CCNP BCMSN Notes - Securing with VLANs

VLAN Access Lists (VACLs) VACLs can filter traffic within a VLAN and do not require a routed interface. A VACL can match traffic from a MAC, IP, or IPX access list. VACL configuration:

```
Switch(config)# vlan access-map <name> [<sequ
Switch(config-access-map)# match {ip | ipx | m
Switch(config-access-map)# action {drop | forw
```

To apply a VACL to a VLAN:

```
Switch(config)# vlan filter <name> vlan-list <VLANs>
```

Private VLANs

Private VLANs (PVLANs) can

Expires: Thu, 06 Mar 2025 19:03:47 GMT

mplem

reven

thin

ating

Pri

Expor
t
d
a
t
e
:
T
h
u

M
a
r

6

1
9
:
0
3
:
4
7

2
0
2
5

/
+
0
0
0
0

G
M
T

(
r
e
g
u

Export date: Thu Mar 6 19:03:47 2025 /+0000 GMT

lar)

Export date: Thu Mar 6 19:03:47 2025 /+0000 GMT

VLANs

Export date: Thu Mar 6 19:03:47 2025 / +0000 GMT

are

Export date: Thu Mar 6 19:03:47 2025 /+0000 GMT

assoc

Export date: Thu Mar 6 19:03:47 2025 /+0000 GMT

seco

ndary

Export date: Thu Mar 6 19:03:47 2025 /+0000 GMT

vate)

Export date: Thu Mar 6 19:03:47 2025 /+0000 GMT

seco

ndary

Expires: Thu, 06 Mar 2025 19:03:47 +0000 GMT

yes:

**   Isolated** - Hosts associated with the VLAN can only reach the primary VLAN. **   Community** - Hosts can communicate with the

primary VLAN and other hosts within the secondary VLAN, but not with other secondary VLANs. PVLAN information is not communicated by VTP. PVLAN ports are configured to operate in one of two modes: **   Promiscuous** - Port attaches to a router, firewall, etc; can communicate with all hosts **   Host** - Can only communicate with a promiscuous port, or ports within the same community PVLAN **Private VLAN Configuration** Defining a secondary PVLAN:

```
Switch(config)# vlan <number>
Switch(config-vlan)# private-vlan {isolated | community}
```

Defining a primary PVLAN:

```
Switch(config)#vlan <number>
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# private-vlan association <secondary VLANs>
```

Designating a host port:

```
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association <primary VLAN> <secondary VLAN>
```

Designating a promiscuous port:

```
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping <primary VLAN> <secondary VLANs>
```

Host ports are associated with one primary and one secondary VLAN, whereas promiscuous ports are mapped to one primary and multiple secondary VLANs. Secondary VLANs can be mapped to an SVI like a promiscuous port, but without the need to specify the primary VLAN:

```
Switch(config)# interface Vlan100
Switch(config-if)# switchport private-vlan mapping <secondary VLANs>
```

Securing VLAN Trunks Explicitly configure all access ports to protect against trunk spoofing: **   **

```
Switch(config-if)# switch
Switch(config-if)# switch
```

] VLAN hopping can be mitigated by ensuring an access VLAN is not used as the native VLAN of a trunk.