Configuring Port ACLs and VLAN ACLs

This chapter describes how to configure port ACLs (PACLs) and VLAN ACLs (VACLs) in Cisco IOS Release 12.2SX.

Note

- For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS Master Command List, at this URL:

  http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html
- 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 49-8), use SPAN to capture traffic.
- Port ACLs do not support the access-list keywords **log** or **reflexive**. These keywords in the access list are ignored. OAL does not support PACLs.
- PACLs are not supported on private VLANs.

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

This chapter consists of these sections:

Understanding ACLs

The following sections describe ACLs in Cisco IOS Release 12.2SX:

Understanding ACLs

Access control lists (ACLs) provide the ability to filter ingress and egress traffic based on conditions specified in the ACL.

Cisco IOS Release 12.2SX supports the following types of ACLs:

- Cisco IOS ACLs are applied to Layer 3 interfaces. They filter traffic routed between VLANs. For more information about Cisco IOS ACLs, see Chapter 49, "Understanding Cisco IOS ACL Support."
- VACLs control access to the VLAN of all packets (bridged and routed). 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.
- Port ACLs perform access control on all traffic entering the specified Layer 2 port.

PACLs and VACLs can provide access control based on the Layer 3 addresses (for IP protocols) or Layer 2 MAC addresses (for non-IP protocols).

You can apply only one IP access list and one MAC access list to a Layer 2 interface.

Understanding 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 or a WAN interface 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 or WAN interface. 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. VACLs applied to WAN interfaces support only IP traffic for VACL capture.

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.

Note IGMP packets are not checked against VACLs.

MAC Policy-Based Forwarding

Cisco IOS Release 12.2(33)SXI and later releases support MAC Policy-Based Forwarding (PBF), a type of MAC-based VACL by which packets can be bridged between VLANs. MAC PBF forwards packets based solely on the source and destination MAC addresses, ignoring any information above Layer 2. Unlike other VACLs, which are processed in the ACL TCAM hardware, MAC PBF is performed in software, with optional rate limiters to control CPU usage. Also, PBF is applied only to incoming packets.

Note Layer 2 port ACLs (PACLs) take precedence over MAC PBF.

Understanding Port ACLs

The port ACL (PACL) feature provides the ability to perform access control on specific Layer 2 ports. A Layer 2 port is a physical LAN or trunk port that belongs to a VLAN. Port ACLs are applied only on the ingress traffic. The port ACL feature is supported only in hardware (port ACLs are not applied to any packets routed in software).

When you create a port ACL, an entry is created in the ACL TCAM. You can use the **show tcam counts** command to see how much TCAM space is available.

The PACL feature does not affect Layer 2 control packets received on the port.

You can use the **access-group mode** command to change the way that PACLs interact with other ACLs.

PACLs use the following modes:

- Prefer port mode—If a PACL is configured on a Layer 2 interface, the PACL takes effect and overwrites the effect of other ACLs (Cisco IOS ACL and VACL). If no PACL feature is configured on the Layer 2 interface, other features applicable to the interface are merged and are applied on the interface.
- Merge mode—In this mode, the PACL, VACL, and Cisco IOS ACLs are merged in the ingress direction following the logical serial model shown in Figure 51-2. This is the default access group mode.

You configure the **access-group mode** command on each interface. The default is merge mode.

Note If we set access-group mode prefer port, it will not only overwrite the effect of other ACLs, but also other features like Netflow (applied to SVI interface) will be affected.

Note A PACL can be configured on a trunk port only after prefer port mode has been selected. Trunk ports do not support merge mode.

To illustrate access group mode, assume a physical port belongs to VLAN100, and the following ACLs are configured:

- Cisco IOS ACL R1 is applied on routed interface VLAN100.
- VACL (VLAN filter) V1 is applied on VLAN100.
- PACL P1 is applied on the physical port.

In this situation, the following ACL interactions occur:

- In prefer port mode, Cisco IOS ACL R1 and VACL V1 are ignored.

- In merge mode, Cisco IOS ACL R1, VACL V1 and PACL P1 are merged and applied on the port.

Note The CLI syntax for creating a PACL is identical to the syntax for creating a Cisco IOS ACL. An instance of an ACL that is mapped to a Layer 2 port is called a PACL. An instance of an ACL that is mapped to a Layer 3 interface is called a Cisco IOS ACL. The same ACL can be mapped to both a Layer 2 port and a Layer 3 interface.

The PACL feature supports MAC ACLs and IPv4 ACLs. The PACL feature does not support ACLs for IPV6, ARP, or Multiprotocol Label Switching (MPLS) traffic.

PACLs are explained in more detail in the following sections:

- EtherChannel and PACL Interactions, page 51-4
- Dynamic ACLs (Applies to Merge Mode Only), page 51-4
- Trunk Ports, page 51-4
- Layer 2 to Layer 3 Port Conversion, page 51-4
- Port-VLAN Association Changes, page 51-5

EtherChannel and PACL Interactions

This section describes the guidelines for the EtherChannel and PACL interactions:

- PACLs are supported on the main Layer 2 channel interface but not on the port members. A port that has a PACL configured on it may not be configured as an EtherChannel member port. The EtherChannel configuration commands are unavailable on ports that are configured with a PACL.
- Changing the configuration on the logical port affects all the ports in the channel. When an ACL is mapped to the logical port belonging to a channel, it is mapped to all ports in the channel.

Dynamic ACLs (Applies to Merge Mode Only)

Dynamic ACLs are VLAN-based and are used by GWIP. The merge mode *does not* support the merging of the dynamic ACLs with the PACLs. In merge mode, the following configurations are not allowed:

- Attempting to apply a PACL on a port where its corresponding VLAN has a dynamic ACL mapped. In this case, the PACL is not applied to traffic on the port.
- Configuring a dynamic ACL on a VLAN where one of its constituent ports has a PACL installed. In this case, the dynamic ACL is not applied.

Trunk Ports

To configure a PACL on a trunk port, you must first configure port prefer mode. The configuration commands to apply a PACL on a trunk or dynamic port will not be available until you configure the port in port prefer mode by entering the **access-group mode prefer port** interface command. Trunk ports do not support merge mode.

Layer 2 to Layer 3 Port Conversion

If you reconfigure a port from Layer 2 to Layer 3, any PACL configured on the port becomes inactive but remains in the configuration. If you subsequently configure the port as Layer 2, any PACL configured on the port becomes active again.

Port-VLAN Association Changes

You can enter port configuration commands that alter the port-VLAN association, which triggers an ACL remerge.

Unmapping and then mapping a PACL, VACL, or Cisco IOS ACL automatically triggers a remerge.

In merge mode, online insertion or removal of a switching module also triggers a remerge, if ports on the module have PACLs configured.

PACL and VACL Interactions

The following sections describe interactions between the different types of ACL:

- PACL Interaction with VACLs and Cisco IOS ACLs, page 51-5
- Bridged Packets, page 51-5
- Routed Packets, page 51-6
- Multicast Packets, page 51-7

PACL Interaction with VACLs and Cisco IOS ACLs

This section describes the guidelines for the PACL interaction with the VACLs and Cisco IOS ACLs.

For an incoming packet on a physical port, the PACL is applied first. If the packet is permitted by the PACL, the VACL on the ingress VLAN is applied next. If the packet is Layer 3 forwarded and is permitted by the VACL, it is filtered by the Cisco IOS ACL on the same VLAN. The same process happens in reverse in the egress direction. However, there is currently no hardware support for output PACLs.

The PACLs override both the VACLs and Cisco IOS ACLs when the port is configured in prefer port mode. The one exception to this rule is when the packets are forwarded in the software by the route processor (RP). The RP applies the ingress Cisco IOS ACL regardless of the PACL mode. Two examples where the packets are forwarded in the software are as follows:

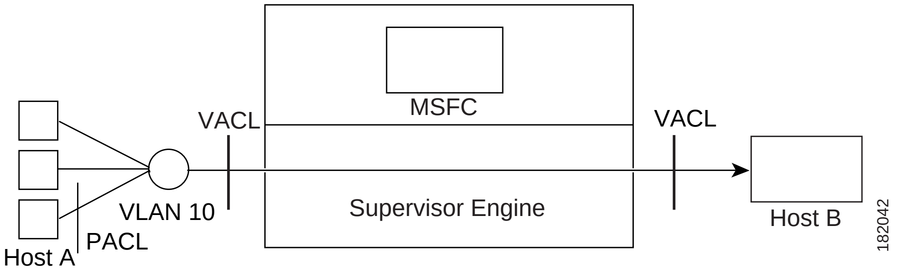
- Packets that are egress bridged (due to logging or features such as NAT)
- Packets with IP options

Bridged Packets

Figure 51-1 shows a PACL and a VACL applied to bridged packets. In merge mode, the ACLs are applied in the following order:

1. PACL for the ingress port
2. VACL for the ingress VLAN
3. VACL for the egress VLAN

Figure 51-1 Applying ACLs on Bridged Packets



In prefer port mode, only the PACL is applied to the ingress packets (the input VACL is not applied).

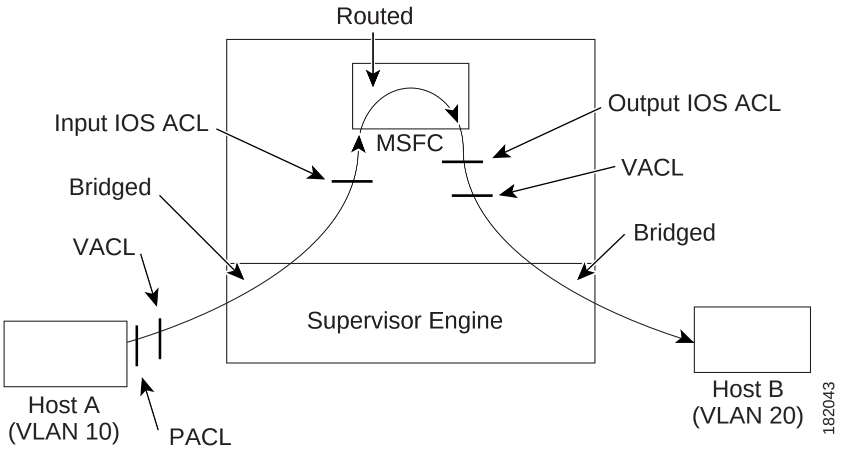
Routed Packets

Figure 51-2 shows how ACLs are applied on routed and Layer 3-switched packets. In merge mode, the ACLs are applied in the following order:

1. PACL for the ingress port
2. VACL for the ingress VLAN
3. Input Cisco IOS ACL
4. Output Cisco IOS ACL
5. VACL for the egress VLAN

In prefer port mode, only the PACL is applied to the ingress packets (the input VACL and Cisco IOS ACL are not applied).

Figure 51-2 Applying ACLs on Routed Packets



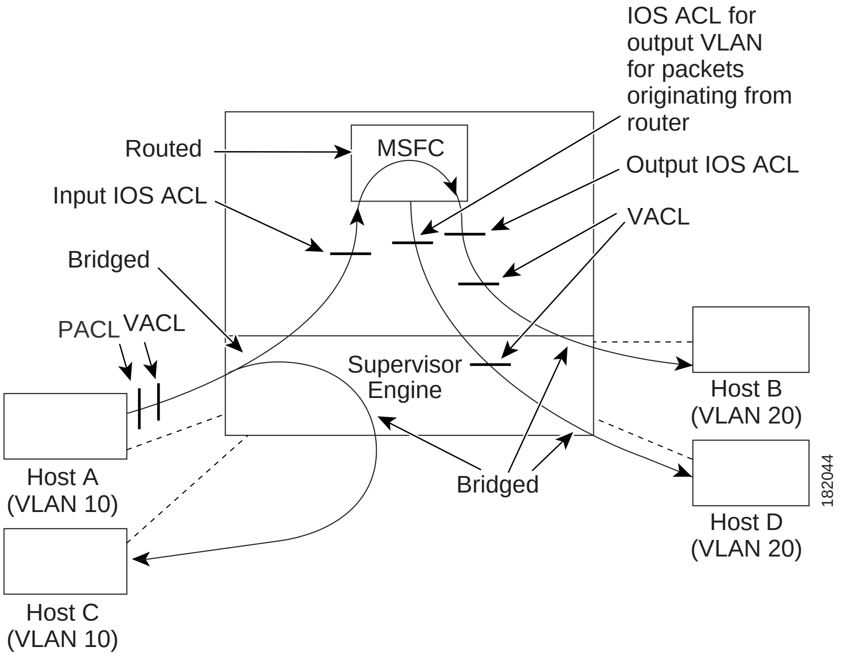
Multicast Packets

Figure 51-3 shows how ACLs are applied on packets that need multicast expansion. For packets that need multicast expansion, the ACLs are applied in the following order:

1. Packets that need multicast expansion:
   a. PACL for the ingress port
   b. VACL for the ingress VLAN
   c. Input Cisco IOS ACL
2. Packets after multicast expansion:
   a. Output Cisco IOS ACL
   b. VACL for the egress VLAN
3. Packets originating from router:
   a. Output Cisco IOS ACL
   b. VACL for the egress VLAN

In prefer port mode, only the PACL is applied to the ingress packets (the input VACL and Cisco IOS ACL are not applied).

Figure 51-3 Applying ACLs on Multicast Packets



Configuring PACLs

Cisco IOS Release 12.2(33)SXH and later releases support PACLs. This section describes how to configure PACLs. PACLs filter incoming traffic on Layer 2 interfaces, using Layer 3 information, Layer 4 header information, or non-IP Layer 2 information.

The PACL feature uses existing Cisco IOS **access-list** commands to create the standard or extended IP ACLs or named MAC-extended ACLs that you want to apply to the port.

Use the **ip access-group** or **mac access-group interface** command to apply an IP ACL or MAC ACL to one or more Layer 2 interfaces.

Note PACLs cannot filter Physical Link Protocols and Logical Link Protocols, such as CDP, VTP, DTP, PAgP, UDLD, and STP, because the protocols are redirected to the switch processor (SP) before the ACL takes effect.

This section contains the following topics:

- PACL Configuration Guidelines, page 51-8
- Configuring IP and MAC ACLs on a Layer 2 Interface, page 51-9
- Configuring Access-group Mode on Layer 2 Interface, page 51-9
- Applying ACLs to a Layer 2 Interface, page 51-10
- Applying ACLs to a Port Channel, page 51-10
- Displaying an ACL Configuration on a Layer 2 Interface, page 51-10

PACL Configuration Guidelines

Consider the following guidelines when configuring PACLs:

- There can be at most one IP access list and one MAC access list applied to the same Layer 2 interface per direction.
- PACLs are not applied to IPv6, MPLS, or ARP messages.
- An IP access list filters only IPv4 packets, For IP access lists, you can define a standard, extended, or named access-list.
- A MAC access list filters ingress packets that are of an unsupported type (not IP, IPv6, ARP, or MPLS packets) based on the fields of the Ethernet datagram. A MAC access list is not applied to IP, IPv6, MPLS, or ARP messages. You can define only named MAC access lists.
- The number of ACLs and ACEs that can be configured as part of a PACL are bounded by the hardware resources on the switch. Those hardware resources are shared by various ACL features (such as VACLs) that are configured on the system. If there are insufficient hardware resources to program a PACL in hardware, the PACL is not applied.
- PACL does not support the access-list **log** and **reflect/evaluate** keywords. These keywords are ignored if you add them to the access list for a PACL.
- OAL does not support PACLs.
- The access group mode can change the way PACLs interact with other ACLs. To maintain consistent behavior across Cisco platforms, use the default access group mode (merge mode).

Configuring IP and MAC ACLs on a Layer 2 Interface

IP and MAC ACLs can be applied to Layer 2 physical interfaces. Standard (numbered, named) and Extended (numbered, named) IP ACLs, and Extended Named MAC ACLs are supported.

To apply IP or MAC ACLs on a Layer 2 interface, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# interface interface`	Enters interface configuration mode for a Layer 2 port.
Step 3	`Switch(config-if)# {ip | mac} access-group {name | number | in | out}`	Applies a numbered or named ACL to the Layer 2 interface.
Step 4	`Switch(config)# show running-config`	Displays the access list configuration.

This example shows how to configure the Extended Named IP ACL simple-ip-acl to permit all TCP traffic and implicitly deny all other IP traffic:

```
Switch(config)# ip access-list extended simple-ip-acl
Switch(config-ext-nacl)# permit tcp any any
Switch(config-ext-nacl)# end
```

This example shows how to configure the Extended Named MAC ACL simple-mac-acl to permit source host 000.000.011 to any destination host:

```
Switch(config)# mac access-list extended simple-mac-acl
Switch(config-ext-macl)# permit host 000.000.011 any
Switch(config-ext-macl)# end
```

Configuring Access-group Mode on Layer 2 Interface

To configure the access mode on a Layer 2 interface, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# interface interface`	Enters interface configuration mode for a Layer 2 port.
Step 3	`Switch(config-if)# [no] access-group mode {prefer port | merge}`	Sets the mode for this Layer 2 interface. The **no** prefix sets the mode to the default value (which is merge).
Step 4	`Switch(config)# show running-config`	Displays the access list configuration.

This example shows how to configure an interface to use prefer port mode:

```
Switch# configure terminal
Switch(config)# interface gigabitEthernet 6/1
Switch(config-if)# access-group mode prefer port
```

This example shows how to configure an interface to use merge mode:

```
Switch# configure terminal
Switch(config)# interface gigabitEthernet 6/1
Switch(config-if)# access-group mode merge
```

Applying ACLs to a Layer 2 Interface

To apply IP and MAC ACLs to a Layer 2 interface, perform one of these tasks:

Command	Purpose
`Switch(config-if)# ip access-group ip-acl in`	Applies an IP ACL to the Layer 2 interface.
`Switch(config-if)# mac access-group mac-acl in`	Applies a MAC ACL to the Layer 2 interface.

This example applies the extended named IP ACL simple-ip-acl to interface GigabitEthernet 6/1 ingress traffic:

```
Switch# configure t
Switch(config)# interface gigabitEthernet 6/1
Switch(config-if)# ip access-group simple-ip-acl in
```

This example applies the extended named MAC ACL simple-mac-acl to interface GigabitEthernet 6/1 ingress traffic:

```
Switch# configure t
Switch(config)# interface gigabitEthernet 6/1
Switch(config-if)# mac access-group simple-mac-acl in
```

Applying ACLs to a Port Channel

To apply IP and MAC ACLs to a port channel logical interface, perform this task:

Command	Purpose
`Switch(config-if)# interface port-channel number`	Enters configuration mode for the port channel.
`Switch(config-if)# ip access-group ip-acl {in | out}`	Applies an IP ACL to the port channel interface.
`Switch(config-if)# mac access-group mac-acl {in | out}`	Applies a MAC ACL to the port channel interface.

This example applies the extended named IP ACL simple-ip-acl to port channel 3 ingress traffic:

```
Switch# configure t
Switch(config)# interface port-channel 3
Switch(config-if)# ip access-group simple-ip-acl in
```

Displaying an ACL Configuration on a Layer 2 Interface

To display information about an ACL configuration on Layer 2 interfaces, perform one of these tasks:

Command	Purpose
`Switch# show ip access-lists [interface interface-name]`	Shows the IP access group configuration on the interface.
`Switch# show mac access-group [interface interface-name]`	Shows the MAC access group configuration on the interface.
`Switch# show access-group mode [interface interface-name]`	Shows the access group mode configuration on the interface.

This example shows that the IP access group simple-ip-acl is configured on the inbound direction of interface fa6/1:

```
Switch# show ip interface fast 6/1
FastEthernet6/1 is up, line protocol is up
  Inbound  access list is simple-ip-acl
  Outgoing access list is not set
```

This example shows that MAC access group simple-mac-acl is configured on the inbound direction of interface fa6/1:

```
Switch# show mac access-group interface fast 6/1
Interface FastEthernet6/1:
   Inbound access-list is simple-mac-acl
   Outbound access-list is not set
```

This example shows that access group merge is configured on interface fa6/1:

```
Switch# show access-group mode interface fast 6/1
Interface FastEthernet6/1:
   Access group mode is: merge
```

Configuring VACLs

These sections describe how to configure VACLs:

- VACL Configuration Guidelines, page 51-11
- Defining a VLAN Access Map, page 51-13
- Configuring a Match Clause in a VLAN Access Map Sequence, page 51-13
- Configuring an Action Clause in a VLAN Access Map Sequence, page 51-14
- Applying a VLAN Access Map, page 51-15
- Verifying VLAN Access Map Configuration, page 51-15
- VLAN Access Map Configuration and Verification Examples, page 51-16
- Configuring a Capture Port, page 51-16
- Configuring MAC PBF, page 51-18

VACL Configuration Guidelines

Consider the following guidelines when configuring VACLs:

- VACLs use standard and extended Cisco IOS IP and MAC layer-named ACLs (see the "Configuring MAC ACLs" section on page 43-68) and VLAN access maps.
- VLAN access maps can be applied to VLANs or to WAN interfaces for VACL capture. VACLs attached to WAN interfaces support only standard and extended Cisco IOS IP ACLs.
- 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.
- When VACL capture is configured with Policy Based Routing (PBR) on the same interface, do not select BDD as the ACL merge algorithm. We recommend using ODM, the default ACL merge algorithm for the Supervisor Engine 720.
- 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.
- By default, software-switched WAN packets are not subjected to ACL lookup in the ACL TCAM and are therefore not affected by hardware-only features. As a result, VACL capture will fail for software-switched WAN packets. In Cisco IOS Release 12.2(33)SXI2 and later releases, you can allow ACLs to be applied to egress or ingress software-switched WAN packets by entering the **platform cwan acl software-switched** {**egress** | **ingress**} command in global configuration mode. To verify whether ACLs will be applied to software-switched WAN packets, enter the **show platform acl software-switched** command as shown in this example:

```
Router (config)# platform cwan acl software-switched ingress
Router (config)# exit
Router# show platform acl software-switched
 CWAN: ACL treatment for software switched in INGRESS is enabled
 CWAN: ACL treatment for software switched in EGRESS is disabled
```

- The action clause in a VACL can be forward, drop, capture, or redirect. Traffic can also be logged. VACLs applied to WAN interfaces do not support the redirect or log actions.
- VACLs cannot be applied to IGMP, MLD, or PIM traffic.
- When the WAN logical interface (Multilink or Multilink Frame Relay) is removed, the corresponding VACL filter applied to the WAN logical interface is also removed and the error message VACL-4-VLANFILTER_CWAN_DELETE appears. The following example displays an illustration of this behavior:

```
Router (config)# do show vlan filter
VLAN Map capture_all:
        Configured on VLANs:  100
            Active on VLANs:  100

        Configured on Interfaces:  Multilink100
            Active on Interfaces:

Router (config)# no interface multilink 100
% Please 'shutdown' this interface before trying to delete it
Router (config)# interface multilink 100
Router (config-if)# show
Router (config-if)# exit
Router (config)# no interface multilink 100
Router (config)#
```

```
%VACL-4-VLANFILTER_CWAN_DELETE: VLAN ACCESS-MAP capture_all applied on Multilink100
will be removed.
Router (config)# do show vlan filter
VLAN Map capture_all:
        Configured on VLANs:  100
            Active on VLANs:  100

Router (config)#
```

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.

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.
Router(config)# **no vlan access-map** *map_name* **0-65535**	Deletes a map sequence from the VLAN access map.
Router(config)# **no vlan access-map** *map_name*	Deletes the VLAN access map.

When defining a VLAN access map, note the following information:

- 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 51-16.

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 address** {**1-199** | **1300-2699** | *acl_name*} | {**mac address** *acl_name*}}	Configures the match clause in a VLAN access map sequence.
Router(config-access-map)# **no match** {**ip address** {**1-199** | **1300-2699** | *acl_name*} | {**mac address** *acl_name*}}	Deletes the match clause in a VLAN access map sequence.

When configuring a match clause in a VLAN access map sequence, note the following information:

- You can select one or more ACLs.
- VACLs attached to WAN interfaces support only standard and extended Cisco IOS IP ACLs.
- Use the **no** keyword to remove a match clause or specified ACLs in the clause.
- For information about named MAC-Layer ACLs, see the "Configuring MAC ACLs" section on page 43-68.
- For information about Cisco IOS ACLs, see the "Traffic Filtering and Firewalls" section of the *Cisco IOS Security Configuration Guide, Release 12.2*, at this URL:

  http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/fsecur_c.html

See the "VLAN Access Map Configuration and Verification Examples" section on page 51-16.

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** {{**ethernet** | **fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot*/*port*} | {**port-channel** *channel_id*}}	Configures the action clause in a VLAN access map sequence.
Router(config-access-map)# **no action** {**drop** [**log**]} | {**forward** [**capture** | **vlan** *vlan_ID*]} | {**redirect** {{**ethernet** | **fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot*/*port*} | {**port-channel** *channel_id*}}	Deletes the action clause in from the VLAN access map sequence.

When configuring an action clause in a VLAN access map sequence, note the following information:

- You can set the action to drop, forward, forward capture, or redirect packets.
- VACLs applied to WAN interfaces support only the forward capture action. VACLs applied to WAN interfaces do not support the drop, forward, or redirect actions.
- 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 51-16.
- The **forward vlan** action implements Policy-Based Forwarding (PBF), bridging between VLANs.
- VACLs applied to WAN interfaces do not support the **log** action.
- 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 interface.
- 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 51-16.

Applying a VLAN Access Map

To apply a VLAN access map, perform this task:

Command	Purpose
`Router(config)# `**`vlan filter`**` `*`map_name`*` {`**`vlan-list`**` `*`vlan_list`*`	`**`interface`**` `*`type`*[1]` `*`number`*[2]`}`	Applies the VLAN access map to the specified VLANs or WAN interfaces.

1. *type* = **pos**, **atm**, or **serial**
2. number = *slot/port* or *slot/port_adapter/port*; can include a subinterface or channel group descriptor

When applying a VLAN access map, note the following information:

- You can apply the VLAN access map to one or more VLANs or WAN interfaces.
- 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*).
- If you delete a WAN interface that has a VACL applied, the VACL configuration on the interface is also removed.
- You can apply only one VLAN access map to each VLAN or WAN interface.
- 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 or WAN interfaces.

See the "VLAN Access Map Configuration and Verification Examples" section on page 51-16.

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`*`	`**`interface`**` `*`type`*[1]` `*`number`*[2]`]`	Verifies VLAN access map configuration by displaying the mappings between VACLs and VLANs.

1. *type* = **pos**, **atm**, or **serial**

2. number = *slot*/*port* or *slot*/*port_adapter*/*port*; can include a subinterface or channel group descriptor

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

A port configured to capture VACL-filtered traffic is called a capture port.

Note To apply IEEE 802.1Q or ISL tags to the captured traffic, configure the capture port to trunk unconditionally (see the "Configuring the Layer 2 Switching Port as an ISL or 802.1Q Trunk" section on page 17-10 and the "Configuring the Layer 2 Trunk Not to Use DTP" section on page 17-11).

To configure a capture port, perform this task:

	Command	Purpose
Step 1	`Router(config)#` **`interface`** `{{`*`type`*[1] *`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.

[1] *type* = **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

When configuring a capture port, note the following information:

- 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 17-10) 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 17-16) 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 Fast 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 MAC PBF

To configure MAC policy-based forwarding (PBF), perform this task on each source VLAN:

	Command	Purpose
Step 1	Router(config)# **mac host** *my_host mac_addr*	(Optional) Assigns a name to the MAC address of the source host.
Step 2	Router(config)# **mac access-list extended** *macl_name*	Configures a MAC ACL.
Step 3	Router(config-ext-macl)# **permit host** *my_host* **any**	Configures an access control entry (ACE) to permit traffic from the named host to any other address. Hosts can be specified by a name or by a MAC address.
	Router(config-ext-macl)# **permit host** *my_host* **host** *other_host*	Configures an ACE to permit traffic from the named host to one other host.
Step 4	Router(config-ext-macl)# **exit**	Exits ACL configuration.
Step 5	Router(config)# **vlan access-map** *map_name*	Defines a VLAN access map.
Step 6	Router(config-access-map)# **match mac address** *macl_name*	Applies the MAC ACL to this VLAN access map.
Step 7	Router(config-access-map)# **action forward vlan** *other_vlan_ID* [**local**]	Forwards matching traffic to the other VLAN. **Note** By default, PBF-specified devices on the same VLAN cannot communicate with each other. To allow local communication by the host, use the **local** keyword.
Step 8	Router(config-access-map)# **exit**	Exits access map configuration.
Step 9	Router(config)# **vlan filter** *map_name* **vlan-list** *my_vlan_ID*	Applies the VLAN access map to the specified VLAN.
Step 10	Router(config)# **interface vlan** *my_vlan_ID*	Enters interface configuration mode for the VLAN.
Step 11	Router(config-if)# **mac packet-classify**	Classifies incoming or outgoing Layer 3 packets on this VLAN as Layer 2 packets.
Step 12	Router(config-if)# **exit**	Exits interface configuration.
Step 13	Router(config)# **mls rate-limit unicast acl mac-pbf** *pps* [*burst_size*]	(Optional) Sets a rate limit on PBF packets. • *pps*—Maximum number of packets per second. The range is 10 to 1000000 packets per second. • *burst_siz*e—Maximum number of packets in a burst. The range is 1 to 255 packets.
Step 14	Router(config)# **exit**	Exits global configuration mode.
Step 15	Router# **show vlan mac-pbf config**	Displays MAC PBF configuration and statistics.
Step 16	Router# **clear vlan mac-pbf counters**	(Optional) Clears MAC PBF packet counters.

When configuring MAC PBF, note the following information:

- To allow traffic in both directions between two VLANs, you must configure MAC PBF in both VLANs.
- You can configure MAC PBF between hosts in different switches.

- By default, MAC PBF hosts in the same VLAN cannot communicate with each other. To allow local communication, use the **local** keyword.
- When configuring the **vlan filter** command, specify only one VLAN after the **vlan-list** keyword. If you specify more than one VLAN, MAC PBF will ignore all but the last VLAN in the list.
- The output of the **show vlan mac-pbf config** command displays the following fields for configured PBF paths:
  - Rcv Vlan — The number of the VLAN to which packets are forwarded by PBF.
  - Snd Vlan — The number of the VLAN which will forward packets by PBF.
  - DMAC — The MAC address of the destination host on the receiving VLAN.
  - SMAC — The MAC address of the source host on the sending VLAN.
  - (Local) — Displays 1 if the **local** keyword is configured in the **action forward vlan** command on the sending VLAN; displays 0 if the **local** keyword is not configured.
  - (Packet counter) — The number of packets that have been forwarded from the sending VLAN to the receiving VLAN. To clear this counter, enter the **clear vlan mac-pbf counters** command.
  - Pkts dropped — The number of packets that have been dropped by the sending VLAN. To clear this counter, enter the **clear vlan mac-pbf counters** command.
- If the sending VLAN is shut down, MAC PBF will still function. Shutting down a VLAN disables Layer 3 functionality, but MAC PBF is a Layer 2 function.

This example shows how to configure and display MAC PBF to allow two hosts in separate VLANs (“red” VLAN 100 and “blue” VLAN 200) on the same switch to exchange packets:

```
Router(config)# mac host host_red3 0001.0002.0003
Router(config)# mac access-list extended macl_red
Router(config-ext-macl)# permit host host_red host host_blue
Router(config-ext-macl)# exit
Router(config)# vlan access-map red_to_blue
Router(config-access-map)# match mac address macl_red
Router(config-access-map)# action forward vlan 200 local
Router(config-access-map)# exit
Router(config)# vlan filter red_to_blue vlan-list 100
Router(config)# interface vlan 100
Router(config-if)# mac packet-classify
Router(config-if)# exit
Router(config)#
Router(config)# mac host host_blue5 0001.0002.0005
Router(config)# mac access-list extended macl_blue
Router(config-ext-macl)# permit host host_blue host host_red
Router(config-ext-macl)# exit
Router(config)# vlan access-map blue_to_red
Router(config-access-map)# match mac address macl_blue
Router(config-access-map)# action forward vlan 100
Router(config-access-map)# exit
Router(config)# vlan filter blue_to_red vlan-list 200
Router(config)# interface vlan 200
Router(config-if)# mac packet-classify
Router(config-if)# exit
Router#
Router# show vlan mac-pbf config
 Rcv Vlan 100, Snd Vlan 200, DMAC 0001.0002.0003, SMAC 0001.0002.0005 1 15
 Rcv Vlan 200, Snd Vlan 100, DMAC 0001.0002.0005, SMAC 0001.0002.0003 0 23
 Pkts Dropped 0
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 PACLs" section on page 51-8 for configuration information) 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.
Step 5	Router# **show vlan access-log config**	(Optional) Displays the configured VACL logging properties.
Step 6	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*]	(Optional) Displays the content of the VACL log table.
Step 7	Router# **show vlan access-log statistics**	(Optional) Displays packet and message counts and other statistics.

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
```

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