CHAPTER 11

Configuring Access Control Lists

This chapter describes the access control list (ACL) features built into the Catalyst 2948G-L3 and the 4908G-L3 switch routers. This chapter contains the following sections:

Understanding ACLs

This section describes the types of ACLs:

Note ACLs are supported only on Gigabit Ethernet ports and corresponding Gigabit Ethernet subinterfaces.

Note ACLs are not supported on Bridge-Group Virtual Interface (BVI), Fast EtherChannel (FEC), Gigabit EtherChannel (GEC), and Fast Ethernet interfaces.

Note Reflexive and dynamic ACLs are not supported on the Catalyst 2948G-L3 and 4908G-L3 switch routers.

Note Access violations accounting is not supported on the Catalyst 2948G-L3 and 4908G-L3 switch routers.

Note ACL logging is supported only for packets going to the CPU. ACL logging is not supported for switched packets.

ACLs provide network control and security, allowing you to filter packet flow into or out of Catalyst 2948G-L3 and 4908G-L3 switch router interfaces. ACLs, which are sometimes called filters, allow you to restrict network use by certain users or devices. ACLs are created for each protocol and applied on the interface either for inbound or outbound traffic. They can be configured for all routed network protocols (IP or IPX) to filter packets for the protocol as they pass through a router. Only one ACL filter can be applied per direction, per protocol per (sub)interface.

When creating ACLs, you define criteria to apply to each packet processed by the switch router; the switch router decides whether to forward or block the packet based on whether or not the packet matches the criteria in your list. Packets that do not match any criteria in your list are automatically blocked by the implicit "deny all traffic" criteria statement at the end of every ACL.

Traffic that is switched by interface modules do not support ACL logging. ACL logging is supported for all traffic that goes to the CPU.

Note The enhanced Gigabit Ethernet interface module supports ternary content addressable memory (TCAM) sizes of 32K (32-bit) entries. The combined size of the protocol regions and access lists should not exceed your TCAM space. The default size of the ACL in a 32K TCAM is 512 (128-bit) entries. Before you configure the access-list region in TCAM, make sure that TCAM has enough space to accommodate the access-list region. The ACL content-addressable memory (CAM) size can be changed using Switching Database Manager (SDM) commands. If you are planning on supporting bigger ACLs, CAM space has to be reclaimed from other areas such as IPX, IP, or bridging.

IP ACLs

The following styles of ACLs for IP are supported:

- Standard IP ACLs use source addresses for matching operations.
- Extended IP ACLs use source and destination addresses for matching operations and optional protocol type and port numbers for finer granularity of control.
- Named ACLs use source addresses for matching operations.

Note By default, the end of the ACL contains an implicit deny statement for everything if it did not find a match before reaching the end. With standard ACLs, if you omit the mask from an associated IP host address ACL specification, 0.0.0.0 is assumed to be the mask.

After creating an ACL, you must apply it to an interface, as shown in the "Applying the ACL to an Interface" section on page 11-5.

Named IP ACLs

You can identify IP ACLs with an alphanumeric string (a name) or a number. Named IP ACLs allow you to configure more IP ACLs in a router than if you were to use numbered ACLs. If you identify your ACL with a name instead of a number, the mode and command syntax are slightly different.

Consider the following before configuring named ACLs:

- A standard ACL and an extended ACL cannot have the same name.
- Numbered ACLs are also available, as described in the section, "Creating Numbered Standard and Extended IP ACLs."

User Guidelines

Follow these guidelines when configuring IP network access control:

- ACL entries are programmed into TCAM.
- An implicit deny everything is defined at the end of all ACLs.
- You can enter ACL entries in any order without any performance impact.
- One entry is used for TCAM management purposes for every eight TCAM entries.
- ACL names must be unique across all protocols.
- Do not set up conditions that result in packets getting lost. This situation can happen when a device or interface is configured to advertise services on a network that has ACLs that deny these packets.

Creating IP ACLs

This section describes the types of ACLs supported by the 2948G-L3 and 4908G-L3 switch routers:

- Creating Numbered Standard and Extended IP ACLs, page 11-3
- Creating Named Standard IP ACLs, page 11-4

Creating Numbered Standard and Extended IP ACLs

To create a numbered standard IP ACL, perform one of the following tasks in global configuration mode:

Command	Purpose
access-list *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	Define a standard IP ACL using a source address and wildcard.
access-list *access-list-number* {**deny** | **permit**} **any**	Define a standard IP ACL using an abbreviation for the source and source mask of 0.0.0.0 255.255.255.255.

To create a numbered extended IP ACL, perform one of the following tasks in global configuration mode:

Command	Purpose
access-list *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*]	Define an extended IP ACL number and the access conditions.
access-list *access-list-number* {**deny** | **permit**} *protocol* **any any**	Define an extended IP ACL using an abbreviation for a source and source wildcard of 0.0.0.0 255.255.255.255 and an abbreviation for a destination and destination wildcard of 0.0.0.0 255.255.255.255.
access-list *access-list-number* {**deny** | **permit**} *protocol* **host** *source* **host** *destination*	Define an extended IP ACL using an abbreviation for a source and source wildcard of source 0.0.0.0, and an abbreviation for a destination and destination wildcard of destination 0.0.0.0.

Creating Named Standard IP ACLs

To create a named standard IP ACL, perform the following tasks beginning in global configuration mode:

Command	Purpose
ip access-list standard *name*	Define a standard IP ACL using a name.
deny {*source* [*source-wildcard*] | **any**} or **permit** {*source* [*source-wildcard*] | **any**}	In access-list configuration mode, specify one or more conditions permitted or denied. This determines whether the packet is passed or dropped.
exit	Exit access-list configuration mode.

Creating Named Extended IP ACLs

To create a named extended IP ACL, perform the following tasks beginning in global configuration mode:

Command	Purpose
ip access-list extended *name*	Define an extended IP ACL using a name.
{**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*]	In access-list configuration mode, specify the conditions allowed or denied.
	or
{**deny** | **permit**} *protocol* **any any**	Define an extended IP ACL using an abbreviation for a source and source wildcard of 0.0.0.0 255.255.255.255 and an abbreviation for a destination and destination wildcard of 0.0.0.0 255.255.255.255.
	or
{**deny** | **permit**} *protocol* **host** *source* **host** *destination*	Define an extended IP ACL using an abbreviation for a source and source wildcard of *source* 0.0.0.0 and an abbreviation for a destination and destination wildcard of *destination* 0.0.0.0.

Applying the ACL to an Interface

After you create an ACL, you can apply it to one or more interfaces. ACLs can be applied on either inbound or outbound direction of an interface. When controlling access to an interface, you can use a name or number.

To control access to the IP interface, perform the following task in interface configuration mode:

Command	Purpose
ip access-group {*access-list-number* | *name*} {**in** | **out**}	Control access to an interface.

If the ACL is applied on an interface in the inbound direction, the switch router performs one of the following operations:

- If a standard ACL is applied, the switch router compares the source IP address with the ACL.
- If an extended ACL is applied, the switch router compares the 5 tuple against the ACL.

If the comparison succeeds, the packet is permitted into the router and the switch router will make a decision to forward the packet to a particular interface. If the comparison fails, the packet will be dropped.

If the ACL is applied on an interface in the outbound direction, the switch router performs one of the following operations:

- If a standard ACL is applied, the switch router compares the source IP address with the ACL.
- If an extended ACL is applied, the switch router compares the 5 tuple against the ACL.

If the comparison succeeds, the switch router will transmit the packet out of the interface. If the comparison fails, the packet will be dropped.

Note An ICMP Host Unreachable message is not sent by the Catalyst 2948G-L3 or 4908G-L3 switch routers when a packet is discarded due to a deny ACL.

IPX ACLs

The following types of ACLs are supported for IPX:

- Standard IPX ACLs.
- Named IPX ACLs

To control access to IPX networks, first create ACLs and then apply them to individual interfaces using filters.

To control access to IPX networks, you must create ACLs. You can create ACLs using numbers or names. If you use numbers to identify your ACLs, you are limited to 100 ACLs per filter type. If you use names to identify your ACLs, you can have an unlimited number of ACLs.

ACL names must be unique across all protocols before configuring IPX-named ACLs. IPX-named ACLs allow you to identify IPX ACLs with an alphanumeric string (a name) rather than a number. You can configure an unlimited number of standard IPX-named ACLs.

IPX-named ACLs allow you to maintain security by using a separate and easily identifiable ACL for each user or interface. IPX-named ACLs also remove the limit of 100 lists.

IPX-named ACLs restrict traffic based on the source network number. You can further restrict traffic by specifying a destination address and a source and destination address mask. Standard IPX ACLs use numbers from 800 to 899 or names to identify them.

In the Catalyst 2948G-L3 and 4908G-L3 switch routers, ACLs are applied to the Gigabit Ethernet interface. Only generic filters for inbound and outbound packets based on the contents of the IPX network header are supported.

User Guidelines

Follow these guidelines when configuring IPX network access control:

- In the Catalyst 2948G-L3 switch router, the processing performance does not depend on the number of ACEs in the ACL.
- An implicit deny everything entry is defined at the end of an ACL.
- The ACL entries are programmed into TCAM.
- An implicit deny everything is defined at the end of all ACLs.
- You can enter ACL entries in any order without any impact on performance. This is true for all TCAM-based support for access lists.

- One entry is used for TCAM management purposes for every eight TCAM entries.
- Do not set up conditions that result in packets getting lost. This situation can happen when a device or interface is configured to advertise services on a network that has ACLs that deny these packets.
- ACL names must be unique across all protocols.

Note IPX-extended ACL numbers 900 to 999 and the names that identify them are not supported on the Catalyst 2948G-L3 and 4908G-L3 switch routers.

Creating IPX ACLs

The following sections describe how to perform these tasks:

- Creating IPX ACLs Using Numbers, page 11-7
- Creating IPX ACLs Using Names, page 11-7

Note The Catalyst 2948G-L3 and 4908G-L3 switch routers do not support the *.source-node* and *source node-mask* command variables.

Creating IPX ACLs Using Numbers

To create IPX ACLs using numbers, perform the following task in global configuration mode:

Command	Purpose
access-list *access-list-number* {**deny** | **permit**} *source-network* [*destination-network* [*.destination-node* [*destination-node-mask*]]]	Create a standard IPX ACL using a number. Generic, routing, and broadcast filters use this type of ACL.

Creating IPX ACLs Using Names

To create a named standard IPX ACL, perform the following tasks in global configuration mode:

Command	Purpose
ipx access-list standard *name*	Define a standard IPX ACL using a name. (Generic, routing, and broadcast filters use this type of ACL.)
{**deny** | **permit**} *source-network* [*destination-network* [*.destination-node* [*destination-node-mask*]]]	In access-list configuration mode, specify one or more conditions allowed or denied. The condition determines whether the packet is passed or dropped.
exit	Exit access-list configuration mode.

Applying the IPX ACL to an Interface

IPX ACLs determine which data packets to receive from or send to an interface, based on the packet's source and destination addresses, IPX protocol type, and source and destination socket numbers.

To create an IPX ACL, create a standard or an extended access list as described in the "Creating IPX ACLs" section on page 11-7 and then apply the ACL to an interface.

To apply an IPX ACL to an interface, perform the following task in interface configuration mode:

Command	Purpose
ipx access-group {*access-list-number* | *name*} [**in** | **out**]	Apply a generic filter to an interface.

Modifying ACL TCAM Size

You can change the TCAM size by entering the **sdm access-list** command. For more information on ACL TCAM sizes, see the "Configuring Access Control List Size in TCAM" section on page 10-4.

Note To increase the ACL TCAM size, you must decrease another region's TCAM size, such as IP, IPX, IP multicast, or bridging.

Caution You will need to increase the TCAM size if you see the following error message:

```
Warning:Programming TCAM entries failed
Please remove last ACL command to re-activate ACL operation.
!<ACL number or name> <IP or IPX> <INPUT_ACL or OUTPUT_ACL> from TCAM group for
!<interface>
Please see the documentation to see if TCAM space can be
increased on this platform to alleviate the problem.
```