



IPv4 ACLs

- [Information about Network Security with ACLs, on page 1](#)
- [Restrictions for Configuring IPv4 Access Control Lists, on page 7](#)
- [How to Configure ACLs, on page 8](#)

Information about Network Security with ACLs

This chapter describes how to configure network security on the switch by using access control lists (ACLs), which in commands and tables are also referred to as access lists.

ACL Overview

Packet filtering can help limit network traffic and restrict network use by certain users or devices. ACLs filter traffic as it passes through a controller and permit or deny packets crossing specified interfaces. An ACL is a sequential collection of permit and deny conditions that apply to packets. When a packet is received on an interface, the switch compares the fields in the packet against any applied ACLs to verify that the packet has the required permissions to be forwarded, based on the criteria specified in the access lists. One by one, it tests packets against the conditions in an access list. The first match decides whether the controller accepts or rejects the packets. Because the controller stops testing after the first match, the order of conditions in the list is critical. If no conditions match, the controller rejects the packet. If there are no restrictions, the controller forwards the packet; otherwise, the controller drops the packet. The controller can use ACLs on all packets it forwards. There is implicit any host deny deny rule.

You configure access lists on a controller to provide basic security for your network. If you do not configure ACLs, all packets passing through the switch could be allowed onto all parts of the network. You can use ACLs to control which hosts can access different parts of a network or to decide which types of traffic are forwarded or blocked at router interfaces. For example, you can allow e-mail traffic to be forwarded but not Telnet traffic.



Note EWC does not support ACL on the Gi0 port as EWC does not support interface or port ACLs.

Access Control Entries

An ACL contains an ordered list of access control entries (ACEs). Each ACE specifies *permit* or *deny* and a set of conditions the packet must satisfy in order to match the ACE. The meaning of *permit* or *deny* depends on the context in which the ACL is used.



Note The maximum number of ACEs that can be applied under an access policy (ACL) for central switching is 256 ACEs. The maximum number of ACEs applicable for Flex Mode or Local Switching is 64 ACEs.

ACL Supported Types

The switch supports IP ACLs and Ethernet (MAC) ACLs:

- IP ACLs filter IPv4 traffic, including TCP, User Datagram Protocol (UDP), Internet Group Management Protocol (IGMP), and Internet Control Message Protocol (ICMP).
- Ethernet ACLs filter non-IP traffic.

This switch also supports quality of service (QoS) classification ACLs.

ACEs and Fragmented and Unfragmented Traffic

IP packets can be fragmented as they cross the network. When this happens, only the fragment containing the beginning of the packet contains the Layer 4 information, such as TCP or UDP port numbers, ICMP type and code, and so on. All other fragments are missing this information.

Some access control entries (ACEs) do not check Layer 4 information and therefore can be applied to all packet fragments. ACEs that do test Layer 4 information cannot be applied in the standard manner to most of the fragments in a fragmented IP packet. When the fragment contains no Layer 4 information and the ACE tests some Layer 4 information, the matching rules are modified:

- Permit ACEs that check the Layer 3 information in the fragment (including protocol type, such as TCP, UDP, and so on) are considered to match the fragment regardless of what the missing Layer 4 information might have been.



Note For TCP ACEs with L4 Ops, the fragmented packets will be dropped per RFC 1858.

- Deny ACEs that check Layer 4 information never match a fragment unless the fragment contains Layer 4 information.

ACEs and Fragmented and Unfragmented Traffic Examples

Consider access list 102, configured with these commands, applied to three fragmented packets:

```
Device(config)# access-list 102 permit tcp any host 10.1.1.1 eq smtp
Device(config)# access-list 102 deny tcp any host 10.1.1.2 eq telnet
Device(config)# access-list 102 permit tcp any host 10.1.1.2
```

```
Device(config)# access-list 102 deny tcp any any
```



Note In the first and second ACEs in the examples, the *eq* keyword after the destination address means to test for the TCP-destination-port well-known numbers equaling Simple Mail Transfer Protocol (SMTP) and Telnet, respectively.

- Packet A is a TCP packet from host 10.2.2.2, port 65000, going to host 10.1.1.1 on the SMTP port. If this packet is fragmented, the first fragment matches the first ACE (a permit) as if it were a complete packet because all Layer 4 information is present. The remaining fragments also match the first ACE, even though they do not contain the SMTP port information, because the first ACE only checks Layer 3 information when applied to fragments. The information in this example is that the packet is TCP and that the destination is 10.1.1.1.
- Packet B is from host 10.2.2.2, port 65001, going to host 10.1.1.2 on the Telnet port. If this packet is fragmented, the first fragment matches the second ACE (a deny) because all Layer 3 and Layer 4 information is present. The remaining fragments in the packet do not match the second ACE because they are missing Layer 4 information. Instead, they match the third ACE (a permit).

Because the first fragment was denied, host 10.1.1.2 cannot reassemble a complete packet, so packet B is effectively denied. However, the later fragments that are permitted will consume bandwidth on the network and resources of host 10.1.1.2 as it tries to reassemble the packet.

- Fragmented packet C is from host 10.2.2.2, port 65001, going to host 10.1.1.3, port ftp. If this packet is fragmented, the first fragment matches the fourth ACE (a deny). All other fragments also match the fourth ACE because that ACE does not check any Layer 4 information and because Layer 3 information in all fragments shows that they are being sent to host 10.1.1.3, and the earlier permit ACEs were checking different hosts.

Standard and Extended IPv4 ACLs

This section describes IP ACLs.

An ACL is a sequential collection of permit and deny conditions. One by one, the switch tests packets against the conditions in an access list. The first match determines whether the switch accepts or rejects the packet. Because the switch stops testing after the first match, the order of the conditions is critical. If no conditions match, the switch denies the packet.

The software supports these types of ACLs or access lists for IPv4:

- Standard IP access lists use source addresses for matching operations.
- Extended IP access lists use source and destination addresses for matching operations and optional protocol-type information for finer granularity of control.



Note Only extended ACLs are supported while the standard ACLs are not supported.

IPv4 ACL Switch Unsupported Features

Configuring IPv4 ACLs on the switch is the same as configuring IPv4 ACLs on other Cisco switches and routers.

The following ACL-related features are not supported:

- Non-IP protocol ACLs
- IP accounting
- Reflexive ACLs, URL Redirect ACLs and Dynamic ACLs are not supported.

Access List Numbers

The number you use to denote your ACL shows the type of access list that you are creating.

This lists the access-list number and corresponding access list type and shows whether or not they are supported in the switch. The switch supports IPv4 standard and extended access lists, numbers 1 to 199 and 1300 to 2699.

Table 1: Access List Numbers

| Access List Number | Type | Supported |
|--------------------|--|-----------|
| 1–99 | IP standard access list | Yes |
| 100–199 | IP extended access list | Yes |
| 200–299 | Protocol type-code access list | No |
| 300–399 | DECnet access list | No |
| 400–499 | XNS standard access list | No |
| 500–599 | XNS extended access list | No |
| 600–699 | AppleTalk access list | No |
| 700–799 | 48-bit MAC address access list | No |
| 800–899 | IPX standard access list | No |
| 900–999 | IPX extended access list | No |
| 1000–1099 | IPX SAP access list | No |
| 1100–1199 | Extended 48-bit MAC address access list | No |
| 1200–1299 | IPX summary address access list | No |
| 1300–1999 | IP standard access list (expanded range) | Yes |
| 2000–2699 | IP extended access list (expanded range) | Yes |

In addition to numbered standard and extended ACLs, you can also create standard and extended named IP ACLs by using the supported numbers. That is, the name of a standard IP ACL can be 1 to 99; the name of

an extended IP ACL can be 100 to 199. The advantage of using named ACLs instead of numbered lists is that you can delete individual entries from a named list.

Numbered Standard IPv4 ACLs

When creating an ACL, remember that, by default, the end of the ACL contains an implicit deny statement for all packets that it did not find a match for before reaching the end. With standard access lists, if you omit the mask from an associated IP host address ACL specification, 0.0.0.0 is assumed to be the mask.

The switch always rewrites the order of standard access lists so that entries with **host** matches and entries with matches having a *don't care* mask of 0.0.0.0 are moved to the top of the list, above any entries with non-zero *don't care* masks. Therefore, in **show** command output and in the configuration file, the ACEs do not necessarily appear in the order in which they were entered.

After creating a numbered standard IPv4 ACL, you can apply it to terminal lines (virtual teletype (VTY) lines), or to interfaces.

Numbered Extended IPv4 ACLs

Although standard ACLs use only source addresses for matching, you can use extended ACL source and destination addresses for matching operations and optional protocol type information for finer granularity of control. When you are creating ACEs in numbered extended access lists, remember that after you create the ACL, any additions are placed at the end of the list. You cannot reorder the list or selectively add or remove ACEs from a numbered list.

The switch does not support dynamic or reflexive access lists. It also does not support filtering based on the type of service (ToS) minimize-monetary-cost bit.

Some protocols also have specific parameters and keywords that apply to that protocol.

You can define an extended TCP, UDP, ICMP, IGMP, or other IP ACL. The switch also supports these IP protocols:

These IP protocols are supported:

- Authentication Header Protocol (**ahp**)
- Encapsulation Security Payload (**esp**)
- Enhanced Interior Gateway Routing Protocol (**eigrp**)
- generic routing encapsulation (**gre**)
- Internet Control Message Protocol (**icmp**)
- Internet Group Management Protocol (**igmp**)
- any Interior Protocol (**ip**)
- IP in IP tunneling (**ipinip**)
- KA9Q NOS-compatible IP over IP tunneling (**nos**)
- Open Shortest Path First routing (**ospf**)
- Payload Compression Protocol (**pcp**)
- Protocol-Independent Multicast (**pim**)
- Transmission Control Protocol (**tcp**)

- User Datagram Protocol (**udp**)

Named IPv4 ACLs

You can identify IPv4 ACLs with an alphanumeric string (a name) rather than a number. You can use named ACLs to configure more IPv4 access lists in a router than if you were to use numbered access lists. If you identify your access list with a name rather than a number, the mode and command syntax are slightly different. However, at times, not all commands that use IP access lists accept a named access list.



Note The name you give to a standard or extended ACL can also be a number in the supported range of access list numbers. That is, the name of a standard IP ACL can be 1 to 99 and . The advantage of using named ACLs instead of numbered lists is that you can delete individual entries from a named list.

Consider these guidelines before configuring named ACLs:

- Numbered ACLs are also available.
- A standard ACL and an extended ACL cannot have the same name.

ACL Logging

The controller software can provide logging messages about packets permitted or denied by a standard IP access list. That is, any packet that matches the ACL causes an informational logging message about the packet to be sent to the console. The level of messages logged to the console is controlled by the **logging console** commands controlling the syslog messages.



Note Because routing is done in hardware and logging is done in software, if a large number of packets match a *permit* or *deny* ACE containing a **log** keyword, the software might not be able to match the hardware processing rate, and not all packets will be logged.

The first packet that triggers the ACL causes a logging message right away, and subsequent packets are collected over 5-minute intervals before they appear or logged. The logging message includes the access list number, whether the packet was permitted or denied, the source IP address of the packet, and the number of packets from that source permitted or denied in the prior 5-minute interval.



Note The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing due to too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list.

Hardware and Software Treatment of IP ACLs

ACL processing is performed in hardware. If the hardware reaches its capacity to store ACL configurations, all packets on that interface are dropped.

The ACL scale for controllers is as follows:

- Cisco Catalyst 9800-40 Wireless Controller, Cisco Catalyst 9800-L Wireless Controller, Cisco Catalyst 9800-CL Wireless Controller (small and medium) support 128 ACLs with 128 Access List Entries (ACEs).
- Cisco Catalyst 9800-80 Wireless Controller and Cisco Catalyst 9800-CL Wireless Controller (large) support 256 ACLs and 256 ACEs.
- FlexConnect and Fabric mode APs support 96 ACLs.



Note If an ACL configuration cannot be implemented in the hardware due to an out-of-resource condition on the controller, then only the traffic in that VLAN arriving on that controller is affected.

When you enter the **show ip access-lists** privileged EXEC command, the match count displayed does not account for packets that are access controlled in hardware. Use the `show ip access-lists hardware` privileged EXEC command to obtain some basic hardware ACL statistics for switched and routed packets.

IPv4 ACL Interface Considerations

For inbound ACLs, after receiving a packet, the controller checks the packet against the ACL. If the ACL permits the packet, the controller continues to process the packet. If the ACL rejects the packet, the controller discards the packet.

For outbound ACLs, after receiving and routing a packet to a controlled interface, the controller checks the packet against the ACL. If the ACL permits the packet, the controller sends the packet. If the ACL rejects the packet, the controller discards the packet.

If an undefined ACL has nothing listed in it, it is an empty access list.

Restrictions for Configuring IPv4 Access Control Lists

The following are restrictions for configuring network security with ACLs:

General Network Security

The following are restrictions for configuring network security with ACLs:

- A standard ACL and an extended ACL cannot have the same name.
- Though visible in the command-line help strings, **AppleTalk** is not supported as a matching condition for the **deny** and **permit** MAC access-list configuration mode commands.
- DNS traffic is permitted by default with or without ACL entries for clients that are awaiting web authentication.

IP Access List Entry Sequence Numbering

- This feature does not support dynamic, reflexive, or firewall access lists.

How to Configure ACLs

Configuring IPv4 ACLs (GUI)

Procedure

- Step 1** Choose **Configuration > Security > ACL**.
- Step 2** Click **Add**.
- Step 3** In the **Add ACL Setup** dialog box, enter the following parameters.
- **ACL Name:** Enter the name for the ACL.
 - **ACL Type:** IPv4 Standard.
 - **Sequence:** Enter the sequence number.
 - **Action:** Choose **Permit** or **Deny** the packet flow from the drop-down list.
 - **Source Type:** Choose **any**, **Host** or **Network** from which the packet is sent.
 - **Log:** Enable or disable logging.
- Step 4** Click **Add**.
- Step 5** Add the rest of the rules and click **Apply to Device**.
-

Configuring IPv4 ACLs

Follow the procedure given below to use IP ACLs on the switch:

Procedure

- Step 1** Create an ACL by specifying an access list number or name and the access conditions.
- Step 2** Apply the ACL to interfaces or terminal lines..
-

Creating a Numbered Standard ACL (GUI)

Procedure

- Step 1** Choose **Configuration > Security > ACL**.
- Step 2** On the **ACL** page, click **Add**.

- Step 3** In the **Add ACL Setup** window, enter the following parameters.
- **ACL Name:** Enter the name for the ACL.
 - **ACL Type:** IPv4 Standard.
 - **Sequence:** Enter the sequence number.
 - **Action:** Choose **Permit** or **Deny** access from the drop-down list.
 - **Source Type:** Choose **any**, **Host** or **Network**
 - **Log:** Enable or disable logging, this is limited to ACLs associated to Layer 3 interface only.
- Step 4** Click **Add**.
- Step 5** Click **Save & Apply to Device**.

Creating a Numbered Standard ACL (CLI)

Follow the procedure given below to create a numbered standard ACL:

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | enable Example: <pre>Device> enable</pre> | Enables privileged EXEC mode. Enter your password if prompted. |
| Step 2 | configure terminal Example: <pre>Device# configure terminal</pre> | Enters global configuration mode. |
| Step 3 | access-list <i>access-list-number</i> {deny permit} <i>source source-wildcard</i>] Example: <pre>Device(config)# access-list 2 deny your_host</pre> | Defines a standard IPv4 access list by using a source address and wildcard. The <i>access-list-number</i> is a decimal number from 1 to 99 or 1300 to 1999. Enter deny or permit to specify whether to deny or permit access if conditions are matched. The <i>source</i> is the source address of the network or host from which the packet is being sent specified as: <ul style="list-style-type: none"> • The 32-bit quantity in dotted-decimal format. |

| | Command or Action | Purpose |
|---------------|---|--|
| | | <ul style="list-style-type: none"> The keyword any as an abbreviation for <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. You do not need to enter a source-wildcard. The keyword host as an abbreviation for <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0. <p>(Optional) The <i>source-wildcard</i> applies wildcard bits to the source.</p> <p>Note Logging is supported only on ACLs attached to Layer 3 interfaces.</p> |
| Step 4 | end Example: <pre>Device(config)# end</pre> | Returns to privileged EXEC mode. |
| Step 5 | show running-config Example: <pre>Device# show running-config</pre> | Verifies your entries. |
| Step 6 | copy running-config startup-config Example: <pre>Device# copy running-config startup-config</pre> | (Optional) Saves your entries in the configuration file. |

Creating a Numbered Extended ACL (GUI)

Procedure

-
- Step 1** Choose **Configuration > Security > ACL**.
- Step 2** On the **ACL** page, click **Add**.
- Step 3** In the **Add ACL Setup** window, enter the following parameters.
- **ACL Name:** Enter the name for the ACL.
 - **ACL Type:** IPv4 Extended.
 - **Sequence:** Enter the sequence number.

- **Action:** Choose **Permit** or **Deny** the packet flow from the drop-down list.
- **Source Type:** Choose **any**, **Host** or **Network** from which the packet is sent.
- **Destination Type:** Choose **any**, **Host** or **Network** to which the packet is sent.
- **Protocol:** Choose a protocol from the drop-down list.
- **Log:** Enable or disable logging.
- **DSCP:** Enter to match packets with the DSCP value

Step 4 Click **Add**.

Step 5 Click **Save & Apply to Device**.

Creating a Numbered Extended ACL (CLI)

Follow the procedure given below to create a numbered extended ACL:

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | configure terminal Example: Device# <code>configure terminal</code> | Enters global configuration mode. |
| Step 2 | access-list <i>access-list-number</i> { deny permit } <i>protocol source source-wildcard destination</i> <i>destination-wildcard</i> [precedence <i>precedence</i>] [tos <i>tos</i>] [fragments] [time-range <i>time-range-name</i>] [dscp <i>dscp</i>] Example: Device(config)# <code>access-list 101 permit</code> <code>ip host 10.1.1.2 any precedence 0 tos 0</code> <code>log</code> | Defines an extended IPv4 access list and the access conditions. The <i>access-list-number</i> is a decimal number from 100 to 199 or 2000 to 2699. Enter deny or permit to specify whether to deny or permit the packet if conditions are matched. For <i>protocol</i> , enter the name or number of an IP protocol: ahp , eigrp , esp , gre , icmp , igmp , igrp , ip , ipinip , nos , ospf , pcp , pim , tcp , or udp , or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the keyword ip . Note This step includes options for most IP protocols. For additional specific parameters for TCP, UDP, ICMP, and IGMP, see the following steps. |

| | Command or Action | Purpose |
|--|-------------------|--|
| | | <p>The <i>source</i> is the number of the network or host from which the packet is sent.</p> <p>The <i>source-wildcard</i> applies wildcard bits to the source.</p> <p>The <i>destination</i> is the network or host number to which the packet is sent.</p> <p>The <i>destination-wildcard</i> applies wildcard bits to the destination.</p> <p>Source, source-wildcard, destination, and destination-wildcard can be specified as:</p> <ul style="list-style-type: none"> • The 32-bit quantity in dotted-decimal format. • The keyword any for 0.0.0.0 255.255.255.255 (any host). • The keyword host for a single host 0.0.0.0. <p>The other keywords are optional and have these meanings:</p> <ul style="list-style-type: none"> • precedence—Enter to match packets with a precedence level specified as a number from 0 to 7 or by name: routine (0), priority (1), immediate (2), flash (3), flash-override (4), critical (5), internet (6), network (7). • fragments—Enter to check non-initial fragments. • tos—Enter to match by type of service level, specified by a number from 0 to 15 or a name: normal (0), max-reliability (2), max-throughput (4), min-delay (8). • time-range—Specify the time-range name. • dscp—Enter to match packets with the DSCP value specified by a number from 0 to 63, or use the question mark (?) to see a list of available values. |

| | Command or Action | Purpose |
|---------------|---|---|
| | | <p>Note Your embedded controller must support the ability to:</p> <ul style="list-style-type: none"> • Mark DCSP • Mark UP • Map DSCP and UP <p>For more information on DSCP-to-UP Mapping, see:</p> <p>https://tools.ietf.org/html/draft-ietf-tsvwg-ieee-802-11-01</p> <p>Note If you enter a dscp value, you cannot enter tos or precedence. You can enter both a tos and a precedence value with no dscp.</p> |
| Step 3 | <p>access-list <i>access-list-number</i> {deny permit} tcp <i>source source-wildcard</i> [<i>operator port</i>] <i>destination destination-wildcard</i> [<i>operator port</i>] [precedence <i>precedence</i>] [tos <i>tos</i>] [fragments] [time-range <i>time-range-name</i>] [dscp <i>dscp</i>] [<i>flag</i>]</p> <p>Example:</p> <pre>Device(config)# access-list 101 permit tcp any any eq 500</pre> | <p>Defines an extended TCP access list and the access conditions.</p> <p>The parameters are the same as those described for an extended IPv4 ACL, with these exceptions:</p> <p>(Optional) Enter an <i>operator</i> and <i>port</i> to compare source (if positioned after <i>source source-wildcard</i>) or destination (if positioned after <i>destination destination-wildcard</i>) port. Possible operators include eq (equal), gt (greater than), lt (less than), neq (not equal), and range (inclusive range). Operators require a port number (range requires two port numbers separated by a space).</p> <p>Enter the <i>port</i> number as a decimal number (from 0 to 65535) or the name of a TCP port. Use only TCP port numbers or names when filtering TCP.</p> <p>The other optional keywords have these meanings:</p> <ul style="list-style-type: none"> • <i>flag</i>—Enter one of these flags to match by the specified TCP header bits: ack (acknowledge), fin (finish), psh (push), rst (reset), syn (synchronize), or urg (urgent). |

| | Command or Action | Purpose |
|--------|--|--|
| Step 4 | <p>access-list <i>access-list-number</i> {deny permit} udp <i>source source-wildcard</i> [<i>operator port</i>] <i>destination destination-wildcard</i> [<i>operator port</i>] [precedence <i>precedence</i>] [tos <i>tos</i>] [fragments] [time-range <i>time-range-name</i>] [dscp <i>dscp</i>]</p> <p>Example:</p> <pre>Device(config)# access-list 101 permit udp any any eq 100</pre> | <p>(Optional) Defines an extended UDP access list and the access conditions.</p> <p>The UDP parameters are the same as those described for TCP except that the [operator [port]] port number or name must be a UDP port number or name, and the flag not valid for UDP.</p> |
| Step 5 | <p>access-list <i>access-list-number</i> {deny permit} icmp <i>source source-wildcard destination</i> <i>destination-wildcard</i> [<i>icmp-type</i> [<i>icmp-type</i> <i>icmp-code</i>] [<i>icmp-message</i>]] [precedence <i>precedence</i>] [tos <i>tos</i>] [fragments] [time-range <i>time-range-name</i>] [dscp <i>dscp</i>]</p> <p>Example:</p> <pre>Device(config)# access-list 101 permit icmp any any 200</pre> | <p>Defines an extended ICMP access list and the access conditions.</p> <p>The ICMP parameters are the same as those described for most IP protocols in an extended IPv4 ACL, with the addition of the ICMP message type and code parameters. These optional keywords have these meanings:</p> <ul style="list-style-type: none"> • <i>icmp-type</i>—Enter to filter by ICMP message type, a number from 0 to 255. • <i>icmp-code</i>—Enter to filter ICMP packets that are filtered by the ICMP message code type, a number from 0 to 255. • <i>icmp-message</i>—Enter to filter ICMP packets by the ICMP message type name or the ICMP message type and code name. |
| Step 6 | <p>access-list <i>access-list-number</i> {deny permit} igmp <i>source source-wildcard destination</i> <i>destination-wildcard</i> [<i>igmp-type</i>] [precedence <i>precedence</i>] [tos <i>tos</i>] [fragments] [time-range <i>time-range-name</i>] [dscp <i>dscp</i>]</p> <p>Example:</p> <pre>Device(config)# access-list 101 permit igmp any any 14</pre> | <p>(Optional) Defines an extended IGMP access list and the access conditions.</p> <p>The IGMP parameters are the same as those described for most IP protocols in an extended IPv4 ACL, with this optional parameter.</p> <p><i>igmp-type</i>—To match IGMP message type, enter a number from 0 to 15, or enter the message name: dvmrp, host-query, host-report, pim, or trace.</p> |
| Step 7 | <p>end</p> <p>Example:</p> <pre>Device(config)# end</pre> | <p>Returns to privileged EXEC mode.</p> |

Creating Named Standard ACLs (GUI)

Procedure

-
- Step 1** Click **Configuration > Security > ACL**.
- Step 2** Click **Add** to create a new ACL setup.
- Step 3** In the **Add ACL Setup** window, enter the following parameters.
- **ACL Name:** Enter the name for the ACL
 - **ACL Type:** IPv4 Standard
 - **Sequence:** The valid range is between 1 and 99 or 1300 and 1999
 - **Action:** Choose **Permit** or **Deny** access from the drop-down list.
 - **Source Type:** Choose **any**, **Host** or **Network**
 - **Log:** Enable or disable logging, this is limited to ACLs associated to Layer 3 interface only.
- Step 4** Click **Add** to add the rule.
- Step 5** Click **Save & Apply to Device**.
-

Creating Named Standard ACLs

Follow the procedure given below to create a standard ACL using names:

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | ip access-list standard <i>name</i> Example: Device(config)# ip access-list standard 20 | Defines a standard IPv4 access list using a name, and enter access-list configuration mode. The name can be a number from 1 to 99. |

| | Command or Action | Purpose |
|---------------|---|---|
| Step 4 | <p>Use one of the following:</p> <ul style="list-style-type: none"> • deny {<i>source</i> [<i>source-wildcard</i>] host <i>source</i> any} [log] • permit {<i>source</i> [<i>source-wildcard</i>] host <i>source</i> any} [log] <p>Example:</p> <pre>Device(config-std-nacl)# deny 192.168.0.0 0.0.255.255 255.255.0.0 0.0.255.255</pre> <p>or</p> <pre>Device(config-std-nacl)# permit 10.108.0.0 0.0.0.0 255.255.255.0 0.0.0.0</pre> | <p>In access-list configuration mode, specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.</p> <ul style="list-style-type: none"> • host <i>source</i>—A source and source wildcard of <i>source</i> 0.0.0.0. • any—A source and source wildcard of 0.0.0.0 255.255.255.255. |
| Step 5 | <p>end</p> <p>Example:</p> <pre>Device(config-std-nacl)# end</pre> | Returns to privileged EXEC mode. |
| Step 6 | <p>show running-config</p> <p>Example:</p> <pre>Device# show running-config</pre> | Verifies your entries. |
| Step 7 | <p>copy running-config startup-config</p> <p>Example:</p> <pre>Device# copy running-config startup-config</pre> | (Optional) Saves your entries in the configuration file. |

Creating Extended Named ACLs (GUI)

Procedure

-
- Step 1** Choose **Configuration > Security > ACL**.
- Step 2** Click **Add**.
- Step 3** In the **Add ACL Setup** window, enter the following parameters.
- **ACL Name:** Enter the name for the ACL.

- **ACL Type:** IPv4 Extended.
- **Sequence:** Enter the sequence number.
- **Action:** Choose **Permit** or **Deny** the packet flow from the drop-down list.
- **Source Type:** Choose **any**, **Host** or **Network** from which the packet is sent.
- **Destination Type:** Choose **any**, **Host** or **Network** to which the packet is sent.
- **Protocol:** Choose a protocol from the drop-down list.
- **Log:** Enable or disable logging.
- **DSCP:** Enter to match packets with the DSCP value

Step 4 Click **Add**.

Step 5 Add the rest of the rules and click **Apply to Device**.

Creating Extended Named ACLs

Follow the procedure given below to create an extended ACL using names:

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | ip access-list extended <i>name</i> Example: Device(config)# ip access-list extended 150 | Defines an extended IPv4 access list using a name, and enter access-list configuration mode. The name can be a number from 100 to 199. |
| Step 4 | {deny permit} protocol {source [source-wildcard] host source any} {destination [destination-wildcard] host destination any} [precedence precedence] [tos tos] [log] [time-range time-range-name] | In access-list configuration mode, specify the conditions allowed or denied. Use the log keyword to get access list logging messages, including violations. |

| | Command or Action | Purpose |
|---------------|---|---|
| | <p>Example:</p> <pre>Device(config-ext-nacl)# permit 0 any any</pre> | <ul style="list-style-type: none"> • host source—A source and source wildcard of <i>source</i> 0.0.0.0. • host destination—A destination and destination wildcard of <i>destination</i> 0.0.0.0. • any—A source and source wildcard or destination and destination wildcard of 0.0.0.0 255.255.255.255. |
| Step 5 | <p>end</p> <p>Example:</p> <pre>Device(config-ext-nacl)# end</pre> | Returns to privileged EXEC mode. |
| Step 6 | <p>show running-config</p> <p>Example:</p> <pre>Device# show running-config</pre> | Verifies your entries. |
| Step 7 | <p>copy running-config startup-config</p> <p>Example:</p> <pre>Device# copy running-config startup-config</pre> | (Optional) Saves your entries in the configuration file. |

When you are creating extended ACLs, remember that, 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. For standard ACLs, if you omit the mask from an associated IP host address access list specification, 0.0.0.0 is assumed to be the mask.

After you create an ACL, any additions are placed at the end of the list. You cannot selectively add ACL entries to a specific ACL. However, you can use **no permit** and **no deny** access-list configuration mode commands to remove entries from a named ACL.

Being able to selectively remove lines from a named ACL is one reason you might use named ACLs instead of numbered ACLs.

What to do next

After creating a named ACL, you can apply it to interfaces or to VLANs.