



CHAPTER 14

Private VLANs

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

This chapter includes the following sections:

- [Information About Private VLANs, page 14-1](#)
- [Troubleshooting Guidelines, page 14-2](#)
- [Private VLAN Troubleshooting Commands, page 14-2](#)

Information About Private VLANs

Private VLANs (PVLANS) are used to segregate Layer 2 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 Layer 2 isolated. In turn, the use of larger subnets reduces address management overhead. Three separate port designations are used, each having its own unique set of rules regulating 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; and 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 need not be aware of the special VLAN type and carry frames tagged with these VLANs just like they do 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 along with the packet, it is possible to maintain consistent behavior throughout the network. Therefore, the mechanism which 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.

Send document comments to nexus1k-docfeedback@cisco.com.

Private VLAN Ports

Within a private VLAN domain, there are three separate port designations. Each port designation has its own unique set of rules which 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 Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(3)*.

Troubleshooting Guidelines

Follow these guidelines when troubleshooting private VLAN issues:

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

Private VLAN Troubleshooting Commands

Use the commands listed in this section to troubleshoot problems related to private VLANs.

To verify that a private VLAN is configured correctly, use the following 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, use the following command:

- **show interface**

```
n1000V# show int eth3/4
Ethernet3/4 is up
Hardware: Ethernet, address: 0050.565a.ca50 (bia 0050.565a.ca50)
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
Beacon is turned off
Auto-Negotiation is turned off
Input flow-control is off, output flow-control is off
Auto-mdix is turned on
```

Send document comments to nexus1k-docfeedback@cisco.com.

```
Switchport monitor is off
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
2 interface resets
```

To verify if a virtual Ethernet interface in private VLAN host mode is up, use the following command:

- **show interface**

```
n1000V# show int v3
Vethernet3 is up
Hardware is Virtual, address is 0050.56bb.6330
Owner is VM "fedora9", adapter is Network Adapter 1
Active on module 3
VMware 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, use the following command:

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

```
n1000V# module vem 3 execute vemcmd show port
  LTL   IfIndex  Vlan   Bndl  SG_ID  Pinned_SGID  Type  Admin  State  CBL  Mode  Name
    8     0    3969     0     2      2      VIRT  UP     UP     4  Access  120
    9     0    3969     0     2      2      VIRT  UP     UP     4  Access  121
   10     0     150     0     2      2      VIRT  UP     UP     4  Access  122
   11     0    3968     0     2      2      VIRT  UP     UP     4  Access  123
   12     0     151     0     2      2      VIRT  UP     UP     4  Access  124
   13     0         1     0     2      2      VIRT  UP     UP     0  Access  125
   14     0    3967     0     2      2      VIRT  UP     UP     4  Access  126
   16  1a020100     1 T     0     2      2      PHYS  UP     UP     4  Trunk
vmnic1
   18  1a020300     1 T     0     2      2      PHYS  UP     UP     4  Trunk
vmnic3
  pvlan promiscuous trunk port
    153 --> 156
    154 --> 156
    155 --> 156
    157 --> 152
    158 --> 152
   19  1a020400     1 T     0     2      2      PHYS  UP     UP     4  Trunk
vmnic4
  pvlan promiscuous trunk port
    153 --> 156
    154 --> 156
    155 --> 156
    157 --> 152
    158 --> 152
```

Send document comments to nexus1k-docfeedback@cisco.com.

```
47 1b020000 154 0 2 0 VIRT UP UP 4 Access  
fedora9.eth0  
pvlan community 156 153
```

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**