CHAPTER 9

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 Media Access Control (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 7-1.

This section includes the following topics:

VACLs and Access Maps

VACLs use access maps to link an IP ACL or a MAC ACL to an action. The device takes the configured action on packets permitted by the VACL.

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 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.

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
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 *Cisco DCNM Licensing Guide*.
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 4.0*.

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 7-1.

Guidelines and Limitations

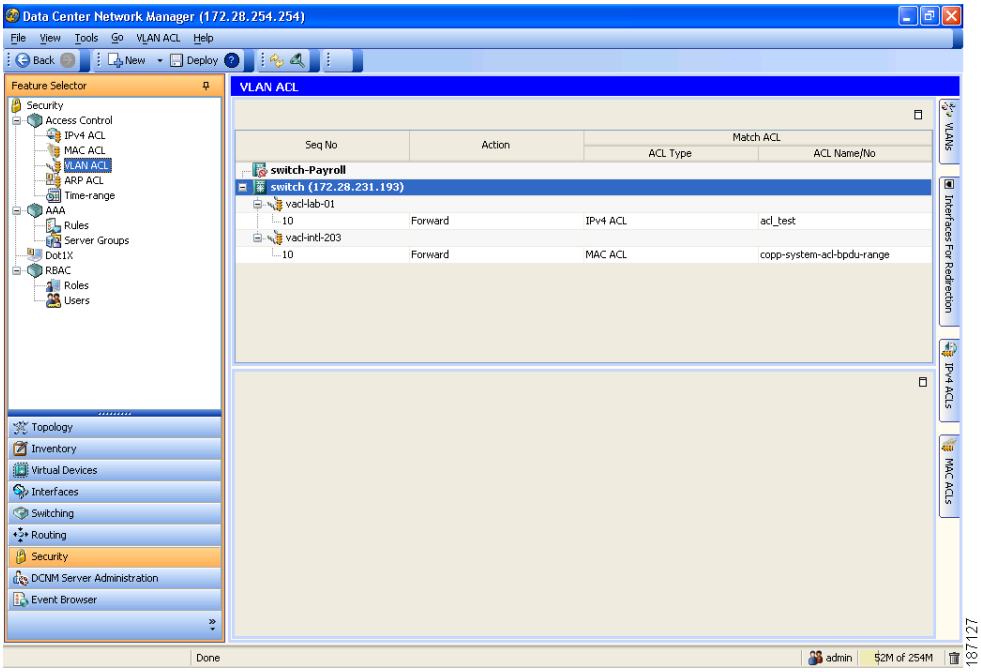
VACLs have the following configuration guidelines and limitations:

- ACL statistics are not supported if the DHCP snooping feature is enabled.
- See the "Information About ACLs" section on page 7-1 section for more information about ACLs.

Configuring VACLs

Figure 9-1 shows the VLAN ACL content pane.

Figure 9-1 VLAN ACL Content Pane



This section includes the following topics:

- Creating or Changing a VACL, page 9-3
- Removing a VACL, page 9-4
- Applying a VACL to a VLAN, page 9-5

Creating or Changing a VACL

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

BEFORE YOU BEGIN

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. For more information about configuring IP ACLs, see the "Configuring IP ACLs" section on page 7-1. For more information about configuring MAC ACLs, see the "Configuring MAC ACLs" section on page 8-1.

DETAILED STEPS

To create or change a VACL, follow these steps:

Step 1 From the Feature Selector pane, choose **Security > Access Control > VLAN ACL**.

The Summary pane displays available devices.

Step 2 To create a VACL, do the following:

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

b. From the menu bar, choose **File > New > VLAN Access Map**.

Below the device that you selected, a new row appears in the Summary pane.

c. In the new row, enter a name for the VACL.

The VACL remains selected in the Summary pane.

d. From the menu bar, choose **File > New > VLAN Access Map Entry**.

Below the VACL, a new row appears in the Summary pane.

e. On the Details tab, in the Name field, type a name for the VACL.

Step 3 To change a VACL, from the Summary pane, double-click the device that contains the VACL and then click the VACL.

Step 4 From the Details pane, click the **Details** tab and expand the **Match Condition And Action** section, if necessary.

Step 5 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 or MAC ACL.

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

Step 6 From the ACLs drop-down list, select the ACL that you want to use.

Step 7 From the Action drop-down list, select the action that the device should take upon traffic matching the VACL.

Step 8 From the menu bar, choose **File > Save** to apply your changes to the device.

Removing a VACL

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

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.

DETAILED STEPS

To remove a VACL, follow these steps:

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 Click the VACL that you want to remove, and then from the menu bar, choose **VLAN ACL > Delete**.

The VACL disappears from the Summary pane.

Step 4 From the menu bar, choose **File > Save** 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. For more information about creating VACLs, see the "Creating or Changing a VACL" section on page 9-3.

If you are unapplying a VACL, ensure that you are unapplying the correct VACL and that you understand how the VACL is currently applied.

DETAILED STEPS

To apply a VACL to a VLAN, follow these steps:

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 From the menu bar, choose **File > Save** to apply your changes to the device.

Field Descriptions for VACLs

This section includes the following topics:

VLAN Access Map Entry: Details Tab

Table 9-1 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 9-2 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 • 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. • 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 additional information related to implementing IP ACLs, see the following sections:

Related Documents

Related Topic	Document Title
Concepts about ACLs	*Information About ACLs, page 7-1*

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.	—