ipv6-prefix: Destination IPv6 network address or network type for matching.

prefix-length: IPv6 address mask length for matching.

source-ipv6-address: Source IPv6 address for matching.

destination-ipv6-address: Destination IPv6 address for matching.

source-ipv6-mask: Source IPv6 address mask for matching.

destination-ipv6-mask: Destination IPv6 address mask for matching.

flow-label *flow-label*: Matches the flow label value. The value range is from 0 to 1048575.

hex: Matching field in hexadecimal notation. It is used when expert advanced ACL rules are configured.

hex-mask: Matching field mask in hexadecimal notation. It is used when expert advanced ACL rules are configured.

offset: Matching start position, in bytes. It is used when expert advanced ACL rules are configured. The value range is from 0 to 79.

hex hex-mask offset: Combination of *hex*, *hex-mask*, and *offset*. Multiple such combinations can be configured.

Command Modes

ACL configuration mode

Default Level

14

Usage Guidelines

To deny some packets access to a network, you can run this command to add rules of deny type to an ACL.

Examples

The following example creates an IP standard ACL and adds a rule: Deny packets sent from the source host with the IP address 192.168.4.12.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip access-list standard 34
Hostname(config-ext-nacl)# deny host 192.168.4.12
```

The following example creates an IP extended ACL and adds a rule: Deny services provided by the source host with the IP address 192.168.4.12 through TCP port 100.

```
Hostname# configure terminal
Hostname(config)# ip access-list extended ip-ext-acl
Hostname(config-ext-nacl)# deny tcp host 192.168.4.12 eq 100 any
```

The following example creates an expert extended ACL and adds a rule: Deny all the TCP packets with the source IP address 192.168.4.12 and the source MAC address 0013.0049.8272.

```
Hostname# configure terminal
Hostname(config)# expert access-list extended 2702
```

```
Hostname(config-exp-nacl)# deny tcp host 192.168.4.12 host 0013.0049.8272 any any
Hostname(config-exp-nacl)# permit any any any any
```

The following example creates a MAC extended ACL and adds a rule: Deny Ethernet frames of the AARP protocol type sent by the source host with the MAC address 0013.0049.8272.

```
Hostname# configure terminal
Hostname(config)# mac access-list extended mac1
Hostname(config-mac-nacl)# deny host 0013.0049.8272 any aarp
```

The following example creates an IPv6 extended ACL and adds a rule numbered 11: Deny packets sent from the source host with the IP address 2000::1.

```
Hostname# configure terminal
Hostname(config)# ipv6 access-list v6-acl
Hostname(config-ipv6-acl)# 11 deny ipv6 host 2000::1 any
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- expert access-list extended
- ip access-list
- ip access-group
- mac access-list extended
- mac access-group
- ipv6 access-list
- ipv6 traffic-filter

1.7 expert access-group

Function

Run the **expert access-group** command to apply an expert ACL.

Run the **no** form of this command to cancel the application.

Run the **default** form of this command to restore the default configuration.

No expert ACL is applied by default.

Syntax

expert access-group { *acl-name* | *acl-number* } { **in** | **out** } [**control-plan** | **counter-only** | **forward-control-plane** | **forward-plane**]

no expert access-group { *acl-name* | *acl-number* } { **in** | **out** } [**control-plan** | **counter-only** | **forward-control-plane** | **forward-plane**]

default expert access-group { *acl-name* | *acl-number* } { **in** | **out** } [**control-plan** | **counter-only** | **forward-control-plane** | **forward-plane**]

Parameter Description

acl-name: Name of an expert ACL. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of an expert ACL. The value range is from 2700 to 2899.

in: Filters the incoming packets of a port.

out: Filters the outgoing packets of a port.

counter-only: Configures a special ACL for packet counting on a port.

control-plane: Configures a control plane ACL.

forward-control-plane: Configures a control and forwarding plane ACL.

forward-plane: Configures a forwarding plane ACL.

Command Modes

Global configuration mode

Interface configuration mode

SVI interface configuration mode

Default Level

14

Usage Guidelines

To make an expert ACL take effect, run this command to apply the ACL in global configuration mode, interface configuration mode, or switch virtual interface (SVI) interface configuration mode. The **counter-only** option is not supported in global configuration mode. The **expert access-group** { *acl-name* | *acl-number* } { **in** | **out** } **counter-only** command configured on a port collects statistics on packets only, without filtering them.

Examples

The following example applies the expert extended ACL named accept_00d0f8xxxxxx_only to the inbound direction of the L3 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-Gigabitethernet 0/1)# expert access-group
accept_00d0f8xxxxxx_only in
```

The following example applies the expert extended ACL numbered 2700 to the inbound direction of the L3 Ethernet interface GigabitEthernet0/1, and collects statistics on the incoming packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# expert access-group 2700 in counter-only
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- expert access-list advanced
- expert access-list extended

1.8 expert access-list advanced

Function

Run the **expert access-list advanced** command to create an expert advanced ACL.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No expert advanced ACL is configured by default.

Syntax

expert access-list advanced *acl-name*

no expert access-list advanced *acl-name*

default expert access-list advanced *acl-name*

Parameter Description

acl-name: Name of an expert advanced ACL. The value is a case-sensitive string of 1 to 99 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To filter packets by user-defined fields, you can use an expert advanced ACL (namely, ACL 80).

Figure 1-1 shows the first 64 bytes of an L2 data frame, where each letter represents one hexadecimal number and every two letters represent one byte.

Figure 1-1First 64 Bytes of an L2 Data Frame

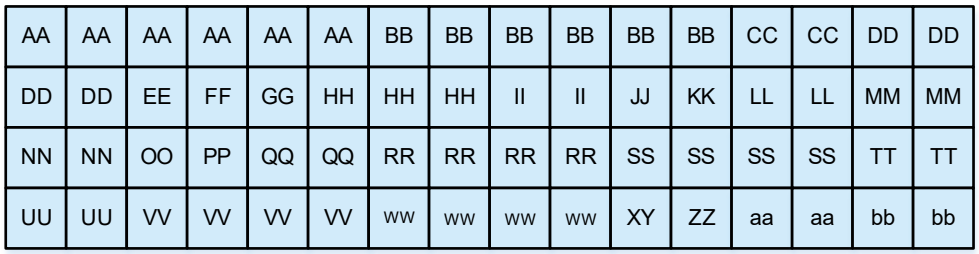

Table 1-1 lists the offsets of fields in an ACL 80. The offset of each field in the table is their offset in the IEEE 802.3 data frame containing the SNAP+Tag fields.

Table 1-1Offsets of Fields in an ACL 80

Letter	Description	Offset	Letter	Description	Offset
A	Destination MAC address	0	O	TTL field	34
B	Source MAC address	6	P	Protocol number	35
C	Data frame length field	12	Q	IP checksum	36
D	VLAN tag field	14	R	Source IP address	38
E	Destination service access point (DSAP) field	18	S	Destination IP address	42
F	Source service access point (SSAP) field	19	T	TCP source port	46
G	Control field	20	U	TCP destination port	48
H	Org code field	21	V	Serial number	50
I	Encapsulated data type	24	W	Acknowledgment field	54
J	IP version No.	26	XY	IP header length and reserved bits	58
K	ToS field	27	Z	Reserved bits and flags bits	59
L	IP packet length	28	a	Windows size field	60
M	ID	30	b	Others	62
N	Flags field	32			

Examples

The following example creates an expert advanced ACL named adv-acl.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# expert access-list advanced adv-acl
Hostname(config-exp-dacl)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- expert access-group

1.9 expert access-list counter

Function

Run the **expert access-list counter** command to enable the packet matching counting function of a specified expert extended ACL.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The packet matching counting function of an expert extended ACL is disabled by default.

Syntax

expert access-list counter { *acl-name* | *acl-number* }

no expert access-list counter { *acl-name* | *acl-number* }

default expert access-list counter { *acl-name* | *acl-number* }

Parameter Description

acl-name: Name of an expert extended ACL. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of an expert extended ACL. The value range is from 2700 to 2899.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can run this command to enable the packet matching counting function to know the packet filtering situation of a specified expert extended ACL, especially to find out whether the network is attacked by a large number of illegitimate packets.

Examples

The following example enables the packet matching counting function of an expert extended ACL named exp-acl.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# expert access-list counter exp-acl
```

Notifications

When the packet matching counting function of an expert extended ACL is enabled before this ACL is configured, the following notification will be displayed:

```
Create the access-list first
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 expert access-list extended

Function

Run the **expert access-list extended** command to create an expert extended ACL.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No expert extended ACL is configured by default.

Syntax

expert access-list extended { *acl-name* | *acl-number* }

no expert access-list extended { *acl-name* | *acl-number* }

default expert access-list extended { *acl-name* | *acl-number* }

Parameter Description

acl-name: Name of an expert extended ACL. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of an expert extended ACL. The value range is from 2700 to 2899.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To achieve the filtering effects of the IP standard ACL, IP extended ACL, and MAC extended ACL in an ACL, configure an expert extended ACL.

Examples

The following example creates an expert advanced ACL named exp-acl.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# expert access-list extended exp-acl
Hostname(config-exp-nacl)#
```

The following example creates an expert extended ACL numbered 2704.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# expert access-list extended 2704
Hostname(config-exp-nacl)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- expert access-group

1.11 expert access-list new-fragment-mode

Function

Run the **expert access-list new-fragment-mode** command to switch the fragmented packet matching mode of an expert extended ACL from the default matching mode to the new matching mode.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The fragmented packet matching mode of an expert extended ACL is the default matching mode by default.

Syntax

expert access-list new-fragment-mode { *acl-name* | *acl-number* }

no expert access-list new-fragment-mode { *acl-name* | *acl-number* }

default expert access-list new-fragment-mode { *acl-name* | *acl-number* }

Parameter Description

acl-name: Name of an expert extended ACL. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of an expert extended ACL. The value range is from 2700 to 2899.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When an ACL rule carries the fragment flag, there is no difference between the default fragmented packet matching mode and the new matching mode.

When an ACL rule does not carry the fragment flag, if the first fragment is required to match all the user-defined matching fields (including L3 and L4 information) in the ACL rule and the non-first fragments need to only match the non-L4 information in the ACL rule, you can run this command to switch the fragmented packet matching mode of the specified ACL to the new matching mode.

Examples

The following example switches the fragmented packet matching mode of an ACL numbered 2700 from the default matching mode to the new matching mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# expert access-list new-fragment-mode 2700
```

Notifications

When the fragmented packet matching mode of an expert extended ACL is configured before this ACL is configured, the following notification will be displayed:

```
Create the access-list first
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 expert access-list resequence

Function

Run the **expert access-list resequence** command to configure the start value and step of rule sequence numbers in an expert extended ACL.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The default start value and step of rule sequence numbers in an expert extended ACL are both **10**.

Syntax

expert access-list resequence { *acl-name* | *acl-number* } *start-value step-value*

no expert access-list resequence { *acl-name* | *acl-number* }

default expert access-list resequence { *acl-name* | *acl-number* }

Parameter Description

acl-name: Name of an expert extended ACL. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of an expert extended ACL. The value range is from 2700 to 2899.

start-value: Start value of rule sequence numbers. The value range is from 1 to 2147483647.

step-value: Step of rule sequence numbers. The value range is from 1 to 2147483647.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To insert a new rule into an expert extended ACL, run this command to rearrange the sequence numbers of ACL rules.

Examples

The following example configures an expert extended ACL named exp-acl, and sets the start value of rule sequence numbers to 21 and step to 43.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# expert access-list resequence exp-acl 21 43
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 global access-group

Function

Run the **global access-group** command to make a global security ACL take effect on a port.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

A port is an excluded port of the global security ACL by default.

Syntax

global access-group

no global access-group

default global access-group

Parameter Description

N/A

Command Modes

L3 Ethernet interface configuration mode

Default Level

14

Usage Guidelines

When a port is an excluded port of the global security ACL and a global security ACL needs to take effect on the port, run this command.

Examples

The following example enables the global security ACL on the L3 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# global access-group
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 global access-group disable

Function

Run the **global access-group disable** command to disable the global security ACL function.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The global security ACL function is enabled by default.

Syntax

global access-group disable

no global access-group disable

default global access-group disable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If it is forbidden to configure the global security ACL, disable the global security ACL function. Running this command will delete all global security ACLs.

Examples

The following example disables the global security ACL function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# global access-group disable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 global ip access-group

Function

Run the **global ip access-group** command to make a global security ACL of IP type take effect on a port.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

A port is an excluded port of the global security ACL of the IP type by default.

Syntax

global ip access-group

no global ip access-group

default global ip access-group

Parameter Description

N/A

Command Modes

L3 Ethernet interface configuration mode

Default Level

14

Usage Guidelines

When a port is an excluded port of the global security ACL of IP type and a global security ACL of IP type needs to take effect on the port, run this command.

Examples

The following example enables the global security ACL of IP type on the L3 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# global ip access-group
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.16 ip access-group

Function

Run the **ip access-group** command to apply an IP standard ACL or IP extended ACL.

Run the **no** form of this command to cancel the application.

Run the **default** form of this command to restore the default configuration.

No IP standard ACL or IP extended ACL is applied by default.

Syntax

ip access-group { *acl-name* | *acl-number* } { **in** | **out** } [**control-plane** | **counter-only** | **forward-control-plane** | **forward-plane**]

no ip access-group { *acl-name* | *acl-number* } { **in** | **out** } [**control-plane** | **counter-only** | **forward-control-plane** | **forward-plane**]

default ip access-group { *acl-name* | *acl-number* } { **in** | **out** } [**control-plane** | **counter-only** | **forward-control-plane** | **forward-plane**]

Parameter Description

acl-name: Name of an IP standard ACL or IP extended ACL. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of an IP standard ACL or IP extended ACL. The following value ranges are supported:

The value range of IP standard ACLs is 1 to 99 or 1300 to 1999; the value range of IP extended ACLs is 100 to 199 or 2000 to 2699.

in: Filters the incoming packets of a port.

out: Filters the outgoing packets of a port.

control-plane: Configures a control plane ACL.

counter-only: Configures a special ACL for packet counting on a port.

forward-control-plane: Configures a control and forwarding plane ACL.

forward-plane: Configures a forwarding plane ACL.

Command Modes

Global configuration mode

Interface configuration mode

SVI interface configuration mode

Default Level

14

Usage Guidelines

To make an IP standard ACL or IP extended ACL take effect, run this command to apply the ACL in global configuration mode, interface configuration mode, or SVI interface configuration mode. The ACL controls the incoming/outgoing packets of all ports, a specified SVI, or a specified port. The **counter-only** option is not supported in global configuration mode. The **ip access-group** { *acl-name* | *acl-number* } { **in** | **out** } **counter-only** command configured on a port collects statistics on packets only, without filtering them.

Examples

The following example applies the IP extended ACL numbered 120 to the inbound direction of the L3 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip access-group 120 in
```

The following example applies the IP extended ACL numbered 120 to the inbound direction globally.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip access-group 120 in control-plane
```

The following example applies the IP extended ACL numbered 120 to the inbound direction of the L3 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip access-group 120 in counter-only
```

Notifications

When an ACL is applied to the global control plane, if an ACL has been applied to the global control plane, the following notification will be displayed:

```
Another acl has attached at global control-plane, Operation fail
```

When an ACL is applied to a global network segment policy, if an ACL has been applied to the global network segment policy, the following notification will be displayed:

```
Another acl has attached at network-policy, Operation fail
```

When an ACL is applied to a global user group policy, if an ACL has been applied to the global user group policy, the following notification will be displayed:

```
Another acl has attached at user-group-policy, Operation fail
```

When a counter-only ACL is applied to a port, if the counter function of the ACL has been enabled globally, the following notification will be displayed:

```
ACL 1 has been used as a traffic matching statistics ACL.
```

When a counter-only ACL is applied to a port, if an ACL (IP standard ACL, IP extended ACL, MAC extended ACL, or expert ACL) has been applied to the same direction of the port, the following notification will be displayed:

```
Another counter-only acl has attached at GigabitEthernet 0/1, Operation fail.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- ip access-list

1.17 ip access-list

Function

Run the **ip access-list** command to create an IP standard ACL or IP extended ACL.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No IP standard ACL or extended ACL is configured by default.

Syntax

ip access-list { **extended** | **standard** } { *acl-name* | *acl-number* }

no ip access-list { **extended** | **standard** } { *acl-name* | *acl-number* }

default ip access-list { **extended** | **standard** } { *acl-name* | *acl-number* }

Parameter Description

acl-name: Name of an IP standard ACL or IP extended ACL. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of an IP standard ACL or IP extended ACL. The following value ranges are supported:

The value range of IP standard ACLs is 1 to 99 or 1300 to 1999; the value range of IP extended ACLs is 100 to 199 or 2000 to 2699.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To filter packets based on the source IP address only, create an IP standard ACL. To control IP packets more finely, for example, filter packets based on the destination IP address or L4 information, create an IP extended ACL. For the matching fields of the two kinds of IP ACLs, refer to the standard and extended forms of the **deny** and **permit** commands. Run the **show access-lists** command to display the ACL configuration.

Examples

The following example creates an IP standard ACL named std-acl.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip access-list standard std-acl
Hostname(config-std-nacl)#
```

The following example creates an IP extended ACL numbered 123.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip access-list extended 123
Hostname(config-ext-nacl)#
```

Notifications

When you create a named IP standard or IP extended ACL, if the specified name has been used by another type of ACL, the following notification will be displayed:

```
ACL type error, current ACL has been set to type mac extended.
```

When you create a named IP standard or IP extended ACL, if the number of named ACLs (all types of named ACLs) created in the device has reached 500, the following notification will be displayed:

```
Failed to create user-defined acl for the max-limit has been reached
```

When you create a named IP standard or IP extended ACL, if the length of the name entered is longer than 99 characters, the following notification will be displayed:

```
Name is too long
```

When you create a named IP standard or IP extended ACL, if the entered name begins with a number or the name is in or out, the following notification will be displayed:

```
Invalid name
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- ip access-group

1.18 ip access-list counter

Function

Run the **ip access-list counter** command to enable the packet matching counting function of an IP standard ACL or IP extended ACL.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The packet matching counting function of an IP standard ACL or IP extended ACL is disabled by default.

Syntax

ip access-list counter { *acl-name* | *acl-number* }

no ip access-list counter { *acl-name* | *acl-number* }

default ip access-list counter { *acl-name* | *acl-number* }

Parameter Description

acl-name: Name of an IP standard ACL or IP extended ACL. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of an IP standard ACL or IP extended ACL. The following value ranges are supported:

The value range of IP standard ACLs is 1 to 99 or 1300 to 1999; the value range of IP extended ACLs is 100 to 199 or 2000 to 2699.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can run this command to enable the packet matching counting function to know the packet filtering situation of a specified IP standard ACL or IP extended ACL.

Examples

The following example enables the packet matching counting function of an IP standard ACL.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip access-list counter std-acl
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.19 ip access-list log-update interval

Function

Run the **ip access-list log-update interval** command to configure the update interval of IPv4 ACL packet matching logs.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The default update interval of packet matching logs is 0 minutes, that is, no ACL matching log is output.

Syntax

ip access-list log-update interval *time-value*

no ip access-list log-update interval

default ip access-list log-update interval

Parameter Description

interval *time-value*: Log update interval, in minutes. For the ACL rules with the log output option, it indicates the interval for (in minutes) outputting the ACL matching logs of a data flow. The range is from 0 to 1440. Here, **0** indicates that no ACL matching log is output.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

For the IP standard or IP extended ACL rules with the log function enabled, if packets are matched within the log output interval, a log of packet matching count is output when the log output interval expires. To change the log output interval, run this command.

Examples

The following example sets the update interval threshold of IPv4 ACL packet matching logs to 10 minutes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip access-list log-update interval 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 ip access-list new-fragment-mode

Function

Run the **ip access-list new-fragment-mode** command to configure the fragmented packet matching mode of an IP standard ACL or IP extended ACL.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The fragmented packet matching mode of an IP standard ACL or IP extended ACL is the default matching mode by default.

Syntax

ip access-list new-fragment-mode { *acl-name* | *acl-number* }

no ip access-list new-fragment-mode { *acl-name* | *acl-number* }

default ip access-list new-fragment-mode { *acl-name* | *acl-number* }

Parameter Description

acl-name: Name of an IP standard ACL or IP extended ACL. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of an IP standard ACL or IP extended ACL. The following value ranges are supported:

The value range of IP standard ACLs is 1 to 99 or 1300 to 1999; the value range of IP extended ACLs is 100 to 199 or 2000 to 2699.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When an ACL rule carries the fragment flag, there is no difference between the default fragmented packet matching mode and the new matching mode.

When the ACL rule does not carry the fragment flag, if the first fragment is required to match all the user-defined matching fields (including L3 and L4 information) in the ACL and the non-first fragments need to only match the non-L4 information in the ACL rule, you can run this command to switch the fragmented packet matching mode of the specified ACL to the new matching mode.

Examples

The following example switches the fragmented packet matching mode of an ACL numbered 100 from the default matching mode to a new matching mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip access-list new-fragment-mode 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.21 ip access-list resequence

Function

Run the **ip access-list resequence** command to configure the start value and step of rule sequence numbers in an IP ACL.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The default start value and step of rule sequence numbers in an IP ACL are both **10**.

Syntax

ip access-list resequence { *acl-name* | *acl-number* } *start-value step-value*

no ip access-list resequence { *acl-name* | *acl-number* }

default ip access-list resequence { *acl-name* | *acl-number* }

Parameter Description

acl-name: Name of an IP standard ACL or IP extended ACL. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of an IP standard ACL or IP extended ACL. The following value ranges are supported:

The value range of IP standard ACLs is 1 to 99 or 1300 to 1999; the value range of IP extended ACLs is 100 to 199 or 2000 to 2699.

start-value: Start value of rule sequence numbers. The value range is from 1 to 2147483647.

step-value: Step of rule sequence numbers. The value range is from 1 to 2147483647.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To insert a new rule into an IP standard ACL or IP extended ACL, run this command to rearrange the sequence numbers of ACL rules.

Examples

The following example configures an IP standard ACL numbered 1, and sets the start value of rule sequence numbers to 21 and step to 43.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip access-list resequence 1 21 43
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.22 ipv6 access-list

Function

Run the **ipv6 access-list** command to create an IPv6 ACL.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No IPv6 ACL is configured by default.

Syntax

ipv6 access-list *acl-name*

no ipv6 access-list *acl-name*

default ipv6 access-list *acl-name*

Parameter Description

acl-name: Name of an IPv6 ACL. The value is a case-sensitive string of 1 to 99 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To filter IPv6 packets in the network, run this command to create an IPv6 ACL.

Examples

The following example creates an IPv6 ACL named v6-acl.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list v6-acl
Hostname(config-ipv6-nacl)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- ipv6 traffic-filter

1.23 ipv6 access-list counter

Function

Run the **ipv6 access-list counter** command to enable the packet matching counting function of an IPv6 ACL.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The packet matching counting function of an IPv6 ACL is disabled by default.

Syntax

ipv6 access-list counter *acl-name*

no ipv6 access-list counter *acl-name*

default ipv6 access-list counter *acl-name*

Parameter Description

acl-name: Name of an IPv6 ACL. The value is a case-sensitive string of 1 to 99 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can run this command to enable the packet matching counting function to know the packet filtering situation of a specified IPv6 ACL.

Examples

The following example enables the packet matching counting function of an IPv6 ACL.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list counter v6-acl
```

The following example disables the packet matching counting function of an IPv6 ACL.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ipv6 access-list counter v6-acl
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.24 ipv6 access-list log-update interval

Function

Run the **ipv6 access-list log-update interval** command to configure the update interval of IPv6 ACL packet matching logs.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The default update interval of packet matching logs is 0 minutes, that is, no ACL matching log is output.

Syntax

ipv6 access-list log-update interval *time-value*

no ipv6 access-list log-update interval

default ipv6 access-list log-update interval

Parameter Description

interval *time-value*: Log update interval, in minutes. For the ACL rules with the log output option, it indicates the interval for (in minutes) outputting the ACL matching logs of a data flow. The range is from 0 to 1440. Here, **0** indicates that no ACL matching log is output.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

For the IPv6 ACL rules with the log function enabled, if packets are matched within the log output interval, a log of packet matching count is output when the log output interval expires. To change the log output interval, run this command.

Examples

The following example sets the update interval of IPv6 ACL packet matching logs to 10 minutes.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# ipv6 access-list log-update interval 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.25 ipv6 access-list resequence

Function

Run the **ipv6 access-list resequence** command to configure the start value and step of rule sequence numbers in an IPv6 ACL.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The default start value and step of rule sequence numbers in an IPv6 ACL are both **10**.

Syntax

ipv6 access-list resequence *acl-name start-value step-value*

no ipv6 access-list resequence *acl-name*

default ipv6 access-list resequence *acl-name*

Parameter Description

acl-name: Name of an IPv6 ACL. The value is a case-sensitive string of 1 to 99 characters.

start-value: Start value of rule sequence numbers. The value range is from 1 to 2147483647.

step-value: Step of rule sequence numbers. The value range is from 1 to 2147483647.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To insert a new rule into an IPv6 ACL, run this command to rearrange the sequence numbers of ACL rules.

Examples

The following example configures an IPv6 ACL named v6-acl, sets the start value of rule sequence numbers to 21 and step to 43.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list resequence v6-acl 21 43
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.26 ipv6 traffic-filter

Function

Run the **ipv6 traffic-filter** command to apply an IPv6 ACL.

Run the **no** form of this command to cancel the application.

Run the **default** form of this command to restore the default configuration.

No IPv6 ACL is applied by default.

Syntax

ipv6 traffic-filter *acl-name* { **in** | **out** } [**control-plan** | **counter-only** | **forward-control-plane** | **forward-plane**]

no ipv6 traffic-filter *acl-name* { **in** | **out** } [**control-plan** | **counter-only** | **forward-control-plane** | **forward-plane**]

default ipv6 traffic-filter *acl-name* { **in** | **out** } [**control-plan** | **counter-only** | **forward-control-plane** | **forward-plane**]

Parameter Description

acl-name: Name of an IPv6 ACL. The value is a case-sensitive string of 1 to 99 characters.

in: Filters the incoming packets of a port.

out: Filters the outgoing packets of a port.

counter-only: Configures a special ACL only for packet counting on a port.

control-plane: Configures a control plane ACL.

forward-control-plane: Configures a control and forwarding plane ACL.

forward-plane: Configures a forwarding plane ACL.

Command Modes

Global configuration mode

Interface configuration mode

SVI interface configuration mode

Default Level

14

Usage Guidelines

To make an IPv6 ACL take effect, run this command to apply the ACL in global configuration mode, interface configuration mode, or SVI interface configuration mode. The ACL controls the incoming/outgoing IPv6 packets of all ports, a specified SVI, or a specified port. The **counter-only** option is not supported in global configuration mode. The **ipv6 traffic-filter** *acl-name* { **in** | **out** } **counter-only** command configured on a port collects statistics on packets only, without filtering them.

Examples

The following example applies the IPv6 ACL named v6-acl to the inbound direction of the L3 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 traffic-filter v6-acl in
```

The following example applies the IPv6 ACL named v6-acl to the inbound direction of the L3 Ethernet interface GigabitEthernet 0/1, and collects statistics on incoming packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 traffic-filter v6-acl in counter-
only
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- ipv6 access-list

1.27 list-remark

Function

Run the **list-remark** command to add a remark to an ACL.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No remark is added to an ACL by default.

Syntax

list-remark *text*

no list-remark

default list-remark

Parameter Description

text: Remark of an ACL. The value is a case-sensitive string of 1 to 100 characters.

Command Modes

ACL configuration mode

Default Level

14

Usage Guidelines

To view the function of an ACL conveniently in the future, run this command to add a remark to the ACL. You can also directly run the **access-list list-remark** command in global configuration mode to add a remark to an ACL.

Examples

The following example adds the following remark to an IP extended ACL numbered 102: this acl is to filter the host 192.168.4.12.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip access-list extended 102
Hostname(config-ext-nacl)# list-remark this acl is to filter the host
192.168.4.12
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- expert access-list advanced
- expert access-list extended
- ip access-list
- ipv6 access-list
- mac access-list extended

1.28 mac access-group

Function

Run the **mac access-group** command to apply a MAC extended ACL.

Run the **no** form of this command to cancel the application.

Run the **default** form of this command to restore the default configuration.

No MAC extended ACL is applied by default.

Syntax

mac access-group { *acl-name* | *acl-number* } { **in** | **out** } [**control-plan** | **counter-only** | **forward-control-plane** | **forward-plane**]

no mac access-group { *acl-name* | *acl-number* } { **in** | **out** } [**control-plan** | **counter-only** | **forward-control-plane** | **forward-plane**]

default mac access-group { *acl-name* | *acl-number* } { **in** | **out** } [**control-plan** | **counter-only** | **forward-control-plane** | **forward-plane**]

Parameter Description

acl-name: Name of a MAC extended ACL. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of a MAC extended ACL. The value range is from 700 to 799.

in: Filters the incoming packets of a port.

out: Filters the outgoing packets of a port.

counter-only: Configures a special ACL for packet counting on a port.

control-plane: Configures a control plane ACL.

forward-control-plane: Configures a control and forwarding plane ACL.

forward-plane: Configures a forwarding plane ACL.

Command Modes

Global configuration mode

Interface configuration mode

SVI interface configuration mode

Default Level

14

Usage Guidelines

To make a MAC extended ACL take effect, run this command to apply the ACL in global configuration mode, interface configuration mode, or SVI interface configuration mode. The ACL controls the incoming/outgoing Ethernet packets of all ports, a specified SVI, or a specified port. The **counter-only** option is not supported in global configuration mode. The **mac access-group** { *acl-name* | *acl-number* } { **in** | **out** } **counter-only** command configured on a port collects statistics on packets only, without filtering them.

Examples

The following example applies the MAC extended ACL named accept_00d0f8xxxxxx_only to the inbound direction of the L3 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# mac access-group
accept_00d0f8xxxxxx_only in
```

The following example applies an ACL numbered 700 to the inbound direction of the L3 Ethernet interface GigabitEthernet0/1 and collects statistics on the incoming packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# mac access-group 700 in counter-only
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- mac access-list extended

1.29 mac access-list counter

Function

Run the **mac access-list counter** command to enable the packet matching counting function of a MAC extended ACL.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The packet matching counting function of a MAC extended ACL is disabled by default.

Syntax

mac access-list counter { *acl-name* | *acl-number* }

no mac access-list counter { *acl-name* | *acl-number* }

default mac access-list counter { *acl-name* | *acl-number* }

Parameter Description

acl-name: Name of a MAC extended ACL. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of a MAC extended ACL. The value range is from 700 to 799.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can run this command to enable the packet matching counting function to know the filtering situation of L2 packets.

Examples

The following example enables the packet matching counting function of a MAC extended ACL named mac-acl.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# mac access-list counter mac-acl
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.30 mac access-list extended

Function

Run the **mac access-list extended** command to configure a MAC extended ACL.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No MAC extended ACL is configured by default.

Syntax

mac access-list extended { *acl-name* | *acl-number* }

no mac access-list extended { *acl-name* | *acl-number* }

default mac access-list extended { *acl-name* | *acl-number* }

Parameter Description

acl-name: Name of a MAC extended ACL. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of a MAC extended ACL. The value range is from 700 to 799.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To filter L2 packets in the network, run this command to create a MAC extended ACL.

Examples

The following example configures a MAC extended ACL named mac-acl.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# mac access-list extended mac-acl
Hostname(config-mac-nacl)#
```

The following example configures a MAC extended ACL numbered 704.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# mac access-list extended 704
Hostname(config-mac-nacl)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- mac access-group

1.31 mac access-list resequence

Function

Run the **mac access-list resequence** command to configure the start value and step of rule sequence numbers in a MAC extended ACL.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

The default start value and step of rule sequence numbers in a MAC extended ACL are both **10**.

Syntax

mac access-list resequence { *acl-name* | *acl-number* } *start-value step-value*

no mac access-list resequence { *acl-name* | *acl-number* }

default mac access-list resequence { *acl-name* | *acl-number* }

Parameter Description

acl-name: Name of a MAC extended ACL. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of a MAC extended ACL. The value range is from 700 to 799.

start-value: Start value of rule sequence numbers. The value range is from 1 to 2147483647.

step-value: Step of rule sequence numbers. The value range is from 1 to 2147483647.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To insert a new rule into a MAC extended ACL, run this command to rearrange the sequence numbers of ACL rules.

Examples

The following example configures a MAC extended ACL named mac-acl, sets the start value of rule sequence numbers to 21 and step to 43.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# mac access-list resequence mac-acl 21 43
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.32 permit

Function

Run the **permit** command to add a rule of permit type to an ACL.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

There is no rule of permit type in an ACL by default.

Syntax

The commands for adding/deleting a rule of permit type to/from ACLs of different types are as follows:

- IP standard ACL

  Add a rule of permit type to an IP standard ACL.

  [*sequence-number*] **permit** { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } [**time-range** *time-range-name*] [**log**]

  Delete a rule of permit type from an IP standard ACL.

  no { *sequence-number* | { **permit** { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } [**time-range** *time-range-name*] [**log**] } }

- IP extended ACL

  Add a rule of permit type to an IP extended ACL.

  [*sequence-number*] **permit** *protocol* { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**time-range** *time-range-name*] [**log**]

  Delete a rule of permit type from an IP extended ACL.

  no { *sequence-number* | { **permit** *protocol* { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**time-range** *time-range-name*] [**log**] } }

Note

The commands for adding a rule of permit type to IP extended ACLs that specify some important protocols in the protocol field are as follows:

The ICMP field is selected.

[*sequence-number*] **permit icmp** { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**time-range** *time-range-name*] [**log**]

The TCP field is selected.

[*sequence-number*] **permit tcp** { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag* | **established**] [**log**]

The UDP field is selected.

[*sequence-number*] **permit udp** { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] [**time-range** *time-range-name*] [**log**]

- MAC extended ACL

  Add a rule of permit type to a MAC extended ACL.

  [*sequence-number*] **permit** { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [*ethernet-type*] [**cos** [*cos-value*] [**inner** *cos-value*]] [**time-range** *time-range-name*]

  Delete a rule of permit type from a MAC extended ACL.

  no { *sequence-number* | { **permit** { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [*ethernet-type*] [**cos** [*cos-value*] [**inner** *cos-value*]] [**time-range** *time-range-name*] } }

- Expert extended ACL

  Add a rule of permit type to an expert extended ACL.

  [*sequence-number*] **permit** [*protocol* | [*ethernet-type*] [**cos** [*cos-value*] [**inner** *cos-value*]]] [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source*-mac-*address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**time-range** *time-range-name*]

  Delete a rule of permit type from an expert extended ACL.

  no { *sequence-number* | { **permit** [*protocol* | [*ethernet-type*] [**cos** [*cos-value*] [**inner** *cos-value*]]] [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source*-mac-*address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**time-range** *time-range-name*] } }

  The Ethernet type or **cos** field is selected.

[*sequence-number*] **permit** { [*ethernet-type*] [**cos** [*cos-value*] [**inner** *cos-value*]] } [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [**time-range** *time-range-name*]

Note

The commands for adding a rule of permit type to expert extended ACLs that specify some important protocols in the protocol field are as follows:

The ICMP field is selected.

[*sequence-number*] **permit icmp** [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**time-range** *time-range-name*]

The TCP field is selected.

[*sequence-number*] **permit tcp** [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag* | **established**]

The UDP field is selected.

[*sequence-number*] **permit udp** [**VID** [*vlan-id*] [**inner** *vlan-id*]] { *source-ipv4-address source-*ipv4-*wildcard* | **host** *source-ipv4-address* | **any** } { *source-mac-address source-mac-wildcard* | **host** *source-mac-address* | **any** } [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] { *destination-ipv4-address destination-ipv4-wildcard* | **host** *destination-ipv4-address* | **any** } { *destination-mac-address destination-mac-wildcard* | **host** *destination-mac-address* | **any** } [[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]] [**fragment**] [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] [**time-range** *time-range-name*]

- Expert advanced ACL

  Add a rule of permit type to an expert advanced ACL.

  [*sequence-number*] **permit** *hex hex-mask offset*

  Delete a rule of permit type from an expert advanced ACL.

  no { *sequence-number* | **permit** *hex hex-mask offset* }

- IPv6 extended ACL

  Add a rule of permit type to an IPv6 extended ACL.

  [*sequence-number*] **permit** [*protocol* { *source-ipv6-prefix* / *prefix-length* | *source-ipv6-address source-ipv6-mask* | **host** *source-ipv6-address* | **any** } { *destination-ipv6-prefix* / *prefix-length* | *destination-ipv6-address destination-ipv6-mask* | **host** *destination-ipv6-address* | **any** }] [**cos** *cos-value* [**inner** *cos-*

value]] [{ **any** | **host** *source-mac-address* | *source-mac-address source-mac-wildcard* } { **any** | **host** *destination–mac-address* | *destination-mac-address destination-mac-wildcard* }] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**VID** [*vlan-id*] [**inner** *vlan-id*]] [**time-range** *time-range-name*] [**log**]

Delete a rule of permit type from an IPv6 extended ACL.

no { *sequence-number* | { **permit** [*protocol* { *source-ipv6-prefix* / *prefix-length* | *source-ipv6-address source-ipv6-mask* | **host** *source-ipv6-address* | **any** } { *destination-ipv6-prefix* / *prefix-length* | *destination-ipv6-address destination-ipv6-mask* | **host** *destination-ipv6-address* | **any** }] [**cos** *cos-value* [**inner** *cos-value*]] [{ **any** | **host** *source-mac-address* | *source-mac-address source-mac-wildcard* } { **any** | **host** *destination–mac-address* | *destination–mac-address destination-mac-wildcard* }] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**VID** [*vlan-id*] [**inner** *vlan-id*]] [**time-range** *time-range-name*] [**log**] } }

Note

The commands for adding a rule of permit type to IPv6 extended ACLs that specify some important protocols in the protocol field are as follows:

The ICMP field is selected.

[*sequence-number*] **permit icmp** { *source-ipv6-prefix* / *prefix-length* | *source-ipv6-address source-ipv6-mask* | **host** *source-ipv6-address* | **any** } { *destination-ipv6-prefix* / *prefix-length* | *destination-ipv6-address destination-ipv6-mask* | **host** *destination-ipv6-address* | **any** } [{ **any** | **host** *source-mac-address* | *source-mac-address source-mac-wildcard* } { **any** | **host** *destination–mac-address* | *destination–mac-address destination-mac-wildcard* }] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**VID** [*vlan-id*] [**inner** *vlan-id*]] [**time-range** *time-range-name*] [**log**]

The TCP field is selected.

[*sequence-number*] **permit tcp** { *source-ipv6-prefix* / *prefix-length* | *source-ipv6-address source-ipv6-mask* | **host** *source-ipv6-address* | **any** } [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] { *destination-ipv6-prefix* / *prefix-length* | *destination-ipv6-address destination-ipv6-mask* | **host** *destination-ipv6-address* | **any** } [{ **any** | **host** *source-mac-address* | *source-mac-address source-mac-wildcard* } { **any** | **host** *destination–mac-address* | *destination–mac-address destination-mac-wildcard* }] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**VID** [*vlan-id*] [**inner** *vlan-id*]] [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag* | **established**] [**log**]

The UDP field is selected.

[*sequence-number*] **permit udp** { *source-ipv6-prefix* / *prefix-length* | *source-ipv6-address source-ipv6-mask* | **host** *source-ipv6-address* | **any** } [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] { *destination-ipv6-prefix* / *prefix-length* | *destination-ipv6-address destination-ipv6-mask* | **host** *destination-ipv6-address* | **any** } [{ **any** | **host** *source-mac-address* | *source-mac-address source-mac-wildcard* } { **any** | **host** *destination–mac-address* | *destination–mac-address destination-mac-wildcard* }] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**VID** [*vlan-id*] [**inner** *vlan-id*]] [**eq** *port* | **gt** *port* | **lt** *port* | **neq** *port* | **range** *lower upper*] [**time-range** *time-range-name*] [**log**]

Parameter Description

sequence-number: Sequence number of an ACL rule. The value range is from 1 to 2147483647.

permit: Configures the processing action for an ACL rule. If packets match this rule, the packets are permitted.

source-ipv4-address: Source IP address (host address or network address) for packet matching.

source-ipv4-wildcard: Source IP address wildcard mask, which is used to match the source IP addresses of multiple hosts. The wildcard masks can be discontinuous, for example, 0.255.0.32.

protocol: IP protocol number for matching. The value range is from 0 to 255. Some important protocol names such as *icmp*, *ip*, *ipv6*, *tcp, and udp* are listed separately.

destination-ipv4-address: Destination IP address (host address or network address) for packet matching.

destination-ipv4-wildcard: Destination IP address wildcard mask, which is used to match the destination IP addresses of multiple hosts. The wildcard masks can be discontinuous, for example, 0.255.0.32.

fragment: Matches the non-first fragment in the default fragmented packet matching mode.

precedence *precedence*: Matches the precedence value of packets. The value range is from 0 to 7. Some important precedence names such as *routine*, *priority*, *immediate*, *flash*, *flash-override*, *critical*, *internet*, and *network* are listed separately.

eq *port*: Matches packets with the L4 port ID equal to the specified value. The value range is from 0 to 65535.

gt *port*: Matches packets with the L4 port ID greater than the specified value. The value range is from 0 to 65535.

lt *port*: Matches packets with the L4 port ID less than the specified value. The value range is from 0 to 65535.

neq *port*: Matches packets with the L4 port ID not equal to the specified value. The value range is from 0 to 65535.

range: Matches the range of L4 port IDs of packets.

lower: Lower limit of the L4 port ID range for matching. The value range is from 0 to 65535.

upper: Upper limit of the L4 port ID range for matching. The value range is from 0 to 65535.

time-range *time-range-name*: Configures the name of the time range for packet filtering.

tos *tos*: Matches the ToS value of packets. The value range is from 0 to 15. Some important service type names such as *max-reliability*, *max-throughput*, *min-delay*, *min-monetary-cost*, and *normal* are listed separately.

dscp *dscp*: Matches the DSCP value of packets. The value range is from 0 to 63. Some important differentiated service names such as *default*, *ef*, *af11*, and *cs1* are listed separately.

icmp-type: Message type for matching ICMP packets. The value range is from 0 to 255.

icmp-code: Message type code for matching ICMP packets. The value range is from 0 to 255.

icmp-message: Message type name for matching ICMP packets.

source-mac-address: MAC address of the source host for matching.

source-mac-wildcard: MAC address wildcard of the source host, which is used to match the source MAC addresses of multiple hosts.

destination-mac-address: MAC address of the destination host for matching.

destination-mac-wildcard: MAC address wildcard of the destination host, which is used to match the destination MAC addresses of multiple hosts.

cos *cos-value*: Matches the priority field value in the outer tag in the L2 packets. The value range is from 0 to 7.

inner *cos-value*: Matches the priority field value in the inner tag in the L2 packets. The value range is from 0 to 7.

VID *vlan-id*: Matches the VLAN ID. The value range is from 1 to 4094.

inner *vlan-id*: Matches the inner VLAN ID. The value range is from 1 to 4094.

ethernet-type: Matches the Ethernet protocol type. The value range is from 0x0000 to 0xFFFF. Some important Ethernet protocol type names such as *arp*, *aarp*, and *IPX* are listed separately.

match-all *tcp-flag*: Matches all the bits of the TCP flag.

established: Matches only the RST or ACK bit in the TCP flag, not the other bits.

source-ipv6-prefix: Source IPv6 network address or network type for matching.

destination-ipv6-prefix: Destination IPv6 network address or network type for matching.

prefix-length: IPv6 address mask length for matching.

source-ipv6-address: Source IPv6 address for matching.

destination-ipv6-address: Destination IPv6 address for matching.

source-ipv6-mask: Source IPv6 address mask for matching.

destination-ipv6-mask: Destination IPv6 address mask for matching.

flow-label *flow-label*: Matches the flow label value. The value range is from 0 to 1048575.

hex: Matching field in hexadecimal notation. It is used when expert advanced ACL rules are configured.

hex-mask: Matching field masks in hexadecimal notation. It is used when expert advanced ACL rules are configured.

offset: Matching start position, in bytes. It is used when expert advanced ACL rules are configured. The value range is from 0 to 79.

hex hex-mask offset: Combination of *hex, hex-mask*, and *offset*. Multiple such combinations can be configured.

Command Modes

ACL configuration mode

Default Level

14

Usage Guidelines

To permit some packets to enter a network, you can run this command to add rules of permit type to an ACL.

Examples

The following example creates an IP standard ACL and adds a rule: Permit packets sent from the source host with the IP address 192.168.4.12.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip access-list standard std-acl
Hostname(config-std-nacl)# permit host 192.168.4.12
```

The following example creates an IP extended ACL and adds a rule: Permit the services provided by the source host with the IP address 192.168.4.12 through TCP port 100.

```
Hostname# configure terminal
Hostname(config)# ip access-list extended 102
Hostname(config-ext-nacl)# permit tcp host 192.168.4.12 eq 100 any
```

The following example creates an expert extended ACL and adds a rule: Permit all the TCP packets with the source IP address 192.168.4.12 and the source MAC address 0013.0049.8272.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# expert access-list extended exp-acl
Hostname(config-exp-nacl)# permit tcp host 192.168.4.12 host 0013.0049.8272 any
any
Hostname(config-exp-nacl)# deny any any any any
```

The following example creates a MAC extended ACL and adds a rule: Permit the Ethernet frames of the AARP protocol type sent from the source host with the MAC address 0013.0049.8272.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# mac access-list extended 702
Hostname(config-mac-nacl)# permit host 0013.0049.8272 any aarp
```

The following example creates an IPv6 extended ACL and adds a rule numbered 11: Permit packets sent from the source host with the IP address 2000::1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 access-list v6-acl
Hostname(config-ipv6-nacl)# 11 permit ipv6 host 2000::1 any
```

The following example creates an expert advanced ACL and adds a rule: Permit packets sent from the source host with the IP address 192.168.4.12.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# expert access-list advanced adv-acl
Hostname(config-exp-dacl)# permit c0a8040c ffffffff 38
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- expert access-list extended
- ip access-list
- ip access-group
- mac access-list extended
- mac access-group
- ipv6 access-list

- ipv6 traffic-filter

1.33 redirect destination interface

Function

Run the **redirect destination interface** command to configure an ACL redirection port.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No ACL redirection port is configured by default.

Syntax

redirect destination interface *interface-type interface-number* **acl** { *acl-name* | *acl-number* } **in**

no redirect destination interface *interface-type interface-number* **acl** { *acl-name* | *acl-number* } **in**

default redirect destination interface *interface-type interface-number* **acl** { *acl-name* | *acl-number* } **in**

Parameter Description

interface *interface-type interface-number*: Interface type and number.

acl-name: ACL name. The value is a case-sensitive string of 1 to 99 characters.

acl-number: ACL number.

in: Redirects the incoming packets of a port.

Command Modes

L3 Ethernet interface configuration mode

Default Level

14

Usage Guidelines

You can configure a redirect ACL on a port to redirect the incoming packets of the port that match the ACL rules to a specified port. For example, when you need to monitor the running status of an ACL, run this command.

Examples

The following example redirects the incoming packets from the L3 Ethernet interface GigabitEthernet 0/3 that match the rule acl1 to the L3 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/3
Hostname(config-if-GigabitEthernet 0/3)# redirect destination interface
gigabitethernet 0/1 acl acl1 in
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.34 remark

Function

Run the **remark** command to add a remark to an ACL rule.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No remark is added to an ACL rule by default.

Syntax

[*sequence-number*] **remark** *text*

no [*sequence-number*] **remark** *text*

default [*sequence-number*] **remark** *text*

Parameter Description

sequence-number: Sequence number of an ACL rule, to which a remark needs to be added. The value range is from 1 to 2147483647.

remark *text*: Configures a remark for an ACL rule. The value is a case-sensitive string of 1 to 100 characters.

Command Modes

ACL configuration mode

Default Level

14

Usage Guidelines

Two content remarks are forbidden in an ACL rule.

Deleting an ACL rule will delete the rule and its remark.

If the *sequence-number* parameter is specified, the remark is added to the specified ACL rule; if the *sequence-number* parameter is not specified, the remark is added to the last ACL rule.

Examples

The following example adds a remark to an ACL rule in an IP extended ACL numbered 102.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip access-list extended 102
```

```
Hostname(config-ext-nacl)# permit tcp 1.1.1.1 0.0.0.0 2.2.2.2 0.0.0.0
Hostname(config-ext-nacl)# remark first_remark
Hostname(config-ext-nacl)# permit tcp 3.3.3.3 0.0.0.0 4.4.4.4 0.0.0.0
Hostname(config-ext-nacl)# remark second_remark
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- expert access-list extended
- ip access-list
- ip access-group
- mac access-list extended
- mac access-group
- ipv6 access-list
- ipv6 traffic-filter

1.35 security access-group

Function

Run the **security access-group** command to configure a security channel for a port.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No security channel is configured for a port by default.

Syntax

security access-group { *acl-name* | *acl-number* }

no security access-group

default security access-group

Parameter Description

acl-name: ACL name. The value is a case-sensitive string of 1 to 99 characters.

acl-number: ACL number. The following value ranges are supported:

IP standard ACLs: 1 to 99 or 1300 to 1999; IP extended ACLs: 100 to 199 or 2000 to 2699; MAC extended ACLs: 700 to 799; expert extended ACLs: 2700 to 2899.

Command Modes

L3 Ethernet interface configuration mode

Default Level

14

Usage Guidelines

When the authentication function is configured on a device, such as IEEE 802.1x or Web authentication, users must pass the authentication before accessing the external network. To enable users connected to a port to access the external network without undergoing authentication, run this command to configure a security channel.

Examples

The following example configures the ACL numbered 1 as a security channel on the L3 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# security access-group 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.36 security global access-group

Function

Run the **security global access-group** command to configure a global security channel.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No global security channel is configured by default.

Syntax

security global access-group { *acl-name* | *acl-number* }

no security global access-group

default security global access-group

Parameter Description

acl-name: ACL name. The value is a case-sensitive string of 1 to 99 characters.

acl-number: ACL number. The following value ranges are supported:

IP standard ACLs: 1 to 99 or 1300 to 1999; IP extended ACLs: 100 to 199 or 2000 to 2699; MAC extended ACLs: 700 to 799; expert extended ACLs: 2700 to 2899.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When the authentication function is configured on a device, such as IEEE 802.1x or Web authentication, users must pass the authentication before accessing the external network. To enable users connected to different ports to access the external network without undergoing authentication, run this command to configure a global security channel.

Examples

The following example configures the ACL numbered 1 as a global security channel.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# security global access-group 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.37 security uplink enable

Function

Run the **security uplink enable** command to configure an excluded port of a global security channel.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No excluded port is configured for a global security channel by default.

Syntax

security uplink enable

no security uplink enable

default security uplink enable

Parameter Description

N/A

Command Modes

L3 Ethernet interface configuration mode

Default Level

14

Usage Guidelines

The global security channel takes effect on all the ports. To disable the global security channel on some ports, configure these ports as excluded ports of the global security channel.

Examples

The following example configures the L3 Ethernet interface GigabitEthernet 0/1 as an excluded port of a global security channel.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# security uplink enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.38 show access-group

Function

Run the **show access-group** command to display the ACL configuration applied to a port.

Syntax

show access-group [**interface** { *interface-type interface-number* | **vlan** *vlan-id* }]

Parameter Description

interface *interface-type interface-number*: Specifies the interface type and number.

vlan *vlan-id*: Displays the ACL configuration applied to a specified VLAN port. The value range is from 1 to 4094.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

To check whether an ACL is applied to a specified port or to find out the ports that have ACLs applied, run this command. If the parameter **interface** is not specified, ACLs applied to all ports are displayed.

Examples

The following example displays information about the ACL applied to a port of the device.

```
Hostname> enable
Hostname# show access-group
ip access-list standard ipstd3 in
Applied On interface GigabitEthernet 0/1.
ip access-list standard ipstd4 out
Applied On interface GigabitEthernet 0/1.
ip access-list extended 101 in
Applied On interface GigabitEthernet 0/3.
ip access-list extended 102 in
Applied On interface GigabitEthernet 0/8.
ipv6 traffic-filter vlan_in in
ipv6 traffic-filter vlan_out out
Applied On vlan 1
```

Table 1-1Output Fields of the show access-group Command

Field	Description
in	Applied to the inbound direction of a port.
out	Applied to the outbound direction of a port.
Applied On interface X	Applied to interface X.

The following example displays information about the ACL applied to the port GigabitEthernet 0/3.

```
Hostname> enable
Hostname# show access-group interface gigabitethernet 0/3
ip access-list extended 101
Applied On interface GigabitEthernet 0/3 in.
```

Table 1-2Output Fields of the show access-group interface Command

Field	Description
in	Applied to the inbound direction of a port.
out	Applied to the outbound direction of a port.
Applied On interface X	Applied to interface X.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.39 show access-lists

Function

Run the **show access-lists** command to display the configuration of all ACLs or a specified ACL.

Syntax

show access-lists [*acl-name* | *acl-number*] [**summary**]

Parameter Description

acl-name: Name of an IP standard ACL or IP extended ACL. The value is a case-sensitive string of 1 to 99 characters.

acl-number: ACL number. IP standard ACLs: 1 to 99 or 1300 to 1999; IP extended ACLs: 100 to 199 or 2000 to 2699; MAC extended ACLs: 700 to 799; expert extended ACLs: 2700 to 2899.

summary: Displays the summary of an ACL.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the configuration of a specified ACL. If no ACL number or name is specified, the configuration of all ACLs is displayed.

Examples

The following example displays the configuration of the ACL named n_acl.

```
Hostname> enable
Hostname# show access-lists n_acl
ip access-list standard n_acl
```

The following example displays the configuration of the ACL numbered 102.

```
Hostname# show access-lists 102
ip access-list extended 102
```

The following example displays the configuration of all the ACLs.

```
Hostname> enable
Hostname# show access-lists
ip access-list standard n_acl
ip access-list extended 101
permit icmp host 192.168.1.1 any log (1080 matches)
  permit tcp host 1.1.1.1 any established
  deny ip any any (80021 matches)
mac access-list extended mac-acl
expert access-list extended exp-acl
ipv6 access-list extended v6-acl
petmit ipv6 ::192.168.4.12 any (100 matches)
deny any any (9 matches)
```

Table 1-1Output Fields of the show access-lists Command

Field	Description
ip access-list standard	IP standard ACL.
ip access-list extended	IP extended ACL.
mac access-list extended	MAC extended ACL.
expert access-list extened	Expert extended ACL.
ipv6 access-list extended	IPv6 extended ACL.
permit	Rule of permit type.
deny	Rule of deny type.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.40 show acl res

Function

Run the **show acl res** command to display information about all or a specified TCAM.

Syntax

show acl res [**dev** *dev-number* [**slot** *slot-number*]]

Parameter Description

dev *dev-number*: Displays the TCAM information of a specified device number.

slot *slot-number*: Displays the TCAM information of a specified slot number.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the TCAM information of a specified device slot. If no slot number of a device is specified, the TCAM information of all the slots in the device is displayed. If no device number is specified, the TCAM information of all devices is displayed.

Examples

The following example displays the TCAM resources used, usage, and number of remaining entries on all devices.

```
Hostname> enable
Hostname# show acl res
acl usage warn limit: 100%
type            total           used            free            usage
------------    --------        --------        --------        --------
##Dev=1,Slot=0,unit=0 ACL RES
VFP ACL         256             0               256             0%
    slice0      256             0               256             0%
IFP ACL         8000            14              7986            1%
    slice0      2000            14              1986            0%
    slice1      2000            0               2000            0%
    slice2      2000            0               2000            0%
    slice3      2000            0               2000            0%
EFP ACL         1500            0               1500            0%
    slice0      500             0               500             0%
    slice1      500             0               500             0%
    slice2      500             0               500             0%
##Dev=1,Slot=0,unit=0 TOP3
IFP ACL      time:2020/09/25 19:58:35: used=82
```

```
IFP ACL      time:2020/09/25 20:00:05: used=83
IFP ACL      time:2020/09/25 23:45:25: used=84
EFP ACL      time:2020/09/26 12:35:47: used=4
```

Table 1-1Output Fields of the show acl res dev Command

Field	Description
type	ACL installation stage and slice.
total	Total number of ACLs that can be installed.
used	Number of installed ACLs.
free	Number of remaining ACLs that can be installed.
usage	Usage

The following example displays the TCAM resource used, usage, and number of remaining entries in all slots in device 1.

```
Hostname> enable
Hostname# show acl res dev 1
acl usage warn limit: 100%
type            total           used            free            usage
------------    --------        --------        --------        --------
##Dev=1,Slot=0,unit=0 ACL RES
VFP ACL         256             0               256             0%
    slice0      256             0               256             0%
IFP ACL         8000            14              7986            1%
    slice0      2000            14              1986            0%
    slice1      2000            0               2000            0%
    slice2      2000            0               2000            0%
    slice3      2000            0               2000            0%
EFP ACL         1500            0               1500            0%
    slice0      500             0               500             0%
    slice1      500             0               500             0%
    slice2      500             0               500             0%
##Dev=1,Slot=0,unit=0 TOP3
IFP ACL      time:2020/09/25 19:58:35: used=82
IFP ACL      time:2020/09/25 20:00:05: used=83
IFP ACL      time:2020/09/25 23:45:25: used=84
EFP ACL      time:2020/09/26 12:35:47: used=4
```

Table 1-2Output Fields of the show acl res dev Command

Field	Description
type	ACL installation stage and slice.

Field	Description
total	Total number of ACLs that can be installed.
used	Number of installed ACLs.
free	Number of remaining ACLs that can be installed.
usage	Usage

Notifications

For the products that share the inter-stage TCAM resources, the displayed resource occupancy at the stages is consistent.

Platform Description

N/A

Related Commands

N/A

1.41 show acl res detail

Function

Run the **show acl res detail** command to display detailed usage information of all or a specified TCAM.

Syntax

show acl res detail [**dev** *dev-number* [**slot** *slot-number*]]

Parameter Description

dev *dev-number*: Displays the detailed usage information of TCAMs in a specified device.

slot *slot-number*: Displays the detailed usage information of the TCAM in a specified slot.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the detailed usage information of the TCAM in a specified device slot. If no slot number of a device is specified, the detailed usage information of TCAMs in all the slots of the device is displayed. If no device number is specified, the detailed usage information of TCAMs in all devices is displayed.

Examples

The following example displays the detailed resource usage of TCAMs in all devices.

```
Hostname> enable
Hostname# show acl res detail
Dev: 1           Slot: 0         unit: 0                stage: IFP
group id: 2      group pri: 2    total entry: 2000      used entry: 2
width: SINGLE    slice id: 1
app type                         used entry
--------                         ----------
SECURITY-ACL                     2

group id: 1      group pri: 1    total entry: 2000      used entry: 14
width: SINGLE    slice id: 0
app type                         used entry
--------                         ----------
CPP                              14
```

Table 1-1Output Fields of the show acl res detail Command

Field	Description
group_id	Group ID.
group_pri	Group priority.
total_entry	Number of ACL entries that can be installed.
used_entry	Number of installed ACL entries.
width	Template width.
slice_id	Occupied slice ID.
app_type	Application type.

The following example displays the detailed resource usage of TCAMs in all slots of device 1.

```
Hostname> enable
Hostname# show acl res detail dev 1
Dev: 1           Slot: 0         unit: 0                stage: IFP
group id: 2      group pri: 2    total entry: 2000      used entry: 2
width: SINGLE    slice id: 1
app type                         used entry
--------                         ----------
SECURITY-ACL                     2

group id: 1      group pri: 1    total entry: 2000      used entry: 14
width: SINGLE    slice id: 0
app type                         used entry
--------                         ----------
CPP                              14
```

Table 1-2Output Fields of the show acl res detail dev Command

Field	Description
group_id	Group ID.
group_pri	Group priority.
total_entry	Number of ACL entries that can be installed.
used_entry	Number of installed ACL entries.
width	Template width.
slice_id	Occupied slice ID.
app_type	Application type.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.42 show expert access-group

Function

Run the **show expert access-group** command to display the configuration of an expert extended ACL applied to a port.

Syntax

show expert access-group [**interface** { *interface-type interface-number* | **vlan** *vlan-id* }]

Parameter Description

interface *interface-type interface-number*: Specifies the interface type and number.

vlan *vlan-id*: Displays the ACL configuration applied to a specified VLAN port. The value range is from 1 to 4094.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the expert ACL applied to a port. If the parameter **interface** is not specified, the expert ACLs applied to all ports are displayed.

Examples

The following example displays information about the expert extended ACL applied to the L3 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show expert access-group interface gigabitethernet 0/1
expert access-group ee in
Applied On interface GigabitEthernet 0/1.
```

Table 1-1Output Fields of the show expert access-group Command

Field	Description
in	Applied to the inbound direction of a port.
Applied On interface X	Applied to interface X.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.43 show ip access-group

Function

Run the **show ip access-group** command to display the configuration of IP standard and IP extended ACLs applied to a port.

Syntax

show ip access-group [**interface** { *interface-type interface-number* | **vlan** *vlan-id* }]

Parameter Description

interface *interface-type interface-number*: Specifies the interface type and number.

vlan *vlan-id*: Displays the ACL configuration applied to a specified VLAN port. The value range is from 1 to 4094.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the IP standard and IP extended ACLs applied to a port. If the parameter **interface** is not specified, the IP standard and IP extended ACLs applied to all ports are displayed.

Examples

The following example displays information about the IP standard and IP extended ACLs applied to the L3 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show ip access-group interface gigabitethernet 0/1
ip access-group aaa in
Applied On interface GigabitEthernet 0/1.
```

Table 1-1Output Fields of the show ip access-group Command

Field	Description
in	Applied to the inbound direction of a port.
Applied On interface X	Applied to interface X.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.44 show ipv6 traffic-filter

Function

Run the **show ipv6 traffic-filter** command to display the configuration of the IPv6 ACL applied to a port.

Syntax

show ipv6 traffic-filter [**interface** { *interface-type interface-number* | **vlan** *vlan-id* }]

Parameter Description

interface *interface-type interface-number*: Specifies the interface type and number.

vlan *vlan-id*: Displays the ACL configuration applied to a specified VLAN port. The value range is from 1 to 4094.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the IPv6 ACL applied to a port. If the parameter **interface** is not specified, the IPv6 ACLs applied to all ports are displayed.

Examples

The following example displays information about the IPv6 ACL applied to the L3 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show ipv6 traffic-filter interface gigabitethernet 0/1
ipv6 traffic-filter v6 in
Applied On interface GigabitEthernet 0/1.
```

Table 1-1 Output Fields of the show ipv6 traffic-filter Command

Field	Description
in	Applied to the inbound direction of a port.
Applied On interface X	Applied to interface X.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.45 show mac access-group

Function

Run the **show mac access-group** command to display the MAC extended ACL applied to a port.

Syntax

show mac access-group [**interface** { *interface-type interface-number* | **vlan** *vlan-id* }]

Parameter Description

interface *interface-type interface-number*: Specifies the interface type and number.

vlan *vlan-id*: Displays the ACL configuration applied to a specified VLAN port. The value range is from 1 to 4094.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the MAC extended ACL applied to a port. If the parameter **interface** is not specified, the MAC extended ACLs applied to all ports are displayed.

Examples

The following example displays information about the MAC extended ACL applied to the L3 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show mac access-group interface gigabitethernet 0/1
mac access-group mm in
Applied On interface GigabitEthernet 0/1.
```

Table 1-1Output Fields of the show mac access-group Command

Field	Description
in	Applied to the inbound direction of a port.
Applied On interface X	Applied to interface X.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.46 show redirect

Function

Run the **show redirect** command to display the redirect ACL configuration.

Syntax

show redirect [**interface** { *interface-type interface-number* | **vlan** *vlan-id* }]

Parameter Description

interface *interface-type interface-number*: Specifies the interface type and number.

vlan *vlan-id*: Displays the ACL configuration applied to a specified VLAN port. The value range is from 1 to 4094.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the redirect ACL configuration. If the parameter **interface** is not specified, information about the redirect ACLs configured on all the ports is displayed.

Examples

The following example displays information about the redirect ACL configured on the L3 Ethernet interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show redirect interface gigabitethernet 0/1
acl redirect configuration on interface Gigabitethernet 0/1
redirect destination interface Gigabitethernet 0/1 acl 1 in
```

Table 1-1Output Fields of the show redirect Command

Field	Description
in	Applied to the inbound direction of a port.
redirect destination interface	Destination interface for redirection.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.47 show svi router-acls state

Function

Run the **show svi router-acls state** command to check whether an ACL applied to an SVI takes effect on L2 and L3 packets.

Syntax

show svi router-acls state

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to check whether an ACL applied to an SVI takes effect on L2 and L3 packets.

Examples

The following example checks whether an ACL applied to an SVI takes effect on L2 and L3 packets.

```
Hostname> enable
Hostname# show svi router-acls state
------------svi router acls state------------
VLAN 2 IN (ip standard 1)
                     L2:enable      L3:enable
```

Table 1-1 Output Fields of the show svi router-acls state Command

Field	Description
IN	Applied to the inbound direction of a port.
L2	Whether it takes effect on L2 packets.
L3	Whether it takes effect on L3 packets.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.48 svi router-acls enable

Function

Run the **svi router-acls enable** command to enable the function of making an ACL applied to an SVI effective only for L3 forwarded packets.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The function of making an ACL applied to an SVI effective only for L3 forwarded packets is disabled by default. Namely, the ACL applied to an SVI is effective for both L2 and L3 forwarded packets.

Syntax

svi router-acls enable

no svi router-acls enable

default svi router-acls enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The ACL applied to an SVI is effective for both L2 and L3 forwarded packets by default. To make the ACL applied to an SVI effective only for the L3 forwarded packets, run this command. This command affects only the ACL applied to an SVI.

Examples

The following example enables the function of making the ACL applied to an SVI effective only for L3 forwarded packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# svi router-acls enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- show svi router-acls state