VLAN Access Control Lists

This chapter provides information about VLAN Access Control Lists (ACLs) and how to configure them.

Information About VLAN Access Control Lists

VLAN access control lists (VACLs) or VLAN maps are used to control network traffic within a VLAN. VACLs are configured globally, and the rules are applied on VLANs. VACLs are supported in both ingress and egress directions. In ingress direction VACLs are applied after Port ACL and before Routed ACL. In egress direction VACLs are applied after Routed ACL and before Port ACL. VLAN map is applied to both routed and switched traffic. VLAN map can contain both IP and MAC ACLs to be applied to IP and non-IP traffic respectively.

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.

Configuring VACLs

VACL allows you to define VLAN maps and attach them to VLANs. This allows the ability to apply a single access policy across the VLAN and have different policies across different VLANs.

- VLAN map is attached using **vlan filter** <*word*> **vlan-list** <*vlanid*> command
- VLAN map is defined using **vlan access-map** <*word*> command

- In this mode, a match for IP Access-lists is specified using **match ip address** command. This will filter the traffic based on L3/L4 fields specified in the IP ACL. Match for IPv6 access lists can be configured using **match ipv6 address** command. This will filter traffic based on L3/L4 fields specified in IPv6 ACL
- A match for MAC Access-lists is specified using **match mac address** command. This will filter the traffic based on L2 fields specified in the MAC ACL.
- Each VLAN map sequence has an action forward or drop specified which specifies what should happen when the traffic matches a specified match criteria in the VLAN map.

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.

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.

- Use the **no** keyword to remove a match clause or specified ACLs in the clause.

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.

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 number*}	Applies the VLAN access map to the specified VLANs or WAN interfaces.

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 number*]	Verifies VLAN access map configuration by displaying the mappings between VACLs and VLANs.
Router# **show platform software fed 0/1 acl info**	Verifies that VACL is installed correctly.
Router# **show platform software fed 0/1 acl cam**	Verifies that VACL is installed correctly on TCAM.

Debugging VACLs

To enable debugs for ACl/VACL, perform this task:

Command	Purpose
Router# **set platform software trace fed 0/1 acl** <*level*>	Enable debug for FED ACL.
Router# **set platform software trace forwarding-manager RP/FP active vlan-acl** <*level*>	Enable debug for Forward-mgr VACL.