Private VLANs (PVLANs)

This chapter describes how to identify and resolve problems related to private VLANs and includes the following sections:

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 Layer 2 isolated. 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 Domains

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 do not need to be aware of the special VLAN type and can carry frames tagged with these VLANs as like 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 along with the packet, you can maintain consistent behavior throughout the network. 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 1000VE Layer 2 Switching Configuration Guide*.

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** *switchport* command to verify the interface is up.
- Use the **module vse** *module-number* **execute vemcmd show port** command to verify the VSE is configured correctly.

Private VLAN Troubleshooting Commands

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

Command	Purpose
show vlan private-vlan	Displays that a private VLAN is configured correctly. See Example 12-1 on page 12-2.
show interface *name*	Displays that a physical Ethernet interface in a private VLAN trunk promiscuous mode is up. See Example 12-2 on page 12-3.
show interface *veth-name*	Displays that a virtual Ethernet interface in private VLAN host mode is up. See Example 12-3 on page 12-3.
module vse *module-number* **execute vemcmd show port**	Displays that a VSE is configured correctly. See Example 12-4 on page 12-3.

Example 12-1   show vlan private-vlan Command

```
switch# show vlan private-vlan
    Primary  Secondary  Type           Ports
    -------  ---------  -------------- -----------------------------------------
    152      157        community
```

```
152     158       isolated
156     153       community
156     154       community
156     155       isolated
```

Example 12-2 show interface *name* ***Command***

```
switch# show interface eth3/1
    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
      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
```

Example 12-3 show interface *veth* ***Command***

```
switch# show interface vethernet3
    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
```

Example 12-4 module vse *module-number* ***execute vemcmd show port Command***

```
switch# module vse 3 execute vemcmd show port-old
    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
        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**
- **show system internal private-vlan event-history errors**
- **show system internal private-vlan event-history events**