# Layer 2 Access Control Lists

This chapter introduces you to Layer 2 Access Control Lists and describe how you can configure the Layer 2 access control lists.

# Layer 2 Access Control Lists

*Table 1: Feature History Table*

| Feature Name | Release Information | Description |
|---|---|---|
| Layer 2 Access Control Lists | Release 7.5.3 | The feature allows ACLs in the router to classify the packets in the ingress direction based on Layer 2 header information such as source and destination MAC address, ether type, or 802.1ad DEI (Drop Eligible Indicator).<br>Layer 2 access control lists perform packet filtering to control which packets move through the network and where. Such controls help to limit incoming and outgoing network traffic and restrict the access of users and devices to the network at the port level.<br>This feature introduces the following commands:<br>• **ethernet-services access-group**<br>• **ethernet-services access-list**<br>• **show access-lists ethernet-services**<br>• **show access-lists ethernet-services usage pfilter** |

A Layer 2 access control lists (ACLs) consist of one or more access control entries (ACE) that collectively define the Layer 2 network traffic profile. This profile can then be referenced by Cisco IOS XR software features. Layer 2 access control list is also known as Ethernet services control access list. Each Ethernet services ACL includes an action element (permit or deny) based on criteria such as source and destination MAC address, Class of Service (CoS), ether-type, or 802.1ad DEI.

Layer 2 ACLs enable the router to copy the contents of an existing access list to another access list, clear counters for an access list using a specific sequence number, and apply sequence numbers to permit or deny statements.

**Note** For more information about Access Control list, see the *Implementing Access Lists* in I*P Addresses and Services Configuration Guide for Cisco 8000 Series Routers*.

# How a Layer 2 Access Control List Works

A Layer 2 access control list is a sequential list consisting of permit and deny statements that apply to Layer 2 configurations. The access list has a name by which it is referenced.

An access list can be configured and named, but it is not in effect until the access list is referenced by a command that accepts an access list. Multiple commands can reference the same access list. An access list can control Layer 2 traffic arriving at the router, but not traffic originating at the router and leaving the router.

# Layer 2 Access Control List Process and Rules

Use this process and rules when configuring Layer 2 access control list:

- The software tests the source or destination address of each packet being filtered against the conditions in the access list, one condition (permit or deny statement) at a time.
- If a packet does not match an access list statement, the packet is then tested against the next statement in the list.
- If a packet and an access list statement match, the remaining statements in the list are skipped and the packet is permitted or denied as specified in the matched statement. The first entry that the packet matches determines whether the software permits or denies the packet. That is, after the first match, no subsequent entries are considered.
- If the access list denies the address or protocol, the software discards the packet.
- If no conditions match, the software drops the packet because each access list ends with an unwritten or implicit deny statement. That is, if the packet has not been permitted or denied by the time it was tested against each statement, it is denied.
- The access list should contain at least one permit statement or else all packets are denied.
- Because the software stops testing conditions after the first match, the order of the conditions is critical. The same permit or deny statements specified in a different order could result in a packet being passed under one circumstance and denied in another circumstance.
- Inbound access lists process packets arriving at the router. An inbound access list is efficient because it saves the overhead of routing lookups if the packet is to be discarded because it is denied by the filtering tests. If the packet is permitted by the tests, it is then processed for routing. For inbound lists, permit means continue to process the packet after receiving it on an inbound interface; deny means discard the packet.
- An access list can not be removed if that access list is being applied by an access group in use. To remove an access list, remove the access group that is referencing the access list and then remove the access list.
- An access list must exist before you can use the **ethernet-services access-group** command.

# Restrictions

These restrictions apply to configuring Layer 2 access control lists:

- Layer 2 access control lists configuration is available only over physical and bundle interfaces and not over management interfaces.
- Layer 2 access control lists configuration is possible only in the ingress direction on an interface.
- Layer 2 access control lists are supported only for the field's L2 source and destination address, EtherType, Outer VLAN ID, Inner VLAN ID, Class of Service (COS), and VLAN DEI.
- Configuring VLAN range fields is not available in Layer 2 access control lists.
- Layer 2 access control lists do not support ACL logging.
- Layer 2 access control lists do not support User-Defined TCAM Keys for IPv4 and IPv6.
- Per Interface Statistics mode is not available in the Layer 2 access control list.
- Layer 2 access control lists do not support ERSPAN rate limit.

# Create Layer 2 Access Control List

Consider these when creating a Layer 2 access control list:

- Create the access list before applying it to an interface.
- Organize your access list so that more specific references appear before more general ones.

# Configuration

This section describes how you can configure Layer 2 access control lists.

```
Router# configure
Router(config)# ethernet-services access-list es_acl_1
Router(config-es-acl)# deny 00ff.eedd.0010 ff00.0000.00ff 0000.0100.0001 0000.0000.ffff
Router(config-es-acl)# permit host 000a.000b.000c host 00aa.ab99.1122 cos 1 dei
Router(config-es-acl)# deny host 000a.000b.000c host 00aa.dc11.ba99 cos 7 dei
Router(config-es-acl)# commit
Router(config)# interface HundredGigE 0/1/0/1
Router(config-if)# l2transport
Router(config-if-l2)# commit
Router(config-if-l2)# exit
Router(config-if)# ethernet-services access-group es_acl_1 ingress
Router(config-if)# commit
```

## Running Configuration

```
!
ethernet-services access-list es_acl_1
 10 deny 00ff.eedd.0000 ff00.0000.00ff 0000.0100.0000 0000.0000.ffff
 20 permit host 000a.000b.000c host 00aa.ab99.1122 cos 1 dei
 30 deny host 000a.000b.000c host 00aa.dc11.ba99 cos 7 dei
!
interface HundredGigE 0/1/0/1
 l2transport
```

```
  !
 ethernet-services access-group es_acl_1 ingress
!
```

# Verification

Verify that you have configured Layer 2 access control lists.

```
/* Verify the Layer 2 access control lists configuration */
Router# show access-lists ethernet-services es_acl_1  hardware ingress location 0/0/CPU0
Fri Oct 21 09:39:52.904 UTC
ethernet-services access-list es_acl_1
10 deny 00ff.eedd.0000 ff00.0000.00ff 0000.0100.0000 0000.0000.ffff (2051 matches)
20 permit host 000a.000b.000c host 00aa.ab99.1122 cos 1 dei
30 deny host 000a.000b.000c host 00aa.dc11.ba99 cos 7 dei (2050 matches)


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
```

The following example configuration includes capture keyword for local SPAN in Layer ACL:

```
monitor-session lspan1 ethernet
destination interface HundredGigE0/7/0/4

ethernet-services access-list l2spanacl1
50 permit 0000.1100.5105 0000.0000.0000 0000.2200.5105 0000.0000.0000 capture
60 deny 0000.1100.5106 0000.0000.0000 0000.2200.5106 0000.0000.0000 capture

interface Bundle-Ether302.52 l2transport
encapsulation dot1q 52
monitor-session lspan1 ethernet direction rx-only
acl
!
ethernet-services access-group l2spanacl1 ingress
```