CHAPTER 13

Configuring VLAN ACLs

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

This chapter includes the following sections:

Information About VLAN ACLs

A VLAN ACL (VACL) is one application of a MAC ACL or IP ACL. You can configure VACLs to apply to all packets that are routed into or out of a VLAN or are bridged within a VLAN. VACLs are strictly for security packet filtering and for redirecting traffic to specific physical interfaces. VACLs are not defined by direction (ingress or egress).

For more information about the types and applications of ACLs, see the "Information About ACLs" section on page 11-1.

This section includes the following topics:

Access Maps and Entries

VACLs use access maps to contain an ordered list of one or more map entries. Each map entry associates IP or MAC ACLs to an action. Each entry has a sequence number, which allows you to control the precedence of entries.

When the device applies a VACL to a packet, it applies the action that is configured in the first access map entry that contains an ACL that permits the packet.

Actions

Each VLAN access map entry can specify one of the following actions:

- Forward—Sends the traffic to the destination determined by normal operation of the switch.
- Redirect—Redirects the traffic to one or more specified interfaces.
- Drop—Drops the traffic. If you specify drop as the action, you can also specify that the device logs the dropped packets.

In access map configuration mode, you use the **action** command to specify the action for a map entry.

Statistics

The device can maintain global statistics for each rule in a VACL. If a VACL is applied to multiple VLANs, the maintained rule statistics are the sum of packet matches (hits) on all the interfaces on which that VACL is applied.

Note The device does not support interface-level VACL statistics.

For each VLAN access map that you configure, you can specify whether the device maintains statistics for that VACL. This feature allows you to turn VACL statistics on or off as needed to monitor traffic filtered by a VACL or to help troubleshoot VLAN access-map configuration.

For information about displaying VACL statistics, see the "Displaying and Clearing VACL Statistics" section on page 13-9.

Session Manager Support

Session Manager supports the configuration of VACLs. This feature allows you to verify ACL configuration and confirm that the resources required by the configuration are available prior to committing them to the running configuration. For more information about Session Manager, see the *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.1*.

Virtualization Support

The following information applies to VACLs used in Virtual Device Contexts (VDCs):

- ACLs are unique per VDC. You cannot use an ACL that you created in one VDC in a different VDC.
- Because ACLs are not shared by VDCs, you can reuse ACL names in different VDCs.

- The device does not limit ACLs or rules on a per-VDC basis.

Licensing Requirements for VACLs

The following table shows the licensing requirements for this feature:

Product	License Requirement
NX-OS	VACLs 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 VACLs

VACLs have the following prerequisites:

- You must be familiar with VLANs to configure VACLs.
- You must be familiar with the concepts in the "Information About ACLs" section on page 11-1.

Guidelines and Limitations

VACLs have the following configuration guidelines and limitations:

- We recommend that you perform ACL configurations using the Session Manager. This feature allows you to verify ACL configuration and confirm that the resources required by the configuration are available prior to committing them to the running configuration. For more information about Session Manager, see the *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.1*.
- ACL statistics are not supported if the DHCP snooping feature is enabled.
- See the "Information About ACLs" section on page 11-1 section for more information about ACLs.

Configuring VACLs

This section includes the following topics:

- Creating a VACL or Adding a VACL Entry, page 13-4
- Changing a VACL Entry, page 13-5
- Removing a VACL or a VACL Entry, page 13-6
- Applying a VACL to a VLAN, page 13-7

Creating a VACL or Adding a VACL Entry

You can create a VACL or add entries to an existing VACL. In both cases, you create a VACL entry, which is a VLAN access-map entry that associates one or more ACLs with an action to be applied to the matching traffic.

BEFORE YOU BEGIN

Ensure that ACLs that you want to use in the VACL exists and is configured to filter traffic in the manner that you need for this application. For more information about configuring IP ACLs, see the "Configuring IP ACLs" section on page 11-1. For more information about configuring MAC ACLs, see the "Configuring MAC ACLs" section on page 12-1.

SUMMARY STEPS

1. **config t**
2. **vlan access-map** *map-name* [*sequence-number*]
3. **match** {**ip** | **ipv6**} **address** *ip-access-list*

   match mac address *mac-access-list*
4. **action** {**drop** | **forward** | **redirect**}
5. **statistics per-entry**
6. **show running-config aclmgr**
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

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

Step 2	**`vlan access-map`** *`map-name`* [*`sequence-number`*]
	
	Example:
	`switch(config)# vlan access-map acl-mac-map`
	`switch(config-access-map)#`
		Enters VLAN access-map configuration mode for the VLAN access map specified. If the VLAN access map does not exist, the device creates it.
		
		If you do not specify a sequence number, the device creates a new entry whose sequence number is 10 greater than the last sequence number in the access map.

Step 3	**`match`** {**`ip`** | **`ipv6`**} **`address`** *`ip-access-list`*
	
	Example:
	`switch(config-access-map)# match ip address acl-ip-lab`
		Specifies an IP ACL for the map.

	`match mac address` *`mac-access-list`*
	
	Example:
	`switch(config-access-map)# match mac address acl-mac-01`
		Specifies a MAC ACL for the map.

	Command	Purpose
Step 4	`action {drop	forward	redirect}` **Example:** `switch(config-access-map)# action forward`	Specifies the action that the device applies to traffic that matches the ACL. The **action** command supports many options. For more information, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.1*.

Step 5	`statistics per-entry`
	Example:
	`switch(config-access-map)# statistics per-entry`
		(Optional) Specifies that the device maintains global statistics for packets that match the rules in the VACL.

Step 6	`show running-config aclmgr`
	Example:
	`switch(config-access-map)# show running-config aclmgr`
		(Optional) Displays the ACL configuration.

Step 7	`copy running-config startup-config`
	Example:
	`switch(config-access-map)# copy running-config startup-config`
		(Optional) Copies the running configuration to the startup configuration.

Changing a VACL Entry

You can add VLAN access-map entries to an existing VACL, you can change VLAN access-map entries, and can configure whether the device maintains statistics for the VACL.

Note You cannot change the sequence number of a VLAN access-map entry. Instead, create a new VLAN access-map entry with the desired sequence number and remove the VLAN access-map entry with the undesired sequence number.

SUMMARY STEPS

1. **config t**
2. **vlan access-map** *map-name* [*sequence-number*]
3. [**no**] **match** {**ip** | **ipv6**} **address** *ip-access-list*

   [**no**] **match mac address** *mac-access-list*
4. **action** {**drop** | **forward** | **redirect**}
5. [**no**] **statistics per-entry**
6. **show running-config aclmgr**
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Enters global configuration mode.
Step 2	**vlan access-map** *map-name* [*sequence-number*] **Example:** switch(config)# vlan access-map acl-mac-map switch(config-access-map)#	Enters access map configuration mode for the access map specified. If you do not specify a sequence number, the device creates a new entry whose sequence number is 10 greater than the last sequence number in the access map.
Step 3	[**no**] **match** {**ip** | **ipv6**} **address** *ip-access-list* **Example:** switch(config-access-map)# no match ip address acl-ip-lab	(Optional) Specifies an IP ACL for the access-map entry. The **no** option removes the IP ACL from the access-map entry.
	[**no**] **match mac address** *mac-access-list* **Example:** switch(config-access-map)# no match mac address acl-mac-01	(Optional) Specifies a MAC ACL for the access-map entry. The **no** option removes the MAC ACL from the access-map entry.
Step 4	**action** {**drop** | **forward** | **redirect**} **Example:** switch(config-access-map)# action forward	(Optional) Specifies the action that the device applies to traffic that matches the ACL. The **action** command supports many options. For more information, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.1*.
Step 5	[**no**] **statistics per-entry** **Example:** switch(config-access-map)# statistics per-entry	(Optional) Specifies that the device maintains global statistics for packets that match the rules in the VACL. The **no** option stops the device from maintaining global statistics for the VACL.
Step 6	**show running-config aclmgr** **Example:** switch(config-access-map)# show running-config aclmgr	(Optional) Displays the ACL configuration.
Step 7	**copy running-config startup-config** **Example:** switch(config-access-map)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Removing a VACL or a VACL Entry

You can remove a VACL, which means that you will delete the VLAN access map.

You can also remove a single VLAN access-map entry from a VACL.

BEFORE YOU BEGIN

Ensure that you know whether the VACL is applied to a VLAN. The device allows you to remove VACLs that are currently applied. Removing a VACL does not affect the configuration of VLANs where you have applied the VACL. Instead, the device considers the removed VACL to be empty.

SUMMARY STEPS

1. **config t**
2. **no vlan access-map** *map-name* [*sequence-number*]
3. **show running-config aclmgr**
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

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

Step 2	`no vlan access-map map-name [sequence-number]`
	Example:
	`switch(config)# no vlan access-map acl-mac-map 10`
		Removes the VLAN access map configuration for the specified access map. If you specify the *sequence-number* argument and the VACL contains more than one entry, the command removes only the entry specified.

Step 3	`show running-config aclmgr`
	Example:
	`switch(config)# show running-config aclmgr`
		(Optional) Displays the ACL configuration.

Step 4	`copy running-config startup-config`
	Example:
	`switch(config)# copy running-config startup-config`
		(Optional) Copies the running configuration to the startup configuration.

Applying a VACL to a VLAN

You can apply a VACL to a VLAN.

BEFORE YOU BEGIN

If you are applying a VACL, ensure that the VACL exists and is configured to filter traffic in the manner that you need for this application. For more information about creating VACLs, see the "Creating a VACL or Adding a VACL Entry" section on page 13-4.

If you are unapplying a VACL, ensure that you are unapplying the correct VACL and that you understand how the VACL is currently applied. For more information about verifying the VACL configuration, see the "Verifying VACL Configuration" section on page 13-8.

SUMMARY STEPS

1. **config t**
2. [**no**] **vlan filter** *map-name* **vlan-list** *list*
3. **show running-config aclmgr**
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

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

Step 2	`[no] vlan filter map-name vlan-list list`
	Example:
	`switch(config)# vlan filter acl-mac-map vlan-list 1-20,26-30`
	`switch(config)#`
		Applies the VACL to the VLANs by the list that you specified. The **no** option unapplies the VACL.

Step 3	**`show running-config aclmgr`**
	Example:
	`switch(config)# show running-config aclmgr`
		(Optional) Displays the ACL configuration.

Step 4	**`copy running-config startup-config`**
	Example:
	`switch(config)# copy running-config startup-config`
		(Optional) Copies the running configuration to the startup configuration.

Verifying VACL Configuration

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

Command	Purpose
show running-config aclmgr	Displays the ACL configuration, including VACL-related configuration.
show vlan filter	Displays information about VACLs that are applied to a VLAN.
show vlan access-map	Displays information about VLAN access maps.

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 VACL Statistics

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

Command	Purpose
show vlan access-list	Displays the VACL configuration. If the VLAN access-map includes the **statistics per-entry** command, then the **show vlan access-list** command output includes the number of packets that have matched each rule.
clear vlan access-list counters	Clears statistics for all VACLs or for a specific VACL.

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

Example Configuration for VACL

The following example shows how to configure a VACL to forward traffic permitted by a MAC ACL named acl-mac-01 and how to apply the VACL to VLANs 50 through 82.

```
conf t
vlan access-map acl-mac-map
  match mac address acl-mac-01
  action forward
vlan filter acl-mac-map vlan-list 50-82
```

Default Settings

Table 13-1 lists the default settings for VACL parameters.

Table 13-1 Default VACL Parameters

Parameters	Default
VACLs	No IP 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 IP ACLs, see the following sections:

- Related Documents, page 13-10
- Standards, page 13-10

Related Documents

Related Topic	Document Title
Concepts about ACLs	*Information About ACLs, page 11-1*
VACL 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 VLAN ACLs

Table 13-2 lists the release history for this feature.

Table 13-2 Feature History for VLAN ACLs

Feature Name	Releases	Feature Information
VLAN access maps	4.1(2)	Support was added for multiple entries in VLAN access maps. In addition, each entry supports multiple **match** commands.