

Configurando VLAN privados isolados em Catalyst Switches

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Material de Suporte](#)

[Regras e limitações](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurar o preliminar e os vlan isolada](#)

[Atribua portas aos PVLAN](#)

[Configuração de camada 3](#)

[Configurações](#)

[VLAN privados através dos switch múltiplos](#)

[Verificar](#)

[Troubleshooting](#)

[Pesquise defeitos PVLAN](#)

[Informações Relacionadas](#)

[Introdução](#)

Em algumas situações, é necessário impedir a conectividade da Camada 2 (L2) entre dispositivos finais em um switch sem a colocação dos dispositivos em sub-redes IP diferentes. Esta instalação impede o desperdício de endereços IP. As VLAN Privadas (PVLAN) permitem o isolamento na Camada 2 de dispositivos na mesma sub-rede IP. É possível restringir algumas portas no switch para se obter apenas algumas portas específicas que têm um gateway padrão, um servidor de backup ou um Cisco LocalDirector integrado.

Este documento descreve o procedimento para configurar PVLAN isolados no Switches do Cisco catalyst com o OS do catalizador (Cactos) ou o software de Cisco IOS®.

[Pré-requisitos](#)

[Requisitos](#)

Este documento supõe que você tem uma rede que já exista e pode estabelecer a Conectividade entre as várias portas para a adição a um PVLAN. Se você tem switch múltiplos, certifique-se de

que o tronco entre as funções de Switches corretamente e permita-se os PVLAN no tronco.

Nem todos os switches e versões de software oferecem suporte a PVLAN. Refira a [matriz de suporte do Catalyst Switch do VLAN privado](#) para determinar se sua plataforma e suporte de versão de software PVLAN antes que você comece a configuração.

Note: Alguns Switches (como especificado na [matriz de suporte do Catalyst Switch do VLAN privado](#)) apoia atualmente somente a característica da ponta de PVLAN. O termo “portas protegidas” igualmente refere esta característica. As portas da ponta de PVLAN têm uma limitação que impeça uma comunicação com outras portas protegidas no mesmo interruptor. As portas protegidas em switch separados, contudo, podem comunicar-se um com o outro. Não confunda esta característica com as configurações de PVLAN normais que este documento mostra. Para obter mais informações sobre as portas protegidas, refira a seção [configurando da Segurança de portas do](#) documento que [configura o controle de tráfego com base na porta](#).

[Componentes Utilizados](#)

As informações neste documento são baseadas nestas versões de software e hardware:

- Catalyst 4003 Switch com módulo do Supervisor Engine 2 que executa a versão cactos 6.3(5)
- Catalyst 4006 Switch com módulo do Supervisor Engine 3 que executa o Cisco IOS Software Release 12.1(12c)EW1

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

[Convenções](#)

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

[Material de Suporte](#)

Um PVLAN é um VLAN com configuração para o isolamento da camada 2 de outras portas dentro do mesmo domínio de transmissão ou sub-rede. Você pode atribuir um conjunto específico de portas dentro de um PVLAN e desse modo controlar o acesso entre as portas na camada 2. Você pode configurar PVLAN e VLAN normais no mesmo interruptor.

Há três tipos de portas PVLAN: misturado, isolado e comunidade.

- Uma porta misturada comunica-se com todas as portas restantes PVLAN. A porta misturada é a porta que você se usa tipicamente para comunicar com os roteadores externos, o LocalDirectors, os dispositivos de gerenciamento de rede, os servidores de backup, as estações de trabalho administrativas, e os outros dispositivos. Em alguns Switches, a porta ao módulo da rota (por exemplo, [MSFC] do Multilayer Switch Feature Card) precisa de ser promíscuo.
- Uma porta isolada tem a separação completa da camada 2 de outras portas dentro do mesmo PVLAN. Esta separação inclui transmissões, e a única exceção é a porta misturada. Uma concessão da privacidade a nível da camada 2 ocorre com o bloco de tráfego de saída

a todas as portas isoladas. Trafique que vem de uma porta isolada para a frente a todas as portas misturadas somente.

- As portas da comunidade podem comunicar-se um com o outro e com as portas misturadas. Estas portas têm o isolamento da camada 2 de todas as portas restantes em outras comunidades, ou as portas isoladas dentro do PVLAN. As difusões são propagadas apenas entre as portas de comunidade associadas e a porta heterogênea (sem restrições). **Note:** Este documento não cobre a configuração do VLAN de comunidade.

Para obter mais informações sobre os PVLAN, refira a seção [configurando dos VLAN privados](#) do documento que [compreende e que configura VLAN](#).

[Regras e limitações](#)

Esta seção fornece algumas regras e limitações para que você deve olhar quando você executa PVLAN. Para mais lista completa, refira a seção das [diretrizes de configuração do VLAN privado](#) do documento que [configura VLAN](#).

- Os PVLAN não podem incluir VLAN 1 ou 1002 – 1005.
- Você deve ajustar o modo do protocolo VLAN Trunk (VTP) a `transparente`.
- Você só pode especificar uma VLAN isolada por VLAN primária.
- Você pode somente designar um VLAN como um PVLAN se esse VLAN não tem nenhuma atribuição atual da porta de acesso. Remova todas as portas nesse VLAN antes que você faça ao VLAN um PVLAN.
- Não configurar portas PVLAN como EtherChannels.
- Devido às limitações do hardware, os módulos de Fast Ethernet switch do Catalyst 6500/6000 restringem a configuração de um isolado ou a porta do VLAN de comunidade quando uma porta dentro do mesmo BOSA os circuitos integrados do aplicativo específicos (ASIC) é uma destas: Um tronco Um destino do Switched Port Analyzer (SPAN) Uma porta promíscua PVLAN Esta tabela indica a faixa de porta que pertence ao mesmo ASIC nos módulos rápidos de Ethernet do Catalyst 6500/6000: **O comando `show pvlan capability` (Cactos)** igualmente indica se você pode fazer a uma porta uma porta PVLAN. Não há nenhum comando equivalente no Cisco IOS Software.
- Se você suprime de um VLAN que você use na configuração de PVLAN, as portas que associam com o VLAN tornam-se inativas.
- Configurar interfaces de VLAN da camada 3 (L3) somente para os VLAN principais. As interfaces de VLAN para isolado e VLAN de comunidade são inativas quando o VLAN tiver uma configuração isolado ou do VLAN de comunidade. Para obter mais informações, consulte [Configurando VLANs Privados](#).
- Você pode estender PVLAN através dos Switches com o uso dos troncos. As portas de tronco levam o tráfego dos VLAN regulares e igualmente de preliminar, isolado, e VLAN de comunidade. Cisco recomenda o uso de portas de tronco padrão se ambos os Switches que se submetem ao suporte de entroncamento PVLAN. **Note:** Você deve manualmente incorporar a mesma configuração de PVLAN em cada interruptor com participação porque o VTP no modo `transparente` não propaga esta informação.

[Configurar](#)

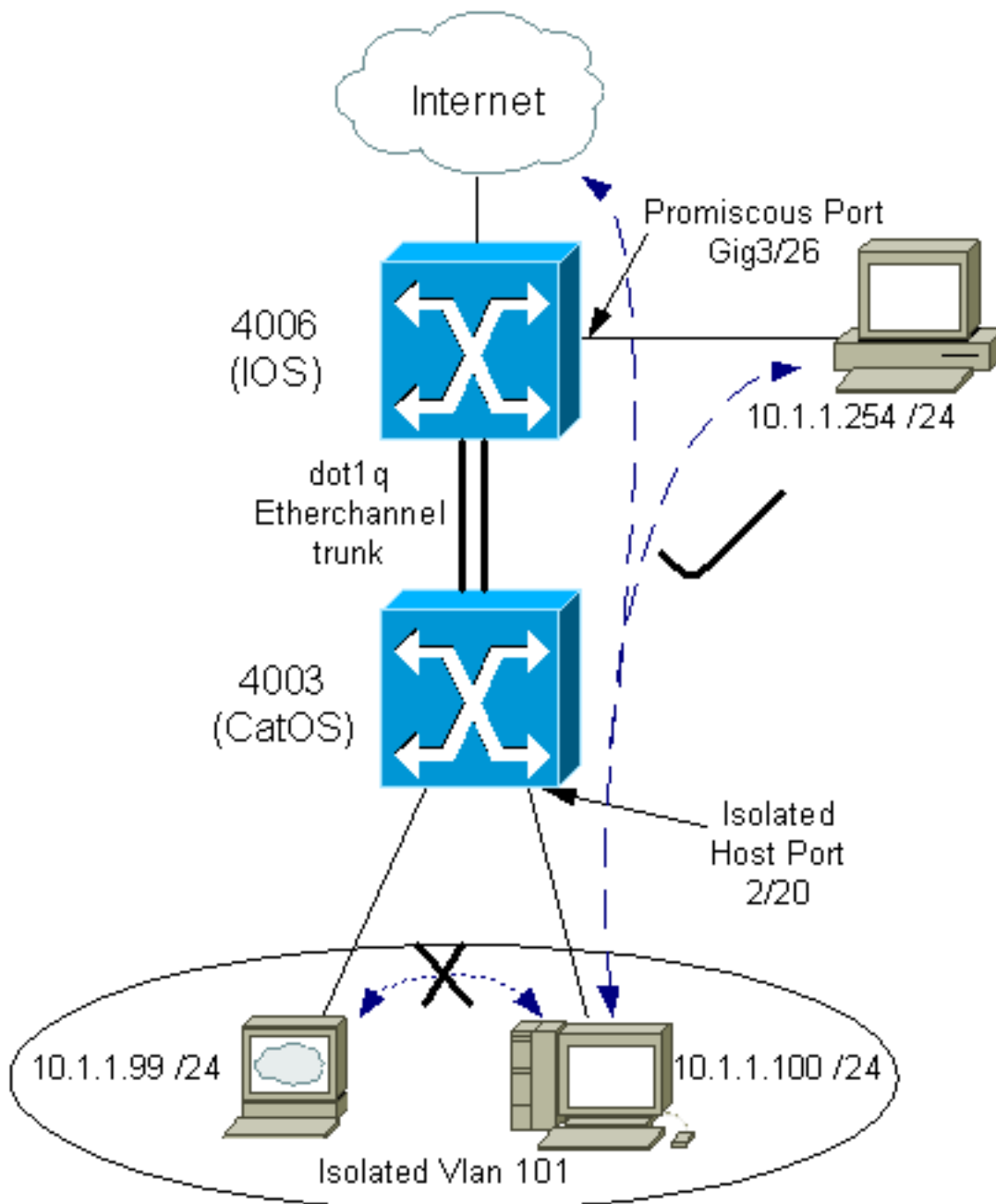
Nesta seção, você encontrará informações para configurar os recursos descritos neste

documento.

Note: Use a ferramenta [Command Lookup Tool](#) ([apenas para clientes registrados](#)) para obter mais informações sobre os comandos usados neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Nesta encenação, os dispositivos no vlan isolada ("101") têm uma limitação de uma comunicação na camada 2 um com o outro. Contudo, os dispositivos podem conectar ao Internet. Além, atuação 3/26" da porta a "nos 4006 tem a designação misturada. Esta configuração opcional permite que um dispositivo no gigabitethernet 3/26 conecte a todos os dispositivos no vlan isolada. Esta configuração igualmente permite, por exemplo, o backup dos dados de todos os dispositivos host PVLAN a uma estação de trabalho de administração. Outros usos para portas misturadas incluem a conexão a um roteador externo, a um LocalDirector, a um dispositivo de gerenciamento de rede, e a uns outros dispositivos.

[Configurar o preliminar e os vlan isolada](#)

Execute estas etapas para criar o preliminar e os VLAN secundários, assim como para ligar as várias portas a estes VLAN. As etapas incluem exemplos para Cactos e Cisco IOS Software. Emita o comando apropriado ajustado para sua instalação de OS.

1. Crie o PVLAN preliminar.CatOS

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

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

Cisco IOS Software

```
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. Crie o vlan isolada ou os 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 Software

```
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. Ligue o VLAN/VLANs isolado ao VLAN principal.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 Software

```
Switch_IOS(config)#vlan primary_vlan_id  
Switch_IOS(config-vlan)#private-vlan association secondary_vlan_id  
Switch_IOS(config-vlan)#exit
```

4. Verifique a configuração do VLAN privado.CatOS

```
Switch_CatOS> (enable) show pvlan  
Primary Secondary Secondary-Type Ports  
-----  
100 101 isolated
```

Cisco IOS Software

```
Switch_IOS#show vlan private-vlan  
Primary Secondary Type Ports  
-----  
100 101 isolated
```

[Atribua portas aos PVLAN](#)

Tip: Antes que você execute este procedimento, emita o comando `show pvlan capability mod/port`

(para Cactos) determinar se uma porta pode se transformar uma porta PVLAN.

Note: Antes que você execute etapa 1 deste procedimento, emita o **comando switchport** no modo de configuração da interface configurar a porta como uma interface comutada da camada 2.

1. Configurar as portas de host em todo o Switches apropriado. 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 Software

```
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. Configurar a porta misturada em um do Switches. 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

Note: Para o Catalyst 6500/6000 quando o Supervisor Engine executa Cactos como o software do sistema, a porta MSFC no Supervisor Engine (15/1 ou 16/1) deve ser promiscuo se você deseja ao switch de camada 3 entre os VLAN. Cisco IOS Software

```
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
```

Configuração de camada 3

Esta seção opcional descreve as etapas de configuração para permitir a rota do tráfego de ingresso PVLAN. Se você precisa somente de permitir a Conectividade da camada 2, você pode omitir esta fase.

1. Configurar a interface de VLAN da mesma forma que você configura para o roteamento normal da camada 3. Esta configuração envolve: Configuração de um endereço IP de Um ou Mais Servidores Cisco ICM NTAtivação da relação com o comando no shutdownVerificação que o VLAN existe na base de dados de VLANRefira o [Suporte técnico VLANs/VTP](#) para exemplos de configuração.
2. Trace os VLAN secundários que você deseja distribuir com o VLAN principal.

```
Switch_IOS(config)#interface vlan primary_vlan_id  
Switch_IOS(config-if)#private-vlan mapping secondary_vlan_list  
Switch_IOS(config-if)#end
```

Note: Configurar interfaces de VLAN da camada 3 somente para VLAN principais. As interfaces de VLAN para isolado e VLAN de comunidade são inativas com uma configuração

isolado ou do VLAN de comunidade.

3. Emita o **mapeamento de vlan privada das relações da mostra** (Cisco IOS Software) ou o comando do **show pvlan mapping** (Cactos) verificar o mapeamento.
4. Se você precisa de alterar a lista do VLAN secundário após a configuração do mapeamento, use **adicionar** ou **remova a** palavra-chave.

```
Switch_IOS(config-if)#private-vlan mapping add secondary_vlan_list  
or  
Switch_IOS(config-if)#private-vlan mapping remove secondary_vlan_list
```

Para mais informação, refira os [VLAN secundários do mapeamento à interface de VLAN da camada 3 de uma](#) seção do [VLAN principal do](#) documento que [configura VLAN privados](#).

Note: Para o Catalyst 6500/6000 comuta com MSFC, asseguram-se de que a porta do Supervisor Engine ao Engine de roteamento (por exemplo, porta 15/1 ou 16/1) seja promíscuo.

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

Emita o comando **show pvlan mapping** para verificar o mapeamento.

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

Configurações

Este documento utiliza as seguintes configurações:

- [Access Layer \(Catalyst 4003: Cactos\)](#)
- [Núcleo \(Catalyst 4006: Cisco IOS Software\)](#)

Access_Layer (Catalyst 4003: Cactos)

```
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

```

Núcleo (Catalyst 4006: Cisco IOS Software)

```

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-channell !--- 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.
```

VLAN privados através dos switch múltiplos

Os VLAN privados podem ser tomados através dos switch múltiplos em dois métodos. Esta seção discute estes métodos:

- [Troncos regulares](#)
- [Troncos do VLAN privado](#)

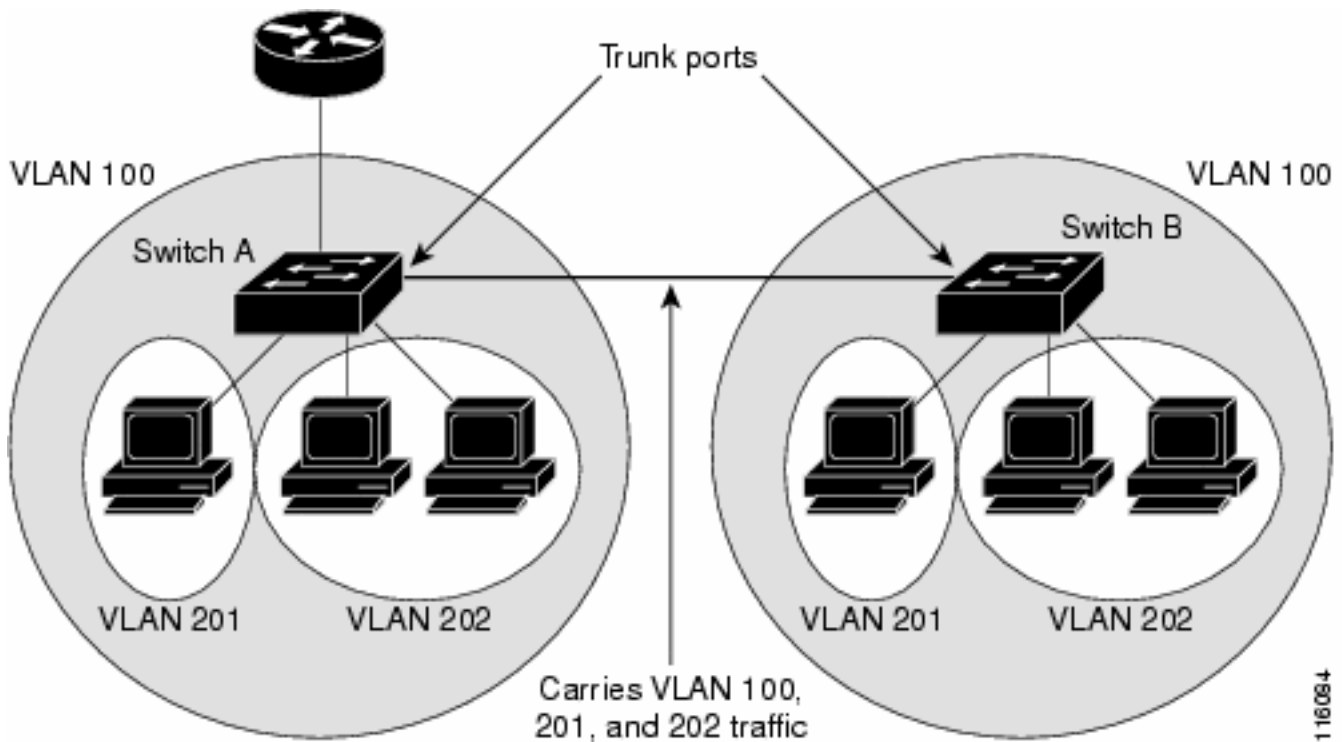
Troncos regulares

Como com VLAN regulares, os PVLAN podem medir switch múltiplos. Uma porta de tronco leva o VLAN principal e os VLAN secundários a um switch confinante. A porta de tronco trata o VLAN privado como todo o outro VLAN. Uma característica dos PVLAN através dos switch múltiplos é que o tráfego de uma porta isolada em um interruptor não alcança uma porta isolada em um outro interruptor.

Configurar PVLAN em todos os dispositivos intermediários, que inclui os dispositivos que não têm nenhuma porta PVLAN, a fim manter a Segurança de sua configuração de PVLAN e evitar o outro uso dos VLAN configurados como PVLAN.

As portas de tronco levam o tráfego dos VLAN regulares e igualmente de preliminar, isolado, e VLAN de comunidade.

Tip: Cisco recomenda o uso de portas de tronco padrão se ambo o Switches que se submete ao suporte de entroncamento PVLAN.



VLAN 100 = Primary VLAN
 VLAN 201 = Secondary isolated VLAN
 VLAN 202 = Secondary community VLAN

Porque o VTP não apoia PVLAN, você deve manualmente configurar PVLAN em todo o Switches na rede da camada 2. Se você não configura a associação preliminar e do VLAN secundário em algum Switches na rede, os bases de dados da camada 2 neste Switches não estão fundidos. Esta situação pode conduzir à inundação desnecessária do tráfego PVLAN naquele Switches.

[Troncos do VLAN privado](#)

Um trunkport PVLAN pode levar secundário e NON-PVLAN múltiplos. Os pacotes são recebidos e transmitidos com as etiquetas secundárias ou regulares VLAN nas portas de tronco PVLAN.

Somente o encapsulamento do IEEE 802.1Q é apoiado. As portas de tronco isoladas permitem que você combine o tráfego para todas as portas secundárias sobre um tronco. As portas de tronco promíscuos permitem que você combine as portas misturadas múltiplas exigidas nesta topologia em uma única porta de tronco que leve VLAN principais múltiplos.

Use portas de tronco isoladas do VLAN privado quando você antecipa o uso de portas de host isoladas VLAN privado levar vlan múltiplos, VLAN normais ou para domínios múltiplos do VLAN privado. Isto faz útil para conectar um interruptor a jusante que não apoie VLAN privados.

Os troncos promíscuos do VLAN privado são usados nas situações onde uma porta de host promíscuo do VLAN privado é usada normalmente mas onde é necessário levar vlan múltiplos, ou vlans normais ou para domínios múltiplos do VLAN privado. Isto faz útil para conectar um roteador fluxo acima que não apoie VLAN privados.

Refira [troncos do VLAN privado](#) para mais informação.

Refira [configurar uma interface de camada 2 como uma porta de tronco PVLAN](#) a fim configurar uma relação como a porta de tronco PVLAN.

Refira [configurar uma interface de camada 2 como uma porta de tronco promíscuo](#) a fim configurar uma relação como uma porta de tronco promíscuo.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A [Output Interpreter Tool \(apenas para clientes registrados\)](#) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

CatOS

- **mostra pvlan** — Indica a configuração de PVLAN. Verifique que isolado e os VLAN principais associam um com o outro. Também, verifique que todas as portas de host aparecem.
- **show pvlan mapping** — Indica o mapeamento PVLAN com configuração em portas misturadas.

Cisco IOS Software

- **mostre privado-VLAN vlan** — Indica a informação PVLAN, que inclui as portas que associam.
- **show interface mod/port switchport** — Indica a informação relação-específica. Verifique que o modo operacional assim como os ajustes operacionais PVLAN estão corretos.
- **mostre o mapeamento de vlan privada das relações** — Indica o mapeamento PVLAN que você configurou.

Procedimento de verificação

Conclua estes passos:

1. Verifique a configuração de PVLAN no Switches. Verifique para determinar se os PVLAN preliminares e secundários associam/mapas entre si. Também, verifique a inclusão das portas necessárias.

```
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. Verifique a configuração correta da porta misturada. Esta saída indica que o modo operacional da porta é **promíscuo** e que os VLAN operacionais são 100 e 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. Inicie um pacote de ping do ICMP (Protocolo de Mensagens de Controle da Internet) da porta do host para a porta misturada. Mantenha na mente que, desde que ambos os dispositivos estão no mesmo VLAN principal, os dispositivos devem estar na mesma sub-rede.

```

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. Inicie um ping ICMP entre portas de host. Neste exemplo, host_port_2 (10.1.1.99) tenta sibilar o host_port (10.1.1.100). Este sibilo falha. Um sibilo de uma outra porta de host à porta misturada, contudo, ainda sucede.

```

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.

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.

Troubleshooting

[Pesquisa defeitos PVLAN](#)

Esta seção endereça alguns problemas comuns que ocorrem com configurações de PVLAN.

[Problema 1](#)

Você recebe esta Mensagem de Erro: %PM-SP-3-ERR_INCOMP_PORT: o <mod/port> é ajustado a inativo porque o <mod/port> é uma porta de tronco

Este Mensagem de Erro pode ser indicado para razões múltiplas, como discutido aqui.

Explicação - 1: Devido às limitações do hardware, os módulos do Catalyst 6500/6000 10/100-Mbps restringem a configuração de uma porta isolado ou do VLAN de comunidade quando uma porta dentro da mesma BOBINA ASIC é um tronco, um destino do PERÍODO, ou uma porta promíscuo PVLAN. (A BOBINA ASIC controla 12 portas na maioria de módulos e 48 portas no módulo do catalizador 6548.) [A tabela na](#) seção das [regras e das limitações](#) deste documento fornece uma divisão da limitação da porta nos módulos do Catalyst 6500/6000 10/100-Mbps.

Procedimento de resolução - 1: Se não há nenhum apoio para o PVLAN nessa porta, escolha uma porta em um ASIC diferente no módulo ou em um módulo diferente. A fim reactivate as portas, remova a configuração de porta isolado ou do VLAN de comunidade e emita o comando **shutdown** e o comando **no shutdown**.

Explicação - 2: Se as portas são configuradas manualmente ou à revelia ao modo *dinâmico desejável* ou de *auto dinâmico*.

Procedimento de resolução - 2: Configurar as portas como o modo de acesso com o comando **switchport mode access**. A fim reactivate as portas, emita o comando **shutdown** e o comando **no shutdown**.

Note: Em liberações do Cisco IOS Software Release 12.2(17a)SX e Mais Recente, a limitação de 12 portas não se aplica aos módulos de switching do Ethernet WS-X6548-RJ-45, WS-X6548-RJ-21 e WS-X6524-100FX-MM. Para obter mais informações sobre as limitações de configuração do PVLAN com outros recursos, refira as [limitações com](#) seção dos [outros recursos de configurar os VLAN privados \(PVLAN\)](#).

[Problema 2](#)

Durante a configuração de PVLAN, você encontra *uma* destas mensagens:

- ```
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.*

**Explicação:** Devido às limitações do hardware, os módulos do Catalyst 6500/6000 10/100-Mbps restringem a configuração de uma porta isolado ou do VLAN de comunidade quando uma porta dentro da mesma BOBINA ASIC é um tronco, um destino do PERÍODO, ou uma porta promíscuo PVLAN. (A BOBINA ASIC controla 12 portas na maioria de módulos e 48 portas no módulo do catalizador 6548.) [A tabela na](#) seção das [regras e das limitações](#) deste documento fornece uma divisão da limitação da porta nos módulos do Catalyst 6500/6000 10/100-Mbps.

**Procedimento de solução:** Emita o comando `show pvlan capability` (Cactos), que indica se uma porta pode se transformar uma porta PVLAN. Se não há nenhum apoio para o PVLAN nessa porta particular, escolha uma porta em um ASIC diferente no módulo ou em um módulo diferente.

**Note:** Em liberações do Cisco IOS Software Release 12.2(17a)SX e Mais Recente, a limitação de 12 portas não se aplica aos módulos de switching do Ethernet WS-X6548-RJ-45, WS-X6548-RJ-21 e WS-X6524-100FX-MM. Para obter mais informações sobre das limitações de configuração do PVLAN com outros recursos, refira [limitações com](#) seção dos [outros recursos de configurar os VLAN privados \(PVLAN\)](#).

### [Problema 3](#)

Não é possível configurar PVLANS em algumas plataformas.

**Resolução:** Verifique que os suportes a plataforma PVLAN. Refira a [matriz de suporte do Catalyst Switch do VLAN privado](#) para determinar se seus plataforma e suporte de versão de software PVLAN antes que você comece a configuração.

### [Problema 4](#)

Em um Catalyst 6500/6000 MSFC, você não pode sibilhar um dispositivo que conecte à porta isolada no interruptor.

**Resolução:** No Supervisor Engine, verifique que a porta ao MSFC (15/1 ou 16/1) é promíscuo.

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

Também, configurar a interface de VLAN no MSFC como a [camada 3 seções de configuração](#) deste documento especifica.

## [Problema 5](#)

Com introdução do **comando no shutdown**, você não pode ativar a interface de VLAN para isolado ou VLAN de comunidade.

**Resolução:** Devido à natureza dos PVLANS, não é possível ativar a interface de VLAN para VLANs isoladas ou de comunidade. Você pode somente ativar a interface de VLAN que pertence ao VLAN principal.

## [Problema 6](#)

Em dispositivos do Catalyst 6500/6000 com MSFC/MSFC2, as entradas de ARP aprendidas em relações da camada 3 PVLAN não envelhecem para fora.

**Resolução:** As entradas de ARP que são aprendidas em relações do VLAN privado da camada 3 são entradas de ARP pegajosas e não envelhecem para fora. A conexão do equipamento novo com o mesmo endereço IP de Um ou Mais Servidores Cisco ICM NT gerencie uma mensagem, e não há nenhuma criação da entrada de ARP. Portanto, é necessário remover as entradas ARP da porta PVLAN manualmente caso um endereço MAC seja alterado. A fim adicionar manualmente ou remover entradas de ARP PVLAN, emita estes comandos:

```
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
```

Uma outra opção é emitir o **comando no ip sticky-arp** no Cisco IOS Software Release 12.1(11b)E e Mais Recente.

## [Informações Relacionadas](#)

- [Matriz de suporte de Switch de Catalyst de VLAN particular](#)
- [Protegendo redes com VLANs privados e listas de controle de acesso de VLAN](#)
- [Configurando VLANs privadas](#)
- [Suporte a Produtos de LAN](#)
- [Suporte de tecnologia de switching de LAN](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)