Configuring MAC ACLs

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

Note The Cisco NX-OS release that is running on a managed device may not support all the features or settings described in this chapter. For the latest feature information and caveats, see the documentation and release notes for your platform and software release.

This chapter contains the following sections:

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.

Licensing Requirements for MAC ACLs

This table shows the licensing requirements for this feature.

Product	License Requirement
Cisco DCNM	MAC ACLs require no license. Any feature not included in a license package is bundled with the Cisco DCNM and is provided at no charge to you. For an explanation of the Cisco DCNM licensing scheme, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.
Cisco NX-OS	MAC ACLs require no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For an explanation of the Cisco NX-OS licensing scheme for your platform, see the licensing guide for your platform.

Platform Support for MAC ACLs

The following platforms support this feature but may implement it differently. For platform-specific information, including guidelines and limitations, system defaults, and configuration limits, see the corresponding documentation.

Platform	Documentation
Cisco Nexus 1000V Series Switches	Cisco Nexus 1000V Series Switches Documentation
Cisco Nexus 4000 Series Switches	Cisco Nexus 4000 Series Switches Documentation
Cisco Nexus 5000 Series Switches	Cisco Nexus 5000 Series Switches Documentation
Cisco Nexus 7000 Series Switches	Cisco Nexus 7000 Series Switches Documentation

Configuring MAC ACLs

Creating a MAC ACL

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

Procedure

Step 1 From the Feature Selector pane, choose **Security** ➤ **Access Control** ➤ **MAC ACL**.
The Summary pane displays available devices.

Step 2 From the Summary pane, double-click the device to which you want to add an ACL.

Step 3 (Optional) From the menu bar, choose **File** ➤ **New** ➤ **MAC ACL**.

A new row appears in the Summary pane and the ACL Details tab appears in the Details pane.

Step 4 On the ACL Details tab, in the Name field, type a name for the ACL.

Step 5 (Optional) If you want the device to maintain global statistics for rules in this MAC ACL, check **Statistics**.

Step 6 For each rule that you want to add to the ACL, from the menu bar, choose **File** ➤ **New** and choose the type of rule. On the Details tab, configure fields as needed.

Step 7 (Optional) From the menu bar, choose **File** ➤ **Deploy** to apply your changes to the device.

Changing a MAC ACL

In an existing MAC ACL, you can change, reorder, add, and remove rules.

Procedure

Step 1 From the Feature Selector pane, choose **Security** ➤ **Access Control** ➤ **MAC ACL**.
The Summary pane displays available devices.

Step 2 (Optional) From the Summary pane, double-click the device that has the ACL you want to change and then double-click the ACL.
The ACLs on the device and the rules of the ACL that you double-clicked appear in the Summary pane.

Step 3 (Optional) If you change whether the device maintains global statistics for rules in this MAC ACL, click the ACL in the Summary pane and then, on the ACL Details tab, check or uncheck **Statistics** as needed.

Step 4 (Optional) If you want to change the details of a rule, click the rule in the Summary pane and then, on the Details tab, configure fields as needed.

Step 5 (Optional) If you want to add a rule, click the ACL in the Summary pane and then from the menu bar, choose **File** ➤ **New**, choose the type of rule, and then, on the Details tab, configure fields as needed.

Step 6 (Optional) If you want to remove a rule, click the rule and then from the menu bar, choose **Actions** ➤ **Delete**.

Step 7 (Optional) If you want to move a rule to a different position in the ACL, click the rule and then from the menu bar, choose one of the following, as applicable:

- **Actions** ➤ **Move Up**
- **Actions** ➤ **Move Down**

The rule moves up or down, as you chose. The sequence number of the rules adjust accordingly.

Step 8 (Optional) From the menu bar, choose **File** ➤ **Deploy** to apply your changes to the device.

Related Topics

- Changing Sequence Numbers in a MAC ACL, page 4

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

Step 1 From the Feature Selector pane, choose **Security** ➤ **Access Control** ➤ **MAC ACL**.
The available devices appear in the Summary pane.

Step 2 From the Summary pane, double-click the device that has the ACL that you want to change and then double-click the ACL.
The ACLs on the device and the rules of the ACL that you double-clicked appear in the Summary pane. The Seq No column shows the sequence number assigned to each rule.

Step 3 Click the rule whose sequence number you want to change.
The Details pane shows the Sequence Number field for the rule.

Step 4 Click the **Sequence Number** field, edit the number, and press **Tab**.
In the Summary pane, the new sequence number appears and, if applicable, the rule moves to the position determined by the new sequence number.

Step 5 From the menu bar, choose **File** ➤ **Deploy** to apply your changes to the device.

Removing a MAC ACL

You can remove a MAC ACL from the device.

Procedure

Step 1 From the Feature Selector pane, choose **Security** ➤ **Access Control** ➤ **MAC ACL**.
The Summary pane displays available devices.

Step 2 From the Summary pane, double-click the device from which you want to remove an ACL.
The Summary pane displays the ACLs currently on the device.

Step 3 Click the ACL that you want to remove, and then from the menu bar, choose **Actions** ➤ **Delete**.
Cisco DCNM removes the ACL from the Summary pane.

Step 4 (Optional) From the menu bar, choose **File** ➤ **Deploy** to apply your changes to the device.

Applying a MAC ACL to a Physical Port

You can apply a MAC ACL to incoming or outgoing traffic on a physical Ethernet port, regardless of the port mode.

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.

Procedure

Step 1 From the Feature Selector pane, choose **Interfaces** ➤ **Physical** ➤ **Ethernet**.
The Summary pane displays available devices.

Step 2 From the Summary pane, double-click the applicable device and then double-click the slot containing the port.
The Summary pane displays the ports in the slot that you double-clicked.

Step 3 Click the port to which you want to apply a MAC ACL.

Step 4 From the Details pane, click the **Details** tab and expand the **Advanced Settings** section, if necessary.
The following drop-down lists appear in the MAC ACL area:

- Incoming Traffic
- Outgoing Traffic

Step 5 For each traffic direction that you want to apply an ACL, from the applicable drop-down list, choose the ACL that you want to apply.

Step 6 From the menu bar, choose **File** ➤ **Deploy** to apply your changes to the device.

Related Topics

- Creating a MAC ACL, page 2
- Changing a MAC ACL, page 3

Applying a MAC ACL to a Virtual Ethernet Interface

You can apply a MAC ACL to incoming or outgoing traffic on a virtual Ethernet interface.

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.

Procedure

Step 1 From the Feature Selector pane, choose **Interfaces** ➤ **Logical** ➤ **Virtual Ethernet**.
The Summary pane displays available devices.

Step 2 From the Summary pane, double-click the applicable device and then double-click the slot containing the port.

The Summary pane displays the ports in the slot that you double-clicked.

Step 3 Click the port to which you want to apply a MAC ACL.

Step 4 From the Details pane, click the **Details** tab and expand the **Advanced Settings** section, if necessary.
The following drop-down lists appear in the MAC ACL area:

- Incoming Traffic
- Outgoing Traffic

Step 5 For each traffic direction that you want to apply an ACL, from the applicable drop-down list, choose the ACL that you want to apply.

Step 6 From the menu bar, choose **File** ➤ **Deploy** to apply your changes to the device.

Related Topics

- Creating a MAC ACL, page 2
- Changing a MAC ACL, page 3

Applying a MAC ACL to a Port Channel

You can apply a MAC ACL to an Ethernet port channel.

DCNM allows you to apply a MAC ACL in incoming traffic only on an Ethernet port channel.

Before You Begin

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

Procedure

Step 1 From the Feature Selector pane, choose **Interfaces** ➤ **Logical** ➤ **Port Channel**.
Available devices appear in the Summary pane.

Step 2 From the Summary pane, double-click the applicable device.
Port channels on the device that you double-clicked appear in the Summary pane.

Step 3 Click the port channel to which you want to apply a MAC ACL.
Settings about the port channel appear in the Details pane.

Step 4 From the Details pane, click the **Port Channel Advanced Settings** tab and expand the **Advanced Settings** section, if necessary.
In the Advanced Settings section, the MAC ACL areas contains an Incoming Traffic drop-down list.

Step 5 From the Incoming Traffic drop-down list, choose the MAC ACL that you want to apply.

Step 6 From the menu bar, choose **File** ➤ **Deploy** to apply your changes to the device.

Applying a MAC ACL as a VACL

You can apply a MAC ACL as a VACL.

Related Topics

- Creating a MAC ACL, page 2
- Changing a MAC ACL, page 3

Monitoring and Clearing MAC ACL Statistics

The following window appears in the Statistics tab:

- Access Rule Statistics Chart—Information about the number of packets that match the selected MAC ACL rule.

For more information on collecting statistics for this feature, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

Field Descriptions for MAC ACLs

MAC ACL: ACL Details Tab

Table 1: MAC ACL: ACL Details Tab

Field	Description
Name	Specifies the name of the MAC ACL. Names can be alphanumeric characters but must begin with an alphabetic character. Maximum length is 64 characters. No name is assigned by default.
Statistics	Whether the device logs statistics about traffic filtered by the ACL. This check box is unchecked by default.

MAC Access Rule: Details: General Section

Table 2: MAC Access Rule: Details: General Section

Field	Description
Sequence Number	*Display only.* Shows the sequence number assigned to the rule.

Field	Description
Action	Action taken by the device when it determines that the rule applies to the packet. Valid values are as follows: • Deny—Stop processing the packet and drop it. This is the default value. • Permit—Continue processing the packet.
Protocol	Type of traffic that the access rule applies to. By default, no protocol is selected. To specify a protocol, choose the protocol name. The list is ordered by the protocol number but the protocol number is not shown.
Time-range	Named time range that applies to the access rule. If you want the rule to be always in effect, do not specify a time range. This field is blank by default.
Cost of Service	Specifies that the rule matches only packets with an IEEE 802.1Q header that contains the Class of Service (CoS) value given in the cos-value argument. The cos-value argument can be an integer from 0 to 7.
VLAN	Specifies that the rule matches only packets with an IEEE 802.1Q header that contains the VLAN ID of the VLAN that you select.

MAC Access Rule: Details: Source and Destination Section

Table 3: MAC Access Rule: Details: Source and Destination Section

Field	Description
Source	Type of source. Valid values are as follows: • Any—The rule matches packets from any source. This is the default value. When you choose Any, the MAC Address and Wildcard Mask fields below this list are unavailable because you do not need to specify either of them. • Host—The rule matches packets from a specific MAC address. When you choose Host, the MAC Address field below this list is available but the Wildcard Mask field remains unavailable.

Field	Description
	• Network—The rule matches packets from a MAC network. When you choose Network, the MAC Address and Wildcard Mask fields below this list are both available.
MAC Address (Source)	MAC address of a host or a network. Valid addresses are in dotted hexadecimal format. This field is available when you choose Host or Network from the Source drop-down list. By default, this field is blank.
Wildcard Mask (Source)	Wildcard mask of a MAC network. Valid masks are in dotted hexadecimal format. For example, if you specified 00c0.4f03.0000 in the MAC Address field, you would enter 0000.0000.ffff in this field. This field is available when you choose Network from the Source drop-down list. By default, this field is blank.
Destination	Type of destination. Valid values are as follows: • Any—The rule matches packets sent to any source. This is the default value. When you choose Any, the MAC Address and Wildcard Mask fields below this list are unavailable because you do not need to specify either of them. • Host—The rule matches packets sent to a specific MAC address. When you choose Host, the MAC Address field below this list is available but the Wildcard Mask field remains unavailable. • Network—The rule matches packets sent to a MAC network. When you choose Network, the MAC Address and Wildcard Mask fields below this list are both available.
MAC Address (Destination)	MAC address of a host or a network. Valid addresses are in dotted hexadecimal format. This field is available when you choose Host or Network from the Source drop-down list. By default, this field is blank.
Wildcard Mask (Destination)	Wildcard mask of a MAC network. Valid masks are in dotted hexadecimal format. For example, if you specified 00c0.4f03.0000 in the IP Address field, you would enter 0000.0000.ffff in this field. This field is available when you choose Network from the Source drop-down list. By default, this field is blank.

MAC ACL Remark: Remark Details Tab

Table 4: MAC ACL Remark: Remark Details Tab

Field	Description
Remark Sequence Number	*Display only.* Sequence number assigned to the remark.
Remark Description	Remark text. Maximum length is 100 characters. By default, this field is blank.

Additional References for MAC ACLs

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Feature History for MAC ACLs

This table lists the release history for this feature.

Table 5: Feature History for MAC ACLs

Feature Name	Releases	Feature Information
MAC ACLs	5.2(1)	No change from Release 5.1.
MAC ACLs	5.1(1)	No change from Release 5.0.
MAC ACLs	5.0(2)	No change from Release 4.2.
MAC ACLs	4.2(1)	Support was added for MAC packet classification.