



Configuring Access Control Lists

This chapter contains the following sections:

- [Information About ACLs, on page 1](#)
- [Configuring IP ACLs, on page 5](#)
- [Configuring MAC ACLs, on page 11](#)
- [Example Configuration for MAC ACLs, on page 16](#)
- [Information About VLAN ACLs, on page 16](#)
- [Configuring VACLs, on page 17](#)
- [Example Configuration for VACL, on page 20](#)
- [Configuring ACLs on Virtual Terminal Lines, on page 20](#)
- [Default ACL Settings, on page 23](#)

Information About ACLs

An access control list (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.

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.

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 the following table.

Table 1: Security ACL Applications

Application	Supported Interfaces	Types of ACLs Supported
Port ACL	<p>An ACL is considered a port ACL when you apply it to one of the following:</p> <ul style="list-style-type: none"> • Ethernet interface • Ethernet port-channel interface <p>When a port ACL is applied to a trunk port, the ACL filters traffic on all VLANs on the trunk port.</p>	<p>IPv4 ACLs</p> <p>IPv6 ACLs</p> <p>MAC ACLs</p>
VLAN ACL (VACL)	<p>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.</p>	<p>IPv4 ACLs</p> <p>IPv6 ACLs</p> <p>MAC ACLs</p>

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 Port ACLs first.

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.

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.

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

IPv6 ACLs support the following additional filtering options:

- Layer 4 protocol
- Authentication Header Protocol
- Encapsulating Security Payload
- Payload Compression Protocol
- Stream Control Transmission Protocol (SCTP)
- SCTP, TCP, and UDP ports
- ICMP types and codes
- IGMP types
- Flow label
- DSCP value
- TCP packets with the ACK, FIN, PSH, RST, SYN, or URG bit set
- Established TCP connections
- Packet length

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 Cisco 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

Creating an IP ACL

You can create an IPv4 or IPv6 ACL on the switch and add rules to it.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **{ip | ipv6 } access-list name**
3. switch(config-acl)# [*sequence-number*] **{permit|deny} protocol source destination**
4. (Optional) switch(config-acl)# **statistics**
5. (Optional) switch# **show {ip | ipv6} access-lists name**
6. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters configuration mode.
Step 2	switch(config)# {ip ipv6 } access-list name	Creates the IP ACL and enters IP ACL configuration mode. The <i>name</i> argument can be up to 64 characters.
Step 3	switch(config-acl)# [<i>sequence-number</i>] {permit deny} protocol source destination	Creates a rule in the IP ACL. You can create many rules. The <i>sequence-number</i> 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 <i>Cisco Nexus 5000 Series Command Reference</i> .
Step 4	(Optional) switch(config-acl)# statistics	Specifies that the switch maintains global statistics for packets matching the rules in the ACL.
Step 5	(Optional) switch# show {ip ipv6} access-lists name	Displays the IP ACL configuration.
Step 6	(Optional) switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

Example

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
```

The following example shows how to create an IPv6 ACL:

```
switch# configure terminal
switch(config)# ipv6 access-list acl-01-ipv6
switch(config-ipv6-acl)# permit tcp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
```

Changing an IP ACL

You can add and remove rules in an existing IPv4 or IPv6 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.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **{ip | ipv6} access-list name**
3. switch(config-acl)# [*sequence-number*] **{permit | deny} protocol source destination**
4. (Optional) switch(config-acl)# **no {sequence-number | {permit | deny} protocol source destination}**
5. (Optional) switch(config-acl)# [**no**] **statistics**
6. (Optional) switch# **show {ip | ipv6} access-lists name**
7. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters configuration mode.
Step 2	switch(config)# {ip ipv6} access-list name	Enters IP ACL configuration mode for the ACL that you specify by name.
Step 3	switch(config-acl)# [<i>sequence-number</i>] {permit deny} protocol source destination	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 <i>sequence-number</i> 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 <i>Cisco Nexus 5000 Series Command Reference</i> .
Step 4	(Optional) switch(config-acl)# no {sequence-number {permit deny} protocol source destination}	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 <i>Cisco Nexus 5000 Series Command Reference</i> .

	Command or Action	Purpose
Step 5	(Optional) switch(config-acl)# [no] statistics	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	(Optional) switch# show {ip ipv6} access-lists name	Displays the IP ACL configuration.
Step 7	(Optional) switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

Related Topics

[Changing Sequence Numbers in an IP ACL](#), on page 8

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:

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **no {ip | ipv6} access-list name**
3. (Optional) switch# **show running-config**
4. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters configuration mode.
Step 2	switch(config)# no {ip ipv6} access-list name	Removes the IP ACL that you specified by name from the running configuration.
Step 3	(Optional) switch# show running-config	Displays ACL configuration. The removed IP ACL should not appear.
Step 4	(Optional) switch# copy running-config startup-config	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:

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **resequence** {ip | ipv6} **access-list** *name* *starting-sequence-number* *increment*
3. (Optional) switch# **show** {ip | ipv6} **access-lists** *name*
4. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters configuration mode.
Step 2	switch(config)# resequence {ip ipv6} access-list <i>name</i> <i>starting-sequence-number</i> <i>increment</i>	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 <i>starting-sequence-number</i> argument and the <i>increment</i> argument can be a whole number between 1 and 4294967295.
Step 3	(Optional) switch# show {ip ipv6} access-lists <i>name</i>	Displays the IP ACL configuration.
Step 4	(Optional) switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

Applying an IP ACL to mgmt0

You can apply an IPv4 or IPv6 ACL to the management interface (mgmt0).

Before you begin

Ensure that the ACL that you want to apply exists and that it is configured to filter traffic in the manner that you need for this application.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *mgmt port*
3. Enter one of the following commands:
 - ip access-group *access-list* {in|out}
 - ipv6 traffic-filter *access-list* {in|out}
4. (Optional) **show running-config aclmgr**

5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	interface mgmt port Example: switch(config)# interface mgmt0 switch(config-if)#	Enters configuration mode for the management interface.
Step 3	Enter one of the following commands: <ul style="list-style-type: none"> • ip access-group <i>access-list</i> {in out} • ipv6 traffic-filter <i>access-list</i> {in out} Example: switch(config-if)#ip access-group acl-120 out	Applies an IPv4 or IPv6 ACL to the Layer 3 interface for traffic flowing in the direction specified. You can apply one router ACL per direction.
Step 4	(Optional) show running-config aclmgr Example: switch(config-if)# show running-config aclmgr	Displays the ACL configuration.
Step 5	(Optional) copy running-config startup-config Example: switch(config-if)# copy running-config startup-config	Copies the running configuration to the startup configuration.

Related Topics

- Creating an IP ACL

Applying an IP ACL as a Port ACL

You can apply an IPv4 or IPv6 ACL to a physical Ethernet interface or a EtherChannel. ACLs applied to these interface types are considered port ACLs.



Note Some configuration parameters when applied to an EtherChannel are not reflected on the configuration of the member ports.

SUMMARY STEPS

1. switch# **configure terminal**

2. switch(config)# **interface** {**ethernet** [*chassis*]/*slot/port* | **port-channel** *channel-number*}
3. switch(config-if)# {**ip port access-group** | **ipv6 port traffic-filter**} *access-list in*
4. (Optional) switch# **show running-config**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters configuration mode.
Step 2	switch(config)# interface { ethernet [<i>chassis</i>]/ <i>slot/port</i> port-channel <i>channel-number</i> }	Enters interface configuration mode for the specified interface.
Step 3	switch(config-if)# { ip port access-group ipv6 port traffic-filter } <i>access-list in</i>	Applies an IPv4 or IPv6 ACL to the interface or EtherChannel. Only inbound filtering is supported with port ACLs. You can apply one port ACL to an interface.
Step 4	(Optional) switch# show running-config	Displays ACL configuration.
Step 5	(Optional) switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

Verifying IP ACL Configurations

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

Procedure

- switch# **show running-config**

Displays ACL configuration, including IP ACL configuration and interfaces that IP ACLs are applied to.

- switch# **show running-config interface**

Displays the configuration of an interface to which you have applied an ACL.

Example

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** and **show ipv6 access-list** commands 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.

Procedure

- switch# **show** {ip | ipv6} **access-lists** *name*

Displays IP ACL configuration. If the IP ACL includes the **statistics** command, then the **show ip access-lists** and **show ipv6 access-list** command output includes the number of packets that have matched each rule.

- switch# **clear** {ip | ipv6} **access-list counters** [*access-list-name*]

Clears statistics for all IP ACLs or for a specific IP ACL.

Configuring MAC ACLs

Creating a MAC ACL

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

SUMMARY STEPS

1. switch# **configure terminal**
2. switch# **mac access-list** *name*
3. switch(config-mac-acl)# [*sequence-number*] {**permit** | **deny**} *source destination protocol*
4. (Optional) switch(config-mac-acl)# **statistics**
5. (Optional) switch# **show mac access-lists** *name*
6. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters configuration mode.
Step 2	switch# mac access-list <i>name</i>	Creates the MAC ACL and enters ACL configuration mode.
Step 3	switch(config-mac-acl)# [<i>sequence-number</i>] { permit deny } <i>source destination protocol</i>	Creates a rule in the MAC ACL. The permit and deny options support many ways of identifying traffic. For more information, see the <i>Cisco Nexus 5000 Series Command Reference</i> .
Step 4	(Optional) switch(config-mac-acl)# statistics	Specifies that the switch maintains global statistics for packets matching the rules in the ACL.
Step 5	(Optional) switch# show mac access-lists <i>name</i>	Displays the MAC ACL configuration.

	Command or Action	Purpose
Step 6	(Optional) switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

Example

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
```

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.

To change a MAC ACL, perform this task:

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **mac access-list name**
3. switch(config-mac-acl)# [*sequence-number*] {**permit** | **deny**} *source destination protocol*
4. (Optional) switch(config-mac-acl)# **no** {*sequence-number* | {**permit**|**deny**} *source destination protocol*}
5. (Optional) switch(config-mac-acl)# [**no**] **statistics**
6. (Optional) switch# **show mac access-lists name**
7. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters 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)# [<i>sequence-number</i>] { permit deny } <i>source destination protocol</i>	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.

	Command or Action	Purpose
Step 4	(Optional) switch(config-mac-acl)# no { <i>sequence-number</i> { permit deny } <i>source destination protocol</i> }	Removes the rule that you specify from the MAC ACL. The permit and deny commands support many ways of identifying traffic.
Step 5	(Optional) switch(config-mac-acl)# [no] statistics	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	(Optional) switch# show mac access-lists <i>name</i>	Displays the MAC ACL configuration.
Step 7	(Optional) switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

Example

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
```

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.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **no mac access-list** *name*
3. (Optional) switch# **show mac access-lists**
4. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters configuration mode.
Step 2	switch(config)# no mac access-list <i>name</i>	Removes the MAC ACL that you specify by name from the running configuration.

	Command or Action	Purpose
Step 3	(Optional) switch# show mac access-lists	Displays the MAC ACL configuration.
Step 4	(Optional) switch# copy running-config startup-config	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.

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

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **resequence mac access-list name starting-sequence-number increment**
3. (Optional) switch# **show mac access-lists name**
4. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters 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	(Optional) switch# show mac access-lists name	Displays the MAC ACL configuration.
Step 4	(Optional) switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

Related Topics

[Rules](#), on page 2

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:

- Ethernet interfaces
- EtherChannel interfaces

Be sure that the ACL that you want to apply exists and is configured to filter traffic as necessary for this application.



Note Some configuration parameters when applied to an EtherChannel are not reflected on the configuration of the member ports.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** {**ethernet** [*chassis*]/*slot/port* | **port-channel** *channel-number*}
3. switch(config-if)# **mac port access-group** *access-list*
4. (Optional) switch# **show running-config**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

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

Related Topics

[Creating an IP ACL](#), on page 5

Verifying MAC ACL Configurations

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

Procedure

- switch# **show mac access-lists**
Displays the MAC ACL configuration
- switch# **show running-config**
Displays ACL configuration, including MAC ACLs and the interfaces that ACLs are applied to.
- switch# **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.

Procedure

- switch# **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.

- switch# **clear mac access-list counters**

Clears statistics for all MAC ACLs or for a specific MAC ACL.

Example Configuration for MAC ACLs

This example shows how to create a MAC ACL named `acl-mac-01` and apply it to Ethernet interface 1/1:

```
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)# exit
switch(config)# interface ethernet 1/1
switch(config-if)# 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).

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.

Configuring VACLs

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:

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **vlan access-map** *map-name*
3. switch(config-access-map)# **match ip address** *ip-access-list*
4. switch(config-access-map)# **match mac address** *mac-access-list*
5. switch(config-access-map)# **action** {**drop** | **forward**}
6. (Optional) switch(config-access-map)# [**no**] **statistics**
7. (Optional) switch(config-access-map)# **show running-config**
8. (Optional) switch(config-access-map)# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters configuration mode.
Step 2	switch(config)# vlan access-map <i>map-name</i>	Enters access map configuration mode for the access map specified.
Step 3	switch(config-access-map)# match ip address <i>ip-access-list</i>	Specifies an IPv4 and IPV6 ACL for the map.
Step 4	switch(config-access-map)# match mac address <i>mac-access-list</i>	Specifies a MAC ACL for the map.
Step 5	switch(config-access-map)# action { drop forward }	Specifies the action that the switch applies to traffic that matches the ACL.

	Command or Action	Purpose
Step 6	(Optional) switch(config-access-map)# [no] statistics	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 7	(Optional) switch(config-access-map)# show running-config	Displays ACL configuration.
Step 8	(Optional) switch(config-access-map)# copy running-config startup-config	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.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **no vlan access-map** *map-name*
3. (Optional) switch(config)# **show running-config**
4. (Optional) switch(config)# **copy running-config startup-config**

DETAILED STEPS

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

Applying a VACL to a VLAN

You can apply a VACL to a VLAN.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **[no] vlan filter** *map-name* **vlan-list** *list*
3. (Optional) switch(config)# **show running-config**

4. (Optional) switch(config)# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters 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	(Optional) switch(config)# show running-config	Displays ACL configuration.
Step 4	(Optional) switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

Verifying VACL Configuration

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

Procedure

- switch# **show running-config aclmgr**
Displays ACL configuration, including VACL-related configuration.
- switch# **show vlan filter**
Displays information about VACLs that are applied to a VLAN.
- switch# **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:

Procedure

- switch# **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.
- switch# **clear vlan access-list counters**
Clears statistics for all VACLs or for a specific VACL.

Example Configuration for VACL

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

```
switch# configure terminal
switch(config)# vlan access-map acl-ip-map
switch(config-access-map)# match ip address acl-ip-01
switch(config-access-map)# action forward
switch(config-access-map)# exit
switch(config)# vlan filter acl-ip-map vlan-list 50-82
```

Configuring ACLs on Virtual Terminal Lines

To restrict incoming and outgoing connections between a Virtual Terminal (VTY) line and the addresses in an access list, use the `access-class` command in line configuration mode. To remove access restrictions, use the `no` form of this command.

Follow these guidelines when configuring ACLs on VTY lines:

- Set identical restrictions on all VTY lines because a user can connect to any of them.
- Statistics per entry is not supported for ACLs on VTY lines.

Before you begin

Be sure that the ACL that you want to apply exists and is configured to filter traffic as necessary for this application.

SUMMARY STEPS

1. `switch# configure terminal`
2. `switch(config)# line vty`
3. `switch(config-line)# access-class access-list-number {in | out}`
4. `switch(config-line)# no access-class access-list-number {in | out}`
5. `switch(config-line)# exit`
6. `switch# show running-config aclmgr`
7. `switch# copy running-config startup-config`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>switch# configure terminal</code>	Enters global configuration mode.
Step 2	<code>switch(config)# line vty</code> Example:	Enters line configuration mode.

	Command or Action	Purpose
	switch(config)# line vty switch(config-line)#	
Step 3	switch(config-line)# access-class access-list-number {in out} Example: switch(config-line)# access-class ozi2 in switch(config-line)#access-class ozi3 out switch(config)#	Specifies inbound or outbound access restrictions.
Step 4	switch(config-line)# no access-class access-list-number {in out} Example: switch(config-line)# no access-class ozi2 in switch(config-line)# no access-class ozi3 out switch(config)#	(Optional) Removes inbound or outbound access restrictions.
Step 5	switch(config-line)# exit Example: switch(config-line)# exit switch#	Exits line configuration mode.
Step 6	switch# show running-config aclmgr Example: switch# show running-config aclmgr	(Optional) Displays the running configuration of the ACLs on the switch.
Step 7	switch# copy running-config startup-config Example: switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Example

This example shows how to apply the access-class ozi2 command to the in-direction of the vty line.

```
switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# line vty
switch(config-line)# access-class ozi2 in
switch(config-line)# exit
switch#
```

Verifying ACLs on VTY Lines

To display the ACL configurations on VTY lines, perform one of the following tasks:

Command	Purpose
show running-config aclmgr	Displays the running configuration of the ACLs configured on the switch.

Command	Purpose
<code>show users</code>	Displays the users that are connected.
<code>show access-lists <i>access-list-name</i></code>	Display the statistics per entry.

Configuration Examples for ACLs on VTY Lines

The following example shows the connected users on the console line (ttyS0) and the VTY lines (pts/0 and pts/1).

```
switch# show users
NAME      LINE      TIME          IDLE          PID COMMENT
admin     ttyS0     Aug 27 20:45  .            14425 *
admin     pts/0     Aug 27 20:06 00:46       14176 (172.18.217.82) session=ssh
admin     pts/1     Aug 27 20:52  .            14584 (10.55.144.118)
```

This example shows the following:

- Applying the `ip access-list ozi` command to the in direction of the VTY line allows vty connections to all IPv4 hosts except 172.18.217.82.
- Applying the `ip access-list ozi2` command to the out direction of the VTY line, denies vty connections to any IPv4 host except 10.55.144.118, 172.18.217.79, 172.18.217.82, 172.18.217.92.
- Applying the `ipv6 access-list ozi7` command to the in direction of the VTY line, denies VTY connections to all IPv6 hosts.
- Applying the `ipv6 access-list ozip6` command to the out direction of the VTY line, allows VTY connections to all IPv6 hosts.

```
switch# show running-config aclmgr
!Time: Fri Aug 27 22:01:09 2010
version 5.0(2)N1(1)
ip access-list ozi
 10 deny ip 172.18.217.82/32 any
 20 permit ip any any
ip access-list ozi2
 10 permit ip 10.55.144.118/32 any
 20 permit ip 172.18.217.79/32 any
 30 permit ip 172.18.217.82/32 any
 40 permit ip 172.18.217.92/32 any
ipv6 access-list ozi7
 10 deny tcp any any
ipv6 access-list ozip6
 10 permit tcp any any

line vty
 access-class ozi in
 access-class ozi2 out
 ipv6 access-class ozi7 in
 ipv6 access-class ozip6 out
```

The following examples shows how to configure the ip access-list by enabling per-entry statistics for the ACL.

```
switch# conf t
Enter configuration commands, one per line.
End with CNTL/Z.
switch(config)# ip access-list ozi2
switch(config-acl)# statistics per-entry
switch(config-acl)# deny tcp 172.18.217.83/32 any
```

```

switch(config-acl)# exit

switch(config)# ip access-list ozi
switch(config-acl)# statistics per-entry
switch(config-acl)# permit ip 172.18.217.20/24 any
switch(config-acl)# exit
switch#

```

The following example shows how to apply the ACLs on VTY in and out directions.

```

switch(config)# line vty
switch(config-line)# ip access-class ozi in
switch(config-line)# access-class ozi2 out
switch(config-line)# exit
switch#

```

The following example shows how to remove the access restrictions on the VTY line.

```

switch# conf t
Enter configuration commands, one per line. End
with CNTL/Z.
switch(config)# line vty
switch(config-line)# no access-class ozi2 in
switch(config-line)# no ip access-class ozi2 in
switch(config-line)# exit
switch#

```

Default ACL Settings

The following table lists the default settings for IP ACLs parameters.

Table 2: Default IP ACLs Parameters

Parameters	Default
IP ACLs	No IP ACLs exist by default.
ACL rules	Implicit rules apply to all ACLs .

The following table lists the default settings for MAC ACLs parameters.

Table 3: Default MAC ACLs Parameters

Parameters	Default
MAC ACLs	No MAC ACLs exist by default.
ACL rules	Implicit rules apply to all ACLs .

The following table lists the default settings for VACL parameters.

Table 4: Default VACL Parameters

Parameters	Default
VACLs	No IP ACLs exist by default.
ACL rules	Implicit rules apply to all ACLs.