# Configuring MAC ACLs

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


- Information About MAC ACLs, on page 1
- Default Settings for MAC ACLs, on page 2
- Guidelines and Limitations for MAC ACLs, on page 2
- Configuring MAC ACLs, on page 2
- Verifying the MAC ACL Configuration, on page 9
- Clearing MAC ACL Statistics, on page 9


# Information 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 does not work on the Layer 3 control plane protocols such as HSRP, VRRP, OSPF, and so on. If you enable MAC packet classification on the VLANs, the basic functionalities will break on these protocols.

| MAC Packet Classification State | Effect on Interface |
|---|---|
| Enabled | • A MAC ACL that is on the interface applies to all traffic entering the interface, including IP traffic.<br>• You can apply an IP port ACL on the interface, but it will not filter traffic. |
| Disabled | • A MAC ACL that is on the interface applies only to non-IP traffic entering the interface.<br>• You can apply an IP port ACL on the interface and it will filter traffic. |

# 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 |

# Guidelines and Limitations for MAC ACLs

MAC ACLs have the following configuration guidelines and limitations:

- MAC ACLs apply to ingress traffic only.
- Due to a hardware limitation, MAC ACL does not filter ARP packets on Cisco Nexus 3500 platform switches.

# 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** | switch# **configure terminal** | Enters global configuration mode. |
| **Step 2** | switch(config)# **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.<br>The **permit** and **deny** commands support many ways of identifying traffic. |
| **Step 4** | (Optional) switch(config-mac-acl)# **statistics per-entry** | Specifies that the device maintains global statistics for packets that match the rules in the ACL. |
| **Step 5** | (Optional) switch(config-mac-acl)# **show mac access-lists** *name* | Displays the MAC ACL configuration. |

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

### Example

This example shows how to create a MAC ACL:

```
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 per-entry
switch(config-mac-acl)# show mac access-lists acl-mac-01

MAC ACL acl-mac-01
        statistics per-entry
        10 permit 00c0.4f00.0000 0000.00ff.ffff any

switch(config-mac-acl)# copy running-config startup-config
```

# 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 that a MAC ACL is configured on.

### Procedure

| | Command or Action | 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** | (Optional) switch(config-mac-acl)# [*sequence-number*] {**permit** \| **deny**} *source destination protocol* | 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.<br>The **permit** and **deny** commands support many ways of identifying traffic. |
| **Step 4** | (Optional) switch(config-mac-acl)# **no** {*sequence-number* \| {**permit** \| **deny**} *source destination protocol*} | Removes the rule that you specify from the MAC ACL. |

| | Command or Action | Purpose |
|---|---|---|
| | | The **permit** and **deny** commands support many ways of identifying traffic. |
| **Step 5** | (Optional) switch(config-mac-acl)# [**no**] **statistics per-entry** | Specifies that the device maintains global statistics for packets that match the rules in the ACL.<br>The **no** option stops the device from maintaining global statistics for the ACL. |
| **Step 6** | (Optional) switch(config-mac-acl)# **show mac access-lists** *name* | Displays the MAC ACL configuration. |
| **Step 7** | (Optional) switch(config-mac-acl)# **copy running-config startup-config** | Copies the running configuration to the startup configuration. |

### Example

This 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 00c0.4f00.00 0000.00ff.ffff any
switch(config-mac-acl)# 80 permit 00c0.4f00.00 0000.00ff.ffff any
switch(config-mac-acl)# no 80
switch(config-mac-acl)# statistics per-entry
switch(config-mac-acl)# show mac access-lists acl-mac-01

MAC ACL acl-mac-01
        statistics per-entry
        10 permit 00c0.4f00.0000 0000.00ff.ffff any
        100 permit 00c0.4f00.0000 0000.00ff.ffff any

switch(config-mac-acl)# copy running-config startup-config
```

# 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** | 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 |

| | Command or Action | Purpose |
|---|---|---|
| | | is determined by the increment number that you specify. |
| **Step 3** | (Optional) switch(config)# **show mac access-lists** *name* | Displays the MAC ACL configuration. |
| **Step 4** | (Optional) switch(config)# **copy running-config startup-config** | Copies the running configuration to the startup configuration. |

### Example

This example shows how to change the sequence of a MAC ACL:

```
switch# configure terminal
switch(config)# resequence mac access-list acl-mac-01 100 15
switch(config)# show mac access-lists acl-mac-01

MAC ACL acl-mac-01
        statistics per-entry
        100 permit 00c0.4f00.0000 0000.00ff.ffff any
        115 permit 00c0.4f00.0000 0000.00ff.ffff any

switch(config)# copy running-config startup-config
```

# Removing a MAC ACL

You can remove a MAC ACL from the device.

### Procedure

| | Command or Action | 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** | (Optional) switch(config)# **show mac access-lists** *name* **summary** | Displays the MAC ACL configuration. If the ACL remains applied to an interface, the command lists the interfaces. |
| **Step 4** | (Optional) switch(config)# **copy running-config startup-config** | Copies the running configuration to the startup configuration. |

### Example

This example shows how to remove a MAC ACL:

```
switch# configure terminal
switch(config)# show mac access-lists
```

```
MAC ACL acl-mac-01
        statistics per-entry
        100 permit 00c0.4f00.0000 0000.00ff.ffff any
        115 permit 00c0.4f00.0000 0000.00ff.ffff any
MAC ACL acl-mac-02
        statistics per-entry
        10 permit 00a0.3f00.0000 0000.00dd.ffff any
MAC ACL acl-mac-03
        statistics per-entry
        10 permit 00b0.5f00.0000 0000.00aa.fbbf any

switch(config)# no mac access-list acl-mac-02
switch(config)# show mac access-lists acl-mac-02 summary
switch(config)# show mac access-lists

MAC ACL acl-mac-01
        statistics per-entry
        100 permit 00c0.4f00.0000 0000.00ff.ffff any
        115 permit 00c0.4f00.0000 0000.00ff.ffff any
MAC ACL acl-mac-03
        statistics per-entry
        10 permit 00b0.5f00.0000 0000.00aa.fbbf any

switch(config)# copy running-config startup-config
```

# 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 or Layer 3 Ethernet interfaces
- Layer 2 or Layer 3 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** | switch# **configure terminal** | Enters global configuration mode. |
| **Step 2** | Enter one of the following commands:<br>• switch(config)# **interface ethernet** *slot*/*port*<br>• switch(config)# **interface port-channel** *channel-number* | • Enters interface configuration mode for a Layer 2 or Layer 3 interface.<br>• Enters interface configuration mode for a Layer 2 or Layer 3 port-channel interface. |
| **Step 3** | switch(config-if)# **mac port access-group** *access-list* | Applies a MAC ACL to the interface. |
| **Step 4** | (Optional) switch(config-if)#**show running-config aclmgr** | Displays ACL configuration. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | (Optional) switch(config-if)# **copy running-config startup-config** | Copies the running configuration to the startup configuration. |

### Example

This example shows how to apply a MAC ACL as a port ACL to an Ethernet interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# mac port access-group acl-mac-01
switch(config-if)# show running-config aclmgr

!Command: show running-config aclmgr
!Time: Sat Jul 19 23:36:04 2014

version 6.0(2)A4(1)
mac access-list acl-mac-01
  statistics per-entry
  100 permit 00C0.4F00.0000 0000.00FF.FFFF any
  115 permit 00C0.4F00.0000 0000.00FF.FFFF any
mac access-list acl-mac-03
  statistics per-entry
  10 permit 00B0.5F00.0000 0000.00AA.FBBF any
ip access-list copp-system-acl-bfd
  10 permit udp any any eq 3784
ip access-list copp-system-acl-eigrp
  10 permit eigrp any any
ip access-list copp-system-acl-ftp
  10 permit tcp any any eq ftp-data
  20 permit tcp any any eq ftp
  30 permit tcp any eq ftp-data any
  40 permit tcp any eq ftp any

...

interface Ethernet1/3
  mac port access-group acl-mac-01

switch(config-if)# copy running-config startup-config
```

This example shows how to apply a MAC ACL as a port ACL to a port-channel interface:

```
switch# configure terminal
switch(config)# interface port-channel 5
switch(config-if)# mac port access-group acl-mac-01
switch(config-if)# show running-config aclmgr

!Command: show running-config aclmgr
!Time: Sat Jul 19 23:37:04 2014

version 6.0(2)A4(1)
mac access-list acl-mac-01
  statistics per-entry
  100 permit 00C0.4F00.0000 0000.00FF.FFFF any
  115 permit 00C0.4F00.0000 0000.00FF.FFFF any
mac access-list acl-mac-03
  statistics per-entry
  10 permit 00B0.5F00.0000 0000.00AA.FBBF any
```

```
ip access-list copp-system-acl-bfd
  10 permit udp any any eq 3784
ip access-list copp-system-acl-eigrp
  10 permit eigrp any any
ip access-list copp-system-acl-ftp
  10 permit tcp any any eq ftp-data
  20 permit tcp any any eq ftp
  30 permit tcp any eq ftp-data any
  40 permit tcp any eq ftp any


...

interface port-channel5
  mac port access-group acl-mac-01

switch(config-if)# copy running-config startup-config
```

# Enabling or Disabling MAC Packet Classification

You can enable or disable MAC packet classification on a per VLAN basis.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **config t**<br>**Example:**<br>`switch# config t`<br>`switch(config)#` | Enters global configuration mode. |
| **Step 2** | **vlan** *vlan-number*<br>**Example:**<br>`switch(config)# vlan 10`<br>`switch(config-vlan)#` | Creates a VLAN interface. The number range is from 1 to 4094. |
| **Step 3** | [**no**] **mac packet-classify**<br>**Example:**<br>`switch(config-vlan)# mac packet-classify`<br>`switch(config-vlan)#` | Enables MAC packet classification on the vlan. The **no** option disables MAC packet classification on the vlan. |
| **Step 4** | **exit**<br>**Example:**<br>`switch(config-vlan)# exit`<br>`switch(config)#` | Exits the vlan configuration. |
| **Step 5** | (Optional) **show running-config vlan** *vlan-number* | Displays the running configuration. |

### Example

This example shows how to enable MAC packet classification on a per VLAN basis:

```
switch# configure terminal
switch(config)# vlan 50
switch(config-vlan)# mac packet-classify
switch(config-vlan)# exit
switch(config)# show running-config vlan 50

!Command: show running-config interface Vlan50
!Time: Wed Aug  6 20:39:03 2014

version 6.0(2)A4(1)

interface Vlan50
  mac packet-classify

switch(config-if)# copy running-config startup-config
```

# Verifying the MAC ACL Configuration

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 aclmgr** [**all**] | Displays the ACL configuration, including MAC ACLs and the interfaces to which MAC ACLs are applied.<br>**Note** The **all** option displays both the default (CoPP-configured) and user-configured ACLs in the running configuration. |
| **show startup-config aclmgr** [**all**] | Displays the ACL startup configuration.<br>**Note** The **all** option displays both the default (CoPP-configured) and user-configured ACLs in the startup configuration. |

# Clearing MAC ACL Statistics

You can clear MAC ACL statistics by using the **clear mac access-list counters** command

| Command | Purpose |
|---|---|
| **clear mac access-list counters** | Clears statistics for all MAC ACLs or for a specific MAC ACL. |