



Configuring MAC ACLs

This chapter describes how to configure MAC access lists (ACLs) on Cisco NX-OS devices.

This chapter contains the following sections:

- [About MAC ACLs, on page 1](#)
- [Licensing Requirements for MAC ACLs, on page 1](#)
- [Guidelines and Limitations for MAC ACLs, on page 1](#)
- [Default Settings for MAC ACLs, on page 2](#)
- [Configuring MAC ACLs, on page 2](#)
- [Verifying the MAC ACL Configuration, on page 7](#)
- [Monitoring and Clearing MAC ACL Statistics, on page 7](#)
- [Configuration Example for MAC ACLs, on page 7](#)

About MAC ACLs

MAC ACLs are ACLs that use information in the Layer 2 header of packets to filter traffic. MAC ACLs share many fundamental concepts with IP ACLs, including support for virtualization.

Licensing Requirements for MAC ACLs

This table shows the licensing requirements for this feature.

Product	License Requirement
Cisco NX-OS	MAC ACLs require no license. Any feature not included in a license package is bundled with the nx-os image and is provided at no extra charge to you. For an explanation of the Cisco NX-OS licensing scheme, see the <i>Cisco NX-OS Licensing Guide</i> .

Guidelines and Limitations for MAC ACLs

MAC ACLs have the following configuration guidelines and limitations:

- MAC ACLs apply to ingress traffic only.

- If you try to apply too many ACL entries, the configuration might be rejected.
- MAC packet classification is not supported.

Default Settings for MAC ACLs

This table lists the default settings for MAC ACL parameters.

Table 1: Default MAC ACLs Parameters

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

Configuring MAC ACLs

Creating a MAC ACL

You can create a MAC ACL and add rules to it.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	mac access-list <i>name</i> Example: switch(config)# mac access-list acl-mac-01 switch(config-mac-acl)#	Creates the MAC ACL and enters ACL configuration mode.
Step 3	{permit deny} <i>source destination-protocol</i> Example: switch(config-mac-acl)# 100 permit mac 00c0.4f00.0000 0000.00ff.ffff any 0x0806	Creates a rule in the MAC ACL. The permit and deny commands support many ways of identifying traffic.
Step 4	(Optional) statistics per-entry Example: switch(config-mac-acl)# statistics per-entry	Specifies that the device maintains global statistics for packets that match the rules in the ACL.

	Command or Action	Purpose
Step 5	(Optional) show mac access-lists <i>name</i> Example: switch(config-mac-acl)# show mac access-lists acl-mac-01	Displays the MAC ACL configuration.
Step 6	(Optional) copy running-config startup-config Example: switch(config-mac-acl)# copy running-config startup-config	Copies the running configuration to the startup configuration.

Changing a MAC ACL

You can remove a MAC ACL from the device.

Before you begin

Use the **show mac access-lists** command with the **summary** keyword to find the interfaces on which a MAC ACL is configured.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	mac access-list <i>name</i> Example: switch(config)# mac access-list acl-mac-01 switch(config-mac-acl)#	Enters ACL configuration mode for the ACL that you specify by name.
Step 3	(Optional) [<i>sequence-number</i>] {permit deny} <i>source destination-protocol</i> Example: switch(config-mac-acl)# 100 permit mac 00c0.4f00.0000 0000.00ff.ffff any 0x0806	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	(Optional) no <i>{sequence-number {permit deny} source destination-protocol}</i> Example: switch(config-mac-acl)# no 80	Removes the rule that you specify from the MAC ACL. The permit and deny commands support many ways of identifying traffic.

	Command or Action	Purpose
Step 5	(Optional) [no] statistics per-entry Example: switch(config-mac-acl)# statistics per-entry	Specifies that the device maintains global statistics for packets that match the rules in the ACL. The no option stops the device from maintaining global statistics for the ACL.
Step 6	(Optional) show mac access-lists name Example: switch(config-mac-acl)# show mac access-lists acl-mac-01	Displays the MAC ACL configuration.
Step 7	(Optional) copy running-config startup-config Example: switch(config-mac-acl)# 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.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	resequence mac access-list name <i>starting-sequence-number increment</i> Example: switch(config)# resequence mac access-list acl-mac-01 100 10	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) show mac access-lists name Example: switch(config)# show mac access-lists acl-mac-01	Displays the MAC ACL configuration.

	Command or Action	Purpose
Step 4	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Removing a MAC ACL

You can remove a MAC ACL from the device.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	no mac access-list <i>name</i> Example: <pre>switch(config)# no mac access-list acl-mac-01 switch(config)#</pre>	Removes the MAC ACL that you specify by name from the running configuration.
Step 3	(Optional) show mac access-lists <i>name</i> summary Example: <pre>switch(config)# show mac access-lists acl-mac-01 summary</pre>	Displays the MAC ACL configuration. If the ACL remains applied to an interface, the command lists the interfaces.
Step 4	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	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 Ethernet interfaces
- Layer 2 port-channel interfaces

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	Enter one of the following commands: <ul style="list-style-type: none"> • interface ethernet <i>slot/port</i> • interface port-channel <i>channel-number</i> Example: <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre> Example: <pre>switch(config)# interface port-channel 5 switch(config-if)#</pre>	<ul style="list-style-type: none"> • Enters interface configuration mode for a Layer 2 or Layer 3 interface. • Enters interface configuration mode for a Layer 2 or Layer 3 port-channel interface.
Step 3	mac port access-group <i>access-list</i> Example: <pre>switch(config-if)# mac port access-group acl-01</pre>	Applies a MAC ACL to the interface.
Step 4	(Optional) show running-config aclmgr Example: <pre>switch(config-if)# show running-config aclmgr</pre>	Displays the ACL configuration.
Step 5	(Optional) copy running-config startup-config Example: <pre>switch(config-if)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Applying a MAC ACL as a VACL

You can apply a MAC ACL as a VACL.

Verifying the MAC ACL Configuration

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

Command	Purpose
<code>show mac access-lists</code>	Displays the MAC ACL configuration.
<code>show running-config aclmgr</code> [all]	Displays the ACL configuration, including MAC ACLs and the interfaces to which MAC ACLs are applied. Note This command displays the user-configured ACLs in the running configuration. The all option displays both the default (CoPP-configured) and user-configured ACLs in the running configuration.
<code>show startup-config aclmgr</code> [all]	Displays the ACL startup configuration. Note This command displays the user-configured ACLs in the startup configuration. The all option displays both the default (CoPP-configured) and user-configured ACLs in the startup configuration.

Monitoring and Clearing MAC ACL Statistics

To monitor or clear MAC ACL statistics, use one of the commands in this table.

Command	Purpose
<code>show mac access-lists</code>	Displays the MAC ACL configuration. If the MAC ACL includes the statistics per-entry command, the <code>show mac access-lists</code> command output includes the number of packets that have matched each rule.
<code>clear mac access-list counters</code>	Clears statistics for MAC ACLs.

Configuration Example for MAC ACLs

The following 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 0x0806
interface ethernet 2/1
  mac port access-group acl-mac-01
```

