Contents

ACL commands

acl

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

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

Syntax

Command set 1:

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

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

Command set 2:

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

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

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

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

Default

No ACLs exist.

Views

System view

Predefined user roles

network-admin

Parameters

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

basic: Specifies the basic ACL type.

advanced: Specifies the advanced ACL type.

mac: Specifies the Layer 2 ACL type.

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

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

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

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

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

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

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

all: Specifies all ACLs of the specified type.

Usage guidelines

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

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

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

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

If you create a named ACL by using the **acl** { [**ipv6**] { **advanced** | **basic** } | **mac** } **name** *acl-name* command, you can enter the view of the ACL by using the following commands:

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

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

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

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

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

Examples

# Create IPv4 basic ACL 2000 and enter its view.

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

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

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

# Create IPv4 advanced ACL 3000 and enter its view.

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

# Create IPv6 basic ACL 2000 and enter its view.

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

```
[Sysname-acl-ipv6-basic-2000]
```

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

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

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

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

# Create Layer 2 ACL 4000 and enter its view.

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

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

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

Related commands

display acl

acl copy

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

Syntax

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

Views

System view

Predefined user roles

network-admin

Parameters

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

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

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

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

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

- 2000 to 2999 for basic ACLs.

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

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

Usage guidelines

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

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

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

Examples

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

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

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

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

acl logging interval

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

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

Syntax

acl logging interval *interval*

undo acl logging interval

Default

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

Views

System view

Predefined user roles

network-admin

Parameters

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

Usage guidelines

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

You can configure the ACL module to generate log entries for packet filtering and output them to the information center at the output interval. The log entry records the number of matching packets and the matched ACL rules. When the first packet of a flow matches an ACL rule, the output interval starts, and the device immediately outputs a log entry for this packet. When the output interval ends, the device outputs a log entry for subsequent matching packets of the flow. For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

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

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

Related commands

rule (IPv4 advanced ACL view)

rule (IPv4 basic ACL view)

rule (IPv6 advanced ACL view)

rule (IPv6 basic ACL view)

acl trap interval

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

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

Syntax

acl trap interval *interval*

undo acl trap interval

Default

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

Views

System view

Predefined user roles

network-admin

Parameters

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

Usage guidelines

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

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

Examples

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

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

Related commands

rule (IPv4 advanced ACL view)

rule (IPv4 basic ACL view)

rule (IPv6 advanced ACL view)

rule (IPv6 basic ACL view)

description

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

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

Syntax

description *text*

undo description

Default

An ACL does not have a description.

Views

IPv4 basic/advanced ACL view

IPv6 basic/advanced ACL view

Layer 2 ACL view

Predefined user roles

network-admin

Parameters

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

Examples

# Configure a description for IPv4 basic ACL 2000.

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

Related commands

display acl

display acl

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

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

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

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

all: Specifies all ACLs of the specified type.

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

Usage guidelines

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

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

Examples

# Display configuration and match statistics for IPv4 basic ACL 2001.

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

Table 1 Command output

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

display packet-filter

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

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

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

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

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

Usage guidelines

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

Examples

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

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

Table 2 Command output

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

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

display packet-filter statistics

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

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

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

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number.

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

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

brief: Displays brief statistics.

Usage guidelines

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

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

Examples

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

```
<Sysname> display packet-filter statistics interface gigabitethernet 1/0/1 inbound
Interface: GigabitEthernet1/0/1
 Inbound policy:
  IPv4 ACL 2001, Hardware-count
   From 2011-06-04 10:25:21 to 2011-06-04 10:35:57
   rule 0 permit source 2.2.2.2 0 (2 packets)
   rule 5 permit source 1.1.1.1 0 (Failed)
   rule 10 permit vpn-instance test (No resource)
   Totally 2 packets permitted, 0 packets denied
   Totally 100% permitted, 0% denied

  IPv6 ACL 2000

  MAC ACL 4000
   rule 0 permit
```

Table 3 Command output

Field	Description
Interface	Interface to which the ACL applies.
Inbound policy	ACL used for filtering incoming traffic.
Outbound policy	ACL used for filtering outgoing traffic.
IPv4 ACL 2001	IPv4 basic ACL 2001 has been successfully applied.
IPv4 ACL 2002 (Failed)	The device has failed to apply IPv4 basic ACL 2002.
Hardware-count	ACL rule match counting in hardware has been successfully enabled.
Hardware-count (Failed)	The device has failed to enable counting ACL rule matches in hardware.
From 2011-06-04 10:25:21 to 2011-06-04 10:35:57	Start time and end time of the statistics.
2 packets	Two packets matched the rule. This field is not displayed when no packets matched the rule.
No resource	Resources are not enough for counting matches for the rule. In packet filtering statistics, this field is displayed for a rule when resources are not sufficient for rule match counting.
rule 5 permit source 1.1.1.1 0 (Failed)	The device has failed to apply rule 5.
Totally 2 packets permitted, 0 packets denied	Number of packets permitted and denied by the ACL.
Totally 100% permitted, 0% denied	Ratios of permitted and denied packets to all packets.

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

Related commands

reset packet-filter statistics

display packet-filter statistics sum

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

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number.

- 2000 to 2999 for basic ACLs.

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

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

brief: Displays brief statistics.

Usage guidelines

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

Examples

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

```
<Sysname> display packet-filter statistics sum inbound 2001
Sum:
 Inbound policy:
  IPv4 ACL 2001
   rule 0 permit source 2.2.2.2 0 (2 packets)
   rule 5 permit source 1.1.1.1 0
   rule 10 permit vpn-instance test
   Totally 2 packets permitted, 0 packets denied
   Totally 100% permitted, 0% denied
```

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

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

Table 4 Command output

Field	Description
Sum	Accumulated packet filtering statistics.
Inbound policy	Accumulated packet filtering statistics in the inbound direction.
Outbound policy	Accumulated packet filtering statistics in the outbound direction.
IPv4 ACL 2001	Accumulated packet filtering statistics of IPv4 basic ACL 2001.
2 packets	Two packets matched the rule. This field is not displayed when no packets matched the rule.
Totally 2 packets permitted, 0 packets denied	Number of packets permitted and denied by the ACL.
Totally 100% permitted, 0% denied	Ratios of permitted and denied packets to all packets.

Related commands

reset packet-filter statistics

display packet-filter verbose

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

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

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

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number.

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

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

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

Usage guidelines

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

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

Examples

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

```
<Sysname> display packet-filter verbose interface gigabitethernet 1/0/1 inbound
Interface: GigabitEthernet1/0/1
 Inbound policy:
  IPv4 ACL 2001
   rule 0 permit
   rule 5 permit source 1.1.1.1 0 (Failed)
   rule 10 permit vpn-instance test (Failed)

  IPv6 ACL 2000
   rule 0 permit

  MAC ACL 4000
  IPv4 default action: Deny

  IPv6 default action: Deny

  MAC default action: Deny
```

Table 5 Command output

Field	Description
Interface	Interface to which the ACL applies.
Inbound policy	ACL used for filtering incoming traffic.
Outbound policy	ACL used for filtering outgoing traffic.
IPv4 ACL 2001	IPv4 basic ACL 2001 has been successfully applied.
IPv4 ACL 2002 (Failed)	The device has failed to apply IPv4 basic ACL 2002.
Hardware-count	ACL rule match counting in hardware has been successfully enabled.
Hardware-count (Failed)	The device has failed to enable counting ACL rule matches in hardware.
rule 5 permit source 1.1.1.1 0 (Failed)	The device has failed to apply rule 5.
IPv4 default action	Packet filter default action for packets that do not match any IPv4 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.
IPv6 default action	Packet filter default action for packets that do not match any IPv6 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.
MAC default action	Packet filter default action for packets that do not match any Layer 2 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.

display qos-acl resource

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

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

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

Usage guidelines

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

The following features cannot work correctly when QoS and ACL resources are insufficient:

- Packet filtering.
- Device login.
- 802.1X.
- MAC authentication.

For these features to work correctly, reserve enough QoS and ACL resources.

Examples

# Display QoS and ACL resource usage.

```
<Sysname> display qos-acl resource
Interfaces: GE1/0/1 to GE1/0/24, GE1/0/51 to GE1/0/52 (slot 1)
---------------------------------------------------------------------
 Type             Total      Reserved   Configured Remaining  Usage
---------------------------------------------------------------------
 TTI ACL          256        0          1          255        0%
 PCL ACL          1536       19         0          1517       1%
 PCL Counter      2704       19         0          2685       0%
 IPCL Meter       1792       0          0          1792       0%
 EPCL Meter       512        0          0          512        0%

Interfaces: GE1/0/25 to GE1/0/50 (slot 1)
---------------------------------------------------------------------
 Type             Total      Reserved   Configured Remaining  Usage
---------------------------------------------------------------------
 TTI ACL          256        0          1          255        0%
 PCL ACL          1536       19         0          1517       1%
 PCL Counter      2704       19         0          2685       0%
 IPCL Meter       1792       0          0          1792       0%
 EPCL Meter       512        0          0          512        0%
```

Table 6 Command output

Field	Description
Interfaces	Interface range for the resources.
Type	Resource type: • **TTI ACL**—ACL resources used for interfaces. These resources are used only for QinQ and VLAN mapping in the current software version. • **PCL ACL**—ACL resources used for policies, including resources used by protocol packets and used by the application modules that reference ACLs. • **PCL Counter**—Accounting resources used for policies. • **IPCL Meter**—Traffic policing resources used in inbound QoS policies. • **EPCL Meter**—Traffic policing resources used in outbound QoS policies.
Total	Total number of resources.
Reserved	Number of reserved resources.
Configured	Number of resources that has been applied.
Remaining	Number of resources that you can apply.
Usage	Configured and reserved resources as a percentage of total resources. If the percentage is not an integer, this field displays the integer part. For example, if the actual usage is 50.8%, this field displays 50%.

packet-filter

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

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

Syntax

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

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

Default

No ACL is applied to an interface to filter packets.

Views

Layer 2 Ethernet interface view

VLAN interface view

Predefined user roles

network-admin

Parameters

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number.

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

- 4000 to 4999 for Layer 2 ACLs.

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

inbound: Filters incoming packets.

outbound: Filters outgoing packets.

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

Usage guidelines

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

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

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

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

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

Examples

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

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

Related commands

display packet-filter

display packet-filter statistics

display packet-filter verbose

packet-filter default deny

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

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

Syntax

packet-filter default deny

undo packet-filter default deny

Default

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

Views

System view

Predefined user roles

network-admin

Usage guidelines

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

Examples

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

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

Related commands

display packet-filter

display packet-filter statistics

display packet-filter verbose

reset packet-filter statistics

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

Syntax

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

Views

User view

Predefined user roles

network-admin

Parameters

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

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number.

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

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

Usage guidelines

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

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

Examples

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

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

Related commands

display packet-filter statistics

display packet-filter statistics sum

rule (IPv4 advanced ACL view)

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

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

Syntax

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

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

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

Default

No IPv4 advanced ACL rules exist.

Views

IPv4 advanced ACL view

Predefined user roles

network-admin

Parameters

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

deny: Denies matching packets.

permit: Allows matching packets to pass.

protocol: Specifies one of the following values:

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

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

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

Parameters	Function	Description
source { *source-address source-wildcard* | **any** }	Specifies a source address.	The *source-address source-wildcard* arguments specify a source IP address and a wildcard mask in dotted decimal notation. An all-zero wildcard represents a host address. The **any** keyword specifies any source IP address.
destination { *dest-address dest-wildcard* | **any** }	Specifies a destination address.	The *dest-address dest-wildcard* arguments specify a destination IP address and a wildcard mask in dotted decimal notation. An all-zero wildcard mask represents a host address. The **any** keyword represents any destination IP address.
counting	Enables rule match counting in software.	The **counting** keyword enables match counting specific to rules, and the **hardware-count** keyword in the **packet-filter** command enables match counting in hardware for all rules in an ACL. If the **counting** keyword is not specified, matches for the rule are not counted in software.
precedence *precedence*	Specifies an IP precedence value.	The *precedence* argument can be a number in the range of 0 to 7, or in words: **routine** (0), **priority** (1), **immediate** (2), **flash** (3), **flash-override** (4), **critical** (5), **internet** (6), or **network** (7).
tos *tos*	Specifies a ToS preference.	The *tos* argument can be a number in the range of 0 to 15, or in words: **max-reliability** (2), **max-throughput** (4), **min-delay** (8), **min-monetary-cost** (1), or **normal** (0).
dscp *dscp*	Specifies a DSCP priority.	The *dscp* argument can be a number in the range of 0 to 63, or in words: **af11** (10), **af12** (12), **af13** (14), **af21** (18), **af22** (20), **af23** (22), **af31** (26), **af32** (28), **af33** (30), **af41** (34), **af42** (36), **af43** (38), **cs1** (8), **cs2** (16), **cs3** (24), **cs4** (32), **cs5** (40), **cs6** (48), **cs7** (56), **default** (0), or **ef** (46).
fragment	Applies the rule only to fragments.	If you do not specify this keyword, the rule applies to all fragments and non-fragments.
logging	Logs matching packets.	This feature requires that the module (for example, packet filtering) that uses the ACL supports logging.

time-range *time-range-name*	Specifies a time range for the rule.	The *time-range-name* argument is a case-insensitive string of 1 to 32 characters. It must start with an English letter. If the time range is not configured, the system creates the rule. However, the rule using the time range can take effect only after you configure the time range. For more information about time range, see *ACL and QoS Configuration Guide*.
vpn-instance *vpn-instance-name*	Applies the rule to an MPLS L3VPN instance.	The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the rule applies to both non-VPN packets and VPN packets.

If the *protocol* argument is **tcp** (6) or **udp** (17), set the parameters shown in Table 8.

Table 8 TCP/UDP-specific parameters for IPv4 advanced ACL rules

Parameters	Function	Description
source-port *operator port1* [*port2*]	Specifies one or more UDP or TCP source ports.	The *operator* argument can be **lt** (lower than), **gt** (greater than), **eq** (equal to), or **range** (inclusive range). The *port1* and *port2* arguments are TCP or UDP port numbers in the range of 0 to 65535. The *port2* argument is needed only when the *operator* argument is **range**. TCP port numbers can be represented as: **chargen** (19), **bgp** (179), **cmd** (514), **daytime** (13), **discard** (9), **dns** (53), **domain** (53), **echo** (7), **exec** (512), **finger** (79), **ftp** (21), **ftp-data** (20), **gopher** (70), **hostname** (101), **irc** (194), **klogin** (543), **kshell** (544), **login** (513), **lpd** (515), **nntp** (119), **pop2** (109), **pop3** (110), **smtp** (25), **sunrpc** (111), **tacacs** (49), **talk** (517), **telnet** (23), **time** (37), **uucp** (540), **whois** (43), and **www** (80). UDP port numbers can be represented as: **biff** (512), **bootpc** (68), **bootps** (67), **discard** (9), **dns** (53), **dnsix** (90), **echo** (7), **mobilip-ag** (434), **mobilip-mn** (435), **nameserver** (42), **netbios-dgm** (138), **netbios-ns** (137), **netbios-ssn** (139), **ntp** (123), **rip** (520), **snmp** (161), **snmptrap** (162), **sunrpc** (111), **syslog** (514), **tacacs-ds** (65), **talk** (517), **tftp** (69), **time** (37), **who** (513), and **xdmcp** (177).
destination-port *operator port1* [*port2*]	Specifies one or more UDP or TCP destination ports.	
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } *	Specifies one or more TCP flags including ACK, FIN, PSH, RST, SYN, and URG.	Parameters specific to TCP. The value for each argument can be 0 (flag bit not set) or 1 (flag bit set). The TCP flags in a rule are ANDed. For example, a rule configured with **ack** 0 **psh** 1 matches packets that have the ACK flag bit not set and the PSH flag bit set.
established	Specifies the flags for indicating the established status of a TCP connection.	Parameter specific to TCP. The rule matches TCP connection packets with the ACK or RST flag bit set.

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

Table 9 ICMP-specific parameters for IPv4 advanced ACL rules

Parameters	Function	Description
icmp-type { *icmp-type* *icmp-code* | *icmp-message* }	Specifies the ICMP message type and code.	The *icmp-type* argument is in the range of 0 to 255. The *icmp-code* argument is in the range of 0 to 255. The *icmp-message* argument specifies a message name. Supported ICMP message names and their corresponding type and code values are listed in Table 10.

Table 10 ICMP message names supported in IPv4 advanced ACL rules

ICMP message name	ICMP message type	ICMP message code
echo	8	0
echo-reply	0	0
fragmentneed-DFset	3	4
host-redirect	5	1
host-tos-redirect	5	3
host-unreachable	3	1
information-reply	16	0
information-request	15	0
net-redirect	5	0
net-tos-redirect	5	2
net-unreachable	3	0
parameter-problem	12	0
port-unreachable	3	3
protocol-unreachable	3	2
reassembly-timeout	11	1
source-quench	4	0
source-route-failed	3	5
timestamp-reply	14	0
timestamp-request	13	0
ttl-exceeded	11	0

Usage guidelines

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

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

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

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

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

Examples

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

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

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

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

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

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

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

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

Related commands

acl

acl logging interval

display acl

step

time-range

rule (IPv4 basic ACL view)

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

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

Syntax

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

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

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

Default

No IPv4 basic ACL rules exist.

Views

IPv4 basic ACL view

Predefined user roles

network-admin

Parameters

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

deny: Denies matching packets.

permit: Allows matching packets to pass.

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

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

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

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

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

vpn-instance *vpn-instance-name*: Applies the rule to an MPLS L3VPN instance. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the rule applies to both non-VPN packets and VPN packets.

Usage guidelines

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

config

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

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

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

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

Examples

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

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

Related commands

acl

acl logging interval

display acl

step

time-range

rule (IPv6 advanced ACL view)

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

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

Syntax

rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { *dest-address dest-prefix* | *dest-address/dest-prefix* | **any** } | **destination-port** *operator port1* [*port2*] | **dscp** *dscp* | **flow-label** *flow-label-value* | **fragment** | **icmp6-type** { *icmp6-type icmp6-code* | *icmp6-message* } | **logging** | **routing** [**type** *routing-type*] | **hop-by-hop** [**type** *hop-type*] | **source** { *source-address source-prefix* | *source-address/source-prefix* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

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

undo rule { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { *dest-address dest-prefix* | *dest-address/dest-prefix* | **any** } | **destination-port** *operator port1* [*port2*] | **dscp** *dscp* | **flow-label** *flow-label-value* | **fragment** | **icmp6-type** { *icmp6-type icmp6-code* | *icmp6-message* } | **logging** | **routing** [**type** *routing-type*] | **hop-by-hop** [**type** *hop-type*] | **source** { *source-address source-prefix* | *source-address/source-prefix* | **any** } | **source-port**

operator port1 [*port2*] | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

Default

No IPv6 advanced ACL rules exist.

Views

IPv6 advanced ACL view

Predefined user roles

network-admin

Parameters

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

deny: Denies matching packets.

permit: Allows matching packets to pass.

protocol: Specifies one of the following values:

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

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

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

Parameters	Function	Description
source { *source-address source-prefix* | *source-address/source-prefix* | **any** }	Specifies a source IPv6 address.	The *source-address* argument specifies an IPv6 source address. The *source-prefix* argument specifies a prefix length in the range of 1 to 128. The **any** keyword represents any IPv6 source address.
destination { *dest-address dest-prefix* | *dest-address/dest-prefix* | **any** }	Specifies a destination IPv6 address.	The *dest-address* argument specifies a destination IPv6 address. The *dest-prefix* argument specifies a prefix length in the range of 1 to 128. The **any** keyword represents any IPv6 destination address.
counting	Enables rule match counting in software.	The **counting** keyword enables match counting specific to rules, and the **hardware-count** keyword in the **packet-filter ipv6** command enables match counting in hardware for all rules in an ACL. If the **counting** keyword is not specified, matches for the rule are not counted in software.
dscp *dscp*	Specifies a DSCP preference.	The *dscp* argument can be a number in the range of 0 to 63, or in words, **af11**

		(10), **af12** (12), **af13** (14), **af21** (18), **af22** (20), **af23** (22), **af31** (26), **af32** (28), **af33** (30), **af41** (34), **af42** (36), **af43** (38), **cs1** (8), **cs2** (16), **cs3** (24), **cs4** (32), **cs5** (40), **cs6** (48), **cs7** (56), **default** (0), or **ef** (46).
flow-label *flow-label-value*	Specifies a flow label value in an IPv6 packet header.	The *flow-label-value* argument is in the range of 0 to 1048575.
fragment	Applies the rule only to fragments.	If you do not specify this keyword, the rule applies to all fragments and non-fragments.
logging	Logs matching packets.	This feature requires that the module (for example, packet filtering) that uses the ACL supports logging.
routing [**type** *routing-type*]	Specifies an IPv6 routing header type.	*routing-type*: Value of the IPv6 routing header type, in the range of 0 to 255. If you specify the **type** *routing-type* option, the rule applies to the specified type of IPv6 routing header. If you do not specify the **type** *routing-type* option, the rule applies to all types of IPv6 routing headers.
hop-by-hop [**type** *hop-type*]	Specifies an IPv6 Hop-by-Hop Options header type.	*hop-type*: Value of the IPv6 Hop-by-Hop Options header type, in the range of 0 to 255. If you specify the **type** *hop-type* option, the rule applies to the specified type of IPv6 Hop-by-Hop Options header. If you do not specify the **type** *hop-type* option, the rule applies to all types of IPv6 Hop-by-Hop Options header.
time-range *time-range-name*	Specifies a time range for the rule.	The *time-range-name* argument is a case-insensitive string of 1 to 32 characters. It must start with an English letter. If the time range is not configured, the system creates the rule. However, the rule using the time range can take effect only after you configure the time range. For more information about time range, see *ACL and QoS Configuration Guide*.
vpn-instance *vpn-instance-name*	Applies the rule to an MPLS L3VPN instance.	The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the rule applies to both non-VPN packets and VPN packets.

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

Table 12 TCP/UDP-specific parameters for IPv6 advanced ACL rules

Parameters	**Function**	**Description**
source-port	Specifies one or	The *operator* argument can be **lt** (lower than), **gt**

operator port1 [*port2*]	more UDP or TCP source ports.	(greater than), **eq** (equal to), or **range** (inclusive range).
destination-port *operator port1* [*port2*]	Specifies one or more UDP or TCP destination ports.	The *port1* and *port2* arguments are TCP or UDP port numbers in the range of 0 to 65535. The *port2* argument is needed only when the *operator* argument is **range**. TCP port numbers can be represented as: **chargen** (19), **bgp** (179), **cmd** (514), **daytime** (13), **discard** (9), **dns** (53), **domain** (53), **echo** (7), **exec** (512), **finger** (79), **ftp** (21), **ftp-data** (20), **gopher** (70), **hostname** (101), **irc** (194), **klogin** (543), **kshell** (544), **login** (513), **lpd** (515), **nntp** (119), **pop2** (109), **pop3** (110), **smtp** (25), **sunrpc** (111), **tacacs** (49), **talk** (517), **telnet** (23), **time** (37), **uucp** (540), **whois** (43), and **www** (80). UDP port numbers can be represented as: **biff** (512), **bootpc** (68), **bootps** (67), **discard** (9), **dns** (53), **dnsix** (90), **echo** (7), **mobilip-ag** (434), **mobilip-mn** (435), **nameserver** (42), **netbios-dgm** (138), **netbios-ns** (137), **netbios-ssn** (139), **ntp** (123), **rip** (520), **snmp** (161), **snmptrap** (162), **sunrpc** (111), **syslog** (514), **tacacs-ds** (65), **talk** (517), **tftp** (69), **time** (37), **who** (513), and **xdmcp** (177).
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } *	Specifies one or more TCP flags, including ACK, FIN, PSH, RST, SYN, and URG.	Parameters specific to TCP. The value for each argument can be 0 (flag bit not set) or 1 (flag bit set). The TCP flags in a rule are ANDed. For example, a rule configured with **ack** 0 **psh** 1 matches packets that have the ACK flag bit not set and the PSH flag bit set.
established	Specifies the flags for indicating the established status of a TCP connection.	Parameter specific to TCP. The rule matches TCP packets with the ACK or RST flag bit set.

If the *protocol* argument is **icmpv6** (58), set the parameters shown in Table 13.

Table 13 ICMPv6-specific parameters for IPv6 advanced ACL rules

Parameters	Function	Description
icmp6-type { *icmp6-type* *icmp6-code* | *icmp6-message* }	Specifies the ICMPv6 message type and code.	The *icmp6-type* argument is in the range of 0 to 255. The *icmp6-code* argument is in the range of 0 to 255. The *icmp6-message* argument specifies a message name. Supported ICMP message names and their corresponding type and code values are listed in Table 14.

Table 14 ICMPv6 message names supported in IPv6 advanced ACL rules

ICMPv6 message name	ICMPv6 message type	ICMPv6 message code
echo-reply	129	0
echo-request	128	0
err-Header-field	4	0

frag-time-exceeded	3	1
hop-limit-exceeded	3	0
host-admin-prohib	1	1
host-unreachable	1	3
neighbor-advertisement	136	0
neighbor-solicitation	135	0
network-unreachable	1	0
packet-too-big	2	0
port-unreachable	1	4
redirect	137	0
router-advertisement	134	0
router-solicitation	133	0
unknown-ipv6-opt	4	2
unknown-next-hdr	4	1

Usage guidelines

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

- Do not specify the **fragment** keyword.
- Do not specify the **vpn-instance**, **routing**, **hop-by-hop**, or **flow-label** keyword if the ACL is for outbound application.
- Do not specify **ipv6-ah** for the *protocol* argument, or set its value to 0, 43, 44, 51, or 60 if the ACL is for outbound application.

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

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

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

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

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

Examples

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

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

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

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

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

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

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

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

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

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

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

Related commands

acl

acl logging interval

display acl

step

time-range

rule (IPv6 basic ACL view)

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

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

Syntax

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

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

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

Default

No IPv6 basic ACL rules exist.

Views

IPv6 basic ACL view

Predefined user roles

network-admin

Parameters

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

deny: Denies matching packets.

permit: Allows matching packets to pass.

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

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

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

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

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

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

vpn-instance *vpn-instance-name*: Applies the rule to an MPLS L3VPN instance. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the rule applies to both non-VPN packets and VPN packets.

Usage guidelines

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

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

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

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

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

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

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

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

Examples

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

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

Related commands

acl

acl logging interval

display acl

step

time-range

rule (Layer 2 ACL view)

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

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

Syntax

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

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

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

Default

No Layer 2 ACL rules exist.

Views

Layer 2 ACL view

Predefined user roles

network-admin

Parameters

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

deny: Denies matching packets.

permit: Allows matching packets to pass.

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

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

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

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

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

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

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

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

Usage guidelines

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

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

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

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

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

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

Examples

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

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

Related commands

acl

display acl

step

time-range

rule comment

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

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

Syntax

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

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

Default

A rule does not have a comment.

Views

IPv4 basic/advanced ACL view

IPv6 basic/advanced ACL view

Layer 2 ACL view

Predefined user roles

network-admin

Parameters

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

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

Usage guidelines

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

Examples

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

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

Related commands

display acl

step

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

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

Syntax

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

undo step

Default

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

Views

IPv4 basic/advanced ACL view

IPv6 basic/advanced ACL view

Layer 2 ACL view

Predefined user roles

network-admin

Parameters

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

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

Usage guidelines

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

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

Examples

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

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

Related commands

display acl