C H A P T E R 1

Configuring ACLs

This chapter describes how to configure access control lists (ACLs).

This chapter includes the following sections:

Information About ACLs

An ACL is an ordered set of rules that you can use to filter traffic. Each rule specifies a set of conditions that a packet must satisfy to match the rule. When the switch determines that an ACL applies to a packet, it tests the packet against the conditions of all rules. The first match determines whether the packet is permitted or denied. If there is no match, the switch applies the applicable default rule. The switch continues processing packets that are permitted and drops packets that are denied. For more information, see the "Implicit Rules" section on page 1-3.

You can use ACLs to protect networks and specific hosts from unnecessary or unwanted traffic. For example, you could use ACLs to disallow HTTP traffic from a high-security network to the Internet. You could also use ACLs to allow HTTP traffic but only to specific sites, using the IP address of the site to identify it in an IP ACL.

This sections includes the following topics:

IP ACL Types and Applications

The Cisco Nexus 5000 Series switch supports IPv4, IPv6 and MAC ACLs for security traffic filtering. The switch allows you to use IP ACLs as port ACLs and VLAN ACLs, as shown in Table 1-1.

Send feedback to nx5000-docfeedback@cisco.com

Table 1-1   *Security ACL Applications*

Application	Supported Interfaces	Types of ACLs Supported
Port ACL	An ACL is considered a port ACL when you apply it to one of the following: • Ethernet interface • Ethernet port-channel interface When a port ACL is applied to a trunk port, the ACL filters traffic on all VLANs on the trunk port.	IPv4 ACLs IPv6 ACLs MAC ACLs
VLAN ACL (VACL)	An ACL is a VACL when you use an access map to associate the ACL with an action, and then apply the map to a VLAN.	IPv4 ACLs IPv6 ACLs MAC ACLs

Application Order

When the switch processes a packet, it determines the forwarding path of the packet. The path determines which ACLs that the switch applies to the traffic. The switch applies the ACLs in the following order:

• Port ACL

Rules

You can create rules in access-list configuration mode by using the **permit** or **deny** command. The switch allows traffic that matches the criteria in a permit rule and blocks traffic that matches the criteria in a deny rule. You have many options for configuring the criteria that traffic must meet in order to match the rule.

This section includes the following topics:

Source and Destination

In each rule, you specify the source and the destination of the traffic that matches the rule. You can specify both the source and destination as a specific host, a network or group of hosts, or any host.

Protocols

ACLs allow you to identify traffic by protocol. For your convenience, you can specify some protocols by name. For example, in an IPv4 ACL, you can specify ICMP by name.

Send feedback to nx5000-docfeedback@cisco.com

You can specify any protocol by number. In IPv4 ACLs, you can specify protocols by the integer that represents the Internet protocol number. For example, you can use 115 to specify Layer 2 Tunneling Protocol (L2TP) traffic.

Implicit Rules

IP ACLs have implicit rules, which means that although these rules do not appear in the running configuration, the switch applies them to traffic when no other rules in an ACL match.

All IPv4 ACLs include the following implicit rule:

```
deny ip any any
```

This implicit rule ensures that the switch denies unmatched IP traffic.

Additional Filtering Options

You can identify traffic by using additional options. IPv4 ACLs support the following additional filtering options:

- Layer 4 protocol
- TCP and UDP ports
- ICMP types and codes
- IGMP types
- Precedence level
- Differentiated Services Code Point (DSCP) value
- TCP packets with the ACK, FIN, PSH, RST, SYN, or URG bit set
- Established TCP connections

Sequence Numbers

The switch supports sequence numbers for rules. Every rule that you enter receives a sequence number, either assigned by you or assigned automatically by the switch. Sequence numbers simplify the following ACL tasks:

- Adding new rules between existing rules—By specifying the sequence number, you specify where in the ACL a new rule should be positioned. For example, if you need to insert a rule between rules numbered 100 and 110, you could assign a sequence number of 105 to the new rule.

- Removing a rule—Without using a sequence number, removing a rule requires that you enter the whole rule, as follows:

```
switch(config-acl)# no permit tcp 10.0.0.0/8 any
```

However, if the same rule had a sequence number of 101, removing the rule requires only the following command:

```
switch(config-acl)# no 101
```

- Moving a rule—With sequence numbers, if you need to move a rule to a different position within an ACL, you can add a second instance of the rule using the sequence number that positions it correctly, and then you can remove the original instance of the rule. This action allows you to move the rule without disrupting traffic.

If you enter a rule without a sequence number, the switch adds the rule to the end of the ACL and assigns a sequence number that is 10 greater than the sequence number of the preceding rule to the rule. For example, if the last rule in an ACL has a sequence number of 225 and you add a rule without a sequence number, the switch assigns the sequence number 235 to the new rule.

In addition, the Nexus 5000 Series switch allows you to reassign sequence numbers to rules in an ACL. Resequencing is useful when an ACL has rules numbered contiguously, such as 100 and 101, and you need to insert one or more rules between those rules.

Logical Operators and Logical Operation Units

IP ACL rules for TCP and UDP traffic can use logical operators to filter traffic based on port numbers.

The switch stores operator-operand couples in registers called logical operator units (LOUs).

LOU usage for the eq operator is never stored in an LOU. The range operation is inclusive of boundary values.

The following guidelines determine when the switch stores operator-operand couples in LOUs:

- If the operator or operand differs from other operator-operand couples that are used in other rules, the couple is stored in an LOU.

  For example, the operator-operand couples gt 10 and gt 11 would be stored separately in half an LOU each. The couples gt 10 and lt 10 would also be stored separately.

- Whether the operator-operand couple is applied to a source port or a destination port in the rule affects LOU usage. Identical couples are stored separately when one of the identical couples is applied to a source port and the other couple is applied to a destination port.

  For example, if a rule applies the operator-operand couple gt 10 to a source port and another rule applies a gt 10 couple to a destination port, both couples would also be stored in half an LOU, resulting in the use of one whole LOU. Any additional rules using a gt 10 couple would not result in further LOU usage.

Configuring IP ACLs

This section includes the following topics:

Creating an IP ACL

You can create an IPv4 ACL on the switch and add rules to it. To create an IP ACL, perform this task:

	Command	**Purpose**
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **ip access-list** *name*	Creates the IP ACL and enters IP ACL configuration mode. The *name* argument can be up to 64 characters.
Step 3	switch(config-acl)# [*sequence-number*] {**permit**|**deny**} *protocol source destination*	Creates a rule in the IP ACL. You can create many rules. The *sequence-number* argument can be a whole number between 1 and 4294967295. The **permit** and **deny** commands support many ways of identifying traffic. For more information, see the *Cisco Nexus 5000 Series Command Reference*.
Step 4	switch(config-acl)# **statistics**	(Optional) Specifies that the switch maintains global statistics for packets matching the rules in the ACL.
Step 5	switch(config-acl)# **show ip access-lists** *name*	(Optional) Displays the IP ACL configuration.
Step 6	switch(config-acl)# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to create an IPv4 ACL:

```
switch# configure terminal
switch(config)# ip access-list acl-01
switch(config-acl)# permit ip 192.168.2.0/24 any
switch(config-acl)# statistics
switch(config-acl)# show ip access-lists acl-01
switch(config-acl)# copy running-config startup-config
```

Changing an IP ACL

You can add and remove rules in an existing IPv4 ACL. You cannot change existing rules. Instead, to change a rule, you can remove it and recreate it with the desired changes.

If you need to add more rules between existing rules than the current sequence numbering allows, you can use the **resequence** command to reassign sequence numbers. For more information, see the

To change an IP ACL, perform this task:

	Command	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **ip access-list** *name*	Enters IP ACL configuration mode for the ACL that you specify by name.
Step 3	switch(config-acl)# [*sequence-number*] {**permit**|**deny**} *protocol source destination*	(Optional) Creates a rule in the IP ACL. Using a sequence number allows you to specify a position for the rule in the ACL. Without a sequence number, the rule is added to the end of the rules. The *sequence-number* argument can be a whole number between 1 and 4294967295. The **permit** and **deny** commands support many ways of identifying traffic. For more information, see the *Cisco Nexus 5000 Series Command Reference*.
Step 4	switch(config-acl)# **no** {*sequence-number* | {**permit**|**deny**} *protocol source destination*}	(Optional) Removes the rule that you specified from the IP ACL. The **permit** and **deny** commands support many ways of identifying traffic. For more information, see the *Cisco Nexus 5000 Series Command Reference*.
Step 5	switch(config-acl)# [**no**] **statistics**	(Optional) Specifies that the switch maintains global statistics for packets matching the rules in the ACL. The **no** option stops the switch from maintaining global statistics for the ACL.
Step 6	switch(config-acl)# **show ip access-lists** *name*	(Optional) Displays the IP ACL configuration.
Step 7	switch(config-acl)# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

Removing an IP ACL

You can remove an IP ACL from the switch.

Before you remove an IP ACL from the switch, be sure that you know whether the ACL is applied to an interface. The switch allows you to remove ACLs that are currently applied. Removing an ACL does not affect the configuration of interfaces where you have applied the ACL. Instead, the switch considers the removed ACL to be empty.

To remove an IP ACL from the switch, perform this task:

	Command	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **no ip access-list** *name*	Removes the IP ACL that you specified by name from the running configuration.
Step 3	switch(config)# **show running-config**	(Optional) Displays ACL configuration. The removed IP ACL should not appear.
Step 4	switch(config)# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

Changing Sequence Numbers in an IP ACL

You can change all the sequence numbers assigned to the rules in an IP ACL. To change sequence numbers, perform this task:

	Command	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **resequence ip access-list** *name starting-sequence-number increment*	Assigns sequence numbers to the rules contained in the ACL, where the first rule receives the starting sequence number that you specify. Each subsequent rule receives a number larger than the preceding rule. The difference in numbers is determined by the increment that you specify. The *starting-sequence-number* argument and the *increment* argument can be a whole number between 1 and 4294967295.
Step 3	switch(config)# **show ip access-lists** *name*	(Optional) Displays the IP ACL configuration.
Step 4	switch(config)# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

Applying an IP ACL as a Port ACL

You can apply an IPv4 ACL to a physical Ethernet interface or a port channel. ACLs applied to these interface types are considered port ACLs. To apply an IP ACL, perform this task:

	Command	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.

	Command	Purpose
Step 2	switch(config)# **interface ethernet** *slot/port*	Enters interface configuration mode for the specified interface.
	switch(config)# **interface port-channel** *channel-number*	Enters interface configuration mode for a port channel.
Step 3	switch(config)# **interface ethernet** *slot/port* switch(config-if)# **ipv6 port traffic-filter <name> in**	Applies an IPv6 port access-list.
Step 4	switch(config-if)# **ip port access-group access-list in**	Applies an IPv4 ACL to the interface or port channel. Only inbound filtering is supported with port ACLs. You can apply one port ACL to an interface.
Step 5	switch(config-if)# **show running-config**	(Optional) Displays ACL configuration.
Step 6	switch(config-if)# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to apply an IPv4 or IPv6 ACL to the port channel:

```
switch# configure terminal
switch(config)# interface port-channel 5
switch(config-if)# ip port access-group acl-l2-marketing-group in
switch(config-if)# show running-config
switch(config-if)# copy running-config startup-config
```

This example shows how to create an IPv4 ACL named acl-01 and apply it to Ethernet interface 2/1, which is a Layer 2 interface:

```
ip access-list acl-01
  permit ip 192.168.2.0/24 any
interface ethernet 2/1
  ip access-group acl-01 in
```

Applying an IP ACL as a VACL

For information about configuring VACLs, see "Configuring VACLs" section on page 1-15.

Verifying IP ACL Configurations

To display IP ACL configuration information, perform one of the following tasks:

Command	Purpose
show running-config	Displays ACL configuration, including IP ACL configuration and interfaces that IP ACLs are applied to.
show ip access-lists	Displays the IP ACL configuration.
show running-config interface	Displays the configuration of an interface to which you have applied an ACL.

For detailed information about the fields in the output from these commands, refer to the *Cisco Nexus 5000 Series Command Reference*.

Displaying and Clearing IP ACL Statistics

Use the **show ip access-lists** command to display statistics about an IP ACL, including the number of packets that have matched each rule. For detailed information about the fields in the output from this command, refer to the *Cisco Nexus 5000 Series Command Reference*.

> **Note** The mac access-list is applicable to non-IPv4 and non-IPv6 traffic only.

To display or clear VACL statistics, perform one of the following tasks:

Command	Purpose
show ip access-lists	Displays IP ACL configuration. If the IP ACL includes the **statistics** command, then the **show ip access-lists** command output includes the number of packets that have matched each rule.
clear ip access-list counters	Clears statistics for all IP ACLs or for a specific IP ACL.

For detailed information about these commands, refer to the *Cisco Nexus 5000 Series Command Reference*.

Configuring MAC ACLs

This section includes the following topics:

- Creating a MAC ACL, page 1-10
- Changing a MAC ACL, page 1-10

Send feedback to nx5000-docfeedback@cisco.com

- Removing a MAC ACL, page 1-11
- Changing Sequence Numbers in a MAC ACL, page 1-12
- Applying a MAC ACL as a Port ACL, page 1-12
- Applying a MAC ACL as a VACL, page 1-13
- Verifying MAC ACL Configurations, page 1-13
- Displaying and Clearing MAC ACL Statistics, page 1-13

Creating a MAC ACL

To create a MAC ACL and add rules to it, perform this task:

	Command	Purpose
Step 1	`switch# configure terminal`	Enters global configuration mode.
Step 2	`switch# mac access-list` *name*	Creates the MAC ACL and enters ACL configuration mode.
Step 3	`switch(config-mac-acl)# {permit | deny}` *source destination protocol*	Creates a rule in the MAC ACL. The **permit** and **deny** options support many ways of identifying traffic. For more information, see the *Cisco Nexus 5000 Series Command Reference*.
Step 4	`switch(config-mac-acl)# statistics`	(Optional) Specifies that the switch maintains global statistics for packets matching the rules in the ACL.
Step 5	`switch(config-mac-acl)# show mac access-lists` *name*	(Optional) Displays the MAC ACL configuration.
Step 6	`switch(config-mac-acl)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to create a MAC ACL and add rules to it:

```
switch# configure terminal
switch(config)# mac access-list acl-mac-01
switch(config-mac-acl)# permit 00c0.4f00.0000 0000.00ff.ffff any
switch(config-mac-acl)# statistics
switch(config-mac-acl)# show mac access-lists acl-mac-01
switch(config-mac-acl)# copy running-config startup-config
```

Changing a MAC ACL

In an existing MAC ACL, you can add and remove rules. You cannot change existing rules. Instead, to change a rule, you can remove it and recreate it with the desired changes.

If you need to add more rules between existing rules than the current sequence numbering allows, you can use the **resequence** command to reassign sequence numbers. For more information, see the "Changing Sequence Numbers in an IP ACL" section on page 1-7.

To change a MAC ACL, perform this task:

	Command	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **mac access-list** *name*	Enters ACL configuration mode for the ACL that you specify by name.
Step 3	switch(config-mac-acl)# [*sequence-number*] {**permit**|**deny**} *source destination protocol*	(Optional) Creates a rule in the MAC ACL. Using a sequence number allows you to specify a position for the rule in the ACL. Without a sequence number, the rule is added to the end of the rules. The **permit** and **deny** commands support many ways of identifying traffic.
Step 4	switch(config-mac-acl)# **no** {*sequence-number* | {**permit**|**deny**} *source destination protocol*}	(Optional) Removes the rule that you specify from the MAC ACL. The **permit** and **deny** commands support many ways of identifying traffic.
Step 5	switch(config-mac-acl)# [**no**] **statistics**	(Optional) Specifies that the switch maintains global statistics for packets matching the rules in the ACL. The **no** option stops the switch from maintaining global statistics for the ACL.
Step 6	switch(config-mac-acl)# **show mac access-lists** *name*	(Optional) Displays the MAC ACL configuration.
Step 7	switch(config-mac-acl)# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to change a MAC ACL:

```
switch# configure terminal
switch(config)# mac access-list acl-mac-01
switch(config-mac-acl)# 100 permit mac 00c0.4f00.00 0000.00ff.ffff any
switch(config-mac-acl)# statistics
switch(config-mac-acl)# show mac access-lists acl-mac-01
switch(config-mac-acl)# copy running-config startup-config
```

Removing a MAC ACL

You can remove a MAC ACL from the switch.

Be sure that you know whether the ACL is applied to an interface. The switch allows you to remove ACLs that are current applied. Removing an ACL does not affect the configuration of interfaces where you have applied the ACL. Instead, the switch considers the removed ACL to be empty.

To remove a MAC ACL, perform this task:

	Command	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **no mac access-list** *name*	Removes the MAC ACL that you specify by name from the running configuration.
Step 3	switch(config)# **show mac access-lists**	(Optional) Displays the MAC ACL configuration.
Step 4	switch(config)# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

Changing Sequence Numbers in a MAC ACL

You can change all the sequence numbers assigned to rules in a MAC ACL. Resequencing is useful when you need to insert rules into an ACL and there are not enough available sequence numbers. For more information, see the "Rules" section on page 1-2.

To change all the sequence numbers assigned to rules in a MAC ACL, perform this task:

	Command	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **resequence mac access-list** *name starting-sequence-number increment*	Assigns sequence numbers to the rules contained in the ACL, where the first rule receives the number specified by the starting-sequence number that you specify. Each subsequent rule receives a number larger than the preceding rule. The difference in numbers is determined by the increment number that you specify.
Step 3	switch(config)# **show mac access-lists** *name*	(Optional) Displays the MAC ACL configuration.
Step 4	switch(config)# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

Applying a MAC ACL as a Port ACL

You can apply a MAC ACL as a port ACL to any of the following interface types:

- Layer 2 interfaces
- Port-channel interfaces

Be sure that the ACL that you want to apply exists and is configured to filter traffic as necessary for this application. For more information about configuring MAC ACLs, see the "Configuring IP ACLs" section on page 1-4.

To apply a MAC ACL as a port ACL, perform this task:

	Command	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface ethernet** *slot/port*	Enters interface configuration mode for the specified interface.
	switch(config)# **interface port-channel** *channel-number*}	Enters interface configuration mode for a port-channel interface.
Step 3	switch(config-if)# **mac port access-group** *access-list*	Applies a MAC ACL to the interface.
Step 4	switch(config-if)# **show running-config**	(Optional) Displays ACL configuration.
Step 5	switch(config-if)# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

Applying a MAC ACL as a VACL

You can apply a MAC ACL as a VACL. For information about how to create a VACL using a MAC ACL, see the "Creating or Changing a VACL" section on page 1-15.

Verifying MAC ACL Configurations

To display MAC ACL configuration information, perform one of the following tasks:

Command	Purpose
show mac access-lists	Displays the MAC ACL configuration
show running-config	Displays ACL configuration, including MAC ACLs and the interfaces that ACLs are applied to.
show running-config interface	Displays the configuration of the interface to which you applied the ACL.

Displaying and Clearing MAC ACL Statistics

Use the **show mac access-lists** command to display statistics about a MAC ACL, including the number of packets that have matched each rule.

To display or clear MAC ACL statistics, perform one of the following tasks:

Command	Purpose
show mac access-lists	Displays MAC ACL configuration. If the MAC ACL includes the **statistics** command, the **show mac access-lists** command output includes the number of packets that have matched each rule.
clear mac access-list counters	Clears statistics for all MAC ACLs or for a specific MAC ACL.

This example shows how to create a MAC ACL named acl-mac-01 and apply it to Ethernet interface 2/1, which is a Layer 2 interface in this example:

```
mac access-list acl-mac-01
  permit 00c0.4f00.0000 0000.00ff.ffff any
interface ethernet 2/1
  mac access-group acl-mac-01
```

Information About VLAN ACLs

A VLAN ACL (VACL) is one application of a MAC ACL or IP ACL. You can configure VACLs to apply to all packets that are bridged within a VLAN. VACLs are used strictly for security packet filtering. VACLs are not defined by direction (ingress or egress).

For more information about types and applications of ACLs, see the "Information About ACLs" section on page 1-1.

This section includes the following topics:

VACLs and Access Maps

VACLs use access maps to link an IP ACL or a MAC ACL to an action. The switch takes the configured action on packets permitted by the VACL.

VACLs and Actions

In access map configuration mode, you use the **action** command to specify one of the following actions:

- Forward—Sends the traffic to the destination determined by normal operation of the switch.
- Drop—Drops the traffic.

Statistics

The switch can maintain global statistics for each rule in a VACL. If a VACL is applied to multiple VLANs, the maintained rule statistics are the sum of packet matches (hits) on all the interfaces on which that VACL is applied.

> **Note**   The Cisco Nexus 5000 Series switch does not support interface-level VACL statistics.

For each VLAN access map that you configure, you can specify whether the switch maintains statistics for that VACL. This allows you to turn VACL statistics on or off as needed to monitor traffic filtered by a VACL or to help troubleshoot VLAN access-map configuration.

For information about displaying VACL statistics, see the "Displaying and Clearing IP ACL Statistics" section on page 1-9.

Configuring VACLs

This section includes the following topics:

- Creating or Changing a VACL, page 1-15
- Removing a VACL, page 1-16
- Applying a VACL to a VLAN, page 1-16
- Verifying VACL Configuration, page 1-17
- Displaying and Clearing VACL Statistics, page 1-17

Creating or Changing a VACL

You can create or change a VACL. Creating a VACL includes creating an access map that associates an IP ACL or MAC ACL with an action to be applied to the matching traffic.

To create or change a VACL, perform this task:

	Command	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **vlan access-map** *map-name*	Enters access map configuration mode for the access map specified.
Step 3	switch(config-access-map)# **match ip address** *ip-access-list*	Specifies a IPv4, and IPV6 ACL for the map.
	switch(config-access-map)# **match mac address** *mac-access-list*	Specifies a MAC ACL for the map.

	Command	Purpose
Step 4	switch(config-access-map)# **action** {**drop**|**forward** }	Specifies the action that the switch applies to traffic that matches the ACL.
Step 5	switch(config-access-map)# [**no**] **statistics**	(Optional) Specifies that the switch maintains global statistics for packets matching the rules in the VACL. The **no** option stops the switch from maintaining global statistics for the VACL.
Step 6	switch(config-access-map)# **show running-config**	(Optional) Displays ACL configuration.
Step 7	switch(config-access-map)# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

Removing a VACL

You can remove a VACL, which means that you will delete the VLAN access map.

Be sure that you know whether the VACL is applied to a VLAN. The switch allows you to remove VACLs that are current applied. Removing a VACL does not affect the configuration of VLANs where you have applied the VACL. Instead, the switch considers the removed VACL to be empty.

To remove a VACL, perform this task:

	Command	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **no vlan access-map** *map-name*	Removes the VLAN access map configuration for the specified access map.
Step 3	switch(config)# **show running-config**	(Optional) Displays ACL configuration.
Step 4	switch(config)# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

Applying a VACL to a VLAN

You can apply a VACL to a VLAN. The VACL drop-down list appears in the Advanced Settings section.

To apply a VACL to a VLAN, perform this task:

	Command	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# [**no**] **vlan filter** *map-name* **vlan-list** *list*	Applies the VACL to the VLANs by the list that you specified. The **no** option unapplies the VACL. The vlan-list command can specify a list of up to 32 vlans, but multiple vlan-list commands can be configured to cover more than 32 vlans.
Step 3	switch(config)# **show running-config**	(Optional) Displays ACL configuration.
Step 4	switch(config)# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

Verifying VACL Configuration

To display VACL configuration information, perform one of the following tasks:

Command	Purpose
show running-config aclmgr	Displays ACL configuration, including VACL-related configuration.
show vlan filter	Displays information about VACLs that are applied to a VLAN.
show vlan access-map	Displays information about VLAN access maps.

Displaying and Clearing VACL Statistics

To display or clear VACL statistics, perform one of the following tasks:

Command	Purpose
show vlan access-list	Displays VACL configuration. If the VLAN access-map includes the **statistics** command, then the **show vlan access-list** command output includes the number of packets that have matched each rule.
clear vlan access-list counters	Clears statistics for all VACLs or for a specific VACL.

This example shows how to configure a VACL to forward traffic permitted by an IP ACL named acl-ip-01and how to apply the VACL to VLANs 50 through 82:

```
configure terminal
vlan access-map acl-ip-map
  match ip address acl-ip-01
```

```
  action forward
vlan filter acl-ip-map vlan-list 50-82
```

Default Settings

Table 1-2 lists the default settings for IP ACLs parameters.

Table 1-2   Default IP ACLs Parameters

Parameters	Default
IP ACLs	No IP ACLs exist by default.
ACL rules	Implicit rules apply to all ACLs . See the "Implicit Rules" section on page 1-3.

Table 1-3 lists the default settings for MAC ACLs parameters.

Table 1-3   Default MAC ACLs Parameters

Parameters	Default
MAC ACLs	No MAC ACLs exist by default.
ACL rules	Implicit rules apply to all ACLs . See the "Implicit Rules" section on page 1-3.

Table 1-4 lists the default settings for VACL parameters.

Table 1-4   Default VACL Parameters

Parameters	Default
VACLs	No IP ACLs exist by default.
ACL rules	Implicit rules apply to all ACLs. See the "Implicit Rules" section on page 1-3.