

Configuring VLAN ACLs

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

This chapter includes the following sections:

- VLAN ACLs, on page 1
- Prerequisite requirements for VACLs, on page 2
- Best practices and limitations for VACLs, on page 2
- Default settings for VACLs, on page 3
- Configuring VACLs, on page 4
- VACL configuration verification commands, on page 7
- Commands for monitor and clear VACL statistics, on page 8
- Configuration example for VACLs, on page 8
- Additional references for VACLs, on page 8

VLAN ACLs

A VLAN ACL is a network security rule set that

- applies to all packets that are routed into, out of, or bridged within a VLAN,
- filters or redirects traffic within the VLAN for security purposes, and
- directionless and does not distinguish between ingress and egress.

VLAN access maps and entries

VACLs use access maps to contain an ordered list of map entries. Each map entry associates an IP or MAC ACL with an action. Each entry has a sequence number. The sequence number determines the precedence of entries.

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

Actions in VACLs

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

You can view global statistics for each rule in a VACL. When you apply a VACL to multiple VLANs, the rule statistics show the sum of packet matches (hits) on all interfaces where you applied the VACL.



Note You cannot view VACL statistics at the interface level.

For each VLAN access map you configure, you decide whether to keep statistics for that VACL. Turn VACL statistics on or off to monitor filtered traffic or troubleshoot VLAN access map configuration.

VACLs in session manager

A Session manager VACL is a configuration feature that

- allows you to verify ACL configurations prior to applying them,
- ensures required resources are available before committing changes, and
- helps prevent errors in running configurations.

For more information about Session Manager, see *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide* .

Prerequisite requirements for VACLs

Learn about the prerequisites you need to configure VACLs on your network devices. Make sure the IP access control list (ACL) or MAC ACL you use for a VACL exists. Configure it to filter traffic according to your specified criteria.

Best practices and limitations for VACLs

General guidelines

Follow these configuration guidelines to set up VACLs:

- Use Session Manager to configure access control lists. This feature allows you to verify ACL configuration and check that required resources are available before you commit them to the running configuration. For more information about Session Manager, see the Nexus 9000 Series NX-OS System Management Configuration Guide.

- Apply the necessary number of ACL entries. If you add too many entries, your configuration will be rejected.
- You can redirect VACLs only to supported ports. You cannot use VACL redirects on SPAN destination ports.
- You cannot configure logging with VACLs.
- When you apply a VACL to multiple VLANs, TCAM resources are not shared.
- To drop traffic, use permit statements with the action 'drop' on VACLs; deny statements are not supported.
- When you configure a VACL with the 'redirect' option, define the redirect interface as a member of the VLAN where you apply the VACL. Make sure this VLAN is in the forwarding state on the interface to enable redirection. If the VLAN is not in the forwarding state, packets matched by the VACL will be dropped.
- If a VLAN access-map entry does not include a match statement, the default behavior is to deny (drop) the traffic for that packet type. To allow traffic, you must configure a match statement under an "action forward" entry that specifies the permit ACL.
- Configure active VLAN filters to enable clearing of VACL counters.

Platform and software guidelines

These guidelines apply to the platform and software release:

- To redirect traffic on Nexus 9200 and 9300-EX Series switches, use the VACL redirect option and specify one physical or port-channel interface.
- Avoid configuring VACLs on Nexus 9500 Series switches equipped with the 36-port 40 to 100 Gigabit Ethernet QSFP28 line card (with additional TCAM) or the 36-port 40 Gigabit Ethernet QSFP line card, because these configurations are not supported.
- As of NX-OS Release 10.1(2), you can use VACLs on the 24-port 400 to 100 Gigabit Ethernet QSFP-DD line card 438.91/100 Gigabit Ethernet (438.91 or 100 billion bits per second) and on the Fabric Module for Nexus 9508 R2-Series line cards.
- On Nexus 9332D-GX2B platform switches running NX-OS Release 10.2(1q)F, you can configure VACL, DACL, and CoPP.

VACLs for VXLANs guidelines

These guidelines apply to VACLs for VXLANs:

- The inner payload supports VACLs applied on a VXLAN VLAN in the access to network direction (Layer 2 to Layer 3 encapsulation path).
- Use VACLs on the access side to filter traffic entering the overlay network.
- You cannot use egress VACLs for decapsulated VXLAN traffic.

Default settings for VACLs

This table lists the default settings for VACL parameters.

Table 1: Default VACL parameters

Parameters	Default
VACLs	No IP access control lists (ACLs) exist by default.
ACL rules	Implicit rules apply to all access control lists (ACLs).

Configuring VACLs

Explains configuring VACLs.

Create 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

To use an ACL in the VACL, make sure it already exists and is configured to filter traffic as needed for this application.

Procedure

Step 1 Enter the global configuration mode using the **configure terminal** command.

Example:

```
switch#configure terminal
switch(config)#
```

Step 2 Enter VLAN access-map configuration mode for the specified VLAN access map using the **vlan access-map** *map-name* [*sequence-number*] command.

Example:

```
switch(config)#vlan access-map acl-mac-map
switch(config-access-map)#
```

- 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 Specify an ACL for the access-map entry using 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
```

Step 4 Specify the action that the device applies to traffic that matches the ACL using the **action** {**drop** | **forward** | **redirect**} command.

Example:

```
switch(config-access-map)#action forward
```

Example:

```
switch(config-access-map)#action redirect e1/1
switch(config-access-map)#action redirect po100
```

The **action** command supports the **drop** , **forward** , and **redirect** options.

Step 5 (Optional) Specify that the device maintains global statistics for packets that match the rules in the VACL using the [**no**] **statistics per-entry** command.

Example:

```
switch(config-access-map)#statistics per-entry
```

The **no** option stops the device from maintaining global statistics for the VACL.

Step 6 (Optional) Display the ACL configuration using the **show running-config aclmgr** command.

Example:

```
switch#show running-config aclmgr
```

Step 7 (Optional) Copy the running configuration to the startup configuration using the **copy running-config startup-config** command.

Example:

```
switch#copy running-config startup-config
```

A VACL entry is created or updated. Traffic is filtered, redirected, or forwarded, according to your configuration.

What to do next

- Verify operation by using the appropriate show commands.
- Review device behavior for correct traffic processing.

Remove a VACL or VACL entry

Remove a VLAN access control list (VACL) or an individual entry from a VACL in your network switch configuration.

Perform this task if you need to delete a VACL or a specific VACL entry. You can delete the VLAN access map as part of this process.

To remove a VACL or VACL entry, complete these steps.

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 the VACL was applied. After removal, the device treats the VACL as an empty configuration.

Procedure

Step 1 Enter the global configuration mode using the **configure terminal** command.

Example:

```
switch#configure terminal
switch(config)#
```

Step 2 Delete the VLAN access map configuration for the specified access map using the **no vlan access-map** *map-name* [*sequence-number*] command.

Example:

```
switch(config)#no vlan access-map acl-mac-map 10
```

The command removes only the specified entry if you provide the *sequence-number* argument and the VACL contains more than one entry.

Step 3 (Optional) Display the ACL configuration using the **show running-config aclmgr** command.

Example:

```
switch#show running-config aclmgr
```

Step 4 (Optional) Copy the running configuration to the startup configuration using the **copy running-config startup-config** command.

Example:

```
switch#copy running-config startup-config
```

The specified VACL or VACL entry is removed from the device configuration.

What to do next

Verify that the intended VACL or entry is deleted and that network access policies function as expected.

Apply a VACL to your VLAN

You can apply a VACL to a VLAN.

Before you begin

Before you apply a VACL, make sure that the VACL exists and filters traffic for your application.

Procedure

Step 1 Enter global configuration mode using the **configure terminal** command.

Example:

```
switch#configure terminal
switch(config)#
```

Step 2 Apply the VACL to the specified VLANs using the [**no**] **vlan filter** *map-name* **vlan-list** *list* command.

Example:

```
switch(config)#vlan filter acl-mac-map vlan-list 1-20,26-30
switch(config)#
```

Use the **no** option to not apply the VACL.

Step 3 (Optional) Display the ACL configuration using the **show running-config aclmgr** command.

Example:

```
switch#show running-config aclmgr
```

Step 4 (Optional) Copy the running configuration to the startup configuration using the **copy running-config startup-config** command.

Example:

```
switch#copy running-config startup-config
```

VACL configuration verification commands

Use these commands to verify VACL (VLAN Access Control List) configuration.

Table 2: Commands for VACL configuration verification.

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

Commands for monitor and clear VACL statistics

Use one of these commands to monitor or clear VACL statistics.

Table 3: Commands for monitoring and clearing VACL statistics

Command	Purpose
show vlan access-list	Displays the VACL configuration. If the VLAN access-map includes the **statistics per-entry** command, 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 VACLs.

Configuration example for VACLs

Configure a VACL to forward traffic permitted by a MAC ACL named acl-mac-01 and apply the VACL to VLANs 50 to 82.

```
configure terminal
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

Use this table to find documents about VACL configuration and related topics.

Table 4: Related documents

Related Topic	Document Title
QoS configuration	*Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide*