



## Configuring VLAN ACLs

---

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

This chapter includes the following sections:

- [About VLAN ACLs, on page 1](#)
- [Licensing Requirements for VACLs, on page 2](#)
- [Prerequisites for VACLs, on page 2](#)
- [Guidelines and Limitations for VACLs, on page 2](#)
- [Default Settings for VACLs, on page 3](#)
- [Configuring VACLs, on page 3](#)
- [Verifying the VACL Configuration, on page 6](#)
- [Monitoring and Clearing VACL Statistics, on page 7](#)
- [Configuration Example for VACLs, on page 7](#)
- [Additional References for VACLs, on page 7](#)

### About VLAN ACLs

A VLAN ACL (VACL) is one application of an IP ACL or a MAC 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).

### 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 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.

### 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 device.

**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.

## 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.

## Licensing Requirements for VACLs

This table shows the licensing requirements for this feature.

| Product     | License Requirement   |
|-------------|---|
| Cisco NX-OS | VACLs require no license. Any feature not included in a license package is bundled with the image and is provided at no extra charge to you. For an explanation of the Cisco NX-OS licensing scheme, see the <i>Cisco NX-OS Licensing Guide</i> . |

## Prerequisites for VACLs

VACLs have the following prerequisite:

- Ensure that the IP ACL or MAC 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:

- Cisco recommends using the Session Manager to configure ACLs. This feature allows you to verify the 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 3400-S NX-OS System Management Configuration guide*.
- If you try to apply too many ACL entries, the configuration might be rejected.
- VACL redirects to SPAN destination ports are not supported.
- VACL logging is not supported.
- Deny statements are not supported on VACLs. Alternatively, you can use permit statements with the action 'drop' to achieve a similar outcome.
- To clear VACL counters, you must ensure that you have active VLAN filters configured.

## 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 exist and are configured to filter traffic in the manner that you need for this application.

#### Procedure

|               | Command or Action   | Purpose                           |
|---------------|---|-----------------------------------|
| <b>Step 1</b> | <b>configure terminal</b><br><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre> | Enters global configuration mode. |

|               | Command or Action   | Purpose  |
|---------------|---|--|
| <b>Step 2</b> | <b>vlan access-map</b> <i>map-name</i> [ <i>sequence-number</i> ]<br><b>Example:</b><br><pre>switch(config)# vlan access-map acl-mac-map switch(config-access-map)#</pre>   | Enters VLAN access-map configuration mode for the VLAN access map specified. If the VLAN access map does not exist, the device creates it.<br><br>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. |
| <b>Step 3</b> | Enter one of the following commands: <ul style="list-style-type: none"> <li>• <b>match</b> {<b>ip</b>   <b>ipv6</b>} <b>address</b> <i>ip-access-list</i></li> <li>• <b>match mac address</b> <i>mac-access-list</i></li> </ul> <b>Example:</b><br><pre>switch(config-access-map)# match mac address acl-ip-lab</pre> <b>Example:</b><br><pre>switch(config-access-map)# match mac address acl-mac-01</pre> | Specifies an ACL for the access-map entry.   |
| <b>Step 4</b> | <b>action</b> { <b>drop</b>   <b>forward</b>   <b>redirect</b> }<br><b>Example:</b><br><pre>switch(config-access-map)# action forward</pre>   | Specifies the action that the device applies to traffic that matches the ACL.<br><br>The <b>action</b> command supports the <b>drop</b> , <b>forward</b> , and <b>redirect</b> options.  |
| <b>Step 5</b> | (Optional) [ <b>no</b> ] <b>statistics per-entry</b><br><b>Example:</b><br><pre>switch(config-access-map)# statistics per-entry</pre>   | Specifies that the device maintains global statistics for packets that match the rules in the VACL.<br><br>The <b>no</b> option stops the device from maintaining global statistics for the VACL.  |
| <b>Step 6</b> | (Optional) <b>show running-config aclmgr</b><br><b>Example:</b><br><pre>switch(config-access-map)# show running-config aclmgr</pre>   | Displays the ACL configuration.  |
| <b>Step 7</b> | (Optional) <b>copy running-config startup-config</b><br><b>Example:</b><br><pre>switch(config-access-map)# copy running-config startup-config</pre>   | 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.

**Procedure**

|               | Command or Action  | Purpose   |
|---------------|--|---|
| <b>Step 1</b> | <b>configure terminal</b><br><br><b>Example:</b><br>switch# configure terminal<br>switch(config)#  | Enters global configuration mode.   |
| <b>Step 2</b> | <b>no vlan access-map</b> <i>map-name</i><br>[ <i>sequence-number</i> ]<br><br><b>Example:</b><br>switch(config)# no vlan access-map<br>acl-mac-map 10 | Removes the VLAN access map configuration for the specified access map. If you specify the <i>sequence-number</i> argument and the VACL contains more than one entry, the command removes only the entry specified. |
| <b>Step 3</b> | (Optional) <b>show running-config aclmgr</b><br><br><b>Example:</b><br>switch(config)# show running-config<br>aclmgr                                   | Displays the ACL configuration.   |
| <b>Step 4</b> | (Optional) <b>copy running-config startup-config</b><br><br><b>Example:</b><br>switch(config)# copy running-config<br>startup-config                   | 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.

**Procedure**

|               | Command or Action   | Purpose                           |
|---------------|---|-----------------------------------|
| <b>Step 1</b> | <b>configure terminal</b><br><br><b>Example:</b><br>switch# configure terminal<br>switch(config)# | Enters global configuration mode. |

|               | Command or Action  | Purpose  |
|---------------|--|--|
| <b>Step 2</b> | <p>[no] <b>vlan filter</b> <i>map-name</i> <b>vlan-list</b> <i>list</i></p> <p><b>Example:</b></p> <pre>switch(config)# vlan filter acl-mac-map vlan-list 1-20,26-30 switch(config)#</pre> | Applies the VACL to the VLANs by the list that you specified. The <b>no</b> option unapplies the VACL. |
| <b>Step 3</b> | <p>(Optional) <b>show running-config aclmgr</b></p> <p><b>Example:</b></p> <pre>switch(config)# show running-config aclmgr</pre>   | Displays the ACL configuration.  |
| <b>Step 4</b> | <p>(Optional) <b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>switch(config)# copy running-config startup-config</pre>   | 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   |
|--|---|
| <b>show running-config aclmgr</b><br>[all] | <p>Displays the ACL configuration, including the VACL-related configuration.</p> <p><b>Note</b> This command displays the user-configured ACLs in the running configuration. The <b>all</b> option displays both the default (CoPP-configured) and user-configured ACLs in the running configuration.</p> |
| <b>show startup-config aclmgr</b><br>[all] | <p>Displays the ACL startup configuration.</p> <p><b>Note</b> This command displays the user-configured ACLs in the startup configuration. The <b>all</b> option displays both the default (CoPP-configured) and user-configured ACLs in the startup configuration.</p>                                   |
| <b>show vlan filter</b>                    | Displays information about VACLs that are applied to a VLAN.  |
| <b>show vlan access-map</b>                | 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.

| Command                                      | Purpose   |
|--|---|
| <code>show vlan access-list</code>           | Displays the VACL configuration. If the VLAN access-map includes the <b>statistics per-entry</b> command, the <code>show vlan access-list</code> command output includes the number of packets that have matched each rule. |
| <code>clear vlan access-list counters</code> | Clears statistics for VACLs.  |

## Configuration Example for VACLs

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
```

## Additional References for VACLs

### Related Documents

| Related Topic     | Document Title   |
|-------------------|--|
| QoS configuration | <i>Cisco Nexus 3400-S NX-OS Quality of Service Configuration Guide</i> |

