

ACL Commands

This chapter provides details of the commands used for configuring access control lists (ACL).

- ipv4 access-group, on page 2
- ipv6 access-group, on page 3
- show access-lists ipv4, on page 4
- show access-lists ipv6, on page 6

ipv4 access-group

To configure the Access List (ACL), use the **ipv4 access-group** command at the IPv4 interface in the interface configuration mode.

ipv4 access-group *access-list-name* **ingress**

Syntax Description

access-list-name	Access list name. Names cannot contain a space or quotation marks.
ingress	Specifies an inbound interface.

Command Default

No IPv4 access list is defined.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.5.31	This command was introduced.

Usage Guidelines

Use the **ipv4 access-list** command to configure an IPv4 access list. This command places the system in access list configuration mode, in which the denied or permitted access conditions must be defined with the deny or permit command.

Example

The following examples shows how to configure the Access List at the IPv4 interface in the configuration mode:

```
interface MgmtEth0/RP0/EMS/0
ipv4 address 5.5.5.1 255.255.255.0
ipv4 access-group EMS ingress
!
ipv4 access-list EMS
10 permit udp any any
!
```

Sample Configuration for IPv4 Access Lists

```
ipv4 access-list CRAFT
10 deny icmp any any
ipv4 access-list EMS
10 deny icmp any any (200 matches)
```

ipv6 access-group

To configure the Access List (ACL), use the **ipv6 access-group** command at the IPv6 interface in the interface configuration mode.

ipv6 access-group *access-list-name* **ingress**

Syntax Description

access-list-name	Access list name. Names cannot contain a space or quotation marks.
ingress	Specifies an inbound interface.

Command Default

No IPv6 access list is defined.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.5.31	This command was introduced.

Usage Guidelines

Use the ipv6 access-list command to configure an IPv6access list. This command places the system in access list configuration mode, in which the denied or permitted access conditions must be defined with the deny or permit command.

Example

The following examples shows how to configure the Access List at the IPv6 interface in the configuration mode

```
interface MgmtEth0/RP0/EMS/0
ipv6 address 2001:db8::1/64
ipv6 access-group EMS ingress
!
ipv6 access-list EMS
10 permit udp any any
!
```

Sample Configuration for IPv6 Access Lists

```
ipv6 access-list CRAFT
10 deny icmp any any
ipv6 access-list EMS
10 deny icmp any any (200 matches)
```

show access-lists ipv4

To display the contents of current IPv4 access lists, use the **show access-lists ipv4** command in EXEC mode.

show access-lists ipv4 [**interface MgmtEth** *R/S/I/P* | **maximum** [**detail**] | **summary** [*access-list-name*] | **usage pfilter location** { **location** *node-id* | **all** } | *access-list-name* [*sequence-number* | **usage pfilter location** { **location** *node-id* | **all** }]]

Syntax Description

R/S/I/P	Rack/Slot/Instance/Port/ number of the interface.
access-list-name	(Optional) Name of a particular IPv4 access list. The name cannot contain a space or quotation mark; it may contain numbers.
location *number*	Location of a particular IPv4 access list.
location*node-id*	(Optional) Location of a particular IPv4 access list. The node-id argument is entered in the rack/slot/module notation.
usage	(Optional) Displays the usage of the access list on a given line card.
pfilter	(Optional) Displays the packet filtering usage for the specified line card.
summary	Displays a summary of all current IPv4 access lists.
sequence-number	(Optional) Sequence number of a particular IPv4 access list.
maximum	Displays the current maximum number of configurable IPv4 accesscontrol lists (ACLs) and access control entries (ACEs).
detail	(Optional) Displays complete out-of-resource (OOR) details.
all	(Optional) Displays the location of all the line cards.

Command Default

Displays all IPv4 access lists.

Command Modes

EXEC

Command History

Release	Modification
Release 6.5.31	This command was introduced.

Usage Guidelines

Use the **show access-lists ipv4** command to display the contents of all IPv4 access lists. To display the contents of a specific IPv4 access list, use the name argument. Use the *sequence-number* argument to specify the sequence number of the access list.

Use the **show access-lists ipv4 summary** command to display a summary of all current IPv4 access lists. To display a summary of a specific IPv4 access list, use the name argument.

Use the **show access-lists ipv4 maximum detail** command to display the OOR details for IPv4 access lists. OOR limits the number of ACLs and ACEs that can be configured in the system. When the limit is reached, configuration of new ACLs or ACEs is rejected.

Example

In the following example, the contents of all IPv4 access lists are displayed:

RP/0/RP0/CPU0:ios# **show access-lists ipv4**

```
ipv4 access-list CRAFT
10 deny icmp any any
ipv4 access-list EMS
10 deny icmp any any (200 matches)
```

RP/0/RP0/CPU0:ios# **show access-lists test_ro_traffic_generic**

```
Mon Jun 28 15:32:39.456 IST
ipv4 access-list test_RO_Traffic_Generic
10 permit tcp 100.1.0.0 0.0.255.255 eq bgp 100.1.0.0 0.0.255.255
20 permit tcp 100.1.0.0 0.0.255.255 100.1.0.0 0.0.255.255 eq bgp
30 permit udp 100.1.0.0 0.0.255.255 100.1.0.0 0.0.255.255 eq 6784
40 permit udp 100.1.0.0 0.0.255.255 eq ldp 100.1.0.0 0.0.255.255
50 permit udp 100.1.0.0 0.0.255.255 100.1.0.0 0.0.255.255 eq ldp
60 permit tcp 100.1.0.0 0.0.255.255 eq ldp 100.1.0.0 0.0.255.255
70 permit tcp 100.1.0.0 0.0.255.255 100.1.0.0 0.0.255.255 eq ldp
80 permit icmp 100.1.0.0 0.0.255.255 100.1.0.0 0.0.255.255
87 deny udp host 12.12.12.1 32.32.32.240 0.0.0.15 eq snmp
```

show access-lists ipv6

To display the contents of current IPv6 access lists, use the **show access-lists ipv6** command in EXEC mode.

show access-lists ipv6 [**interface MgmtEth** *R/S/I/P* | **maximum** [**detail**] | **summary** [*access-list-name*] | **usage pfilter location** { **location** *node-id* | **all** } | *access-list-name* [*sequence-number* | **usage pfilter location** { **location** *node-id* | **all** }]]

Syntax Description

R/S/I/P	Rack/Slot/Instance/Port/ number of the interface.
access-list-name	(Optional) Name of a particular IPv6 access list. The name cannot contain a space or quotation mark; it may contain numbers.
location *number*	Location of a particular IPv6 access list.
location *node-id*	(Optional) Location of a particular IPv6 access list. The node-id argument is entered in the rack/slot/module notation.
usage	(Optional) Displays the usage of the access list on a given line card.
pfilter	(Optional) Displays the packet filtering usage for the specified line card.
summary	Displays a summary of all current IPv6 access lists.
sequence-number	(Optional) Sequence number of a particular IPv6 access list.
maximum	Displays the current maximum number of configurable IPv6 accesscontrol lists (ACLs) and access control entries (ACEs).
detail	(Optional) Displays complete out-of-resource (OOR) details.
all	(Optional) Displays the location of all the line cards.

Command Default

Displays all IPv6 access lists.

Command Modes

EXEC

Command History

Release	Modification
Release 6.5.31	This command was introduced.

Usage Guidelines

The **show access-lists ipv6** command is similar to the **show access-lists ipv4** command, except that it is IPv6 specific.

Use the **show access-lists ipv6** command to display the contents of all IPv6 access lists. To display the contents of a specific IPv6 access list, use the name argument. Use the *sequence-number* argument to specify the sequence number of the access list.

Use the **show access-lists ipv6 summary** command to display a summary of all current IPv6 access lists. To display a summary of a specific IPv6 access list, use the name argument.

Use the **show access-lists ipv6 maximum detail** command to display the OOR details for IPv6 access lists. OOR limits the number of ACLs and ACEs that can be configured in the system. When the limit is reached, configuration of new ACLs or ACEs is rejected.

Example

In the following example, the contents of all IPv6 access lists are displayed:

RP/0/RP0/CPU0:ios#**show access-lists ipv6**

```
RP/0/RP0:hostname#show access-lists ipv6
ipv6 access-list CRAFT
10 deny icmp any any
ipv6 access-list EMS
10 deny icmp any any (200 matches)
```