



## VLAN Access Control Lists

---

VLAN access control lists (ACLs) or VLAN maps access-control all packets (bridged and routed). You can use VLAN maps to filter traffic between devices in the same VLAN. VLAN maps are configured to provide access control based on Layer 3 addresses for IPv4. Unsupported protocols are access-controlled through MAC addresses using Ethernet access control entries (ACEs). After a VLAN map is applied to a VLAN, all packets (routed or bridged) entering the VLAN are checked against the VLAN map. Packets can either enter the VLAN through a switch port or through a routed port after being routed.

This module provides more information about VLAN ACLs and how to configure them.

- [Finding Feature Information, on page 1](#)
- [Information About VLAN Access Control Lists, on page 1](#)
- [How to Configure VLAN Access Control Lists, on page 4](#)
- [Configuration Examples for ACLs and VLAN Maps, on page 12](#)
- [Configuration Examples for Using VLAN Maps in Your Network, on page 14](#)
- [Configuration Examples of Router ACLs and VLAN Maps Applied to VLANs, on page 16](#)

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Information About VLAN Access Control Lists

### VLAN Maps

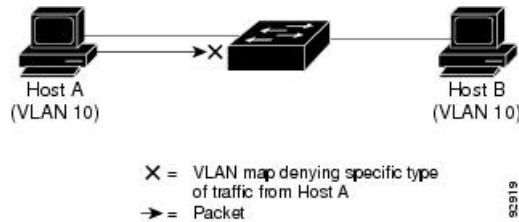
VLAN ACLs or VLAN maps are used to control network traffic within a VLAN. You can apply VLAN maps to all packets that are bridged within a VLAN in the switch or switch stack. VACLs are strictly for security packet filtering and for redirecting traffic to specific physical interfaces. VACLs are not defined by direction (ingress or egress).

All non-IP protocols are access-controlled through MAC addresses and EtherType using MAC VLAN maps. (IP traffic is not access controlled by MAC VLAN maps.) You can enforce VLAN maps only on packets going through the switch; you cannot enforce VLAN maps on traffic between hosts on a hub or on another switch connected to this switch.

With VLAN maps, forwarding of packets is permitted or denied, based on the action specified in the map.

**Figure 1: Using VLAN Maps to Control Traffic**

This shows how a VLAN map is applied to prevent a specific type of traffic from Host A in VLAN 10 from being forwarded. You can apply only one VLAN map to a VLAN.



## VLAN Map Configuration Guidelines

VLAN maps are the only way to control filtering within a VLAN. VLAN maps have no direction. To filter traffic in a specific direction by using a VLAN map, you need to include an ACL with specific source or destination addresses. If there is a match clause for that type of packet (IP or MAC) in the VLAN map, the default action is to drop the packet if the packet does not match any of the entries within the map. If there is no match clause for that type of packet, the default is to forward the packet.

The following are the VLAN map configuration guidelines:

- If there is no ACL configured to deny traffic on an interface and no VLAN map is configured, all traffic is permitted.
- Each VLAN map consists of a series of entries. The order of entries in an VLAN map is important. A packet that comes into the switch is tested against the first entry in the VLAN map. If it matches, the action specified for that part of the VLAN map is taken. If there is no match, the packet is tested against the next entry in the map.
- If the VLAN map has at least one match clause for the type of packet (IP or MAC) and the packet does not match any of these match clauses, the default is to drop the packet. If there is no match clause for that type of packet in the VLAN map, the default is to forward the packet.
- Logging is not supported for VLAN maps.
- When a switch has an IP access list or MAC access list applied to a Layer 2 interface, and you apply a VLAN map to a VLAN that the port belongs to, the port ACL takes precedence over the VLAN map.
- If a VLAN map configuration cannot be applied in hardware, all packets in that VLAN are dropped.

## VLAN Maps with Router ACLs

To access control both bridged and routed traffic, you can use VLAN maps only or a combination of router ACLs and VLAN maps. You can define router ACLs on both input and output routed VLAN interfaces, and you can define a VLAN map to access control the bridged traffic.

If a packet flow matches a VLAN-map deny clause in the ACL, regardless of the router ACL configuration, the packet flow is denied.



**Note** When you use router ACLs with VLAN maps, packets that require logging on the router ACLs are not logged if they are denied by a VLAN map.

If the VLAN map has a match clause for the type of packet (IP or MAC) and the packet does not match the type, the default is to drop the packet. If there is no match clause in the VLAN map, and no action specified, the packet is forwarded if it does not match any VLAN map entry.

## VLAN Maps and Router ACL Configuration Guidelines

These guidelines are for configurations where you need to have an router ACL and a VLAN map on the same VLAN. These guidelines do not apply to configurations where you are mapping router ACLs and VLAN maps on different VLANs.

If you must configure a router ACL and a VLAN map on the same VLAN, use these guidelines for both router ACL and VLAN map configuration:

- You can configure only one VLAN map and one router ACL in each direction (input/output) on a VLAN interface.
- Whenever possible, try to write the ACL with all entries having a single action except for the final, default action of the other type. That is, write the ACL using one of these two forms:

```
permit... permit... permit... deny ip any any
```

or

```
deny... deny... deny... permit ip any any
```

- To define multiple actions in an ACL (permit, deny), group each action type together to reduce the number of entries.
- Avoid including Layer 4 information in an ACL; adding this information complicates the merging process. The best merge results are obtained if the ACLs are filtered based on IP addresses (source and destination) and not on the full flow (source IP address, destination IP address, protocol, and protocol ports). It is also helpful to use *don't care* bits in the IP address, whenever possible.

If you need to specify the full-flow mode and the ACL contains both IP ACEs and TCP/UDP/ICMP ACEs with Layer 4 information, put the Layer 4 ACEs at the end of the list. This gives priority to the filtering of traffic based on IP addresses.

## VACL Logging

When you configure VACL logging, syslog messages are generated for denied IP packets under these circumstances:

- When the first matching packet is received.
- For any matching packets received within the last 5 minutes.
- 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. If a flow does not receive any packets in the 5-minute interval, that flow is removed from the cache. When a syslog message is generated, the timer and packet counter are reset.

VACL logging restrictions:

- Only denied IP packets are logged.
- Packets that require logging on the outbound port ACLs are not logged if they are denied by a VACL.

## How to Configure VLAN Access Control Lists

### Creating Named MAC Extended ACLs

You can filter non-IPv4 traffic on a VLAN or on a Layer 2 interface by using MAC addresses and named MAC extended ACLs. The procedure is similar to that of configuring other extended named ACLs.

Follow these steps to create a named MAC extended ACL:

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device> <b>enable</b>	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>mac access-list extended name</b> <b>Example:</b> Device(config)# <b>mac access-list extended mac1</b>	Defines an extended MAC access list using a name.
<b>Step 4</b>	<b>{deny   permit} {any   host source MAC address   source MAC address mask} {any   host destination MAC address   destination MAC address mask} [type mask   lsap lsap mask   aarp   amber   dec-spanning   decnet-iv   diagnostic   dsm   etype-6000   etype-8042   lat   lavc-sca   mop-console   mop-dump  </b>	In extended MAC access-list configuration mode, specifies to <b>permit</b> or <b>deny</b> any source MAC address, a source MAC address with a mask, or a specific <b>host</b> source MAC address and <b>any</b> destination MAC address, destination MAC address with a mask, or a specific destination MAC address.

	Command or Action	Purpose
	<p><b>msdos   mumps   netbios   vines-echo   vines-ip   xns-idp   0-65535] [cos cos]</b></p> <p><b>Example:</b></p> <pre>Device(config-ext-macl)# deny any any dechnet-iv</pre> <p>or</p> <pre>Device(config-ext-macl)# permit any any</pre>	<p>(Optional) You can also enter these options:</p> <ul style="list-style-type: none"> <li>• <i>type mask</i>—An arbitrary EtherType number of a packet with Ethernet II or SNAP encapsulation in decimal, hexadecimal, or octal with optional mask of <i>don't care</i> bits applied to the EtherType before testing for a match.</li> <li>• <i>lsap lsap mask</i>—An LSAP number of a packet with IEEE 802.2 encapsulation in decimal, hexadecimal, or octal with optional mask of <i>don't care</i> bits.</li> <li>• <i>aarp   amber   dec-spanning   decnet-iv   diagnostic   dsm   etype-6000   etype-8042   lat   larc-sca   mop-console   mop-dump   msdos   mumps   netbios   vines-echo   vines-ip   xns-idp</i>—A non-IP protocol.</li> <li>• <i>cos cos</i>—An IEEE 802.1Q cost of service number from 0 to 7 used to set priority.</li> </ul>
<b>Step 5</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Device(config-ext-macl)# end</pre>	Returns to privileged EXEC mode.
<b>Step 6</b>	<p><b>show running-config</b></p> <p><b>Example:</b></p> <pre>Device# show running-config</pre>	Verifies your entries.
<b>Step 7</b>	<p><b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

## Applying a MAC ACL to a Layer 2 Interface

Follow these steps to apply a MAC access list to control access to a Layer 2 interface:

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b>  Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b>  Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 3</b>	<b>interface <i>interface-id</i></b> <b>Example:</b>  Device(config)# <code>interface gigabitethernet1/0/2</code>	Identifies a specific interface, and enter interface configuration mode. The interface must be a physical Layer 2 interface (port ACL).
<b>Step 4</b>	<b>mac access-group {<i>name</i>} {in   out }</b> <b>Example:</b>  Device(config-if)# <code>mac access-group mac1 in</code>	Controls access to the specified interface by using the MAC access list.  Port ACLs are supported in the outbound and inbound directions .
<b>Step 5</b>	<b>end</b> <b>Example:</b>  Device(config-if)# <code>end</code>	Returns to privileged EXEC mode.
<b>Step 6</b>	<b>show mac access-group [interface <i>interface-id</i>]</b> <b>Example:</b>  Device# <code>show mac access-group interface gigabitethernet1/0/2</code>	Displays the MAC access list applied to the interface or all Layer 2 interfaces.
<b>Step 7</b>	<b>configure terminal</b> <b>Example:</b>  Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 8</b>	<b>configure terminal</b> <b>Example:</b>	Enters global configuration mode.

	Command or Action	Purpose
	Device# <code>configure terminal</code>	

After receiving a packet, the switch checks it against the inbound ACL. If the ACL permits it, the switch continues to process the packet. If the ACL rejects the packet, the switch discards it. When you apply an undefined ACL to an interface, the switch acts as if the ACL has not been applied and permits all packets. Remember this behavior if you use undefined ACLs for network security.

## Configuring VLAN Maps

To create a VLAN map and apply it to one or more VLANs, perform these steps:

### Before you begin

Create the standard or extended IPv4 ACLs or named MAC extended ACLs that you want to apply to the VLAN.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>vlan access-map</b> <i>name</i> [ <i>number</i> ] <b>Example:</b> Device(config)# <code>vlan access-map map_1 20</code>	Creates a VLAN map, and give it a name and (optionally) a number. The number is the sequence number of the entry within the map.  When you create VLAN maps with the same name, numbers are assigned sequentially in increments of 10. When modifying or deleting maps, you can enter the number of the map entry that you want to modify or delete.  VLAN maps do not use the specific permit or deny keywords. To deny a packet by using VLAN maps, create an ACL that would match the packet, and set the action to drop. A permit in the ACL counts as a match. A deny in the ACL means no match.  Entering this command changes to access-map configuration mode.
<b>Step 2</b>	<b>match</b> { <i>ip</i>   <i>mac</i> } <b>address</b> { <i>name</i>   <i>number</i> } [ <i>name</i>   <i>number</i> ] <b>Example:</b> Device(config-access-map)# <code>match ip address ip2</code>	Match the packet (using either the IP or MAC address) against one or more standard or extended access lists. Note that packets are only matched against access lists of the correct protocol type. IP packets are matched against standard or extended IP access lists. Non-IP packets are only matched against named MAC extended access lists.

	Command or Action	Purpose
		<p><b>Note</b> If the VLAN map is configured with a match clause for a type of packet (IP or MAC) and the map action is drop, all packets that match the type are dropped. If the VLAN map has no match clause, and the configured action is drop, all IP and Layer 2 packets are dropped.</p>
<b>Step 3</b>	<p>Enter one of the following commands to specify an IP packet or a non-IP packet (with only a known MAC address) and to match the packet against one or more ACLs (standard or extended):</p> <ul style="list-style-type: none"> <li>• <b>action { forward }</b></li> </ul> <pre>Device(config-access-map)# action forward</pre> <ul style="list-style-type: none"> <li>• <b>action { drop }</b></li> </ul> <pre>Device(config-access-map)# action drop</pre>	Sets the action for the map entry.
<b>Step 4</b>	<p><b>vlan filter mapname vlan-list list</b></p> <p><b>Example:</b></p> <pre>Device(config)# vlan filter map 1 vlan-list 20-22</pre>	<p>Applies the VLAN map to one or more VLAN IDs.</p> <p>The list can be a single VLAN ID (22), a consecutive list (10-22), or a string of VLAN IDs (12, 22, 30). Spaces around the comma and hyphen are optional.</p>

## Creating a VLAN Map

Each VLAN map consists of an ordered series of entries. Beginning in privileged EXEC mode, follow these steps to create, add to, or delete a VLAN map entry:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Device# configure terminal</pre>	Enters global configuration mode.



	Command or Action	Purpose
<b>Step 2</b>	<b>vlan access-map</b> <i>name</i> [ <i>number</i> ] <b>Example:</b> <pre>Device(config)# <b>vlan access-map map_1 20</b></pre>	<p>Creates a VLAN map, and give it a name and (optionally) a number. The number is the sequence number of the entry within the map.</p> <p>When you create VLAN maps with the same name, numbers are assigned sequentially in increments of 10. When modifying or deleting maps, you can enter the number of the map entry that you want to modify or delete.</p> <p>VLAN maps do not use the specific permit or deny keywords. To deny a packet by using VLAN maps, create an ACL that would match the packet, and set the action to drop. A permit in the ACL counts as a match. A deny in the ACL means no match.</p> <p>Entering this command changes to access-map configuration mode.</p>
<b>Step 3</b>	<b>match</b> { <i>ip</i>   <i>mac</i> } <b>address</b> { <i>name</i>   <i>number</i> } [ <i>name</i>   <i>number</i> ] <b>Example:</b> <pre>Device(config-access-map)# <b>match ip address ip2</b></pre>	<p>Match the packet (using either the IP or MAC address) against one or more standard or extended access lists. Note that packets are only matched against access lists of the correct protocol type. IP packets are matched against standard or extended IP access lists. Non-IP packets are only matched against named MAC extended access lists.</p>
<b>Step 4</b>	<b>action</b> { <i>drop</i>   <i>forward</i> } <b>Example:</b> <pre>Device(config-access-map)# <b>action forward</b></pre>	<p>(Optional) Sets the action for the map entry. The default is to forward.</p>
<b>Step 5</b>	<b>end</b> <b>Example:</b> <pre>Device(config-access-map)# <b>end</b></pre>	<p>Returns to global configuration mode.</p>
<b>Step 6</b>	<b>show running-config</b> <b>Example:</b> <pre>Device# <b>show running-config</b></pre>	<p>Displays the access list configuration.</p>
<b>Step 7</b>	<b>copy running-config startup-config</b> <b>Example:</b> <pre>Device# <b>copy running-config</b></pre>	<p>(Optional) Saves your entries in the configuration file.</p>

	Command or Action	Purpose
	<code>startup-config</code>	

## Applying a VLAN Map to a VLAN

Beginning in privileged EXEC mode, follow these steps to apply a VLAN map to one or more VLANs:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>		
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 3</b>	<b>vlan filter mapname vlan-list list</b> <b>Example:</b> Device(config)# <code>vlan filter map 1</code> <code>vlan-list 20-22</code>	Applies the VLAN map to one or more VLAN IDs.  The list can be a single VLAN ID (22), a consecutive list (10-22), or a string of VLAN IDs (12, 22, 30). Spaces around the comma and hyphen are optional.
<b>Step 4</b>	<b>end</b> <b>Example:</b> Device(config)# <code>end</code>	Returns to privileged EXEC mode.
<b>Step 5</b>	<b>show running-config</b> <b>Example:</b> Device# <code>show running-config</code>	Displays the access list configuration.
<b>Step 6</b>	<b>copy running-config startup-config</b> <b>Example:</b> Device# <code>copy running-config</code> <code>startup-config</code>	(Optional) Saves your entries in the configuration file.

## Configuring VACL Logging

Beginning in privileged EXEC mode:

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>vlan access-map name [number]</b> <b>Example:</b> Device(config)# <b>vlan access-map gandymede</b> <b>10</b>	<p>Creates a VLAN map. Give it a name and optionally a number. The number is the sequence number of the entry within the map.</p> <p>The sequence number range is from 0 to 65535.</p> <p>When you create VLAN maps with the same name, numbers are assigned sequentially in increments of 10. When modifying or deleting maps, you can enter the number of the map entry that you want to modify or delete.</p> <p>Specifying the map name and optionally a number enters the access-map configuration mode.</p>
<b>Step 3</b>	<b>action drop log</b> <b>Example:</b> Device(config-access-map)# <b>action drop</b> <b>log</b>	Sets the VLAN access map to drop and log IP packets.
<b>Step 4</b>	<b>exit</b> <b>Example:</b> Device(config-access-map)# <b>exit</b>	Exits the VLAN access map configuration mode and return to the global configuration mode.
<b>Step 5</b>	<b>vlan access-log {maxflow max_number   threshold pkt_count}</b> <b>Example:</b> Device(config)# <b>vlan access-log threshold</b> <b>4000</b>	<p>Configures the VACL logging parameters.</p> <ul style="list-style-type: none"> <li>• <b>maxflow max_number</b>—Sets the log table size. The content of the log table can be deleted by setting the <b>maxflow</b> to 0. When the log table is full, the software drops logged packets from new flows.</li> </ul> <p>The range is from 0 to 2048. The default is 500.</p> <ul style="list-style-type: none"> <li>• <b>threshold pkt_count</b>—Sets the logging threshold. A logging message is generated if the threshold for a flow is reached before the 5-minute interval.</li> </ul>

	Command or Action	Purpose
		The threshold range is from 0 to 2147483647. The default threshold is 0, which means that a syslog message is generated every 5 minutes.
<b>Step 6</b>	<b>end</b>  <b>Example:</b>  Device(config)# <b>end</b>	Returns to privileged EXEC mode.

## Configuration Examples for ACLs and VLAN Maps

### Example: Creating an ACL and a VLAN Map to Deny a Packet

This example shows how to create an ACL and a VLAN map to deny a packet. In the first map, any packets that match the *ip1* ACL (TCP packets) would be dropped. You first create the *ip1* ACL to permit any TCP packet and no other packets. Because there is a match clause for IP packets in the VLAN map, the default action is to drop any IP packet that does not match any of the match clauses.

```
Device(config)# ip access-list extended ip1
Device(config-ext-nacl)# permit tcp any any
Device(config-ext-nacl)# exit
Device(config)# vlan access-map map_1 10
Device(config-access-map)# match ip address ip1
Device(config-access-map)# action drop
```

### Example: Creating an ACL and a VLAN Map to Permit a Packet

This example shows how to create a VLAN map to permit a packet. ACL *ip2* permits UDP packets and any packets that match the *ip2* ACL are forwarded. In this map, any IP packets that did not match any of the previous ACLs (that is, packets that are not TCP packets or UDP packets) would get dropped.

```
Device(config)# ip access-list extended ip2
Device(config-ext-nacl)# permit udp any any
Device(config-ext-nacl)# exit
Device(config)# vlan access-map map_1 20
Device(config-access-map)# match ip address ip2
Device(config-access-map)# action forward
```

### Example: Default Action of Dropping IP Packets and Forwarding MAC Packets

In this example, the VLAN map has a default action of drop for IP packets and a default action of forward for MAC packets. Used with standard ACL 101 and extended named access lists **igmp-match** and **tcp-match**, the map will have the following results:

- Forward all UDP packets

- Drop all IGMP packets
- Forward all TCP packets
- Drop all other IP packets
- Forward all non-IP packets

```
Device(config)# access-list 101 permit udp any any
Device(config)# ip access-list extended igmp-match
Device(config-ext-nacl)# permit igmp any any
```

```
Device(config-ext-nacl)# permit tcp any any
Device(config-ext-nacl)# exit
Device(config)# vlan access-map drop-ip-default 10
Device(config-access-map)# match ip address 101
Device(config-access-map)# action forward
Device(config-access-map)# exit
Device(config)# vlan access-map drop-ip-default 20
Device(config-access-map)# match ip address igmp-match
Device(config-access-map)# action drop
Device(config-access-map)# exit
Device(config)# vlan access-map drop-ip-default 30
Device(config-access-map)# match ip address tcp-match
Device(config-access-map)# action forward
```

## Example: Default Action of Dropping MAC Packets and Forwarding IP Packets

In this example, the VLAN map has a default action of drop for MAC packets and a default action of forward for IP packets. Used with MAC extended access lists **good-hosts** and **good-protocols**, the map will have the following results:

- Forward MAC packets from hosts 0000.0c00.0111 and 0000.0c00.0211
- Forward MAC packets with decnet-iv or vines-ip protocols
- Drop all other non-IP packets
- Forward all IP packets

```
Device(config)# mac access-list extended good-hosts
Device(config-ext-macl)# permit host 000.0c00.0111 any
Device(config-ext-macl)# permit host 000.0c00.0211 any
Device(config-ext-nacl)# exit
Device(config)# action forward
Device(config-ext-macl)# mac access-list extended good-protocols
Device(config-ext-macl)# permit any any vines-ip
Device(config-ext-nacl)# exit
Device(config)# vlan access-map drop-mac-default 10
Device(config-access-map)# match mac address good-hosts
Device(config-access-map)# action forward
Device(config-access-map)# exit
Device(config)# vlan access-map drop-mac-default 20
Device(config-access-map)# match mac address good-protocols
Device(config-access-map)# action forward
```

## Example: Default Action of Dropping All Packets

In this example, the VLAN map has a default action of drop for all packets (IP and non-IP). Used with access lists **tcp-match** and **good-hosts** from Examples 2 and 3, the map will have the following results:

- Forward all TCP packets
- Forward MAC packets from hosts 0000.0c00.0111 and 0000.0c00.0211
- Drop all other IP packets
- Drop all other MAC packets

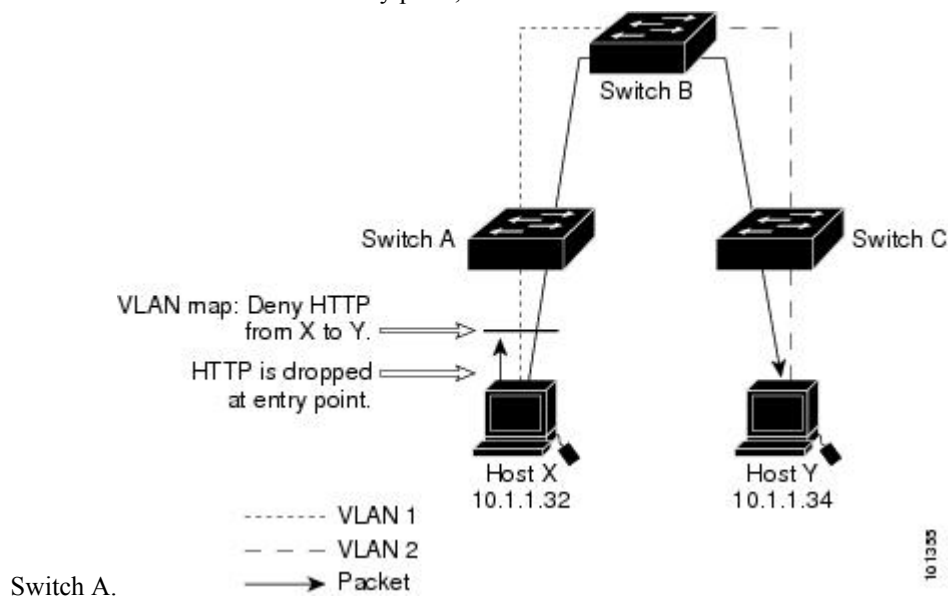
```
Device(config)# vlan access-map drop-all-default 10
Device(config-access-map)# match ip address tcp-match
Device(config-access-map)# action forward
Device(config-access-map)# exit
Device(config)# vlan access-map drop-all-default 20
Device(config-access-map)# match mac address good-hosts
Device(config-access-map)# action forward
```

## Configuration Examples for Using VLAN Maps in Your Network

### Example: Wiring Closet Configuration

*Figure 2: Wiring Closet Configuration*

In a wiring closet configuration, routing might not be enabled on the switch. In this configuration, the switch can still support a VLAN map and a QoS classification ACL. Assume that Host X and Host Y are in different VLANs and are connected to wiring closet switches A and C. Traffic from Host X to Host Y is eventually being routed by Switch B, a Layer 3 switch with routing enabled. Traffic from Host X to Host Y can be access-controlled at the traffic entry point,



If you do not want HTTP traffic switched from Host X to Host Y, you can configure a VLAN map on Switch A to drop all HTTP traffic from Host X (IP address 10.1.1.32) to Host Y (IP address 10.1.1.34) at Switch A and not bridge it to Switch B.

First, define the IP access list *http* that permits (matches) any TCP traffic on the HTTP port.

```
Device(config)# ip access-list extended http
Device(config-ext-nacl)# permit tcp host 10.1.1.32 host 10.1.1.34 eq www
Device(config-ext-nacl)# exit
```

Next, create VLAN access map *map2* so that traffic that matches the *http* access list is dropped and all other IP traffic is forwarded.

```
Device(config)# vlan access-map map2 10
Device(config-access-map)# match ip address http
Device(config-access-map)# action drop
Device(config-access-map)# exit
Device(config)# ip access-list extended match_all
Device(config-ext-nacl)# permit ip any any
Device(config-ext-nacl)# exit
Device(config)# vlan access-map map2 20
Device(config-access-map)# match ip address match_all
Device(config-access-map)# action forward
```

Then, apply VLAN access map *map2* to VLAN 1.

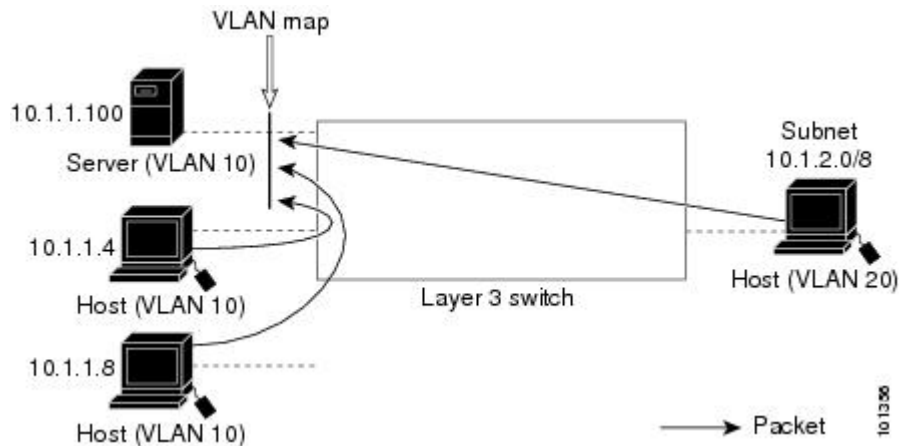
```
Device(config)# vlan filter map2 vlan 1
```

## Example: Restricting Access to a Server on Another VLAN

*Figure 3: Restricting Access to a Server on Another VLAN*

You can restrict access to a server on another VLAN. For example, server 10.1.1.100 in VLAN 10 needs to have access denied to these hosts:

- Hosts in subnet 10.1.2.0/8 in VLAN 20 should not have access.
- Hosts 10.1.1.4 and 10.1.1.8 in VLAN 10 should not have access.



## Example: Denying Access to a Server on Another VLAN

This example shows how to deny access to a server on another VLAN by creating the VLAN map SERVER1 that denies access to hosts in subnet 10.1.2.0/8, host 10.1.1.4, and host 10.1.1.8 and permits other IP traffic. The final step is to apply the map SERVER1 to VLAN 10.

Define the IP ACL that will match the correct packets.

```
Device(config)# ip access-list extended SERVER1_ACL
Device(config-ext-nacl)# permit ip 10.1.2.0 0.0.0.255 host 10.1.1.100
Device(config-ext-nacl)# permit ip host 10.1.1.4 host 10.1.1.100
Device(config-ext-nacl)# permit ip host 10.1.1.8 host 10.1.1.100
Device(config-ext-nacl)# exit
```

Define a VLAN map using this ACL that will drop IP packets that match SERVER1\_ACL and forward IP packets that do not match the ACL.

```
Device(config)# vlan access-map SERVER1_MAP
Device(config-access-map)# match ip address SERVER1_ACL
Device(config-access-map)# action drop
Device(config)# vlan access-map SERVER1_MAP 20
Device(config-access-map)# action forward
Device(config-access-map)# exit
```

Apply the VLAN map to VLAN 10.

```
Device(config)# vlan filter SERVER1_MAP vlan-list 10
```

## Configuration Examples of Router ACLs and VLAN Maps Applied to VLANs

This section gives examples of applying router ACLs and VLAN maps to a VLAN for switched, bridged, routed, and multicast packets. Although the following illustrations show packets being forwarded to their

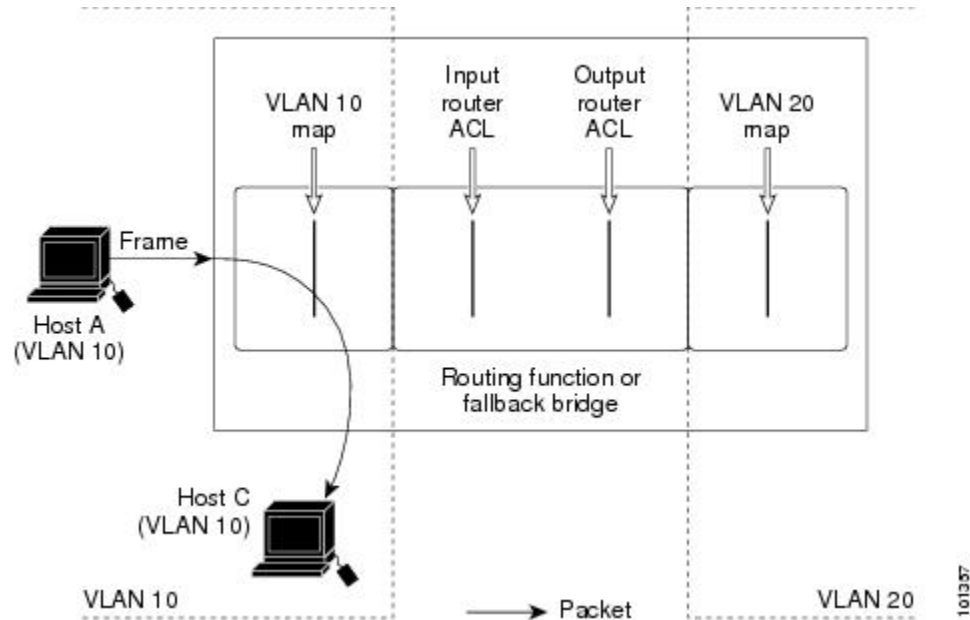


destination, each time the packet's path crosses a line indicating a VLAN map or an ACL, it is also possible that the packet might be dropped, rather than forwarded.

## Example: ACLs and Switched Packets

*Figure 4: Applying ACLs on Switched Packets*

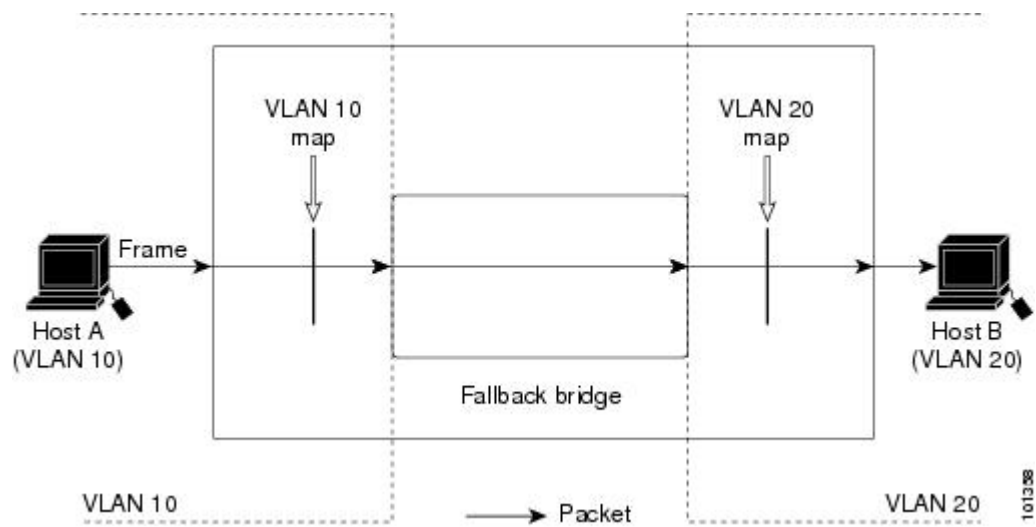
This example shows how an ACL is applied on packets that are switched within a VLAN. Packets switched within the VLAN without being routed or forwarded by fallback bridging are only subject to the VLAN map of the input VLAN.



## Example: ACLs and Bridged Packets

*Figure 5: Applying ACLs on Bridged Packets*

This example shows how an ACL is applied on fallback-bridged packets. For bridged packets, only Layer 2 ACLs are applied to the input VLAN. Only non-IP, non-ARP packets can be fallback-bridged.

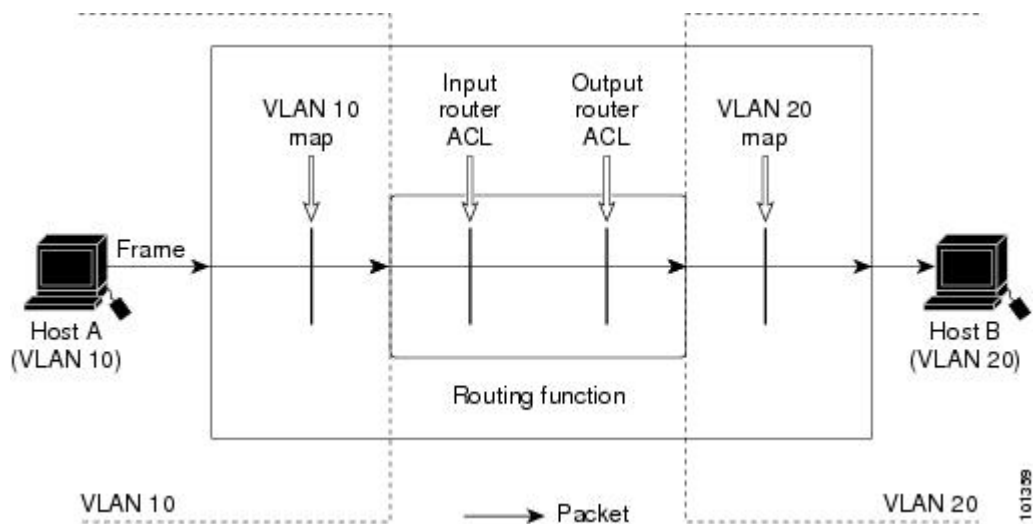


## Example: ACLs and Routed Packets

*Figure 6: Applying ACLs on Routed Packets*

This example shows how ACLs are applied on routed packets. The ACLs are applied in this order:

1. VLAN map for input VLAN
2. Input router ACL
3. Output router ACL
4. VLAN map for output VLAN



## Example: ACLs and Multicast Packets

*Figure 7: Applying ACLs on Multicast Packets*

This example shows how ACLs are applied on packets that are replicated for IP multicasting. A multicast packet being routed has two different kinds of filters applied: one for destinations that are other ports in the input VLAN and another for each of the destinations that are in other VLANs to which the packet has been routed. The packet might be routed to more than one output VLAN, in which case a different router output ACL and VLAN map would apply for each destination VLAN. The final result is that the packet might be permitted in some of the output VLANs and not in others. A copy of the packet is forwarded to those destinations where it is permitted. However, if the input VLAN map drops the packet, no destination receives a copy of the packet.

