VLAN ACL (VACL)

We know ACL (Access list) is used to permit and deny traffic.By using VACL,we can control forwarding or denying of packets that are routed into or out of a VLAN or are bridged within a VLAN. VACLs are strictly for security packet filtering and for redirecting traffic to specific physical interfaces. VACLs are not defined by direction (ingress or egress).

Terms used with VLAN ACLs

Access MAP

VACLs use access maps to contain an ordered list of one or more map entries. Each map entry associates a ACLs to an action. Each entry has a sequence number, which allows you to control the precedence of entries.

Actions

Each VLAN access map entry can specify one of the following actions:

- **Forward**—Sends the traffic to the destination determined by normal operation of the switch.
- **Redirect**—Redirects the traffic to one or more specified interfaces.
- **Drop**—Drops the traffic. If you specify drop as the action, you can also specify that the device logs
the dropped packets.

In access map configuration mode, you use the action command to specify the action for a map entry

Creating of VLAN ACL includes 3 steps

1. Create Access-List
2. Create Access MAP
3. Apply on VLAN

Configuring Access list

1. ***Switch#conf terminal***
2. ***Switch(config)#ip access-list standard 10***
3. ***Switch(config-std-nacl)#permit 172.120.40.0 0.0.0.255***
4. ***Switch(config-std-nacl)#exit***

Create Access MAP

1. ***Switch(config)#vlan access-map SYSNET 1***
2. ***Switch(config-access-map)#match ip address 10***
3. ***Switch(config-access-map)#action forward***

4. ***Switch(config-access-map)#exit***
5. ***Switch(config)# vlan access-map SYSNET 2***
6. ***Switch(config-access-map)# action drop***
7. ***Switch(config-access-map)# exit***

Explanation

1. ”1” is the line number 1 of the access-map named “SYSNET”
2. ”10” is the access-list number used to identify the ACL
3. This is the action that will be applied to the traffic matched on ACL “10” .Here we need to allow traffic so we give "action forward
4. Even there is a implicit deny at the end like normal ACL,here we giving "action drop" statement to deny other traffic

Apply on VLAN

Switch(config)#vlan filter SYSNET vlan-list 20Switch(config)#(config)#exit

Applies the VLAN access-map named “SYSNET” to vlan 20.

To remove VLAN ACL

Switch(config)#no vlan access-map map-name [sequence-number]