CHAPTER 10

Configuring a MAC ACL

This chapter describes how to configure MAC access control lists (ACLs), and includes the following sections:

- Information About MAC ACLs, page 10-1
- Prerequisites for MAC ACLs, page 10-1\
- Default Settings, page 10-2
- Configuring MAC ACLs, page 10-2
- Verifying MAC ACL Configurations, page 10-9
- Monitoring MAC ACLs, page 10-10
- Example Configurations for MAC ACLs, page 10-11
- Additional References, page 10-11
- Feature History for MAC ACL, page 10-12

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 9-1.

Guidelines and Limitations

MAC ACLs have the following configuration guidelines and limitations:

- In most cases, ACL processing for IP packets are processed on the I/O modules. Management interface traffic is always processed on the supervisor module, which is slower.
- ACLs are not supported in port channels.

Default Settings

Table 10-1 lists MAC ACL defaults.

Table 10-1 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 9-3)

Configuring MAC ACLs

This section includes the following topics:

- Creating a MAC ACL, page 10-2
- Changing a MAC ACL, page 10-3
- Removing a MAC ACL, page 10-5
- Changing Sequence Numbers in a MAC ACL, page 10-6
- Applying a MAC ACL as a Port ACL, page 10-7
- Adding a MAC ACL to a Port Profile, page 10-8

Creating a MAC ACL

Use this procedure to create a MAC ACL and add rules to it. You can also use this procedure to add the ACL to a port profile.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.
- You have a name to assign to the ACL you are creating.
- If you want to also add the ACL to a port-profile, you must know or do the following:
  - If using an existing port profile, you have already created it using the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(4)*; and you know its name.
  - If creating a new port profile, you know the interface type (Ethernet or vEthernet) and the name you want to give the profile.
  - You know the direction of packet flow for the access list.

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.

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 4.2(1)SV1(4)*.
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 for verification.
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, for example, to add or remove 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 4.2(1)SV1(4)*.
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 4.2(1)SV1(4)*.
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.

	Command	Purpose
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.

	Command	Purpose
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 "Changing Sequence Numbers in a MAC ACL" section on page 10-6.

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 10-2.
- A MAC ACL can also be applied to a port using a port profile. For information about port profiles, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(4)*.

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.

Adding a MAC ACL to a Port Profile

You can use this procedure to add a MAC ACL to a port profile:

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.
- You have already created the MAC ACL to add to this port profile using the "Creating a MAC ACL" procedure on page 10-2; and you know its name.
- If using an existing port profile, you have already created it and you know its name.
- If creating a new port profile, you know the interface type (Ethernet or vEthernet) and the name you want to give the profile.
- For more information about port profiles, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(4)*;
- You know the direction of packet flow for the access list.

SUMMARY STEPS

1. **config t**

2. **port-profile** [**type** {**ethernet** | **vethernet**}] *profile-name*
3. **mac port access-group** *name* {**in** | **out**}
4. **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Description

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Enters global configuration mode.

Step 2	**port-profile** [**type** {**ethernet** | **vethernet**}] *name*
	
	Example:
	`n1000v(config)# port-profile AccessProf`
	`n1000v(config-port-prof)#`
		Enters port profile configuration mode for the named port profile.

Step 3	**mac port access-group** *name* {**in** | **out**} **Example:** `n1000v(config-port-prof)# mac port access-group allaccess4 out`	Adds the named ACL to the port profile for either inbound or outbound traffic.
Step 4	**show port-profile name** *profile-name* **Example:** `n1000v(config-port-prof)# show port-profile name AccessProf`	(Optional) Displays the configuration for verification.
Step 5	**copy running-config startup-config** **Example:** `n1000v(config-port-prof)# copy running-config startup-config`	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Verifying MAC ACL Configurations

You can use the following commands to verify the MAC ACL configuration:

Command	Purpose
show mac access-lists	Displays the MAC ACL configuration. See Example 10-1 on page 10-10.
show running-config aclmgr	Displays the ACL configuration, including MAC ACLs and the interfaces they are applied to. See Example 10-2 on page 10-10.
show running-config interface	Displays the configuration of the interface to which you applied the ACL. See Example 10-3 on page 10-10.

Example 10-1 show mac access-list

```
n1000v# show mac access-list

MAC access list acl-mac-01
        10 permit 00c0.4f00.0000 0000.00ff.ffff any
n1000v#
```

Example 10-2 show running-config aclmgr

```
n1000v# show running-config aclmgr

!Command: show running-config aclmgr
!Time: Mon Jan  3 15:53:50 2011

version 4.2(1)SV1(4)
mac access-list acl-mac-01
  10 permit 00c0.4f00.0000 0000.00ff.ffff any

interface Vethernet35
  mac port access-group acl-mac-01 in

n1000v#
```

Example 10-3 show running-config interface

```
n1000v# show running-config interface

!Command: show running-config interface
!Time: Mon Jan  3 15:58:25 2011

version 4.2(1)SV1(4)

interface mgmt0
  ip address 172.23.180.75/24

interface Vethernet35
  mac port access-group acl-mac-01 in

interface Vethernet1998

interface control0
  ip address 10.2.10.10/24

n1000v#
```

Monitoring MAC ACLs

Use the following commands for MAC ACL monitoring.

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.

Example Configurations for MAC ACLs

This example shows how to create MAC ACL acl-mac-01 to permit MAC 00c0.4f00.00.000.00ff.ffff for any protocol, and apply the ACL as a port ACL for outbound traffic on vEthernet interface 35.

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

This example shows how to add the MAC ACL *allaccess4* to the port profile *AccessProf*:

```
config t
port-profile AccessProf
mac port access-group allaccess4 out
show port-profile name AccessProf
port-profile AccessProf
  description: allaccess4
  type: vethernet
  status: disabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: none
  port-group:
  max ports: 32
  inherit:
  config attributes:
    mac port access-group allaccess4 out
  evaluated config attributes:
    mac port access-group allaccess4 out
  assigned interfaces:
```

Additional References

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

- Related Documents, page 10-12
- Standards, page 10-12

Related Documents

Related Topic	Document Title
ACL concepts.	*Information About ACLs, page 9-1*
Configuring interfaces.	*Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(4)*
Configuring port profiles.	*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(4)*
Complete command syntax, command modes, command history, defaults, usage guidelines, and examples for all Cisco Nexus 1000V commands.	*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4)*

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(4)SV1(1)	This feature was introduced.