CHAPTER 13

Private VLANs

This chapter describes how to identify and resolve problems related to private VLANs.

Information About Private VLANs

Private VLANs (PVLANs) are used to segregate Layer 2 Internet service provider (ISP) traffic and convey it to a single router interface. PVLANs achieve device isolation by applying Layer 2 forwarding constraints that allow end devices to share the same IP subnet while being isolated at Layer 2. In turn, the use of larger subnets reduces address management overhead. Three separate port designations are used. Each has its own unique set of rules that regulate each connected endpoint's ability to communicate with other connected endpoints within the same private VLAN domain.

Private VLAN Domain

A private VLAN domain consists of one or more pairs of VLANs. The primary VLAN makes up the domain; each VLAN pair makes up a subdomain. The VLANs in a pair are called the primary VLAN and the secondary VLAN. All VLAN pairs within a private VLAN have the same primary VLAN. The secondary VLAN ID is what differentiates one subdomain from another.

Spanning Multiple Switches

Private VLANs can span multiple switches, just like regular VLANs. Inter-switch link ports do not need to be aware of the special VLAN type and can carry frames tagged with these VLANs just as they do with any other frames. Private VLANs ensure that traffic from an isolated port in one switch does not reach another isolated or community port in a different switch even after traversing an inter-switch link. By embedding the isolation information at the VLAN level and by transporting it with the packet, it is possible to maintain consistent behavior throughout the network. Therefore, the mechanism that restricts Layer 2 communication between two isolated ports in the same switch also restricts Layer 2 communication between two isolated ports in two different switches.

Private VLAN Ports

Within a private VLAN domain, there are three separate port designations. Each port designation has its own unique set of rules that regulate the ability of one endpoint to communicate with other connected endpoints within the same private VLAN domain. The following are the three port designations:

- Promiscuous
- Isolated
- Community

For additional information about private VLANs, see the *Cisco Nexus 1000V for Microsoft Hyper-V Layer 2 Switching Configuration Guide*.

Troubleshooting Guidelines

Follow these guidelines when troubleshooting private VLAN issues:

- Verify that a private VLAN is configured correctly by entering the **show vlan private-vlan** command.
- Verify that the interface is up by entering the **show interface** *slot-port* command.
- Verify that the VEM is configured correctly by entering the **module vem** *module-number* **execute vemcmd show port** command.

Private VLAN Troubleshooting Commands

You can use the commands in this section to troubleshoot problems related to private VLANs.

To verify that a private VLAN is configured correctly, enter this command:

- **show vlan private-vlan**

```
n1000V# show vlan private-vlan
Primary  Secondary  Type              Ports
-------  ---------  ----------------  ------------------------------------------
152      157        community
152      158        isolated
156      153        community
156      154        community
156      155        isolated
```

To verify if a physical Ethernet interface in a private VLAN trunk promiscuous mode is up, enter this command:

- **show interface**

```
n1000V# show interface eth3/4
Ethernet3/4 is up
  Hardware: Ethernet, address: 0050.565a.ca50 (bia 0050.565a.ca50)
  Port-Profile is DATA-Macpin
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 0/255, txload 0/255, rxload 0/255
  Encapsulation ARPA
  Port mode is Private-vlan trunk promiscuous
  full-duplex, 1000 Mb/s
    Rx
    158776 Input Packets 75724 Unicast Packets
    76 Multicast Packets 82976 Broadcast Packets
    13861581 Bytes
    Tx
    75763 Output Packets 75709 Unicast Packets
    3 Multicast Packets 51 Broadcast Packets 0 Flood Packets
    7424670 Bytes
    5507 Input Packet Drops 0 Output Packet Drops
```

To verify if a virtual Ethernet interface in private VLAN host mode is up, enter this command:

- **show interface**

```
n1000V# show interface v3
Vethernet3 is up
    Port description is fedora9
    Hardware is Virtual, address is 0050.56bb.6330
    Owner is VM "fedora9", adapter is Network Adapter 1
    Active on module 3
    DVS port 10
    Port-Profile is pvlancomm153
    Port mode is Private-vlan host
    Rx
    14802 Input Packets 14539 Unicast Packets
    122 Multicast Packets 141 Broadcast Packets
    1446568 Bytes
    Tx
    15755 Output Packets 14492 Unicast Packets
    0 Multicast Packets 1263 Broadcast Packets 0 Flood Packets
    1494886 Bytes
    45 Input Packet Drops 0 Output Packet Drops
```

To verify if a VEM is configured correctly, enter this command:

- **module vem** *module-number* **execute vemcmd show port**

```
n1000V# module vem 3 execute vemcmd show port
LTL     VSM     Admin     Link     State     PC-LTL     Vlan     SG_ID     Vem Port
Type
8       Eth3/1     UP       UP        UP         305         3969      2
9       Eth3/2     UP       UP        UP         305         3969      2
10      Eth3/3     UP       UP        UP         306         150       2
11      Eth3/4     UP       UP        UP         306         3968      2
12      Eth3/5     UP       UP        UP         306         151       2
13      Eth3/6     UP       UP        UP         0           1         2
14      Veth33     UP       UP        UP         0           3967      2
16      Veth34     UP       UP        UP         0           1 T       2
```

If additional information is required for Cisco Technical Support to troubleshoot a private VLAN issue, use the following commands:

- **show system internal private-vlan info**
- **show system internal private-vlan event-history traces**