Configuring VLAN ACLs

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

Note The Cisco NX-OS release that is running on a managed device may not support all the features or settings described in this chapter. For the latest feature information and caveats, see the documentation and release notes for your platform and software release.

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).

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 each VLAN access map entry, you can specify one of the following actions:

Forward	Sends the traffic to the destination determined by the 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.

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.

Virtualization Support for VACLs

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

This table shows the licensing requirements for this feature.

Product	License Requirement
DCNM	VACLs require no license. Any feature not included in a license package is bundled with the Cisco DCNM and is provided at no charge to you. For a complete explanation of the DCNM licensing scheme, see the

Product	License Requirement
	Cisco DCNM Fundamentals Configuration Guide, Release 4.2.
Cisco 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 4.2*.

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

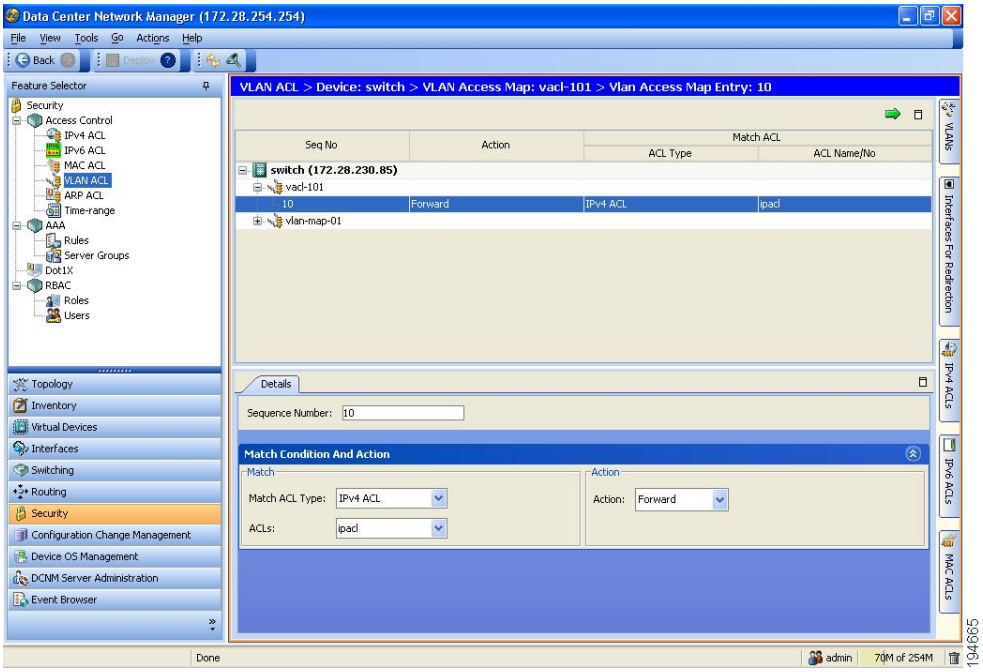
VACLs have the following configuration guideline:

- ACL statistics are not supported if the DHCP snooping feature is enabled.

Configuring VACLs

This figure shows the VLAN ACL content pane.

Figure 1: VLAN ACL Content Pane



Adding a VACL

You can create a VACL. Creating a VACL includes creating at least one VLAN access map entry that associates an IP or MAC ACL with an action to be applied to the matching traffic.

Procedure

Step 1 From the Feature Selector pane, choose **Security ➤ Access Control ➤ VLAN ACL**.
The Summary pane displays available devices.

Step 2 From the Summary pane, double-click the device to which you want to add a VACL.

Step 3 From the menu bar, choose **File ➤ New ➤ VLAN Access Map**.
Below the device that you selected, a new row appears in the Summary pane.

Step 4 In the new row, enter a name for the VACL.
The VACL remains selected in the Summary pane.

Step 5 For each VLAN access map entry that you want to create, follow these steps:

a) From the menu bar, choose **File ➤ New ➤ VLAN Access Map**.
Below the VACL, a new row appears in the Summary pane.

b) From the Details pane, click the **Details** tab and expand the **Match Condition And Action** section, if necessary.

c) From the Match ACL Type drop-down list, select the type of ACL that you want to use in the VACL. You can choose IPv4 ACL, IPv6 ACL, or MAC ACL.

The ACLs drop-down list contains ACLs that are the type you selected and that exist on the currently selected device.

d) From the ACLs drop-down list, select the ACL that you want to use.
e) From the Action drop-down list, select the action that the device should take on traffic matching the VACL.

Step 6 From the menu bar, choose **File ➤ Save** to apply your changes to the device.

Changing a VACL

You can change a VACL.

Procedure

Step 1 From the Feature Selector pane, choose **Security ➤ Access Control ➤ VLAN ACL**.
The Summary pane displays available devices.

Step 2 From the Summary pane, double-click the device that contains the VACL that you want to change and then click the VACL.

Step 3 (Optional) To add a VLAN access map entry, from the menu bar, choose **File ➤ New ➤ VLAN Access Map Entry**.
Below the VACL, the new VLAN access map entry appears in the Summary pane.

Step 4 (Optional) To change a new or existing VLAN access map entry, follow these steps:

a) Click the VLAN access map entry that you want to change.
b) From the Details pane, click the **Details** tab and expand the **Match Condition And Action** section, if necessary.
c) From the Match ACL Type drop-down list, select the type of ACL that you want to use in the VACL. You can choose IPv4 ACL, IPv6 ACL, or MAC ACL.
The ACLs drop-down list contains ACLs that are the type you selected and that exist on the currently selected device.
d) From the ACLs drop-down list, select the ACL that you want to use.
e) From the Action drop-down list, select the action that the device should take upon traffic matching the VACL.

Step 5 (Optional) If you want to move a VLAN access map entry to a different position in the VACL, click the entry in the Summary pane and then from the menu bar, choose one of the following, as applicable:

- **Actions ➤ Move Up**
- **Actions ➤ Move Down**

The entry swaps places and sequence numbers with the entry above it or below it, as you chose.

Step 6 To remove a VLAN access map entry, click the VLAN access map entry and then choose **Actions ➤ Delete**.

Step 7 From the menu bar, choose **File ➤ Deploy** to apply your changes to the device.

Removing a VACL or VLAN Access-Map 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

Step 1 From the Feature Selector pane, choose **Security ➤ Access Control ➤ VLAN ACL**.
Available devices appear in the Summary pane.

Step 2 From the Summary pane, double-click the device from which you want to remove a VACL.
The VACLs on the device appear in the Summary pane.

Step 3 (Optional) If you want to delete a VACL, follow these steps:

a) Click the VACL that you want to remove.

b) From the menu bar, choose **Actions ➤ Delete**.
The VACL disappears from the Summary pane.

Step 4 (Optional) If you want to delete a VLAN access map entry, follow these steps:

a) Double-click the VACL that contains the entry that you want to delete.
The VLAN access-map entries list below the VACL.

b) Click the VLAN access map entry that you want to delete.

c) From the menu bar, choose **Actions ➤ Delete**.
The VLAN access map entry disappears from the Summary pane.

Step 5 (Optional) From the menu bar, choose **File ➤ Deploy** to apply your changes to the device.

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

Step 1 From the Feature Selector pane, choose **Switching ➤ VLAN**.

Available devices appear in the Summary pane.

Step 2 From the Summary pane, double-click the applicable device.
VLANs on the device that you double-clicked appear in the Summary pane.

Step 3 Click the VLAN to which you want to apply a VACL.

Step 4 From the Details pane, click the **VLAN Details** tab and expand the **Advanced Settings** section, if necessary.
The VACL drop-down list appears in the Advanced Settings section.

Step 5 From the VACL drop-down list, choose the VACL that you want to apply.

Step 6 (Optional) From the menu bar, choose **File ➤ Save** to apply your changes to the device.

Field Descriptions for VACLs

VLAN Access Map Entry: Details Tab

Table 1: VLAN Access Map Entry: Details Tab

Field	Description
Sequence Number	*Display only.* Sequence number assigned to the rule.

VLAN Access Map Entry: Details: Match Condition And Action Section

Table 2: VLAN Access Map Entry: Details: Match Condition And Action Section

Field	Description
Match ACL Type	Type of ACL that the VLAN access map entry uses to filter traffic. Valid values are: • IPv4 ACL—This is the default value. • IPv6 ACL • MAC ACL.
ACLs	Name of the ACL that the VLAN access map uses to filter traffic. By default, this list is blank.
Action	Action taken by the device when a packets is permitted by the VLAN access map entry. Valid values are as follows: • Drop—Stop processing the packet and drop it.

Field	Description
	• Forward—Continue processing the packet without modifying the destination. This is the default value. • Redirect—Continue processing the packet but send it to the interfaces that you choose from the Redirect Interfaces drop-down list.
Log this entry	Whether the device logs packets permitted by the VLAN access map entry. This check box appears only when you choose Drop from the Action drop-down list. By default, this check box is unchecked.
Redirect Interfaces	Interfaces to which the device forwards packets permitted by the VLAN access map entry. This check box appears only when you choose Redirect from the Action drop-down list. By default, this list is blank.

Additional References for VACLs

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

This table lists the release history for this feature.

Table 3: Feature History for VLAN ACLs

Feature Name	Releases	Feature Information
VLAN access maps	4.2(1)	No change from Release 4.1.