CHAPTER 9

Configuring a MAC ACL

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.

Prerequisites for MAC ACLs

MAC ACLs have the following prerequisites:

- You are familiar with MAC addressing and non-IP protocols to configure MAC ACLs.
- You are familiar with the concepts in the "Information About ACLs" section on page 8-1.

Configuring MAC ACLs

This section includes the following topics:

Creating a MAC ACL

Use this procedure to create a MAC ACL and add rules to it.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

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

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you into CLI Global Configuration mode.

Step 2	**mac access-list** *name*
	
	Example:
	`n1000v(config)# mac access-list acl-mac-01`
	`n1000v(config-mac-acl)#`
		Creates the MAC ACL and enters ACL configuration mode.

	Command	Purpose
Step 3	{**permit** | **deny**} *source destination protocol* **Example:** `n1000v(config-mac-acl)# permit 00c0.4f00.0000 0000.00ff.ffff any`	Creates a rule in the MAC ACL. The **permit** and **deny** commands support many ways of identifying traffic. For more information, see the *Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(1)*.
Step 4	**statistics per-entry** **Example:** `n1000v(config-mac-acl)# statistics per-entry`	(Optional) Specifies that the device maintains global statistics for packets that match the rules in the ACL.
Step 5	**show mac access-lists** *name* **Example:** `n1000v(config-mac-acl)# show mac access-lists acl-mac-01`	(Optional) Displays the MAC ACL configuration.
Step 6	**copy running-config startup-config** **Example:** `n1000v(config-mac-acl)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Changing a MAC ACL

Use this procedure to change an existing MAC ACL such as adding and removing rules.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- In an existing MAC ACL, you cannot change existing rules.
- In an existing MAC ACL, you can add and remove rules.
- Use the **resequence** command to reassign sequence numbers, such as when adding rules between existing sequence numbers.

SUMMARY STEPS

1. **config t**
2. **mac access-list** *name*
3. [*sequence-number*] {**permit | deny**} *source destination protocol*
4. **no** {*sequence-number* | {**permit | deny**} *source destination protocol*}
5. [**no**] **statistics per-entry**
6. **show mac access-lists** *name*
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you into CLI Global Configuration mode.
Step 2	**mac access-list** *name* **Example:** n1000v(config)# mac access-list acl-mac-01 n1000v(config-mac-acl)#	Places you in ACL configuration mode for the ACL that you specify by name.
Step 3	[*sequence-number*] {**permit** | **deny**} *source destination protocol* **Example:** n1000v(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 **permit** and **deny** commands support many ways of identifying traffic. For more information, see the *Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(1)*.
Step 4	**no** {*sequence-number* | {**permit** | **deny**} *source destination protocol*} **Example:** n1000v(config-mac-acl)# no 80	(Optional) Removes the rule that you specify from the MAC ACL. The **permit** and **deny** commands support many ways of identifying traffic. For more information, see the *Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(1)*.
Step 5	[**no**] **statistics per-entry** **Example:** n1000v(config-mac-acl)# statistics per-entry	(Optional) Specifies that the device maintains global statistics for packets that match the rules in the ACL. The **no** option stops the device from maintaining global statistics for the ACL.
Step 6	**show mac access-lists** *name* **Example:** n1000v(config-mac-acl)# show mac access-lists acl-mac-01	(Optional) Displays the MAC ACL configuration.
Step 7	**copy running-config startup-config** **Example:** n1000v(config-mac-acl)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Removing a MAC ACL

Use this procedure to remove a MAC ACL.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- Make sure that you know whether the ACL is applied to an interface.
- You can remove ACLs that are currently applied. Removing an ACL does not affect the configuration of interfaces where you have applied the ACL. Instead, removed ACLs are considered empty.
- To find the interfaces that a MAC ACL is configured on, use the **show mac access-lists** command with the **summary** keyword.

SUMMARY STEPS

1. **config t**
2. **no mac access-list** *name*
3. **show mac access-lists** *name* **summary**
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you into CLI Global Configuration mode.

Step 2	**no mac access-list** *name*
	
	Example:
	`n1000v(config)# no mac access-list acl-mac-01`
	`n1000v(config)#`
		Removes the specified MAC ACL from the running configuration.

Step 3	**show mac access-lists** *name* **summary** **Example:** `n1000v(config)# show mac access-lists acl-mac-01 summary`	(Optional) Displays the MAC ACL configuration. If the ACL remains applied to an interface, the command lists the interfaces.
Step 4	**copy running-config startup-config** **Example:** `n1000v(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Changing Sequence Numbers in a MAC ACL

Use this procedure to change 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 8-2.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

1. **config t**
2. **resequence mac access-list** *name starting-sequence-number increment*
3. **show mac access-lists** *name*
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you into CLI Global Configuration mode.

Step 2	**resequence mac access-list** *name starting-sequence-number increment* **Example:** `n1000v(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.
Step 3	**show mac access-lists** *name* **Example:** `n1000v(config)# show mac access-lists acl-mac-01`	(Optional) Displays the MAC ACL configuration.
Step 4	**copy running-config startup-config** **Example:** `n1000v(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Applying a MAC ACL as a Port ACL

Use this procedure to apply a MAC ACL as a port ACL.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- Make sure that the ACL that you want to apply exists and is configured to filter traffic in the manner that you need for this application. For more information about configuring MAC ACLs, see the "Configuring MAC ACLs" section on page 9-1.

- A MAC ACL can also be applied to a port using a port profile. For more information, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(1)*.

SUMMARY STEPS

1. **config t**
2. **interface vethernet** *port*
3. **mac port access-group** *access-list* [**in** | **out**]
4. **show running-config aclmgr**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you into CLI Global Configuration mode.
Step 2	**interface vethernet** *port* **Example:** n1000v(config)# interface vethernet 35 n1000v(config-if)#	Places you into Interface Configuration mode for the specified interface.
Step 3	**mac port access-group** *access-list* [**in** | **out**] **Example:** n1000v(config-if)# mac port access-group acl-01 in	Applies a MAC ACL to the interface.
Step 4	**show running-config aclmgr** **Example:** n1000v(config-if)# show running-config aclmgr	(Optional) Displays ACL configuration.
Step 5	**copy running-config startup-config** **Example:** n1000v(config-if)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Verifying MAC ACL Configurations

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

Command	Purpose
show mac access-lists	Displays the MAC ACL configuration

Command	Purpose
show running-config aclmgr	Displays the ACL configuration, including MAC ACLs and the interfaces that ACLs are applied to.
show running-config interface	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 NX-OS Security Command Reference*.

Displaying and Clearing MAC ACL Statistics

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

Command	Purpose
show mac access-lists	Displays the MAC ACL configuration. If the MAC ACL includes the **statistics per-entry** command, the **show mac access-lists** command output includes the number of packets that have matched each rule.
clear mac access-list counters	Clears statistics for all MAC ACLs or for a specific MAC ACL.

For detailed information about these commands, see the *Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(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:

```
mac access-list acl-mac-01
  permit 00c0.4f00.0000 0000.00ff.ffff any
interface vethernet 35
mac port access-group acl-mac-01 in
```

Default Settings

Table 9-1 lists the default settings for MAC ACL parameters.

Table 9-1 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 8-3)

Additional References

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

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

Related Documents

Related Topic	Document Title
Concepts about ACLs	*Information About ACLs, page 8-1*

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 ACL

This section provides the MAC ACL release history.

Feature Name	Releases	Feature Information
MAC ACL	4.0	This feature was introduced.