

Layer 2 Access List Commands

This section describes the commands used to configure Layer 2 access list.

Note All commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router that is introduced from Cisco IOS XR Release 6.3.2. References to earlier releases in Command History tables apply to only the Cisco NCS 5500 Series Router.

Note

- Starting with Cisco IOS XR Release 6.6.25, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 560 Series Routers.
- Starting with Cisco IOS XR Release 6.3.2, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router.
- References to releases before Cisco IOS XR Release 6.3.2 apply to only the Cisco NCS 5500 Series Router.
- Cisco IOS XR Software Release 7.0.1 specific updates are not applicable for the following variants of Cisco NCS 540 Series Routers:
  - N540-28Z4C-SYS-A
  - N540-28Z4C-SYS-D
  - N540X-16Z4G8Q2C-A
  - N540X-16Z4G8Q2C-D
  - N540X-16Z8Q2C-D
  - N540-12Z20G-SYS-A
  - N540-12Z20G-SYS-D
  - N540X-12Z16G-SYS-A
  - N540X-12Z16G-SYS-D

For detailed information about concepts and configuration, see the Configure Layer 2 Access Control Lists chapter in the *L2VPN and Ethernet Services Configuration Guide for Cisco NCS 5500 Series RoutersL2VPN and Ethernet Services Configuration Guide for Cisco NCS 540 Series RoutersL2VPN and Ethernet Services Configuration Guide for Cisco NCS 560 Series Routers*.

- ethernet-services access-group, on page 3
- ethernet-services access-list, on page 4
- show access-lists ethernet-services, on page 5
- show access-lists ethernet-services usage pfilter , on page 7

ethernet-services access-group

To control access to an interface, use the **ethernet-service access-group** command in interface configuration mode. To remove the specified access group, use the **no** form of the command.

ethernet-services access-group *access-list-name* **ingress**
no ethernet-services access-list *access-list-name* **ingress**

Syntax Description

access-list-name	Name of an Ethernet services access list as specified by the **ethernet-service access-list** command.
ingress	Filters on inbound packets.

Command Default

The interface does not have an Ethernet services access list applied to it.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

The **ethernet-services access-group** command to control access to an interface. To remove the specified access group, use the **no** form of the command. Use the *access-list-name* argument to specify a particular Ethernet services access list. Use the ingress keyword to filter on inbound packets.

If the list permits the addresses, the software continues to process the packet. If the access list denies the address, the software discards the packet and returns a host unreachable message.

If the specified access list does not exist, all packets are passed.

By default, the unique or per-interface ACL statistics are disabled.

Task ID

Task ID	Operations
acl	read, write

Examples

The following example shows how to apply filters on inbound packets from an interface.

```
Router# configure
Router(config)# interface tengige0/0/0/4
Router(config-if)# l2transport
Router(config-if)# ethernet-services access-group es_acl_1 ingress
Router(config-if)# commit
```

ethernet-services access-list

To define an Ethernet services (Layer 2) access list by name, use the **ethernet-services access-list** command in global configuration mode. To remove all entries in an Ethernet services access list, use the **no** form of the command.

ethernet-services access-list *access-list-name*
no ethernet-services access-list *access-list-name*

Syntax Description

access-list-name	Name of the Ethernet services access list. The name cannot contain a spaces or quotation marks, but can include numbers.

Command Default

No Ethernet services access list is defined.

Command Modes

Global configuration

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

The **ethernet-services access-list** command places the router in access list configuration mode, in which the denied or permitted access conditions must be defined.

Only cos (Class of Service) and dei (Discard Eligibility Indication) are supported for Layer 2 ACL.

Task ID

Task ID	Operations
acl	read, write

Examples

The following example shows how to configure ethernet-services access-list:

```
Router# configure
Router(config)# ethernet-services access-list es_acl_1
Router(config-es-acl)# 10 deny 00ff.eedd.0010 ff00.0000.00ff 0000.0100.0001 0000.0000.ffff
Router(config-es-acl)# 20 permit host 000a.000b.000c host 00aa.ab99.1122 cos 1 dei
Router(config-es-acl)# 30 deny host 000a.000b.000c host 00aa.dc11.ba99 cos 7 dei
Router(config-es-acl)# commit
Router(config)# interface tengige0/0/0/4
Router(config-if)# l2transport
Router(config-if)# ethernet-services access-group es_acl_1 ingress
Router(config-if)# commit
```

show access-lists ethernet-services

To display the contents of current Ethernet services access lists, use the **show access-lists ethernet-services** command in EXEC mode.

show access-lists ethernet-services *access-list-name* [**hardware**] **ingress** [**detail**] [**location** {*location* | **all**}]

Syntax Description

access-list-name	Name of a specific Ethernet services access list. The name cannot contain a spaces or quotation marks, but can include numbers.
hardware	(Optional) Display Ethernet services access list entries in hardware including the match count for a specific ACL in a particular direction across the line card.
ingress	Filters on inbound packets.
detail	(Optional) Display TCAM entries.
location	(Optional) Display information for a specific node number.
location	Fully qualified location specification.
all	Displays packet filtering usage for all interface cards.

Command Default

The contents of all Ethernet services access lists are displayed.

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Task ID

Task ID	Operations
acl	read, write

Examples

The following example shows sample output for the **show access-lists ethernet-services** command:

```
Router# show access-lists ethernet-services es_acl_1 hardware ingress location 0/0/CPU0
Thu Nov  3 22:02:27.222 UTC
ethernet-services access-list es_acl_1
 10 deny any host fcd7.844c.7486 cos 3   (65334 matches)
 20 deny any host fcd7.844c.7486
 30 permit any any

Router# show access-lists ethernet-services es_acl_1 hardware ingress detail location
0/0/CPU0
```

```
Thu Nov  3 22:01:18.620 UTC
es_acl_1 Details:
Sequence Number: 10
Number of DPA Entries: 1
ACL ID: 1
ACE Action: DENY
ACE Logging: DISABLED
Hit Packet Count: 0
Source MAC: 0000:0000:0000
 Source MAC Mask: 0000:0000:0000
Destination MAC: FCD7:844C:7486
 Destination MAC Mask: FFFF:FFFF:FFFF
COS: 0x03
        Entry Index: 0x0
        DPA Handle: 0x89BF60E8

es_acl_1 Details:
Sequence Number: 20
Number of DPA Entries: 1
ACL ID: 1
ACE Action: DENY
ACE Logging: DISABLED
Hit Packet Count: 0
Source MAC: 0000:0000:0000
 Source MAC Mask: 0000:0000:0000
Destination MAC: FCD7:844C:7486
 Destination MAC Mask: FFFF:FFFF:FFFF
        Entry Index: 0x0
        DPA Handle: 0x89BF62E8

es_acl_1 Details:
Sequence Number: 30
Number of DPA Entries: 1
ACL ID: 1
ACE Action: PERMIT
ACE Logging: DISABLED
Source MAC: 0000:0000:0000
 Source MAC Mask: 0000:0000:0000
Destination MAC: 0000:0000:0000
 Destination MAC Mask: 0000:0000:0000
        Entry Index: 0x0
        DPA Handle: 0x89BF64E8

es_acl_1 Details:
Sequence Number: IMPLICIT DENY
Number of DPA Entries: 1
ACL ID: 1
ACE Action: DENY
ACE Logging: DISABLED
Hit Packet Count: 0
Source MAC: 0000:0000:0000
 Source MAC Mask: 0000:0000:0000
Destination MAC: 0000:0000:0000
 Destination MAC Mask: 0000:0000:0000
        Entry Index: 0x0
        DPA Handle: 0x89BF66E8
```

show access-lists ethernet-services usage pfilter

To identify the modes and interfaces on which a particular access-list is applied, use the **show access-lists ethernet-services usage pfilter** command in EXEC mode. Information displayed includes the application of all or specific access-lists, the interfaces on which they have been applied and the direction in which they are applied.

show access-lists ethernet-services *access-list-name* **usage pfilter location** { *location* | **all** }

Syntax Description

access-list-name	Name of a specific Ethernet services access list. The name cannot contain a spaces or quotation marks, but can include numbers.
location	Interface card on which the access list information is needed.
location	Fully qualified location specification.
all	Displays packet filtering usage for all interface cards.

Command Modes

EXEC mode

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Task ID

Task ID	Operations
acl	read, write

Examples

The following example shows how to display packet filter usage at a specific location:

```
Router# show access-lists ethernet-services es_acl_1 usage pfilter location 0/0/CPU0
Thu Nov  3 21:58:19.706 UTC
Interface : TenGigE0/0/0/0/1
    Input ACL : es_acl_1
    Output ACL : N/A
```