



## 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](#)
- [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.

### 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
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>mac access-list <i>name</i></b>  <b>Example:</b> <pre>switch(config)# mac access-list acl-mac-01 switch(config-mac-acl)#</pre>	Creates the MAC ACL and enters ACL configuration mode.
<b>Step 3</b>	<b>{permit   deny} <i>source destination-protocol</i></b>  <b>Example:</b> <pre>switch(config-mac-acl)# 100 permit mac 00c0.4f00.0000 0000.00ff.ffff any 0x0806</pre>	Creates a rule in the MAC ACL.  The <b>permit</b> and <b>deny</b> commands support many ways of identifying traffic.
<b>Step 4</b>	(Optional) <b>statistics per-entry</b>  <b>Example:</b> <pre>switch(config-mac-acl)# statistics per-entry</pre>	Specifies that the device maintains global statistics for packets that match the rules in the ACL.
<b>Step 5</b>	(Optional) <b>show mac access-lists <i>name</i></b>  <b>Example:</b>	Displays the MAC ACL configuration.

	Command or Action	Purpose
	<pre>switch(config-mac-acl)# show mac access-lists acl-mac-01</pre>	
<b>Step 6</b>	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch(config-mac-acl)# copy running-config startup-config</pre>	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
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>mac access-list name</b>  <b>Example:</b> <pre>switch(config)# mac access-list acl-mac-01 switch(config-mac-acl)#</pre>	Enters ACL configuration mode for the ACL that you specify by name.
<b>Step 3</b>	(Optional) [ <i>sequence-number</i> ] <b>{permit   deny}</b> <i>source destination-protocol</i>  <b>Example:</b> <pre>switch(config-mac-acl)# 100 permit mac 00c0.4f00.0000 0000.00ff.ffff any 0x0806</pre>	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 <b>permit</b> and <b>deny</b> commands support many ways of identifying traffic.
<b>Step 4</b>	(Optional) <b>no</b> { <i>sequence-number</i>   <b>{permit   deny}</b> <i>source destination-protocol</i> }  <b>Example:</b> <pre>switch(config-mac-acl)# no 80</pre>	Removes the rule that you specify from the MAC ACL.  The <b>permit</b> and <b>deny</b> commands support many ways of identifying traffic.

	Command or Action	Purpose
<b>Step 5</b>	(Optional) <b>[no] statistics per-entry</b>  <b>Example:</b> switch(config-mac-acl)# statistics per-entry	Specifies that the device maintains global statistics for packets that match the rules in the ACL.  The <b>no</b> option stops the device from maintaining global statistics for the ACL.
<b>Step 6</b>	(Optional) <b>show mac access-lists name</b>  <b>Example:</b> switch(config-mac-acl)# show mac access-lists acl-mac-01	Displays the MAC ACL configuration.
<b>Step 7</b>	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> 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
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> switch# configure terminal switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>resequence mac access-list name starting-sequence-number increment</b>  <b>Example:</b> 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.
<b>Step 3</b>	(Optional) <b>show mac access-lists name</b>  <b>Example:</b> switch(config)# show mac access-lists acl-mac-01	Displays the MAC ACL configuration.

	Command or Action	Purpose
<b>Step 4</b>	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <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
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>no mac access-list <i>name</i></b>  <b>Example:</b> <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.
<b>Step 3</b>	(Optional) <b>show mac access-lists <i>name</i> summary</b>  <b>Example:</b> <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.
<b>Step 4</b>	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <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**

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

