CHAPTER 45

VLAN ACLs (VACLs)

Note

- For complete syntax and usage information for the commands used in this chapter, see these publications:

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html

- Cisco IOS Release 15.1SY supports only Ethernet interfaces. Cisco IOS Release 15.1SY does not support any WAN features or commands.
- Optimized ACL logging (OAL) and VACL capture are incompatible. Do not configure both features on the switch. With OAL configured (see the "Optimized ACL Logging" section on page 40-13), use SPAN to capture traffic.
- Also see the "PACL Interaction with VACLs and Cisco IOS ACLs" section on page 44-5.

Tip

For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

Participate in the Technical Documentation Ideas forum

Prerequisites for VACLs

None.

Restrictions for VACLs

- VACLs use standard and extended Cisco IOS IP and MAC layer-named ACLs (see "MAC ACLs" section on page 40-9) and VLAN access maps.
- IGMP packets are not checked against VACLs.
- VLAN access maps can be applied to VLANs for VACL capture.
- Each VLAN access map can consist of one or more map sequences; each sequence has a match clause and an action clause. The match clause specifies IP or MAC ACLs for traffic filtering and the action clause specifies the action to be taken when a match occurs. When a flow matches a permit ACL entry, the associated action is taken and the flow is not checked against the remaining sequences. When a flow matches a deny ACL entry, it will be checked against the next ACL in the same sequence or the next sequence. If a flow does not match any ACL entry and at least one ACL is configured for that packet type, the packet is denied.
- To apply access control to both bridged and routed traffic, you can use VACLs alone or a combination of VACLs and ACLs. You can define ACLs on the VLAN interfaces to apply access control to both the ingress and egress routed traffic. You can define a VACL to apply access control to the bridged traffic.
- The following caveats apply to ACLs when used with VACLs:
  - Packets that require logging on the outbound ACLs are not logged if they are denied by a VACL.
  - VACLs are applied on packets before NAT translation. If the translated flow is not subject to access control, the flow might be subject to access control after the translation because of the VACL configuration.
- VACLs check for conflicts with other features using capture like OAL, Lawful Intercept (LI), and IPv6 learning.
- When VACL capture is configured with Policy Based Routing (PBR) on the same interface, do not select BDD as the ACL merge algorithm.
- When VACL capture is configured on an egress interface together with another egress feature that requires software processing of the traffic, packets of the overlapping traffic may be captured twice.
- The action clause in a VACL can be forward, drop, capture, or redirect. Traffic can also be logged.

Note

- VACLs have an implicit deny at the end of the map; a packet is denied if it does not match any ACL entry, and at least one ACL is configured for the packet type.
- If an empty or undefined ACL is specified in a VACL, any packets will match the ACL, and the associated action is taken.

Information About VACLs

VLAN ACLs (VACLs) can provide access control for all packets that are bridged within a VLAN or that are routed into or out of a VLAN for VACL capture. Unlike Cisco IOS ACLs that are applied on routed packets only, VACLs apply to all packets and can be applied to any VLAN. VACLs are processed in the ACL TCAM hardware. VACLs ignore any Cisco IOS ACL fields that are not supported in hardware.

You can configure VACLs for IP and MAC-layer traffic.

If a VACL is configured for a packet type, and a packet of that type does not match the VACL, the default action is to deny the packet.

Packets can either enter the VLAN through a Layer 2 port or through a Layer 3 port after being routed. You can also use VACLs to filter traffic between devices in the same VLAN.

How to Configure VACLs

Defining a VLAN Access Map

To define a VLAN access map, perform this task:

Command	Purpose
`Router(config)# vlan access-map map_name [0-65535]`	Defines the VLAN access map. Optionally, you can specify the VLAN access map sequence number.

- To insert or modify an entry, specify the map sequence number.
- If you do not specify the map sequence number, a number is automatically assigned.
- You can specify only one match clause and one action clause per map sequence.
- Use the **no** keyword with a sequence number to remove a map sequence.
- Use the **no** keyword without a sequence number to remove the map.

See the "VLAN Access Map Configuration and Verification Examples" section on page 45-5.

Configuring a Match Clause in a VLAN Access Map Sequence

To configure a match clause in a VLAN access map sequence, perform this task:

Command	Purpose
`Router(config-access-map)# match {[ip | ipv6] address {1-199 | 1300-2699 | acl_name} | {mac address acl_name}}`	Configures the match clause in a VLAN access map sequence.

- Release 15.0(1)SY1 and later releases support IPv6 ACLs.
- You can select one or more ACLs.
- Use the **no** keyword to remove a match clause or specified ACLs in the clause.
- For information about named MAC-Layer ACLs, see "MAC ACLs" section on page 40-9.
- For information about Cisco IOS ACLs, see Chapter 40, "Cisco IOS ACL Support" and the "VLAN Access Map Configuration and Verification Examples" section on page 45-5.

Configuring an Action Clause in a VLAN Access Map Sequence

To configure an action clause in a VLAN access map sequence, perform this task:

Command	Purpose
Router(config-access-map)# **action** {**drop** [**log**]} | {**forward** [**capture** | **vlan** *vlan_ID*]} | {**redirect** {{**fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port*} | {**port-channel** *channel_id*}}	Configures the action clause in a VLAN access map sequence.

- You can set the action to drop, forward, forward capture, or redirect packets.
- Forwarded packets are still subject to any configured Cisco IOS security ACLs.
- The **capture** action sets the capture bit for the forwarded packets so that ports with the capture function enabled can receive the packets. Only forwarded packets can be captured. For more information about the **capture** action, see the "Configuring a Capture Port" section on page 45-6.
- The **forward vlan** action implements Policy-Based Forwarding (PBF), bridging between VLANs.
- When the **log** action is specified, dropped packets are logged in software. Only dropped IP packets can be logged.
- The **redirect** action allows you to specify up to five interfaces, which can be physical interfaces or EtherChannels. You cannot specify packets to be redirected to an EtherChannel member or a VLAN.
- The redirect interface must be in the VLAN for which the VACL access map is configured.
- If a VACL is redirecting traffic to an egress SPAN source port, SPAN does not copy the VACL-redirected traffic.
- SPAN and RSPAN destination ports transmit VACL-redirected traffic.
- Use the **no** keyword to remove an action clause or specified redirect interfaces.

See the "VLAN Access Map Configuration and Verification Examples" section on page 45-5.

Applying a VLAN Access Map

To apply a VLAN access map, perform this task:

Command	Purpose
Router(config)# **vlan filter** *map_name* **vlan-list**	Applies the VLAN access map to the specified VLANs.

- You can apply the VLAN access map to one or more VLANs.
- The *vlan_list* parameter can be a single VLAN ID or a comma-separated list of VLAN IDs or VLAN ID ranges (*vlan_ID*–*vlan_ID*).
- You can apply only one VLAN access map to each VLAN.
- VACLs applied to VLANs are active only for VLANs with a Layer 3 VLAN interface configured. Applying a VLAN access map to a VLAN without a Layer 3 VLAN interface creates an administratively down Layer 3 VLAN interface to support the VLAN access map.
- VACLs applied to VLANs are inactive if the Layer 2 VLAN does not exist or is not operational.
- You cannot apply a VACL to a secondary private VLAN. VACLs applied to primary private VLANs also apply to secondary private VLANs.
- Use the **no** keyword to clear VLAN access maps from VLANs.

See the "VLAN Access Map Configuration and Verification Examples" section on page 45-5.

Verifying VLAN Access Map Configuration

To verify VLAN access map configuration, perform this task:

Command	Purpose
`Router# show vlan access-map [map_name]`	Verifies VLAN access map configuration by displaying the content of a VLAN access map.
`Router# show vlan filter [access-map map_name | vlan vlan_id]`	Verifies VLAN access map configuration by displaying the mappings between VACLs and VLANs.

VLAN Access Map Configuration and Verification Examples

Assume IP-named ACL **net_10** and **any_host** are defined as follows:

```
Router# show ip access-lists net_10
Extended IP access list net_10
    permit ip 10.0.0.0 0.255.255.255 any

Router# show ip access-lists any_host
Standard IP access list any_host
    permit any
```

This example shows how to define and apply a VLAN access map to forward IP packets. In this example, IP traffic matching net_10 is forwarded and all other IP packets are dropped due to the default drop action. The map is applied to VLAN 12 to 16.

```
Router(config)# vlan access-map thor 10
Router(config-access-map)# match ip address net_10
Router(config-access-map)# action forward
Router(config-access-map)# exit
Router(config)# vlan filter thor vlan-list 12-16
```

This example shows how to define and apply a VLAN access map to drop and log IP packets. In this example, IP traffic matching net_10 is dropped and logged and all other IP packets are forwarded:

```
Router(config)# vlan access-map ganymede 10
Router(config-access-map)# match ip address net_10
Router(config-access-map)# action drop log
Router(config-access-map)# exit
Router(config)# vlan access-map ganymede 20
Router(config-access-map)# match ip address any_host
Router(config-access-map)# action forward
Router(config-access-map)# exit
Router(config)# vlan filter ganymede vlan-list 7-9
```

This example shows how to define and apply a VLAN access map to forward and capture IP packets. In this example, IP traffic matching net_10 is forwarded and captured and all other IP packets are dropped:

```
Router(config)# vlan access-map mordred 10
Router(config-access-map)# match ip address net_10
Router(config-access-map)# action forward capture
Router(config-access-map)# exit
Router(config)# vlan filter mordred vlan-list 2, 4-6
```

Configuring a Capture Port

Note

- A port configured to capture VACL-filtered traffic is called a capture port.
- To apply IEEE 802.1Q tags to the captured traffic, configure the capture port to trunk unconditionally (see the “Configuring the Layer 2 Trunk to Use DTP” section on page 11-8 and the “Configuring the Layer 2 Trunk Not to Use DTP” section on page 11-9).

To configure a capture port, perform this task:

	Command	Purpose
Step 1	`Router(config)# `**`interface`**` {{`*`type slot/port`*`}`	Specifies the interface to configure.
Step 2	`Router(config-if)# `**`switchport capture allowed vlan`**` {`**`add`**` | `**`all`**` | `**`except`**` | `**`remove`**`} `*`vlan_list`*	(Optional) Filters the captured traffic on a per-destination-VLAN basis. The default is **all**.
Step 3	`Router(config-if)# `**`switchport capture`**	Configures the port to capture VACL-filtered traffic.

- You can configure any port as a capture port.
- The *vlan_list* parameter can be a single VLAN ID or a comma-separated list of VLAN IDs or VLAN ID ranges (*vlan_ID*–*vlan_ID*).
- To encapsulate captured traffic, configure the capture port with the **switchport trunk encapsulation** command (see the “Configuring a Layer 2 Switching Port as a Trunk” section on page 11-8) before you enter the **switchport capture** command.
- For unencapsulated captured traffic, configure the capture port with the **switchport mode access** command (see the “Configuring a LAN Interface as a Layer 2 Access Port” section on page 11-13) before you enter the **switchport capture** command.
- The capture port supports only egress traffic. No traffic can enter the switch through a capture port.

This example shows how to configure a Gigabit Ethernet interface 5/1 as a capture port:

```
Router(config)# interface gigabitEthernet 5/1
Router(config-if)# switchport capture
Router(config-if)# end
```

This example shows how to display VLAN access map information:

```
Router# show vlan access-map mymap
Vlan access-map "mymap"  10
        match: ip address net_10
        action: forward capture
Router#
```

This example shows how to display mappings between VACLs and VLANs. For each VACL map, there is information about the VLANs that the map is configured on and the VLANs that the map is active on. A VACL is not active if the VLAN does not have an interface.

```
Router# show vlan filter
VLAN Map mordred:
        Configured on VLANs:  2,4-6
            Active on VLANs:  2,4-6
Router#
```

Configuring VACL Logging

When you configure VACL logging, IP packets that are denied generate log messages in these situations:

- When the first matching packet is received
- For any matching packets received during the last 5-minute interval
- If the threshold is reached before the 5-minute interval

Log messages are generated on a per-flow basis. A flow is defined as packets with the same IP addresses and Layer 4 (UDP or TCP) port numbers. When a log message is generated, the timer and packet count is reset.

These restrictions apply to VACL logging:

- Because of the rate-limiting function for redirected packets, VACL logging counters may not be accurate.
- Only denied IP packets are logged.

To configure VACL logging, use the **action drop log** command action in VLAN access map submode (see the “Configuring an Action Clause in a VLAN Access Map Sequence” section on page 45-4) and perform this task in global configuration mode to specify the global VACL logging parameters:

	Command	Purpose
Step 1	`Router(config)#` **`vlan access-log maxflow`** *`max_number`*	Sets the log table size. The content of the log table can be deleted by setting the maxflow number to 0. The default is 500 with a valid range of 0 to 2048. When the log table is full, logged packets from new flows are dropped by the software.
Step 2	`Router(config)#` **`vlan access-log ratelimit`** *`pps`*	Sets the maximum redirect VACL logging packet rate. The default packet rate is 2000 packets per second with a valid range of 0 to 5000. Packets exceeding the limit are dropped by the hardware.
Step 3	`Router(config)#` **`vlan access-log threshold`** *`pkt_count`*	Sets the logging threshold. A logging message is generated if the threshold for a flow is reached before the 5-minute interval. By default, no threshold is set.
Step 4	`Router(config)#` **`exit`**	Exits VLAN access map configuration mode.

This example shows how to configure global VACL logging in hardware:

```
Router(config)# vlan access-log maxflow 800
Router(config)# vlan access-log ratelimit 2200
Router(config)# vlan access-log threshold 4000
```

Displays the configured VACL logging properties.

```
Router# show vlan access-log config
```

Displays the content of the VACL log table.

```
Router# show vlan access-log flow protocol {{src_addr src_mask} | any | {host {hostname |
host_ip}}} {{dst_addr dst_mask} | any | {host {hostname | host_ip}}}
[vlan vlan_id]
```

Displays packet and message counts and other statistics.

```
Router# show vlan access-log statistics
```

Tip For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

Participate in the Technical Documentation Ideas forum