在 Catalyst 交换机上配置隔离的专用 VLAN

目录

简介

在某些情况下，如果没有将设备放置在不同的 IP 子网上，则需要阻止交换机上终端设备之间的第 2 层 (L2) 连接。此设置可避免浪费 IP 地址。使用专用 VLAN (PVLAN) 可以对同一 IP 子网内的第 2 层设备进行隔离。可以对交换机上的某些端口进行限制，使其只能到达连接了默认网关、备份服务器或 Cisco LocalDirector 的特定端口。

本文档描述了在带有 Catalyst OS (CatOS) 或 Cisco IOS® 软件的 Cisco Catalyst 交换机上配置隔离 PVLAN 的过程。

先决条件

要求

本文档假设您拥有现成的网络并能够在不同端口之间建立连接，作为 PVLAN 的补充。如果有多台交换机，请确保交换机之间的中继正常运行，并允许中继上的 PVLAN。

并非所有交换机和软件版本都支持 PVLAN。开始配置之前，请参阅专用 VLAN Catalyst 交换机支持表，以确定您的平台和软件版本是否支持 PVLAN。

注意： 某些交换机（如专用 VLAN Catalyst 交换机支持表中所指定）目前仅支持 PVLAN 边缘功能。术语“受保护端口”也是指此功能。PVLAN 边缘端口有限制，会阻止与同一交换机上其他受保护端口之间的通信。但不同交换机上的受保护端口能够彼此通信。请勿将此功能与本文档所示的正常 PVLAN 配置相混淆。有关受保护端口的详细信息，请参阅配置基于端口的流量控制文档中的*配置端口安全性*部分。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 配备运行 CatOS 版本 6.3(5) 的 Supervisor 引擎 2 模块的 Catalyst 4003 交换机
- 配备运行 Cisco IOS 软件版本 12.1(12c)EW1 的 Supervisor 引擎 3 模块的 Catalyst 4006 交换机

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景理论

PVLAN 是一种采用第 2 层隔离配置与同一广播域或子网内的其他端口隔离的 VLAN。可以在 PVLAN 中分配一组特定的端口，从而控制第 2 层端口之间的访问。可以在同一交换机上配置 PVLAN 和正常 VLAN。

有三种类型的 PVLAN 端口：混合型、隔离型和社区型。

- 混合端口可以与其他所有 PVLAN 端口进行通信。混合端口通常用来与外部路由器、LocalDirector、网络管理设备、备份服务器、管理工作站及其他设备进行通信。在某些交换机上，到路由模块（例如，Multilayer Switch Feature Card [MSFC]）的端口需为混合端口。
- 隔离端口与同一 PVLAN 内的其他端口之间完全通过第 2 层隔离。此隔离包括广播，唯一的例外是混合端口。第 2 层级别上发生隐私授予时，将封锁到所有隔离端口的传出数据流。来自隔离端口的数据流仅转发到所有混合端口。
- 社区端口可以彼此间通信，也能够与混合端口进行通信。这些端口通过第 2 层隔离与其他社区内的其他所有端口或 PVLAN 内的隔离端口隔离。广播仅在相关的社区端口和混合端口之间传播。**注意：** 本文档不涉及社区 VLAN 配置。

有关 PVLAN 的详细信息，请参阅了解和配置 VLAN 文档中的*配置专用 VLAN* 部分。

规则和限制

本部分提供了一些在实施 PVLAN 时必须留意的规则和限制。要获取更完整的列表，请参阅配置 VLAN 文档中的*专用 VLAN 配置指南*部分。

- PVLAN 不得包括 VLAN 1 或 1002 - 1005。
- 必须将 VLAN 中继协议 (VTP) 模式设置为 transparent。
- 每个主 VLAN 只能指定一个隔离 VLAN。
- 只能将没有当前接入端口分配的 VLAN 指定为 PVLAN。将 VLAN 指定为 PVLAN 之前，请先删除该 VLAN 中的所有端口。

- 请勿将 PVLAN 端口配置为 EtherChannel。
- 由于硬件限制，如果同一 COIL 专用集成电路 (ASIC) 内的某个端口为下列之一，则 Catalyst 6500/6000 快速以太网交换机模块将限制隔离或社区 VLAN 端口的配置：中继交换端口分析程序 (SPAN) 目标混合 PVLAN 端口此表指示属于 Catalyst 6500/6000 FastEthernet 模块上同一 ASIC 的端口范围：**show pvlan capability** 命令（适用于 CatOS）也能指示某个端口能否指定为 PVLAN 端口。Cisco IOS 软件中没有等效命令。
- 如果删除了 PVLAN 配置中使用的某个 VLAN，则与该 VLAN 相关联的端口将变为非活动状态。
- 仅对主 VLAN 配置第 3 层 (L3) VLAN 接口。如果 VLAN 具有隔离或社区 VLAN 配置，则隔离和社区 VLAN 的 VLAN 接口将处于非活动状态。有关详细信息，请参阅配置专用 VLAN。
- 可以使用中继在交换机之间扩展 PVLAN。中继端口承载来自常规 VLAN 的数据流，以及来自主 VLAN、隔离 VLAN 和社区 VLAN 的数据流。如果进行中继的两个交换机都支持 PVLAN，Cisco 建议使用标准中继端口。**注意：** 必须在涉及的每台交换机上都手动输入相同的 PVLAN 配置，因为 transparent 模式下的 VTP 不传播此信息。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 有关本文档所用命令的详细信息，请使用命令查找工具（仅限注册用户）。

网络图

本文档使用以下网络设置：

在这种情况下，隔离 VLAN（“101”）中的设备在第 2 层上的彼此通信受到限制。但设备能够连接到 Internet。此外，4006 上的端口“Gig 3/26”具有混合标识。使用此可选配置可将 GigabitEthernet 3/26 中的设备连接到隔离 VLAN 中的所有设备。例如，使用此配置还可以将所有 PVLAN 主机设备上的数据备份到管理工作站。混合端口的其他用途包括与外部路由器、LocalDirector、网络管理设备及其他设备进行连接。

配置主 VLAN 和隔离 VLAN

执行以下步骤可创建主 VLAN 和辅助 VLAN，并将各种端口绑定到这些 VLAN。这些步骤包括 CatOS 和 Cisco IOS 软件的示例。发出为 OS 安装设置的相应命令。

1. 创建主 PVLAN。CatOS

```
Switch_CatOS> (enable) set vlan primary_vlan_id pvlan-type primary name primary_vlan
!--- Note: Thise command should be on one line.

VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 100 configuration successful
```

Cisco IOS 软件

```
Switch_IOS(config)#vlan primary_vlan_id
Switch_IOS(config-vlan)#private-vlan primary
Switch_IOS(config-vlan)#name primary-vlan
Switch_IOS(config-vlan)#exit
```

2. 创建一个或多个隔离 VLAN。CatOS

```
Switch_CatOS> (enable) set vlan secondary_vlan_id pvlan-type isolated name isolated_pvlan
!--- Note: This command should be on one line.
```

```
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 101 configuration successful
```
Cisco IOS 软件
```
Switch_IOS(config)#vlan secondary_vlan_id
Switch_IOS(config-vlan)#private-vlan isolated
Switch_IOS(config-vlan)#name isolated_pvlan
Switch_IOS(config-vlan)#exit
```

3. 将一个或多个隔离 VLAN 绑定到主 VLAN。CatOS
```
Switch_CatOS> (enable) set pvlan primary_vlan_id secondary_vlan_id
Vlan 101 configuration successful
Successfully set association between 100 and 101.
```
Cisco IOS 软件
```
Switch_IOS(config)#vlan primary_vlan_id
Switch_IOS(config-vlan)#private-vlan association secondary_vlan_id
Switch_IOS(config-vlan)#exit
```

4. 验证专用 VLAN 配置。CatOS
```
Switch_CatOS> (enable) show pvlan
Primary Secondary Secondary-Type   Ports
------- --------- ---------------- ------------
100     101       isolated
```
Cisco IOS 软件
```
Switch_IOS#show vlan private-vlan
Primary  Secondary  Type             Ports
------- --------- ---------------- -------
100     101       isolated
```

将端口分配到 PVLAN

提示：实施此过程之前，请发出 **show pvlan capability mod/port** 命令（适用于 CatOS），以确定某个端口能否变为 PVLAN 端口。

注意：执行此过程的步骤 1 之前，请在接口配置模式下发出 **switchport** 命令，将端口配置为第 2 层交换接口。

1. 在所有合适的交换机上配置主机端口。CatOS
```
Switch_CatOS> (enable)set pvlan primary_vlan_id secondary_vlan_id mod/port
!--- Note: This command should be on one line.

Successfully set the following ports to Private Vlan 100,101: 2/20
```
Cisco IOS 软件
```
Switch_IOS(config)#interface gigabitEthernet mod/port
Switch_IOS(config-if)#switchport private-vlan host
primary_vlan_id secondary_vlan_id
!--- Note: This command should be on one line.

Switch_IOS(config-if)#switchport mode private-vlan host
Switch_IOS(config-if)#exit
```

2. 在其中一台交换机上配置混合端口。CatOS
```
Switch_CatOS> (enable) set pvlan mapping
primary_vlan_id secondary_vlan_id mod/port
!--- Note: This command should be on one line.

Successfully set mapping between 100 and 101 on 3/26
```
注意：对于 Catalyst 6500/6000，Supervisor 引擎将 CatOS 作为系统软件运行时，如果希望在 VLAN 之间进行第 3 层交换，则 Supervisor 引擎上的 MSFC 端口（15/1 或 16/1）应为混合端口。Cisco IOS 软件
```
Switch_IOS(config)#interface interface_type mod/port
Switch_IOS(config-if)#switchport private-vlan
mapping primary_vlan_id secondary_vlan_id
!--- Note: This command should be on one line.

Switch_IOS(config-if)#switchport mode private-vlan promiscuous
Switch_IOS(config-if)#end
```

第 3 层配置

此可选部分描述了允许 PVLAN 输入数据流路由的配置步骤。如果只需启用第 2 层连接，则可以省略此阶段。

1. VLAN 接口的配置方式与正常第 3 层路由的配置方式相同。此配置涉及：配置 IP 地址使用 **no shutdown** 命令激活接口验证 VLAN 是否存在于 VLAN 数据库中有关配置示例，请参阅 VLAN/VTP 技术支持。
2. 将要路由的辅助 VLAN 映射到主 VLAN。
   ```
   Switch_IOS(config)#interface vlan primary_vlan_id
   Switch_IOS(config-if)#private-vlan mapping secondary_vlan_list
   Switch_IOS(config-if)#end
   ```
   注意： 仅对主 VLAN 配置第 3 层 VLAN 接口。在隔离或社区 VLAN 配置下，隔离及社区 VLAN 的 VLAN 接口将处于非活动状态。
3. 发出 **show interfaces private-vlan mapping**（适用于 Cisco IOS 软件）或 show pvlan mapping（适用于 CatOS）命令以验证映射。
4. 如果配置映射后需要修改辅助 VLAN 列表，请使用 **add** 或 remove 关键字。
   ```
   Switch_IOS(config-if)#private-vlan mapping add secondary_vlan_list
   or
   Switch_IOS(config-if)#private-vlan mapping remove secondary_vlan_list
   ```

有关详细信息，请参阅配置专用 VLAN 文档中的*将辅助 VLAN 映射到主 VLAN 的第 3 层 VLAN 接口*部分。

注意： 对于有 MSFC 的 Catalyst 6000 交换机，请确保从 Supervisor 引擎到路由引擎的端口（例如，端口 15/1 或 16/1）为混合端口。

```
cat6000> (enable) set pvlan mapping primary_vlan secondary_vlan 15/1
Successfully set mapping between 100 and 101 on 15/1
```

发出命令 **show pvlan mapping** 以验证映射。

```
cat6000> (enable) show pvlan mapping
Port Primary Secondary
---- ------- ---------
15/1  100      101
```

配置

本文档使用以下配置：

- Access_Layer (Catalyst 4003:CatOS)
- Core（Catalyst 4006:Cisco IOS 软件）

Access_Layer (Catalyst 4003:CatOS)

```
Access_Layer> (enable) show config
 This command shows non-default configurations only.
 Use 'show config all' to show both default and non-
default configurations.
 ..............

 !--- Output suppressed. #system set system name
Access_Layer ! #frame distribution method set port
channel all distribution mac both ! #vtp set vtp domain
Cisco set vtp mode transparent set vlan 1 name default
type ethernet mtu 1500 said 100001 state active set vlan
100 name primary_for_101 type ethernet pvlan-type
primary mtu 1500 said 100100 state active !--- This is
the primary VLAN 100. !--- Note: This command should be
on one line.
```

```
 set vlan 101 name isolated_under_100 type ethernet
pvlan-type isolated mtu
 1500 said 100101 state active
!--- This is the isolated VLAN 101. !--- Note: This
command should be on one line.

 set vlan 1002 name fddi-default type fddi mtu 1500 said
101002 state active

!--- Output suppressed. #module 1 : 0-port Switching
Supervisor ! #module 2 : 24-port 10/100/1000 Ethernet
set pvlan 100 101 2/20
!--- Port 2/20 is the PVLAN host port in primary VLAN
100, isolated !--- VLAN 101. set trunk 2/3 desirable
dot1q 1-1005 set trunk 2/4 desirable dot1q 1-1005 set
trunk 2/20 off dot1q 1-1005 !--- Trunking is
automatically disabled on PVLAN host ports.

 set spantree portfast    2/20 enable
!--- PortFast is automatically enabled on PVLAN host
ports.

 set spantree portvlancost 2/1  cost 3

!--- Output suppressed. set spantree portvlancost 2/24
cost 3 set port channel 2/20 mode off !--- Port
channeling is automatically disabled on PVLAN !--- host
ports.

 set port channel 2/3-4 mode desirable silent
 !
 #module 3 : 34-port 10/100/1000 Ethernet
 end
```

Core（Catalyst 4006:Cisco IOS 软件）

```
Core#show running-config
 Building configuration...

 !--- Output suppressed. ! hostname Core ! vtp domain
Cisco vtp mode transparent !--- VTP mode is transparent,
as PVLANs require. ip subnet-zero ! vlan 2-4,6,10-11,20-
22,26,28 ! vlan 100 name primary_for_101 private-vlan
primary private-vlan association 101 ! vlan 101 name
isolated_under_100 private-vlan isolated ! interface
Port-channel1 !--- This is the port channel for
interface GigabitEthernet3/1 !--- and interface
GigabitEthernet3/2. switchport switchport trunk
encapsulation dot1q switchport mode dynamic desirable !
interface GigabitEthernet1/1 ! interface
GigabitEthernet1/2 ! interface GigabitEthernet3/1 !---
This is the trunk to the Access_Layer switch. switchport
trunk encapsulation dot1q switchport mode dynamic
desirable channel-group 1 mode desirable ! interface
GigabitEthernet3/2 !--- This is the trunk to the
Access_Layer switch. switchport trunk encapsulation
dot1q switchport mode dynamic desirable channel-group 1
mode desirable ! interface GigabitEthernet3/3 ! !---
There is an omission of the interface configuration !---
that you do not use. ! interface GigabitEthernet3/26
  switchport private-vlan mapping 100 101
  switchport mode private-vlan promiscuous
!--- Designate the port as promiscuous for PVLAN 101. !
!--- There is an omission of the interface configuration
!--- that you do not use. ! !--- Output suppressed.
```

```
interface Vlan25 !--- This is the connection to the
Internet. ip address 10.25.1.1 255.255.255.0 ! interface
Vlan100 !--- This is the Layer 3 interface for the
primary VLAN. ip address 10.1.1.1 255.255.255.0 private-
vlan mapping 101 !--- Map VLAN 101 to the VLAN interface
of the primary VLAN (100). !--- Ingress traffic for
devices in isolated VLAN 101 routes !--- via interface
VLAN 100.
```

多个交换机之间的专用 VLAN

有两种方法可以在多个交换机之间采用专用 VLAN。本部分讨论了以下方法：

- 常规中继
- 专用 VLAN 中继

常规中继

与常规 VLAN 一样，PVLAN 也可以在多个交换机之间使用。中继端口将主 VLAN 和辅助 VLAN 传输到相邻的交换机。中继端口处理专用 VLAN 的方式与其他任何 VLAN 相同。来自一台交换机中某个隔离端口的数据流无法到达另一台交换机中的隔离端口，这是多个交换机之间使用 PVLAN 的一项特性。

在所有中间设备（包括没有 PVLAN 端口的设备）上配置 PVLAN，以维护 PVLAN 配置的安全性并避免将配置为 PVLAN 的 VLAN 另作他用。

中继端口承载来自常规 VLAN 的数据流，以及来自主 VLAN、隔离 VLAN 和社区 VLAN 的数据流。

提示： 如果进行中继的两个交换机都支持 PVLAN，Cisco 建议使用标准中继端口。

由于 VTP 不支持 PVLAN，因此必须在第 2 层网络中的所有交换机上手动配置 PVLAN。如果网络中的某些交换机上未配置主 VLAN 和辅助 VLAN 关联，则这些交换机上的第 2 层数据库不会进行合并。此情况可能导致这些交换机上产生不必要的 PVLAN 数据流泛洪。

专用 VLAN 中继

PVLAN 中继端口可以承载多个辅助 PVLAN 及非 PVLAN。在数据包的接收和传输过程中，PVLAN 中继端口上包含辅助或常规 VLAN 标记。

仅支持 IEEE 802.1q 封装。使用隔离中继端口可以通过单个中继对所有辅助端口的数据流进行组合。使用混合中继端口可以将此拓扑中所需的多个混合端口组合到单个承载多个主 VLAN 的中继端口中。

如果预计使用专用 VLAN 隔离主机端口承载多个 VLAN（正常 VLAN 或用于多个专用 VLAN 域），请使用隔离专用 VLAN 中继端口。这可用于连接某个不支持专用 VLAN 的下行交换机。

在专用 VLAN 混合主机端口正常使用但需要承载多个 VLAN（正常 VLAN 或用于多个专用 VLAN 域）的情况下，可以使用专用 VLAN 混合中继。这可用于连接某个不支持专用 VLAN 的上行路由器。

有关详细信息，请参阅专用 VLAN 中继。

要将接口配置为 PVLAN 中继端口，请参阅将第 2 层接口配置为 PVLAN 中继端口。

要将接口配置为混合中继端口，请参阅将第 2 层接口配置为混合中继端口。

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

CatOS

- **show pvlan** — 显示 PVLAN 配置。验证隔离 VLAN 和主 VLAN 是否彼此关联。并验证是否出现任何主机端口。
- **show pvlan mapping** — 以混合端口上的配置显示 PVLAN 映射。

Cisco IOS 软件

- **show vlan private-vlan** — 显示 PVLAN 信息，其中包括相关联的端口。
- **show interface mod/port switchport** — 显示特定于接口的信息。验证操作模式及运行 PVLAN 设置是否均正确。
- **show interfaces private-vlan mapping** — 显示已配置的 PVLAN 映射。

验证过程

完成这些步骤：

1. 验证交换机上的 PVLAN 配置。检查确定主 PVLAN 和辅助 PVLAN 是否彼此关联或是否互相映射到对方。并验证是否包括必需的端口。`Access_Layer> (enable) **show pvlan**`

```
Primary Secondary Secondary-Type   Ports
------- --------- ---------------- ------------
 100     101       isolated         2/20

Core#show vlan private-vlan

Primary Secondary Type              Ports
------- --------- ----------------- -----------
100     101       isolated          Gi3/26
```

2. 验证混合端口的配置是否正确。此输出指示，端口操作模式为 **promiscuous**，而运行的 VLAN 为 100 和 101。`Core#**show interface gigabitEthernet 3/26 switchport**`

```
Name: Gi3/26
Switchport: Enabled
Administrative Mode: private-Vlan promiscuous
Operational Mode: private-vlan promiscuous
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative Private VLAN Host Association: none
Administrative Private VLAN Promiscuous Mapping: 100
(primary_for_101) 101 (isolated_under_100)
Private VLAN Trunk Native VLAN: none
```

```
Administrative Private VLAN Trunk Encapsulation: dot1q
Administrative Private VLAN Trunk Normal VLANs: none
Administrative Private VLAN Trunk Private VLANs: none
Operational Private VLANs:
100 (primary_for_101) 101 (isolated_under_100)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

3. 启动从主机端口到混合端口的 Internet 控制消息协议 (ICMP) ping 数据包。请记住，由于两台设备处于同一个主 VLAN 中，因此它们必须处于同一子网中。host_port#**show arp**

```
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.1.100              -   0008.a390.fc80  ARPA   FastEthernet0/24
!--- The Address Resolution Protocol (ARP) table on the client indicates !--- that no MAC
addresses other than the client addresses are known. host_port#ping 10.1.1.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.254, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/4 ms
!--- The ping is successful. The first ping fails while the !--- device attempts to map via
ARP for the peer MAC address. host_port#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.1.100              -   0008.a390.fc80  ARPA   FastEthernet0/24
Internet  10.1.1.254              0   0060.834f.66f0  ARPA   FastEthernet0/24
!--- There is now a new MAC address entry for the peer.
```

4. 启动主机端口之间的 ICMP ping。在本示例中，host_port_2 (10.1.1.99) 尝试对 host_port (10.1.1.100) 进行 ping 操作。此 ping 操作失败。但从另一个主机端口到混合端口的 ping 操作仍然成功。host_port_2#**ping 10.1.1.100**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.100, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
!--- The ping between host ports fails, which is desirable. host_port_2#ping 10.1.1.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.254, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
!--- The ping to the promiscuous port still succeeds. host_port_2#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.1.99               -   0005.7428.1c40  ARPA   Vlan1
Internet  10.1.1.254              2   0060.834f.66f0  ARPA   Vlan1
!--- The ARP table includes only an entry for this port and !--- the promiscuous port.
```

故障排除

对 PVLAN 进行故障排除

本部分解决了一些常见的 PVLAN 配置问题。

问题 1

收到此错误信息：`%PM-SP-3-ERR_INCOMP_PORT <mod/port> is set to inactive because <mod/port> is a trunk port`

显示此错误信息可能有多种原因，讨论如下。

解释 - 1：由于硬件限制，如果同一 COIL ASIC 内的某个端口为中继、SPAN 目标或混合 PVLAN 端口，则 Catalyst 6500/6000 10/100-Mbps 模块将限制隔离或社区 VLAN 端口的配置。（COIL ASIC 在大多数模块上控制 12 个端口，而在 Catalyst 6548 模块上控制 48 个端口。）本文档规则和限制部分中的表提供了 Catalyst 6500/6000 10/100-Mbps 模块上端口限制的细分信息。

解决过程 - 1：如果该端口不支持 PVLAN，请从该模块的不同 ASIC 中或从不同模块中挑选一个端口。要将端口重新激活，请删除隔离 VLAN 或社区 VLAN 端口配置并发出 **shutdown 命令**和 no shutdown 命令。

解释 - 2：端口是手动配置还是默认为 *dynamic desirable* 或 dynamic auto 模式。

解决过程 - 2：使用 **switchport mode access** 命令将端口配置为 access 模式。要将端口重新激活，请发出 **shutdown 命令**和 no shutdown 命令。

注意： 在 Cisco IOS 软件版本 12.2(17a)SX 及更高版本中，12 个端口的限制并不适用于 WS-X6548-RJ-45、WS-X6548-RJ-21 和 WS-X6524-100FX-MM 以太网交换模块。有关包含其他功能的 PVLAN 配置限制的详细信息，请参阅配置专用 VLAN (PVLAN) 中的其他功能的限制部分。

问题 2

在 PVLAN 配置过程中，出现以下消息之一：

- host_port_2#**ping 10.1.1.100**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.100, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
!--- The ping between host ports fails, which is desirable. host_port_2#ping 10.1.1.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.254, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
!--- The ping to the promiscuous port still succeeds. host_port_2#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.1.99               -   0005.7428.1c40  ARPA   Vlan1
Internet  10.1.1.254              2   0060.834f.66f0  ARPA   Vlan1
!--- The ARP table includes only an entry for this port and !--- the promiscuous port.
```

- host_port_2#**ping 10.1.1.100**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.100, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
!--- The ping between host ports fails, which is desirable. host_port_2#ping 10.1.1.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.254, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
!--- The ping to the promiscuous port still succeeds. host_port_2#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.1.99               -   0005.7428.1c40  ARPA   Vlan1
Internet  10.1.1.254              2   0060.834f.66f0  ARPA   Vlan1
!--- The ARP table includes only an entry for this port and !--- the promiscuous port.
```

说明：由于硬件限制，如果同一 COIL ASIC 内的某个端口为中继、SPAN 目标或混合 PVLAN 端口，则 Catalyst 6500/6000 10/100-Mbps 模块将限制隔离或社区 VLAN 端口的配置。（COIL ASIC 在大多数模块上控制 12 个端口，而在 Catalyst 6548 模块上控制 48 个端口。）本文档规则和限制部分中的表提供了 Catalyst 6500/6000 10/100-Mbps 模块上端口限制的细分信息。

解决过程：发出 **show pvlan capability** 命令（适用于 CatOS），此命令可指示某个端口能否变为 PVLAN 端口。如果该特定端口不支持 PVLAN，请从该模块上的不同 ASIC 中或从不同模块中挑选一个端口。

注意： 在 Cisco IOS 软件版本 12.2(17a)SX 及更高版本中，12 个端口的限制并不适用于 WS-X6548-RJ-45、WS-X6548-RJ-21 和 WS-X6524-100FX-MM 以太网交换模块。有关包含其他功能的 PVLAN 配置限制的详细信息，请参阅配置专用 VLAN (PVLAN) 中的其他功能的限制部分。

问题 3

无法在某些平台上配置 PVLAN。

解决方法：验证该平台是否支持 PVLAN。开始配置之前，请参阅专用 VLAN Catalyst 交换机支持表，以确定您的平台和软件版本是否支持 PVLAN。

问题 4

在 Catalyst 6500/6000 MSFC 上，无法对连接到交换机上隔离端口的设备进行 ping 操作。

解决方法：在 Supervisor 引擎上，验证到 MSFC（15/1 或 16/1）的端口是否为混合端口。

```
cat6000> (enable) set pvlan mapping primary_vlan secondary_vlan 15/1
Successfully set mapping between 100 and 101 on 15/1
```

并请按照本文档中第 3 层配置部分的规定，对 MSFC 上的 VLAN 接口进行配置。

问题 5

发出 **no shutdown** 命令后，无法激活隔离 VLAN 或社区 VLAN 的 VLAN 接口。

解决方法：由于 PVLAN 的性质问题，您无法激活隔离 VLAN 或社区 VLAN 的 VLAN 接口。只能激活属于主 VLAN 的 VLAN 接口。

问题 6

在配备 MSFC/MSFC2 的 Catalyst 6500/6000 设备上，在第 3 层 PVLAN 接口上获取的 ARP 条目不会过期。

解决方法：在第 3 层专用 VLAN 接口上获取的 ARP 条目为粘滞 ARP 条目，不会过期。以相同的 IP 地址连接到新设备将生成一条消息，且不创建 ARP 条目。因此，如果 MAC 地址更改，则必须手动删除 PVLAN 端口 ARP 条目。要手动添加或删除 PVLAN ARP 条目，请发出以下命令：

```
Router(config)#no arp 11.1.3.30
IP ARP:Deleting Sticky ARP entry 11.1.3.30
Router(config)#arp 11.1.3.30 0000.5403.2356 arpa
IP ARP:Overwriting Sticky ARP entry 11.1.3.30, hw:00d0.bb09.266e by
hw:0000.5403.2356
```

或者在 Cisco IOS 软件版本 12.1(11b)E 及更高版本中发出 **no ip sticky-arp** 命令。

相关信息

- 专用 VLAN Catalyst 交换机支持表
- 使用专用 VLAN 和 VLAN 访问控制列表保护网络安全
- 配置专用 VLAN
- LAN 产品支持
- LAN 交换技术支持
- 技术支持和文档 - Cisco Systems