



## Configuring Network Security with ACLs

---

This chapter describes how to configure network security on the Catalyst 2970 switch by using access control lists (ACLs), which are also referred to in commands and tables as access lists.

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release, see the “Configuring IP Services” section in the “IP Addressing and Services” chapter of the *Cisco IOS IP Configuration Guide, Release 12.2*, and to these software configuration guides and command references:

- *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2*
- *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*
- *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.2*

This chapter consists of these sections:

- [Understanding ACLs, page 26-1](#)
- [Configuring IP ACLs, page 26-5](#)
- [Creating Named MAC Extended ACLs, page 26-22](#)
- [Configuring VLAN Maps, page 26-24](#)
- [Displaying ACL Configuration, page 26-31](#)

## Understanding ACLs

Packet filtering can help limit network traffic and restrict network use by certain users or devices. ACLs filter traffic as it passes through a switch and permit or deny packets crossing specified interfaces or VLANs. 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 switch accepts or rejects the packets. Because the switch stops testing after the first match, the order of conditions in the list is critical. If no conditions match, the switch rejects the packet. If there are no restrictions, the switch forwards the packet; otherwise, the switch drops the packet. The switch can use ACLs on all packets it forwards, including packets bridged within a VLAN.

You configure access lists on a switch 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. For example, you can allow e-mail traffic to be forwarded but not Telnet traffic.

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.

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

- IP ACLs filter IP 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. For more information, see the [“Classification Based on QoS ACLs” section on page 27-7](#).

This section includes information on these topics:

- [Supported ACLs, page 26-2](#)
- [Handling Fragmented and Unfragmented Traffic, page 26-4](#)

## Supported ACLs

The switch supports two applications of ACLs to filter traffic:

- Port ACLs access-control traffic entering a Layer 2 interface. The switch does not support port ACLs in the outbound direction. You can apply only one IP access list and one MAC access list to a Layer 2 interface.
- VLAN ACLs or VLAN maps access-control all packets (bridged and routed). You can use VLAN maps to filter traffic between devices in the same VLAN. VLAN maps are configured to provide access-control based on Layer 3 addresses for IP. Unsupported protocols are access-controlled through MAC addresses using Ethernet ACEs. After a VLAN map is applied to a VLAN, all packets (routed or bridged) entering the VLAN are checked against the VLAN map. Packets can either enter the VLAN through a switch port or through a routed port after being routed.

You can use input port ACLs and VLAN maps on the same switch. However, a port ACL takes precedence over a VLAN map. When an input port ACL is applied to an interface that belongs to a VLAN that has a VLAN map applied, incoming packets received at the interface are filtered by the port ACL. Other packets are filtered by the VLAN map.

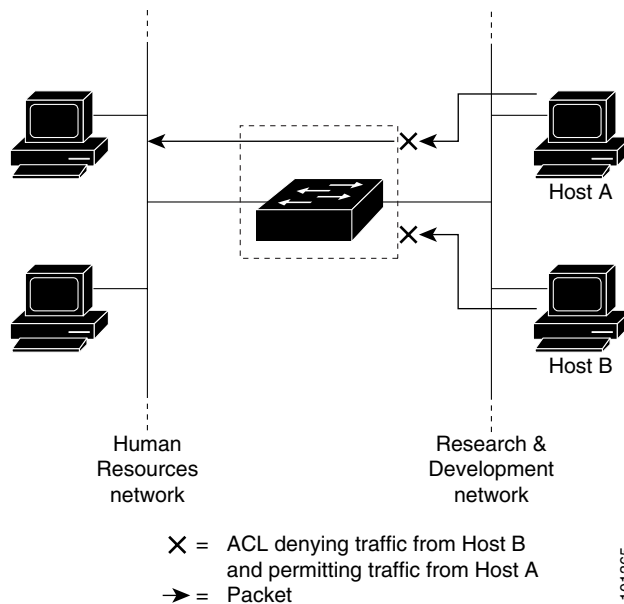
## Port ACLs

Port ACLs are ACLs that are applied to Layer 2 interfaces on a switch. Port ACLs are supported only on physical interfaces and not on EtherChannel interfaces and can be applied only on interfaces in the inbound direction. These access lists are supported on Layer 2 interfaces:

- Standard IP access lists using source addresses
- Extended IP access lists using source and destination addresses and optional protocol type information
- MAC extended access lists using source and destination MAC addresses and optional protocol type information

The switch examines ACLs associated with all inbound features configured on a given interface and permits or denies packet forwarding based on how the packet matches the entries in the ACL. In this way, ACLs are used to control access to a network or to part of a network. Figure 26-1 is an example of using port ACLs to control access to a network when all workstations are in the same VLAN. ACLs applied at the Layer 2 input would allow Host A to access the Human Resources network, but prevent Host B from accessing the same network. Port ACLs can only be applied to Layer 2 interfaces in the inbound direction.

**Figure 26-1 Using ACLs to Control Traffic to a Network**



When you apply a port ACL to a trunk port, the ACL filters traffic on all VLANs present on the trunk port. When you apply a port ACL to a port with voice VLAN, the ACL filters traffic on both data and voice VLANs.

With port ACLs, you can filter IP traffic by using IP access lists and non-IP traffic by using MAC addresses. You can filter both IP and non-IP traffic on the same Layer 2 interface by applying both an IP access list and a MAC access list to the interface.



**Note**

You cannot apply more than one IP access list and one MAC access list to a Layer 2 interface. If an IP access list or MAC access list is already configured on a Layer 2 interface and you apply a new IP access list or MAC access list to the interface, the new ACL replaces the previously configured one.

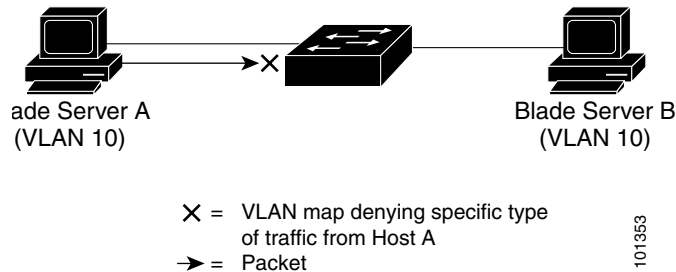
## VLAN Maps

You use VLAN ACLs or VLAN maps to filter traffic between devices in the same VLAN. When a VLAN map is applied to a VLAN, all packets being forwarded in the VLAN are checked against the VLAN map. VLAN maps are used for security packet filtering. VLAN maps are not defined by direction (input or output).

You can configure VLAN maps to match Layer 3 addresses for IP traffic. All non-IP protocols are access-controlled through MAC addresses and EtherType using MAC VLAN maps. (IP traffic *is not* access controlled by MAC VLAN maps.) You can enforce VLAN maps only on packets going through the switch; you cannot enforce VLAN maps on traffic between hosts on a hub or on another switch connected to this switch.

With VLAN maps, forwarding of packets is permitted or denied, based on the action specified in the map. Figure 26-2 illustrates how a VLAN map is applied to deny a specific type of traffic from Host A in VLAN 10 from being forwarded. You can apply only one VLAN map to a VLAN.

**Figure 26-2 Using VLAN Maps to Control Traffic**



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

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

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

## Configuring IP ACLs

Configuring IP ACLs on the switch is the same as configuring IP ACLs on other Cisco switches and routers. The process is briefly described here. For more detailed information on configuring ACLs, see the “Configuring IP Services” section in the “IP Addressing and Services” chapter of the *Cisco IOS IP Configuration Guide, Release 12.2*. For detailed information about the commands, see these documents:

- *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2*
- *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*
- *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.2*

The switch does not support these Cisco IOS router ACL-related features:

- Non-IP protocol ACLs (see [Table 26-1 on page 26-7](#)) or bridge-group ACLs
- IP accounting
- Inbound and outbound rate limiting (except with QoS ACLs)
- Reflexive ACLs or dynamic ACLs (except for some specialized dynamic ACLs used by the switch clustering feature)
- ACL logging

These are the steps to use IP ACLs on the switch:

- 
- 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. You can also apply standard and extended IP ACLs to VLAN maps.
-

This section includes the following information:

- [Creating Standard and Extended IP ACLs, page 26-6](#)
- [Applying an IP ACL to a Terminal Line, page 26-18](#)
- [Applying an IP ACL to an Interface, page 26-18](#)
- [Hardware and Software Treatment of IP ACLs, page 26-19](#)
- [IP ACL Configuration Examples, page 26-19](#)

## Creating Standard and Extended IP 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 IP:

- 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.

These sections describe access lists and how to create them:

- [Access List Numbers, page 26-7](#)
- [Creating a Numbered Standard ACL, page 26-8](#)
- [Creating a Numbered Extended ACL, page 26-9](#)
- [Resequencing ACEs in an ACL, page 26-13](#)
- [Creating Named Standard and Extended ACLs, page 26-13](#)
- [Using Time Ranges with ACLs, page 26-15](#)
- [Including Comments in ACLs, page 26-17](#)

## Access List Numbers

The number you use to denote your ACL shows the type of access list that you are creating. Table 26-1 lists the access-list number and corresponding access list type and shows whether or not they are supported in the switch. The switch supports IP standard and IP extended access lists, numbers 1 to 199 and 1300 to 2699.

**Table 26-1 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



### Note

In addition to numbered standard and extended ACLs, you can also create standard and extended named IP ACLs 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.

## Creating a Numbered Standard ACL

Beginning in privileged EXEC mode, follow these steps to create a numbered standard ACL:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>access-list</b> <i>access-list-number</i> { <b>deny</b>   <b>permit</b> } <i>source</i> [ <i>source-wildcard</i> ]	<p>Define a standard IP access list by using a source address and wildcard.</p> <p>The <i>access-list-number</i> is a decimal number from 1 to 99 or 1300 to 1999.</p> <p>Enter <b>deny</b> or <b>permit</b> to specify whether to deny or permit access if conditions are matched.</p> <p>The <i>source</i> is the source address of the network or host from which the packet is being sent specified as:</p> <ul style="list-style-type: none"> <li>• The 32-bit quantity in dotted-decimal format.</li> <li>• The keyword <b>any</b> 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.</li> <li>• The keyword <b>host</b> as an abbreviation for source and source-wildcard of <i>source</i> 0.0.0.0.</li> </ul> <p>(Optional) The <i>source-wildcard</i> applies wildcard bits to the source.</p>
Step 3	<b>end</b>	Return to privileged EXEC mode.
Step 4	<b>show access-lists</b> [ <i>number</i>   <i>name</i> ]	Show the access list configuration.
Step 5	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

Use the **no access-list** *access-list-number* global configuration command to delete the entire ACL. You cannot delete individual ACEs from numbered access lists.



### Note

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.

This example shows how to create a standard ACL to deny access to IP host 171.69.198.102, permit access to any others, and display the results.

```
Switch (config)# access-list 2 deny host 171.69.198.102
Switch (config)# access-list 2 permit any
Switch(config)# end
Switch# show access-lists
Standard IP access list 2
 10 deny 171.69.198.102
 20 permit any
```

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 IP ACL, you can apply it to terminal lines (see the “[Applying an IP ACL to a Terminal Line](#)” section on page 26-18), to interfaces (see the “[Applying an IP ACL to an Interface](#)” section on page 26-18), or to VLANs (see the “[Configuring VLAN Maps](#)” section on page 26-24).

## Creating a Numbered Extended ACL

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.

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

These IP protocols are supported (protocol keywords are in parentheses in bold):

Authentication Header Protocol (**ahp**), Enhanced Interior Gateway Routing Protocol (**eigrp**), Encapsulation Security Payload (**esp**), 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**), or User Datagram Protocol (**udp**).



---

**Note** ICMP echo-reply cannot be filtered. All other ICMP codes or types can be filtered.

---

For more details on the specific keywords for each protocol, see these software configuration guides and command references:

- *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2*
- *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*
- *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.2*



**Note**

---

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.

---

Supported parameters can be grouped into these categories: TCP, UDP, ICMP, IGMP, or other IP.

Beginning in privileged EXEC mode, follow these steps to create an extended ACL:

Command	Purpose
Step 1 <b>configure terminal</b>	Enter global configuration mode.
Step 2a <b>access-list</b> <i>access-list-number</i> { <b>deny</b>   <b>permit</b> } <i>protocol</i> <i>source source-wildcard</i> <i>destination destination-wildcard</i> [ <b>precedence</b> <i>precedence</i> ] [ <b>tos</b> <i>tos</i> ] [ <b>fragments</b> ] [ <b>time-range</b> <i>time-range-name</i> ] [ <b>dscp</b> <i>dscp</i> ]  <b>Note</b> If you enter a <b>dscp</b> value, you cannot enter <b>tos</b> or <b>precedence</b> . You can enter both a <b>tos</b> and a <b>precedence</b> value with no <b>dscp</b> .	Define an extended IP 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 <b>deny</b> or <b>permit</b> 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: <b>ahp</b> , <b>eigrp</b> , <b>esp</b> , <b>gre</b> , <b>icmp</b> , <b>igmp</b> , <b>igrp</b> , <b>ip</b> , <b>ipinip</b> , <b>nos</b> , <b>ospf</b> , <b>pcp</b> , <b>pim</b> , <b>tcp</b> , or <b>udp</b> , 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 <b>ip</b> .  <b>Note</b> This step includes options for most IP protocols. For additional specific parameters for TCP, UDP, ICMP, and IGMP, see steps 2b through 2e.  The <i>source</i> is the number of the network or host from which the packet is sent. The <i>source-wildcard</i> applies wildcard bits to the source. The <i>destination</i> is the network or host number to which the packet is sent. The <i>destination-wildcard</i> applies wildcard bits to the destination. Source, source-wildcard, destination, and destination-wildcard can be specified as: <ul style="list-style-type: none"><li>• The 32-bit quantity in dotted-decimal format.</li><li>• The keyword <b>any</b> for 0.0.0.0 255.255.255.255 (any host).</li><li>• The keyword <b>host</b> for a single host 0.0.0.0.</li></ul> The other keywords are optional and have these meanings: <ul style="list-style-type: none"><li>• <b>precedence</b>—Enter to match packets with a precedence level specified as a number from 0 to 7 or by name: <b>routin</b>e (0), <b>priority</b> (1), <b>immediate</b> (2), <b>flash</b> (3), <b>flash-override</b> (4), <b>critical</b> (5), <b>internet</b> (6), <b>network</b> (7).</li><li>• <b>fragments</b>—Enter to check non-initial fragments.</li><li>• <b>tos</b>—Enter to match by type of service level, specified by a number from 0 to 15 or a name: <b>normal</b> (0), <b>max-reliability</b> (2), <b>max-throughput</b> (4), <b>min-delay</b> (8).</li><li>• <b>time-range</b>—For an explanation of this keyword, see the “Using Time Ranges with ACLs” section on page 26-15.</li><li>• <b>dscp</b>—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.</li></ul>
or <b>access-list</b> <i>access-list-number</i> { <b>deny</b>   <b>permit</b> } <i>protocol any any</i> [ <b>precedence</b> <i>precedence</i> ] [ <b>tos</b> <i>tos</i> ] [ <b>fragments</b> ] [ <b>time-range</b> <i>time-range-name</i> ] [ <b>dscp</b> <i>dscp</i> ]	In access-list configuration mode, define an extended IP access list 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.  You can use the <b>any</b> keyword in place of source and destination address and wildcard.

	Command	Purpose
or	<b>access-list</b> <i>access-list-number</i> { <b>deny</b>   <b>permit</b> } <i>protocol</i> <b>host</b> <i>source</i> <b>host</b> <i>destination</i> [ <b>precedence</b> <i>precedence</i> ] [ <b>tos</b> <i>tos</i> ] [ <b>fragments</b> ] [ <b>time-range</b> <i>time-range-name</i> ] [ <b>dscp</b> <i>dscp</i> ]	Define an extended IP access list by using an abbreviation for a source and a source wildcard of <i>source</i> 0.0.0.0 and an abbreviation for a destination and destination wildcard of <i>destination</i> 0.0.0.0.  You can use the <b>host</b> keyword in place of the source and destination wildcard or mask.
Step 2b	<b>access-list</b> <i>access-list-number</i> { <b>deny</b>   <b>permit</b> } <b>tcp</b> <i>source</i> <i>source-wildcard</i> [ <i>operator</i> <i>port</i> ] <i>destination</i> <i>destination-wildcard</i> [ <i>operator</i> <i>port</i> ] [ <b>established</b> ] [ <b>precedence</b> <i>precedence</i> ] [ <b>tos</b> <i>tos</i> ] [ <b>fragments</b> ] [ <b>time-range</b> <i>time-range-name</i> ] [ <b>dscp</b> <i>dscp</i> ] [ <i>flag</i> ]	(Optional) Define an extended TCP access list and the access conditions.  Enter <b>tcp</b> for Transmission Control Protocol.  The parameters are the same as those described in Step 2a, with these exceptions:  (Optional) Enter an <i>operator</i> and <i>port</i> to compare source (if positioned after <i>source</i> <i>source-wildcard</i> ) or destination (if positioned after <i>destination</i> <i>destination-wildcard</i> ) port. Possible operators include <b>eq</b> (equal), <b>gt</b> (greater than), <b>lt</b> (less than), <b>neq</b> (not equal), and <b>range</b> (inclusive range). Operators require a port number ( <b>range</b> requires two port numbers separated by a space).  Enter the <i>port</i> number as a decimal number (from 0 to 65535) or the name of a TCP port. To see TCP port names, use the ? or see the “Configuring IP Services” section in the “IP Addressing and Services” chapter of the <i>Cisco IOS IP Configuration Guide, Release 12.2</i> . Use only TCP port numbers or names when filtering TCP.  The other optional keywords have these meanings: <ul style="list-style-type: none"> <li><b>established</b>—Enter to match an established connection. This has the same function as matching on the <b>ack</b> or <b>rst</b> flag.</li> <li><i>flag</i>—Enter one of these flags to match by the specified TCP header bits: <b>ack</b> (acknowledge), <b>fin</b> (finish), <b>psh</b> (push), <b>rst</b> (reset), <b>syn</b> (synchronize), or <b>urg</b> (urgent).</li> </ul>
Step 2c	<b>access-list</b> <i>access-list-number</i> { <b>deny</b>   <b>permit</b> } <b>udp</b> <i>source</i> <i>source-wildcard</i> [ <i>operator</i> <i>port</i> ] <i>destination</i> <i>destination-wildcard</i> [ <i>operator</i> <i>port</i> ] [ <b>precedence</b> <i>precedence</i> ] [ <b>tos</b> <i>tos</i> ] [ <b>fragments</b> ] [ <b>time-range</b> <i>time-range-name</i> ] [ <b>dscp</b> <i>dscp</i> ]	(Optional) Define an extended UDP access list and the access conditions.  Enter <b>udp</b> for the User Datagram Protocol.  The UDP parameters are the same as those described for TCP except that the [ <i>operator</i> [ <i>port</i> ]] port number or name must be a UDP port number or name, and the <b>flag</b> and <b>established</b> parameters are not valid for UDP.

	Command	Purpose
Step 2d	<b>access-list</b> <i>access-list-number</i> {deny   permit} <b>icmp</b> <i>source source-wildcard destination destination-wildcard</i> [ <i>icmp-type</i>   [ <i>icmp-type icmp-code</i> ]   [ <i>icmp-message</i> ]] [ <b>precedence</b> <i>precedence</i> ] [ <b>tos</b> <i>tos</i> ] [ <b>fragments</b> ] [ <b>time-range</b> <i>time-range-name</i> ] [ <b>dscp</b> <i>dscp</i> ]	(Optional) Define an extended ICMP access list and the access conditions. Enter <b>icmp</b> for Internet Control Message Protocol. The ICMP parameters are the same as those described for most IP protocols in Step 2a, with the addition of the ICMP message type and code parameters. These optional keywords have these meanings: <ul style="list-style-type: none"> <li><i>icmp-type</i>—Enter to filter by ICMP message type, a number from 0 to 255.</li> <li><i>icmp-code</i>—Enter to filter ICMP packets that are filtered by the ICMP message code type, a number from 0 to 255.</li> <li><i>icmp-message</i>—Enter to filter ICMP packets by the ICMP message type name or the ICMP message type and code name. To see a list of ICMP message type names and code names, use the <b>?</b>, or see the “Configuring IP Services” section of the <i>Cisco IOS IP Configuration Guide, Release 12.2</i>.</li> </ul>
Step 2e	<b>access-list</b> <i>access-list-number</i> {deny   permit} <b>igmp</b> <i>source source-wildcard destination destination-wildcard</i> [ <i>igmp-type</i> ] [ <b>precedence</b> <i>precedence</i> ] [ <b>tos</b> <i>tos</i> ] [ <b>fragments</b> ] [ <b>time-range</b> <i>time-range-name</i> ] [ <b>dscp</b> <i>dscp</i> ]	(Optional) Define an extended IGMP access list and the access conditions. Enter <b>igmp</b> for Internet Group Management Protocol. The IGMP parameters are the same as those described for most IP protocols in Step 2a, with this optional parameter. <i>igmp-type</i> —To match IGMP message type, enter a number from 0 to 15, or enter the message name ( <b>dvmrp</b> , <b>host-query</b> , <b>host-report</b> , <b>pim</b> , or <b>trace</b> ).
Step 3	<b>show access-lists</b> [ <i>number</i>   <i>name</i> ]	Verify the access list configuration.
Step 4	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

Use the **no access-list** *access-list-number* global configuration command to delete the entire access list. You cannot delete individual ACEs from numbered access lists.

This example shows how to create and display an extended access list to deny Telnet access from any host in network 171.69.198.0 to any host in network 172.20.52.0 and to permit any others. (The **eq** keyword after the destination address means to test for the TCP destination port number equaling Telnet.)

```
Switch(config)# access-list 102 deny tcp 171.69.198.0 0.0.0.255 172.20.52.0 0.0.0.255 eq telnet
Switch(config)# access-list 102 permit tcp any any
Switch(config)# end
Switch# show access-lists
Extended IP access list 102
 10 deny tcp 171.69.198.0 0.0.0.255 172.20.52.0 0.0.0.255 eq telnet
 20 permit tcp any any
```

After an ACL is created, any additions (possibly entered from the terminal) are placed at the end of the list. You cannot selectively add or remove access list entries from a numbered access list.



#### Note

When you are creating an ACL, remember that, by default, the end of the access list contains an implicit deny statement for all packets if it did not find a match before reaching the end.

After creating a numbered extended ACL, you can apply it to terminal lines (see the “Applying an IP ACL to a Terminal Line” section on page 26-18), to interfaces (see the “Applying an IP ACL to an Interface” section on page 26-18), or to VLANs (see the “Configuring VLAN Maps” section on page 26-24).

## Resequencing ACEs in an ACL

In Cisco IOS Release 12.2(18)SE and later, sequence numbers for the entries in an access list are automatically generated when you create a new ACL. You can use the **ip access-list resequence** global configuration command to edit the sequence numbers in an ACL and change the order in which ACEs are applied. For example, if you add a new ACE to an ACL, it is placed at the bottom of the list. By changing the sequence number, you can move the ACE to a different position in the ACL.

For more information about the **ip access-list resequence** command, see this URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fsaclseq.htm>

## Creating Named Standard and Extended ACLs

You can identify IP ACLs with an alphanumeric string (a name) rather than a number. You can use named ACLs to configure more IP 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, 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; 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.

Consider these guidelines and limitations before configuring named ACLs:

- Not all commands that accept a numbered ACL accept a named ACL. ACLs for packet filters and route filters on interfaces can use a name. VLAN maps also accept a name.
- A standard ACL and an extended ACL cannot have the same name.
- Numbered ACLs are also available, as described in the “Creating Standard and Extended IP ACLs” section on page 26-6.
- You can use standard and extended ACLs (named or numbered) in VLAN maps.

Beginning in privileged EXEC mode, follow these steps to create a standard ACL using names:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>ip access-list standard</b> <i>name</i>	Define a standard IP access list using a name, and enter access-list configuration mode.
		<b>Note</b> The name can be a number from 1 to 99.

	Command	Purpose
Step 3	<b>deny</b> { <i>source</i> [ <i>source-wildcard</i> ]   <b>host</b> <i>source</i>   <b>any</b> } or <b>permit</b> { <i>source</i> [ <i>source-wildcard</i> ]   <b>host</b> <i>source</i>   <b>any</b> }	In access-list configuration mode, specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped. <ul style="list-style-type: none"> <li>• <b>host</b> <i>source</i>—A source and source wildcard of <i>source</i> 0.0.0.0.</li> <li>• <b>any</b>—A source and source wildcard of 0.0.0.0 255.255.255.255.</li> </ul>
Step 4	<b>end</b>	Return to privileged EXEC mode.
Step 5	<b>show access-lists</b> [ <i>number</i>   <i>name</i> ]	Show the access list configuration.
Step 6	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To remove a named standard ACL, use the **no ip access-list standard** *name* global configuration command.

Beginning in privileged EXEC mode, follow these steps to create an extended ACL using names:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>ip access-list extended</b> <i>name</i>	Define an extended IP access list using a name and enter access-list configuration mode. <b>Note</b> The name can be a number from 100 to 199.
Step 3	{ <b>deny</b>   <b>permit</b> } <i>protocol</i> { <i>source</i> [ <i>source-wildcard</i> ]   <b>host</b> <i>source</i>   <b>any</b> } { <i>destination</i> [ <i>destination-wildcard</i> ]   <b>host</b> <i>destination</i>   <b>any</b> } [ <b>precedence</b> <i>precedence</i> ] [ <b>tos</b> <i>tos</i> ] [ <b>established</b> ] [ <b>time-range</b> <i>time-range-name</i> ]	In access-list configuration mode, specify the conditions allowed or denied. See the “ <a href="#">Creating a Numbered Extended ACL</a> ” section on page 26-9 for definitions of protocols and other keywords. <ul style="list-style-type: none"> <li>• <b>host</b> <i>source</i>—A source and source wildcard of <i>source</i> 0.0.0.0.</li> <li>• <b>host</b> <i>destination</i>—A destination and destination wildcard of <i>destination</i> 0.0.0.0.</li> <li>• <b>any</b>—A source and source wildcard or destination and destination wildcard of 0.0.0.0 255.255.255.255.</li> </ul>
Step 4	<b>end</b>	Return to privileged EXEC mode.
Step 5	<b>show access-lists</b> [ <i>number</i>   <i>name</i> ]	Show the access list configuration.
Step 6	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To remove a named extended ACL, use the **no ip access-list extended** *name* global configuration command.

When you are creating standard 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. This example shows how you can delete individual ACEs from the named access list *border-list*:

```
Switch(config)# ip access-list extended border-list
Switch(config-ext-nacl)# no permit ip host 10.1.1.3 any
```

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

After creating a named ACL, you can apply it to interfaces (see the [“Applying an IP ACL to an Interface” section on page 26-18](#)) or VLANs (see the [“Configuring VLAN Maps” section on page 26-24](#)).

## Using Time Ranges with ACLs

You can selectively apply extended ACLs based on the time of day and week by using the **time-range** global configuration command. First, define a time-range name and set the times and the dates or the days of the week in the time range. Then enter the time-range name when applying an ACL to set restrictions to the access list. You can use the time range to define when the permit or deny statements in the ACL are in effect, for example, during a specified time period or on specified days of the week. The **time-range** keyword and argument are referenced in the named and numbered extended ACL task tables in the previous sections, the [“Creating Standard and Extended IP ACLs” section on page 26-6](#), and the [“Creating Named Standard and Extended ACLs” section on page 26-13](#).

Time-based access lists trigger CPU activity because the new configuration of the access list must be merged with other features and the combined configuration loaded into the TCAM. For this reason, you should be careful not to have several access lists configured to take affect in close succession (within a small number of minutes of each other.)



### Note

---

The time range relies on the switch system clock; therefore, you need a reliable clock source. We recommend that you use Network Time Protocol (NTP) to synchronize the switch clock. For more information, see the [“Managing the System Time and Date” section on page 5-1](#).

---

Beginning in privileged EXEC mode, follow these steps to configure a time-range parameter for an ACL:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>time-range</b> <i>time-range-name</i>	Assign a meaningful name (for example, <i>workhours</i> ) to the time range to be created, and enter time-range configuration mode. The name cannot contain a space or quotation mark and must begin with a letter.
Step 3	<b>absolute</b> [ <i>start time date</i> ] [ <i>end time date</i> ]  or <b>periodic</b> <i>day-of-the-week hh:mm to</i> [ <i>day-of-the-week</i> ] <i>hh:mm</i>  or <b>periodic</b> { <i>weekdays   weekend   daily</i> } <i>hh:mm to hh:mm</i>	Specify when the function it will be applied to is operational. <ul style="list-style-type: none"> <li>You can use only one <b>absolute</b> statement in the time range. If you configure more than one absolute statement, only the one configured last is executed.</li> <li>You can enter multiple <b>periodic</b> statements. For example, you could configure different hours for weekdays and weekends.</li> </ul> See the example configurations.
Step 4	<b>end</b>	Return to privileged EXEC mode.
Step 5	<b>show time-range</b>	Verify the time-range configuration.
Step 6	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

Repeat the steps if you have multiple items that you want in effect at different times.

To remove a configured time-range limitation, use the **no time-range** *time-range-name* global configuration command.

This example shows how to configure time ranges for *workhours* and for company holidays and to verify your configuration.

```
Switch(config)# time-range workhours
Switch(config-time-range)# periodic weekdays 8:00 to 12:00
Switch(config-time-range)# periodic weekdays 13:00 to 17:00
Switch(config-time-range)# exit
Switch(config)# time-range new_year_day_2003
Switch(config-time-range)# absolute start 00:00 1 Jan 2003 end 23:59 1 Jan 2003
Switch(config-time-range)# exit
Switch(config)# time-range thanksgiving_2003
Switch(config-time-range)# absolute start 00:00 27 Nov 2003 end 23:59 28 Nov 2003
Switch(config-time-range)# exit
Switch(config)# time-range christmas_2003
Switch(config-time-range)# absolute start 00:00 24 Dec 2003 end 23:50 25 Dec 2003
Switch(config-time-range)# end
Switch# show time-range
time-range entry: christmas_2003 (inactive)
    absolute start 00:00 24 December 2003 end 23:50 25 December 2003
time-range entry: new_year_day_2003 (inactive)
    absolute start 00:00 01 January 2003 end 23:59 01 January 2003
time-range entry: thanksgiving_2000 (inactive)
    absolute start 00:00 22 November 2003 end 23:59 23 November 2003
time-range entry: workhours (inactive)
    periodic weekdays 8:00 to 12:00
    periodic weekdays 13:00 to 17:00
```

To apply a time-range, enter the time-range name in an extended ACL that can implement time ranges. This example shows how to create and verify extended access list 188 that denies TCP traffic from any source to any destination during the defined holiday times and permits all TCP traffic during work hours.

```
Switch(config)# access-list 188 deny tcp any any time-range new_year_day_2003
Switch(config)# access-list 188 deny tcp any any time-range thanksgiving_2003
Switch(config)# access-list 188 deny tcp any any time-range christmas_2003
Switch(config)# access-list 188 permit tcp any any time-range workhours
Switch(config)# end
Switch# show access-lists
Extended IP access list 188
 10 deny tcp any any time-range new_year_day_2003 (inactive)
 20 deny tcp any any time-range thanksgiving_2003 (active)
 30 deny tcp any any time-range christmas_2003 (inactive)
 40 permit tcp any any time-range workhours (inactive)
```

This example uses named ACLs to permit and deny the same traffic.

```
Switch(config)# ip access-list extended deny_access
Switch(config-ext-nacl)# deny tcp any any time-range new_year_day_2003
Switch(config-ext-nacl)# deny tcp any any time-range thanksgiving_2003
Switch(config-ext-nacl)# deny tcp any any time-range christmas_2003
Switch(config-ext-nacl)# exit
Switch(config)# ip access-list extended may_access
Switch(config-ext-nacl)# permit tcp any any time-range workhours
Switch(config-ext-nacl)# end
Switch# show ip access-lists
Extended IP access list deny_access
 10 deny tcp any any time-range new_year_day_2003 (inactive)
 20 deny tcp any any time-range thanksgiving_2003 (inactive)
 30 deny tcp any any time-range christmas_2003 (inactive)
Extended IP access list may_access
 10 permit tcp any any time-range workhours (inactive)
```

## Including Comments in ACLs

You can use the **remark** keyword to include comments (remarks) about entries in any IP standard or extended ACL. The remarks make the ACL easier for you to understand and scan. Each remark line is limited to 100 characters.

The remark can go before or after a permit or deny statement. You should be consistent about where you put the remark so that it is clear which remark describes which permit or deny statement. For example, it would be confusing to have some remarks before the associated permit or deny statements and some remarks after the associated statements.

To include a comment for IP numbered standard or extended ACLs, use the **access-list *access-list number* remark *remark*** global configuration command. To remove the remark, use the **no** form of this command.

In this example, the workstation that belongs to Jones is allowed access, and the workstation that belongs to Smith is not allowed access:

```
Switch(config)# access-list 1 remark Permit only Jones workstation through
Switch(config)# access-list 1 permit 171.69.2.88
Switch(config)# access-list 1 remark Do not allow Smith through
Switch(config)# access-list 1 deny 171.69.3.13
```

For an entry in a named IP ACL, use the **remark access-list** configuration command. To remove the remark, use the **no** form of this command.

In this example, the Jones subnet is not allowed to use outbound Telnet:

```
Switch(config)# ip access-list extended telnetting
Switch(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
Switch(config-ext-nacl)# deny tcp host 171.69.2.88 any eq telnet
```

## Applying an IP ACL to a Terminal Line

You can use numbered ACLs to control access to one or more terminal lines. You cannot apply named ACLs to lines. You must set identical restrictions on all the virtual terminal lines because a user can attempt to connect to any of them.

For procedures for applying ACLs to interfaces, see the “Applying an IP ACL to an Interface” section on page 26-18. For applying ACLs to VLANs, see the “Configuring VLAN Maps” section on page 26-24.

Beginning in privileged EXEC mode, follow these steps to restrict incoming and outgoing connections between a virtual terminal line and the addresses in an ACL:

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>line [console   vty] line-number</code>	Identify a specific line to configure, and enter in-line configuration mode. <ul style="list-style-type: none"> <li><b>console</b>—Specify the console terminal line. The console port is DCE.</li> <li><b>vty</b>—Specify a virtual terminal for remote console access.</li> </ul> <p>The <i>line-number</i> is the first line number in a contiguous group that you want to configure when the line type is specified. The range is from 0 to 16.</p>
Step 3	<code>access-class access-list-number {in   out}</code>	Restrict incoming and outgoing connections between a particular virtual terminal line (into a device) and the addresses in an access list.
Step 4	<code>end</code>	Return to privileged EXEC mode.
Step 5	<code>show running-config</code>	Display the access list configuration.
Step 6	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

To remove an ACL from a terminal line, use the `no access-class access-list-number {in | out}` line configuration command.

## Applying an IP ACL to an Interface

This section describes how to apply IP ACLs to network interfaces. You can apply ACLs only to inbound Layer 2 interfaces. Note these guidelines:

- When controlling access to an interface, you can use a named or numbered ACL.
- If you apply an ACL to a Layer 2 interface that is a member of a VLAN, the Layer 2 (port) ACL takes precedence over a VLAN map applied to the VLAN. Incoming packets received on the Layer 2 port are always filtered by the port ACL.

Beginning in privileged EXEC mode, follow these steps to control access to an interface:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> <i>interface-id</i>	Identify a specific interface for configuration, and enter interface configuration mode.
Step 3	<b>ip access-group</b> { <i>access-list-number</i>   <i>name</i> } { <b>in</b> }	Control access to the specified interface.
Step 4	<b>end</b>	Return to privileged EXEC mode.
Step 5	<b>show running-config</b>	Display the access list configuration.
Step 6	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To remove the specified access group, use the **no ip access-group** {*access-list-number* | *name*} {**in**} interface configuration command.

This example shows how to apply access list 2 to a port to filter packets entering the port:

```
Switch(config)# interface gigabitethernet0/1
Router(config-if)# ip access-group 2 in
```

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

By default, the input interface sends ICMP Unreachable messages whenever a packet is discarded. ICMP Unreachables are normally limited to no more than one every one-half second per input interface, but this can be changed by using the **ip icmp rate-limit unreachable** global configuration command.

When you apply an undefined ACL to an interface, the switch acts as if the ACL has not been applied to the interface and permits all packets. Remember this behavior if you use undefined ACLs for network security.

## Hardware and Software Treatment of IP ACLs

ACL processing is primarily accomplished in hardware, but requires forwarding of some traffic flows to the CPU for software processing. If the hardware reaches its capacity to store ACL configurations, packets are sent to the CPU for forwarding. The forwarding rate for software-forwarded traffic is substantially less than for hardware-forwarded traffic. If ACLs cause large numbers of packets to be sent to the CPU, the switch performance can be negatively 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 access-lists hardware counters** privileged EXEC command to obtain some basic hardware ACL statistics for switched packets.

## IP ACL Configuration Examples

This section provides examples of configuring and applying IP ACLs. For detailed information about compiling ACLs, see the *Cisco IOS Security Configuration Guide, Release 12.2* and to the Configuring IP Services” section in the “IP Addressing and Services” chapter of the *Cisco IOS IP Configuration Guide, Release 12.2*.

This example uses a standard ACL to allow a port access to a specific Internet host with the address 172.20.128.64.

```
Switch(config)# access-list 6 permit 172.20.128.64 0.0.0
Switch(config)# end
Switch# show access-lists
Standard IP access list 6
 10 permit 172.20.128.64 wildcard bits 0.0.0.0
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# ip access-group 6 in
```

This example uses an extended ACL to deny a port traffic coming from port 80 (HTTP). It permits all other types of traffic.

```
Switch(config)# access-list 106 deny tcp any any eq 80
Switch(config)# access-list 106 permit ip any any
Switch(config)# end
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 106 in
```

## Numbered ACLs

This ACL accepts addresses on network 36.0.0.0 subnets and denies all packets coming from 56.0.0.0 subnets. The ACL is applied to packets entering a port.

```
Switch(config)# access-list 2 permit 36.0.0.0 0.255.255.255
Switch(config)# access-list 2 deny 56.0.0.0 0.255.255.255
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 2 in
```

## Extended ACLs

In this example, suppose that you have a network connected to the Internet, and you want any host on the network to be able to form TCP connections to any host on the Internet. However, you do not want IP hosts to be able to form TCP connections to hosts on your network, except to the mail (SMTP) port of a dedicated mail host.

SMTP uses TCP port 25 on one end of the connection and a random port number on the other end. The same port numbers are used throughout the life of the connection. Mail packets coming in from the Internet have a destination port of 25. Because the secure system of the network always accepts mail connections on port 25, the incoming services are controlled.

```
Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 23
Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 25
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 102 in
```

## Named ACLs

This example creates an extended ACL named *marketing\_group*. The *marketing\_group* ACL allows any TCP Telnet traffic to the destination address and wildcard 171.69.0.0 0.0.255.255 and denies any other TCP traffic. It permits any other IP traffic.

```
Switch(config)# ip access-list extended marketing_group
Switch(config-ext-nacl)# permit tcp any 171.69.0.0 0.0.255.255 eq telnet
Switch(config-ext-nacl)# deny tcp any any
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
```

The *marketing\_group* ACL is applied to incoming traffic on a port.

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ip access-group marketing_group in
```

## Time Range Applied to an IP ACL

This example denies HTTP traffic on IP on Monday through Friday between the hours of 8:00 a.m. and 6:00 p.m (18:00). The example allows UDP traffic only on Saturday and Sunday from noon to 8:00 p.m. (20:00).

```
Switch(config)# time-range no-http
Switch(config)# periodic weekdays 8:00 to 18:00
!
Switch(config)# time-range udp-yes
Switch(config)# periodic weekend 12:00 to 20:00
!
Switch(config)# ip access-list extended strict
Switch(config-ext-nacl)# deny tcp any any eq www time-range no-http
Switch(config-ext-nacl)# permit udp any any time-range udp-yes
!
Switch(config-ext-nacl)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group strict in
```

## Commented IP ACL Entries

In this example of a numbered ACL, the workstation that belongs to Jones is allowed access, and the workstation that belongs to Smith is not allowed access:

```
Switch(config)# access-list 1 remark Permit only Jones workstation through
Switch(config)# access-list 1 permit 171.69.2.88
Switch(config)# access-list 1 remark Do not allow Smith workstation through
Switch(config)# access-list 1 deny 171.69.3.13
```

In this example of a numbered ACL, the Winter and Smith workstations are not allowed to browse the web:

```
Switch(config)# access-list 100 remark Do not allow Winter to browse the web
Switch(config)# access-list 100 deny host 171.69.3.85 any eq www
Switch(config)# access-list 100 remark Do not allow Smith to browse the web
Switch(config)# access-list 100 deny host 171.69.3.13 any eq www
```

In this example of a named ACL, the Jones subnet is not allowed access:

```
Switch(config)# ip access-list standard prevention
Switch(config-std-nacl)# remark Do not allow Jones subnet through
Switch(config-std-nacl)# deny 171.69.0.0 0.0.255.255
```

In this example of a named ACL, the Jones subnet is not allowed to use outbound Telnet:

```
Switch(config)# ip access-list extended telnetting
Switch(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
Switch(config-ext-nacl)# deny tcp 171.69.0.0 0.0.255.255 any eq telnet
```

## Creating Named MAC Extended ACLs

You can filter non-IP traffic on a VLAN or on a Layer 2 interface by using MAC addresses and named MAC extended ACLs. The procedure is similar to that of configuring other extended named ACLs.

For more information about the supported non-IP protocols in the **mac access-list extended** command, see the command reference for this release.



### Note

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.

Beginning in privileged EXEC mode, follow these steps to create a named MAC extended ACL:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>mac access-list extended</b> <i>name</i>	Define an extended MAC access list using a name.
Step 3	<b>{deny   permit} {any   host</b> <i>source MAC address</i> <b>  source MAC address mask} {any   host</b> <i>destination MAC address</i> <b>  destination MAC address mask} [type mask  </b> <b>lsap</b> <i>lsap mask</i> <b>  aarp   amber   dec-spanning   decnet-iv   diagnostic   dsm   etype-6000   etype-8042   lat   lave-sca   mop-console   mop-dump   msdos   mumps   netbios   vines-echo   vines-ip   xns-idp   0-65535] [cos</b> <i>cos</i>	<p>In extended MAC access-list configuration mode, specify to <b>permit</b> or <b>deny any</b> source MAC address, a source MAC address with a mask, or a specific <b>host</b> source MAC address and <b>any</b> destination MAC address, destination MAC address with a mask, or a specific destination MAC address.</p> <p>(Optional) You can also enter these options:</p> <ul style="list-style-type: none"> <li><b>type mask</b>—An arbitrary EtherType number of a packet with Ethernet II or SNAP encapsulation in decimal, hex, or octal with optional mask of <i>don't care</i> bits applied to the EtherType before testing for a match.</li> <li><b>lsap lsap mask</b>—An LSAP number of a packet with 802.2 encapsulation in decimal, hex, or octal with optional mask of <i>don't care</i> bits.</li> <li><b>aarp   amber   dec-spanning   decnet-iv   diagnostic   dsm   etype-6000   etype-8042   lat   lave-sca   mop-console   mop-dump   msdos   mumps   netbios   vines-echo   vines-ip   xns-idp</b>—A non-IP protocol.</li> <li><b>cos cos</b>—An IEEE 802.1Q cost of service number from 0 to 7 used to set priority.</li> </ul>
Step 4	<b>end</b>	Return to privileged EXEC mode.
Step 5	<b>show access-lists</b> [ <i>number</i>   <i>name</i> ]	Show the access list configuration.
Step 6	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

Use the **no mac access-list extended** *name* global configuration command to delete the entire ACL. You can also delete individual ACEs from named MAC extended ACLs.

This example shows how to create and display an access list named *mac1*, denying only EtherType DECnet Phase IV traffic, but permitting all other types of traffic.

```
Switch(config)# mac access-list extended mac1
Switch(config-ext-mac1)# deny any any decnet-iv
Switch(config-ext-mac1)# permit any any
```

```
Switch(config-ext-macl)# end
Switch # show access-lists
Extended MAC access list mac1
    10 deny any any decnet-iv
    20 permit any any
```

## Applying a MAC ACL to a Layer 2 Interface

After you create a MAC ACL, you can apply it to a Layer 2 interface to filter non-IP traffic coming in that interface. When you apply the MAC ACL, consider these guidelines:

- If you apply an ACL to a Layer 2 interface that is a member of a VLAN, the Layer 2 (port) ACL takes precedence over a VLAN map applied to the VLAN. Incoming packets received on the Layer 2 port are always filtered by the port ACL.
- You can apply no more than one IP access list and one MAC access list to the same Layer 2 interface. The IP access list filters only IP packets, and the MAC access list filters non-IP packets.
- A Layer 2 interface can have only one MAC access list. If you apply a MAC access list to a Layer 2 interface that has a MAC ACL configured, the new ACL replaces the previously configured one.

Beginning in privileged EXEC mode, follow these steps to apply a MAC access list to control access to a Layer 2 interface:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> <i>interface-id</i>	Identify a specific interface, and enter interface configuration mode. The interface must be a physical Layer 2 interface (port ACL).
Step 3	<b>mac access-group</b> { <i>name</i> } { <b>in</b> }	Control access to the specified interface by using the MAC access list. <b>Note</b> Port ACLs are supported only in the inbound direction.
Step 4	<b>end</b>	Return to privileged EXEC mode.
Step 5	<b>show mac access-group</b> [ <b>interface</b> <i>interface-id</i> ]	Display the MAC access list applied to the interface or all Layer 2 interfaces.
Step 6	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To remove the specified access group, use the **no mac access-group** {*name*} interface configuration command.

This example shows how to apply MAC access list *mac1* to a port to filter packets entering the port:

```
Switch(config)# interface gigabitethernet0/2
Router(config-if)# mac access-group mac1 in
```



### Note

The **mac access-group** interface configuration command is only valid when applied to a physical Layer 2 interface. You cannot use the command on EtherChannel port channels.

After receiving a packet, the switch checks it against the inbound ACL. If the ACL permits it, the switch continues to process the packet. If the ACL rejects the packet, the switch discards it. When you apply an undefined ACL to an interface, the switch acts as if the ACL has not been applied and permits all packets. Remember this behavior if you use undefined ACLs for network security.

## Configuring VLAN Maps

This section describes how to configure VLAN maps, which is the only way to control filtering within a VLAN. VLAN maps have no direction. To filter traffic in a specific direction by using a VLAN map, you need to include an ACL with specific source or destination addresses. If there is a match clause for that type of packet (IP or MAC) in the VLAN map, the default action is to drop the packet if the packet does not match any of the entries within the map. If there is no match clause for that type of packet, the default is to forward the packet.



### Note

For complete syntax and usage information for the commands used in this section, see the command reference for this release.

To create a VLAN map and apply it to one or more VLANs, perform these steps:

- Step 1** Create the standard or extended IP ACLs or named MAC extended ACLs that you want to apply to the VLAN. See the [“Creating Standard and Extended IP ACLs”](#) section on page 26-6 and the [“Creating a VLAN Map”](#) section on page 26-25.
- Step 2** Enter the **vlan access-map** global configuration command to create a VLAN ACL map entry.
- Step 3** In access map configuration mode, optionally enter an **action—forward** (the default) or **drop**—and enter the **match** command to specify an IP packet or a non-IP packet (with only a known MAC address) and to match the packet against one or more ACLs (standard or extended).



### Note

If the VLAN map has a match clause for the type of packet (IP or MAC) and the packet does not match the type, the default is to drop the packet. If there is no match clause in the VLAN map for that type of packet, and no action specified, the packet is forwarded.

- Step 4** Use the **vlan filter** global configuration command to apply a VLAN map to one or more VLANs.

This section contains these topics:

- [VLAN Map Configuration Guidelines, page 26-25](#)
- [Creating a VLAN Map, page 26-25](#)
- [Applying a VLAN Map to a VLAN, page 26-28](#)
- [Using VLAN Maps in Your Network, page 26-28](#)

## VLAN Map Configuration Guidelines

Follow these guidelines when configuring VLAN maps:

- If there is no ACL configured to deny traffic on an interface and *no* VLAN map is configured, all traffic is permitted.
- Each VLAN map consists of a series of entries. The order of entries in an VLAN map is important. A packet that comes into the switch is tested against the first entry in the VLAN map. If it matches, the action specified for that part of the VLAN map is taken. If there is no match, the packet is tested against the next entry in the map.
- If the VLAN map has at least one match clause for the type of packet (IP or MAC) and the packet does not match any of these match clauses, the default is to drop the packet. If there is no match clause for that type of packet in the VLAN map, the default is to forward the packet.
- The system might take longer to boot if you have configured a very large number of ACLs.
- Logging is not supported for VLAN maps.
- If VLAN map configuration cannot be applied in hardware, all packets in that VLAN must be forwarded by software.
- When a switch has an IP access list or MAC access list applied to a Layer 2 interface, and you apply a VLAN map to a VLAN that the port belongs to, the port ACL takes precedence over the VLAN map.
- See the [“Using VLAN Maps in Your Network” section on page 26-28](#) for configuration examples.

## Creating a VLAN Map

Each VLAN map consists of an ordered series of entries. Beginning in privileged EXEC mode, follow these steps to create, add to, or delete a VLAN map entry:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>vlan access-map</b> <i>name</i> [ <i>number</i> ]	Create a VLAN map, and give it a name and (optionally) a number. The number is the sequence number of the entry within the map.  When you create VLAN maps with the same name, numbers are assigned sequentially in increments of 10. When modifying or deleting maps, you can enter the number of the map entry that you want to modify or delete.  Entering this command changes to access-map configuration mode.
Step 3	<b>action</b> { <b>drop</b>   <b>forward</b> }	(Optional) Set the action for the map entry. The default is to forward.
Step 4	<b>match</b> { <b>ip</b>   <b>mac</b> } <b>address</b> { <i>name</i>   <i>number</i> } [ <i>name</i>   <i>number</i> ]	Match the packet (using either the IP or MAC address) against one or more standard or extended access lists. Note that packets are only matched against access lists of the correct protocol type. IP packets are matched against standard or extended IP access lists. Non-IP packets are only matched against named MAC extended access lists.
Step 5	<b>end</b>	Return to global configuration mode.
Step 6	<b>show running-config</b>	Display the access list configuration.
Step 7	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

Use the **no vlan access-map** *name* global configuration command to delete a map.

Use the **no vlan access-map** *name number* global configuration command to delete a single sequence entry from within the map.

Use the **no action** access-map configuration command to enforce the default action, which is to forward.

VLAN maps do not use the specific permit or deny keywords. To deny a packet by using VLAN maps, create an ACL that would match the packet, and set the action to drop. A permit in the ACL counts as a match. A deny in the ACL means no match.

## Examples of ACLs and VLAN Maps

These examples show how to create ACLs and VLAN maps that for specific purposes.

### Example 1

This example shows how to create an ACL and a VLAN map to deny a packet. In the first map, any packets that match the *ip1* ACL (TCP packets) would be dropped. You first create the *ip1* ACL to permit any TCP packet and no other packets. Because there is a match clause for IP packets in the VLAN map, the default action is to drop any IP packet that does not match any of the match clauses.

```
Switch(config)# ip access-list extended ip1
Switch(config-ext-nacl)# permit tcp any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map_1 10
Switch(config-access-map)# match ip address ip1
Switch(config-access-map)# action drop
```

This example shows how to create a VLAN map to permit a packet. ACL *ip2* permits UDP packets and any packets that match the *ip2* ACL are forwarded. In this map, any IP packets that did not match any of the previous ACLs (that is, packets that are not TCP packets or UDP packets) would get dropped.

```
Switch(config)# ip access-list extended ip2
Switch(config-ext-nacl)# permit udp any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map_1 20
Switch(config-access-map)# match ip address ip2
Switch(config-access-map)# action forward
```

### Example 2

In this example, the VLAN map has a default action of drop for IP packets and a default action of forward for MAC packets. Used with standard ACL 101 and extended named access lists **igmp-match** and **tcp-match**, the map will have the following results:

- Forward all UDP packets
- Drop all IGMP packets
- Forward all TCP packets
- Drop all other IP packets
- Forward all non-IP packets

```
Switch(config)# access-list 101 permit udp any any
Switch(config)# ip access-list extended igmp-match
Switch(config-ext-nacl)# permit igmp any any
Switch(config)# ip access-list extended tcp-match
Switch(config-ext-nacl)# permit tcp any any
Switch(config-ext-nacl)# exit
```

```
Switch(config)# vlan access-map drop-ip-default 10
Switch(config-access-map)# match ip address 101
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-ip-default 20
Switch(config-access-map)# match ip address igmp-match
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-ip-default 30
Switch(config-access-map)# match ip address tcp-match
Switch(config-access-map)# action forward
```

### Example 3

In this example, the VLAN map has a default action of drop for MAC packets and a default action of forward for IP packets. Used with MAC extended access lists **good-hosts** and **good-protocols**, the map will have the following results:

- Forward MAC packets from hosts 0000.0c00.0111 and 0000.0c00.0211
- Forward MAC packets with decnet-iv or vines-ip protocols
- Drop all other non-IP packets
- Forward all IP packets

```
Switch(config)# mac access-list extended good-hosts
Switch(config-ext-macl)# permit host 000.0c00.0111 any
Switch(config-ext-macl)# permit host 000.0c00.0211 any
Switch(config-ext-nacl)# exit
Switch(config)# mac access-list extended good-protocols
Switch(config-ext-macl)# permit any any decnet-ip
Switch(config-ext-macl)# permit any any vines-ip
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map drop-mac-default 10
Switch(config-access-map)# match mac address good-hosts
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-mac-default 20
Switch(config-access-map)# match mac address good-protocols
Switch(config-access-map)# action forward
```

### Example 4

In this example, the VLAN map has a default action of drop for all packets (IP and non-IP). Used with access lists **tcp-match** and **good-hosts** from Examples 2 and 3, the map will have the following results:

- Forward all TCP packets
- Forward MAC packets from hosts 0000.0c00.0111 and 0000.0c00.0211
- Drop all other IP packets
- Drop all other MAC packets

```
Switch(config)# vlan access-map drop-all-default 10
Switch(config-access-map)# match ip address tcp-match
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-all-default 20
Switch(config-access-map)# match mac address good-hosts
Switch(config-access-map)# action forward
```

## Applying a VLAN Map to a VLAN

Beginning in privileged EXEC mode, follow these steps to apply a VLAN map to one or more VLANs:

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>vlan filter mapname vlan-list list</code>	Apply the VLAN map to one or more VLAN IDs. The list can be a single VLAN ID (22), a consecutive list (10-22), or a string of VLAN IDs (12, 22, 30). Spaces around the comma and hyphen are optional.
Step 3	<code>show running-config</code>	Display the access list configuration.
Step 4	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

To remove the VLAN map, use the `no vlan filter mapname vlan-list list` global configuration command.

This example shows how to apply VLAN map 1 to VLANs 20 through 22:

```
Switch(config)# vlan filter map 1 vlan-list 20-22
```

## Using VLAN Maps in Your Network

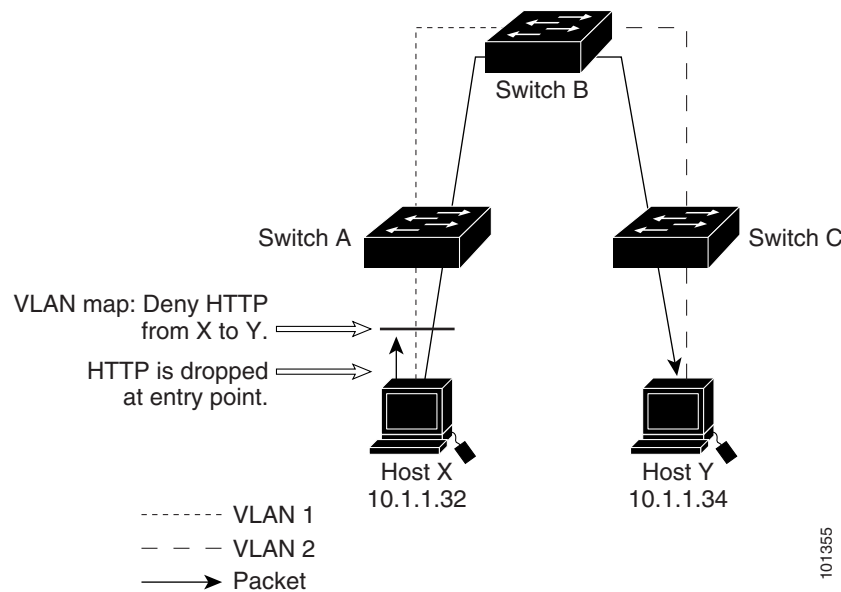
This section describes some typical uses for VLAN maps and includes these topics:

- [Wiring Closet Configuration, page 26-28](#)
- [Denying Access to a Server on a VLAN, page 26-30](#)

### Wiring Closet Configuration

In a wiring closet configuration, the switch can support a VLAN map and a QoS classification ACL. In [Figure 26-3](#), assume that Host X and Host Y are in different VLANs and are connected to wiring closet switches A and C. Traffic from Host X to Host Y is eventually being routed by Switch B, a Layer 3 switch with routing enabled. Traffic from Host X to Host Y can be access-controlled at the traffic entry point, Switch A.

Figure 26-3 Wiring Closet Configuration



If you do not want HTTP traffic switched from Host X to Host Y, you can configure a VLAN map on Switch A to drop all HTTP traffic from Host X (IP address 10.1.1.32) to Host Y (IP address 10.1.1.34) at Switch A and not bridge it to Switch B.

First, define the IP access list *http* that permits (matches) any TCP traffic on the HTTP port.

```
Switch(config)# ip access-list extended http
Switch(config-ext-nacl)# permit tcp host 10.1.1.32 host 10.1.1.34 eq www
Switch(config-ext-nacl)# exit
```

Next, create VLAN access map *map2* so that traffic that matches the *http* access list is dropped and all other IP traffic is forwarded.

```
Switch(config)# vlan access-map map2 10
Switch(config-access-map)# match ip address http
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
Switch(config)# ip access-list extended match_all
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map2 20
Switch(config-access-map)# match ip address match_all
Switch(config-access-map)# action forward
```

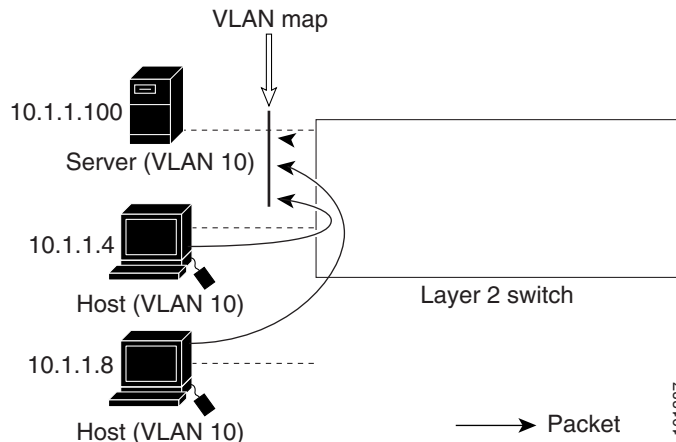
Then, apply VLAN access map *map2* to VLAN 1.

```
Switch(config)# vlan filter map2 vlan 1
```

## Denying Access to a Server on a VLAN

You can restrict access to a server on a VLAN. For example, server 10.1.1.100 in VLAN 10 needs to have access denied to hosts 10.1.1.4 and 10.1.1.8 (see [Figure 26-4](#)).

**Figure 26-4 Deny Access to a Server on a VLAN**



This example shows how to deny access to a server on a VLAN by creating the VLAN map SERVER1 that denies access to hosts in subnet 10.1.2.0.8, host 10.1.1.4, and host 10.1.1.8 and permits other IP traffic. The final step is to apply the map SERVER1 to VLAN 10.

**Step 1** Define the IP ACL that will match the correct packets.

```
Switch(config)# ip access-list extended SERVER1_ACL
Switch(config-ext-nacl)# permit ip host 10.1.1.4 host 10.1.1.100
Switch(config-ext-nacl)# permit ip host 10.1.1.8 host 10.1.1.100
Switch(config-ext-nacl)# exit
```

**Step 2** Define a VLAN map using this ACL that will drop IP packets that match SERVER1\_ACL and forward IP packets that do not match the ACL.

```
Switch(config)# vlan access-map SERVER1_MAP
Switch(config-access-map)# match ip address SERVER1_ACL
Switch(config-access-map)# action drop
Switch(config)# vlan access-map SERVER1_MAP 20
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
```

**Step 3** Apply the VLAN map to VLAN 10.

```
Switch(config)# vlan filter SERVER1_MAP vlan-list 10.
```

# Displaying ACL Configuration

You can display the ACLs that are configured on the switch, and you can display the ACLs that have been applied to interfaces and VLANs.

When you use the **ip access-group** interface configuration command to apply ACLs to a Layer 2 interface, you can display the access groups on the interface. You can also display the MAC ACLs applied to a Layer 2 interface. You can use the privileged EXEC commands as described in [Table 26-2](#) to display this information.

**Table 26-2** Commands for Displaying Access Lists and Access Groups

Command	Purpose
<b>show access-lists</b> [ <i>number</i>   <i>name</i> ]	Display the contents of one or all current IP and MAC address access lists or a specific access list (numbered or named).
<b>show ip access-lists</b> [ <i>number</i>   <i>name</i> ]	Display the contents of all current IP access lists or a specific IP access list (numbered or named).
<b>show running-config</b> [ <b>interface</b> <i>interface-id</i> ]	Displays the contents of the configuration file for the switch or the specified interface, including all configured MAC and IP access lists and which access groups are applied to an interface.
<b>show mac access-group</b> [ <b>interface</b> <i>interface-id</i> ]	Displays MAC access lists applied to all Layer 2 interfaces or the specified Layer 2 interface.

You can also display information about VLAN access maps or VLAN filters. Use the privileged EXEC commands in [Table 26-3](#) to display VLAN map information.

**Table 26-3** Commands for Displaying VLAN Map Information

Command	Purpose
<b>show vlan access-map</b> [ <i>mapname</i> ]	Show information about all VLAN access-maps or the specified access map.
<b>show vlan filter</b> [ <b>access-map</b> <i>name</i>   <b>vlan</b> <i>vlan-id</i> ]	Show information about all VLAN filters or about a specified VLAN or VLAN access map.

