Configuring VLAN ACLs

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

This chapter includes the following sections:

Information About VLAN ACLs

A VLAN ACL (VACL) is one application of an 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).

Note If an IPv4 ACL, applied as a VLAN ACL, contains one or more ACEs with logical operators for TCP/UDP port numbers, the port numbers are matched in the ingress direction but ignored in the egress direction.

VLAN Access Maps and Entries

VACLs use access maps to contain an ordered list of one or more map entries. Each map entry associates IP 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.

VACLs and Actions

In access map configuration mode, you use the **action** command to specify one of the following actions:

Forward

Sends the traffic to the destination determined by the normal operation of the switch.

Drop

Drops the traffic. If you specify drop as the action, you can also specify that the device logs the dropped packets.

VACL 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.

Session Manager Support for VACLs

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.

Licensing Requirements for VACLs

This table shows the licensing requirements for this feature.

Product	License Requirement
Cisco NX-OS	VACLs require no license. However to support up to 128K ACL entries using an XL line card, you must install the scalable services 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, see the *Cisco NX-OS Licensing Guide*.

Prerequisites for VACLs

VACLs have the following prerequisite:

- Ensure that the IP ACL that you want to use in the VACL exists and is configured to filter traffic in the manner that you need for this application.

Guidelines and Limitations for VACLs

VACLs have the following configuration guidelines:

- 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 .
- ACL statistics are not supported if the DHCP snooping feature is enabled.
- The maximum number of supported VACL entries is 64,000 for devices without an XL line card and 128,000 for devices with an XL line card.
- If you try to apply too many ACL entries to a non-XL line card, the configuration is rejected.
- Each forwarding engine on an F1 Series module supports 1000 ingress ACL entries, with 984 entries available for user configuration. The total number of VLAN ACL entries for the F1 Series modules is from 1000 to 16,000, depending on which forwarding engines the policies are applied.
- Each of the 16 forwarding engines in an F1 Series module supports up to 250 IPv6 addresses across multiple ACLs.
- F1 Series modules do not support ACL logging.
- F1 Series modules do not support bank chaining.
- Each VLAN ACL can support up to six different Layer 4 operations for F1 Series modules.
- If the same ACL is applied on multiple VLANs of the same port for F1 Series modules (for example, VLAN 10, 20), it is programmed multiple times (in this case, on VLAN 10 and VLAN 20).

- Each of the 12 forwarding engines in an F2 Series module has 16,000 total TCAM entries, equally split across two banks. 168 default entries are reserved. Each forwarding engine also has 512 IPv6 compression TCAM entries.

Default Settings for VACLs

This table lists the default settings for VACL parameters.

Table 1: Default VACL Parameters

Parameters	Default
VACLs	No IP ACLs exist by default
ACL rules	Implicit rules apply to all ACLs

Configuring VACLs

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 the ACLs that you want to use in the VACL exists and are configured to filter traffic in the manner that you need for this application.

SUMMARY STEPS

1. **configure terminal**
2. **vlan access-map** *map-name* [*sequence-number*]
3. Enter one of the following commands:
   - **match** {**ip** | **ipv6**} **address** *ip-access-list*
   - **match mac address** *mac-access-list*
4. **action** {**drop** | **forward** | **redirect**}
5. (Optional) [**no**] **statistics per-entry**
6. (Optional) **show running-config aclmgr**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`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	Enter one of the following commands:
	• **match** {**ip** | **ipv6**} **address** *ip-access-list*
	• **match mac address** *mac-access-list*
	
	Example:
	`switch(config-access-map)# match mac address acl-ip-lab`
	
	Example:
	`switch(config-access-map)# match mac address acl-mac-01`
		Specifies an ACL for the access-map entry.

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.
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.

Changing a VACL Entry

You change a VACL entry in any of the following ways:

- Add VLAN access-map entries to an existing VACL.
- Change VLAN access-map entries.
- 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. **configure terminal**
2. **vlan access-map** *map-name* [*sequence-number*]
3. (Optional) Enter [**no**] **match** {**ip** | **ipv6**} **address** *ip-access-list*.
4. (Optional) **action** {**drop** | **forward** | **redirect**}
5. (Optional) [**no**] **statistics per-entry**
6. (Optional) **show running-config aclmgr**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`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	Enter [**no**] **match** {**ip**	**ipv6**} **address** *ip-access-list*. **Example:** `switch(config-access-map)# match mac 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.

	Command or Action	Purpose
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*.
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. **configure terminal**
2. **no vlan access-map** *map-name* [*sequence-number*]
3. (Optional) **show running-config aclmgr**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`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.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **vlan filter** *map-name* **vlan-list** *list*
3. (Optional) **show running-config aclmgr**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`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 the VACL Configuration

To display VACL configuration information, perform one of the following tasks.

Command	Purpose
show running-config aclmgr [**all**]	Displays the ACL configuration, including the VACL-related configuration. **Note** Beginning with Cisco NX-OS Release 5.2, this command displays the user-configured ACLs in the running configuration. The **all** option displays both the default (CoPP-configured) and user-configured ACLs in the running configuration.
show startup-config aclmgr [**all**]	Displays the ACL startup configuration. **Note** Beginning with Cisco NX-OS Release 5.2, this command displays the user-configured ACLs in the startup configuration. The **all** option displays both the default (CoPP-configured) and user-configured ACLs in the startup configuration.

Command	Purpose
show vlan filter	Displays information about VACLs that are applied to a VLAN.
show vlan access-map	Displays information about VLAN access maps.

Monitoring and Clearing VACL Statistics

To monitor or clear VACL statistics, use one of the commands in this table. For detailed information about these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

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.