CHAPTER 12

Configuring MAC ACLs

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

This chapter includes the following sections:

Information About MAC ACLs

MAC ACLs are ACLs that filter traffic using information in the Layer 2 header of each packet. MAC ACLs share many fundamental concepts with IP ACLs, including support for virtualization. For information about these shared concepts, see the "Information About ACLs" section on page 11-1.

Licensing Requirements for MAC ACLs

The following table shows the licensing requirements for this feature:

Product	License Requirement
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 a complete explanation of the NX-OS licensing scheme, see the *Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.1*

Prerequisites for MAC ACLs

- You must be familiar with MAC addressing and non-IP protocols to configure MAC ACLs.
- You must be familiar with the concepts in the "Information About ACLs" section on page 11-1.

Guidelines and Limitations

MAC ACLs have the following configuration guidelines and limitations:

- MAC ACLs apply to ingress traffic only.
- ACL statistics are not supported if the DHCP snooping feature is enabled.

Configuring MAC ACLs

-
- , page 12-3

Changing Sequence Numbers in a MAC ACL, page 12-5

Removing a MAC ACL, page 12-6

Applying a MAC ACL as a Port ACL, page 12-6

Applying a MAC ACL as a VACL, page 12-8

Creating a MAC ACL

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

BEFORE YOU BEGIN

switchto vdc command). Because ACL names can be repeated in different VDCs, we recommend that you confirm which VDC you are working in.

SUMMARY STEPS

1. **configure terminal**
2. **mac access-list** *name*
3. {**permit** | **deny**} *destination protocol*
4. **statistics per-entry**
5. **show mac access-lists**
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**`configure terminal`**
	
	`Example:`
	`switch# configure terminal`
	`switch(config)#`	

	`mac access-list` *`name`*
	
	`Example:`
	`switch(config)# mac access-list acl-mac-01`
	`switch(config-mac-acl)#`	

	`{`**`permit`** `|` **`deny`**`}` *`source destination protocol`*
	
	`Example:`
	`switch(config-mac-acl)# permit 00c0.4f00.0000 0000.00ff.ffff any`
		Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.1

	`statistics per-entry`
	
	`Example:`
	`switch(config-mac-acl)# statistics per-entry`	

	`show mac access-lists` *`name`*
	
	`Example:`
	`switch(config-mac-acl)# show mac access-lists acl-mac-01`	

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

Changing a MAC ACL

In an existing MAC ACL, you can add and remove rules. You cannot change existing rules. Instead, to change a rule, you can remove it and recreate it with the desired changes.

If you need to add more rules between existing rules than the current sequence numbering allows, you can use the **resequence** command to reassign sequence numbers. For more information, see the “Changing Sequence Numbers in a MAC ACL” section on page 12-5.

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command). Because ACL names can be repeated in different VDCs, we recommend that you confirm which VDC you are working in.

SUMMARY STEPS

1. **configure terminal**
2. **mac access-list**

[*sequence-number*] { } *source destination protocol*

{*sequence-number* | { } *source destination protocol*}

[ ]

name

7.

DETAILED STEPS

	Command	Purpose
Step 1		Enters global configuration mode.
Step 2	*name*	Enters ACL configuration mode for the ACL that you specify by name.
Step 3	[*sequence-number*] { | } *source destination protocol* `switch(config-mac-acl)# 100 permit mac 00c0.4f00.00 0000.00ff.ffff any`	(Optional) 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 and commands support many ways of identifying traffic. For more information, see the .

Step 4	{*sequence-number* | { | } *source destination protocol*}
	`switch(config-mac-acl)# no 80`
		(Optional) Removes the rule that you specify from the MAC ACL.
		The and commands support many ways of identifying traffic. For more information, see the
		.

Step 5	[ ] `switch(config-mac-acl)# statistics per-entry`	(Optional) Specifies that the device maintains global statistics for packets that match the rules in the ACL. The option stops the device from maintaining global statistics for the ACL.
Step 6	*name* `switch(config-mac-acl)# show mac access-lists acl-mac-01`	(Optional) Displays the MAC ACL configuration.
Step 7	`switch(config-mac-acl)# copy running-config startup-config`	(Optional) 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. For more information, see the “About Rules” section on page 11-5.

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the command). Because ACL names can be repeated in different VDCs, we recommend that you confirm which VDC you are working in.

SUMMARY STEPS

1.
2.
3.
4.

DETAILED STEPS

	Command	Purpose
Step 1		Enters global configuration mode.

Step 2	**`resequence mac access-list`** *`name starting-sequence-number increment`*
	Example:
	`switch(config)# resequence mac access-list acl-mac-01 100 10`	

	`show mac access-lists` *`name`*
	Example:
	`switch(config)# show mac access-lists acl-mac-01`	

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

Removing a MAC ACL

BEFORE YOU BEGIN

SUMMARY STEPS

1.
2.
3.
4.

DETAILED STEPS

	Command	Purpose

Step 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`	

Step 2	**no mac access-list**
	
	Example:
	`switch(config)# no mac access-list acl-mac-01`
	`switch(config)#`	

Step 3	**show mac access-lists summary** **Example:** `switch(config)# show mac access-lists acl-mac-01 summary`	
Step 4	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	

Applying a MAC ACL as a Port ACL

-

-
-

BEFORE YOU BEGIN

SUMMARY STEPS

1.
2. /

   channel-number
3. *access-list*
4.
5.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.
Step 2	**interface ethernet** / **Example:** switch(config)# interface ethernet 2/1 switch(config-if)#	Enters interface configuration mode for a Layer 2 or Layer 3 interface.
	interface port-channel *channel-number* **Example:** switch(config)# interface port-channel 5 switch(config-if)#	Enters interface configuration mode for a port-channel interface.
	mac port access-group **Example:** switch(config-if)# mac port access-group acl-01	Applies a MAC ACL to the interface.
	show running-config aclmgr **Example:** switch(config-if)# show running-config aclmgr	(Optional) Displays ACL configuration.
	copy running-config startup-config **Example:** switch(config-if)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Applying a MAC ACL as a VACL

You can apply a MAC ACL as a VACL. For information about how to create a VACL using a MAC ACL, see the "Creating a VACL or Adding a VACL Entry" section on page 13-4.

Verifying MAC ACL Configurations

To display MAC ACL configuration information, use one of the following commands:

Command	Purpose
	Displays the MAC ACL configuration
	Displays the ACL configuration, including MAC ACLs and the interfaces that ACLs are applied to.
	Displays the configuration of the interface to which you applied the ACL

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.1*.

Displaying and Clearing MAC ACL Statistics

Use the command to display statistics about a MAC ACL, including the number of packets that have matched each rule.

To display or clear MAC ACL statistics, use one of the following commands:

Command	Purpose
	Displays the MAC ACL configuration. If the MAC ACL includes the command, the command output includes the number of packets that have matched each rule.
	Clears statistics for all MAC ACLs or for a specific MAC ACL.

For detailed information about these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.1*.

Example Configuration 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:

Default Settings

Table 12-1 lists the default settings for MAC ACL parameters.

Table 12-1 Default MAC ACLs Parameters

Parameters	Default
MAC ACLs	No MAC ACLs exist by default
ACL rules	Implicit rules apply to all ACLs (see the "Implicit Rules" section on page 11-6)

Additional References

For additional information related to implementing MAC ACLs, see the following sections:

- Related Documents, page 12-9
- Standards, page 12-9

Related Documents

Related Topic	Document Title
Concepts about ACLs	*Information About ACLs, page 11-1*
MAC ACL commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.1*

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

Table 12-2 lists the release history for this feature.

Table 12-2 Feature History for MAC ACLs

Feature Name	Releases	Feature Information
MAC ACLs	4.1(2)	No change from Release 4.0.