



## 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 2](#)
- [Default Settings for MAC ACLs, on page 2](#)
- [Configuring MAC ACLs, on page 2](#)
- [Verifying the MAC ACL Configuration, on page 8](#)
- [Monitoring and Clearing MAC ACL Statistics, on page 9](#)
- [Configuration Example for MAC ACLs, on page 9](#)
- [Additional References for MAC ACLs, on page 9](#)

## 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.

## MAC Packet Classification

MAC packet classification allows you to control whether a MAC ACL that is on a Layer 2 interface applies to all traffic entering the interface, including IP traffic, or to non-IP traffic only.

MAC Packet Classification State	Effect on Interface
Enabled	<ul style="list-style-type: none"><li>• A MAC ACL that is on the interface applies to all traffic entering the interface, including IP traffic.</li><li>• You cannot apply an IP port ACL on the interface.</li></ul>
Disabled	<ul style="list-style-type: none"><li>• A MAC ACL that is on the interface applies only to non-IP traffic entering the interface.</li><li>• You can apply an IP port ACL on the interface</li></ul>

# 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 when a MAC ACL is applied as part of a VACL.
- MAC packet classification is not supported when MAC ACLs are used as match criteria for QoS policies on Cisco Nexus 9300 Series switch 40G uplink ports.
- When you define a MAC ACL on the non EX/FX Cisco Nexus 9000 Series switches, you must define the ethertype for the traffic to be appropriately matched.
- Mac-packet classify knob is partially supported on the Cisco Nexus 9300-EX platform switches. In the absence of a direct field for marking the packet as an L2 packet, the switches match all packets with certain fields, such as src\_mac, dst\_mac, and vlan in the key field. However, they cannot match on the eth\_type field. Therefore, if you install two rules with identical fields, except the MAC protocol number field, then the match conditions will remain identical in the hardware. Hence, although the first entry in the rule sequence will hit for all the packets for all the protocol numbers, the MAC protocol number will be a no-op when the mac-packet classify is configured.
- A MAC access list applied to an interface will not block Bridge Protocol Data Unit (BPDU) traffic, such as Spanning Tree Protocol BPDUs.

## 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**

	<b>Command or Action</b>	<b>Purpose</b>
<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>mac access-list name</b> <b>Example:</b> switch(config)# mac access-list acl-mac-01 switch(config-mac-acl)#	Creates the MAC ACL and enters ACL configuration mode.
<b>Step 3</b>	<b>{permit   deny} source destination-protocol</b> <b>Example:</b> switch(config-mac-acl)# 100 permit mac 00c0.4f00.0000 0000.00ff.ffff any 0x0806	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> switch(config-mac-acl)# statistics per-entry	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 name</b> <b>Example:</b> switch(config-mac-acl)# show mac access-lists acl-mac-01	Displays the MAC ACL configuration.
<b>Step 6</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 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> switch# configure terminal switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>mac access-list name</b>  <b>Example:</b> switch(config)# mac access-list acl-mac-01 switch(config-mac-acl)#	Enters ACL configuration mode for the ACL that you specify by name.
<b>Step 3</b>	(Optional) [ <i>sequence-number</i> ] { <b>permit</b>   <b>deny</b> } <i>source destination-protocol</i>  <b>Example:</b> 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 <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</b>   <b>deny</b> } <i>source destination-protocol</i> }  <b>Example:</b> switch(config-mac-acl)# no 80	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.
<b>Step 5</b>	(Optional) [ <b>no</b> ] <b>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**

	<b>Command or Action</b>	<b>Purpose</b>
<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 <i>name</i> <i>starting-sequence-number increment</i></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 <i>name</i></b> <b>Example:</b> switch(config)# show mac access-lists acl-mac-01	Displays the MAC ACL configuration.
<b>Step 4</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

## Removing a MAC ACL

You can remove a MAC ACL from the device.

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<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>no mac access-list <i>name</i></b> <b>Example:</b> switch(config)# no mac access-list acl-mac-01 switch(config)#	Removes the MAC ACL that you specify by name from the running configuration.

	Command or Action	Purpose
<b>Step 3</b>	(Optional) <b>show mac access-lists</b> <i>name</i> <b>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</b> <b>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

	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>	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>	Applies a MAC ACL to the interface.

	Command or Action	Purpose
	<code>switch(config-if)# mac port access-group acl-01</code>	
<b>Step 4</b>	(Optional) <b>show running-config aclmgr</b>  <b>Example:</b> <code>switch(config-if)# show running-config aclmgr</code>	Displays the ACL configuration.
<b>Step 5</b>	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <code>switch(config-if)# copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

## Applying a MAC ACL as a VACL

You can apply a MAC ACL as a VACL.

## Enabling or Disabling MAC Packet Classification

You can enable or disable MAC packet classification on a Layer 2 interface.

### Before you begin

The interface must be configured as a Layer 2 interface.



**Note** If the interface is configured with the **ip port access-group** command or the **ipv6 port traffic-filter** command, you cannot enable MAC packet classification until you remove the **ip port access-group** and **ipv6 port traffic-filter** commands from the interface configuration.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> <code>switch# configure terminal</code> <code>switch(config)#</code>	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> <code>switch(config)# interface ethernet 2/1</code> <code>switch(config-if)#</code>	<ul style="list-style-type: none"> <li>• Enters interface configuration mode for an Ethernet interface.</li> <li>• Enters interface configuration mode for a port-channel interface.</li> </ul>

	Command or Action	Purpose
	<b>Example:</b> <pre>switch(config)# interface port-channel 5 switch(config-if)#</pre>	
<b>Step 3</b>	<b>[no] mac packet-classify</b> <b>Example:</b> <pre>switch(config-if)# mac packet-classify</pre>	Enables MAC packet classification on the interface. The <b>no</b> option disables MAC packet classification on the interface.
<b>Step 4</b>	(Optional) Enter one of the following commands: <ul style="list-style-type: none"> <li>• <b>show running-config interface ethernet <i>slot/port</i></b></li> <li>• <b>show running-config interface port-channel <i>channel-number</i></b></li> </ul> <b>Example:</b> <pre>switch(config-if)# show running-config interface ethernet 2/1</pre> <b>Example:</b> <pre>switch(config-if)# show running-config interface port-channel 5</pre>	<ul style="list-style-type: none"> <li>• Displays the running configuration of the Ethernet interface.</li> <li>• Displays the running configuration of the port-channel interface.</li> </ul>
<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.

## Verifying the MAC ACL Configuration

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

Command	Purpose
<b>show mac access-lists</b>	Displays the MAC ACL configuration.
<b>show running-config aclmgr [all]</b>	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.



Command	Purpose
<code>show startup-config aclmgr [all]</code>	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
```

## Additional References for MAC ACLs

### Related Documents

Related Topic	Document Title
TAP aggregation	<a href="#">Configuring TAP Aggregation and MPLS Stripping</a>

