

Configurar Verificar Troubleshooting de QinQ e L2PT nos Catalyst 9000 Switches

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Verificar](#)

[Troubleshooting](#)

[Comandos de depuração adicionais](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar, verificar e solucionar problemas de túneis 802.1Q (QinQ) e Tunelamento de Protocolo de Camada 2 (L2PT) na família de switches Catalyst 9000 que executam o software Cisco IOS® XE.

Consulte as Notas de versão e os Guias de configuração oficiais da Cisco para obter informações atualizadas sobre limitações, restrições, opções de configuração e advertências, bem como qualquer outro detalhe relevante sobre esse recurso.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Arquitetura dos switches Catalyst 9000 Series
- Arquitetura do software Cisco IOS XE
- Redes locais virtuais (VLAN), troncos VLAN e encapsulamento IEEE 802.1Q
- Protocolos de camada 2, como o Cisco Discovery Protocol (CDP), o Link Layer Discovery Protocol (LLDP), o Spanning Tree Protocol (STP), o Link Aggregation Control Protocol (LACP) e o Port Aggregation Protocol (PAgP).
- Conhecimento básico de túneis QinQ, túneis QinQ seletivos e túnel de protocolo de camada 2 (L2PT)
- Switched Port Analyzer (SPAN) e Embedded Packet Captures (EPC)

Componentes Utilizados

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

- Cisco Catalyst C9500-12Q com Cisco IOS XE 17.3.3

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 rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Produtos Relacionados

Este documento também pode ser usado com as seguintes versões de hardware e software:

- Switches das séries Catalyst 3650 e 3850 com o software Cisco IOS XE
- Switches das séries Catalyst 9200, 9300, 9400 e 9600 com software Cisco IOS XE

Configurar

Esta seção apresenta uma topologia básica para a implantação de Túneis IEEE 802.1Q (QinQ) em switches Catalyst 9000, bem como exemplos de configuração para cada switch Catalyst.

Diagrama de Rede

Na topologia apresentada, há dois locais, Local A e Local B, que são fisicamente separados por uma rede comutada do provedor de serviços onde a LAN virtual de serviço (SVLAN) 1010 é usada. Os switches Provider Edge (PE) ProvSwitchA e ProvSwitchB concedem acesso ao Site A e ao Site B, respectivamente, à rede do provedor. O local A e o local B usam VLANs do cliente (CVLAN) 10, 20 e 30 e exigem que essas VLANs sejam estendidas na camada 2 (L2). O local A se conecta à rede do provedor através do switch CusSwitchA da borda do cliente (CE) e o local B através do switch CusSwitchB do CE.

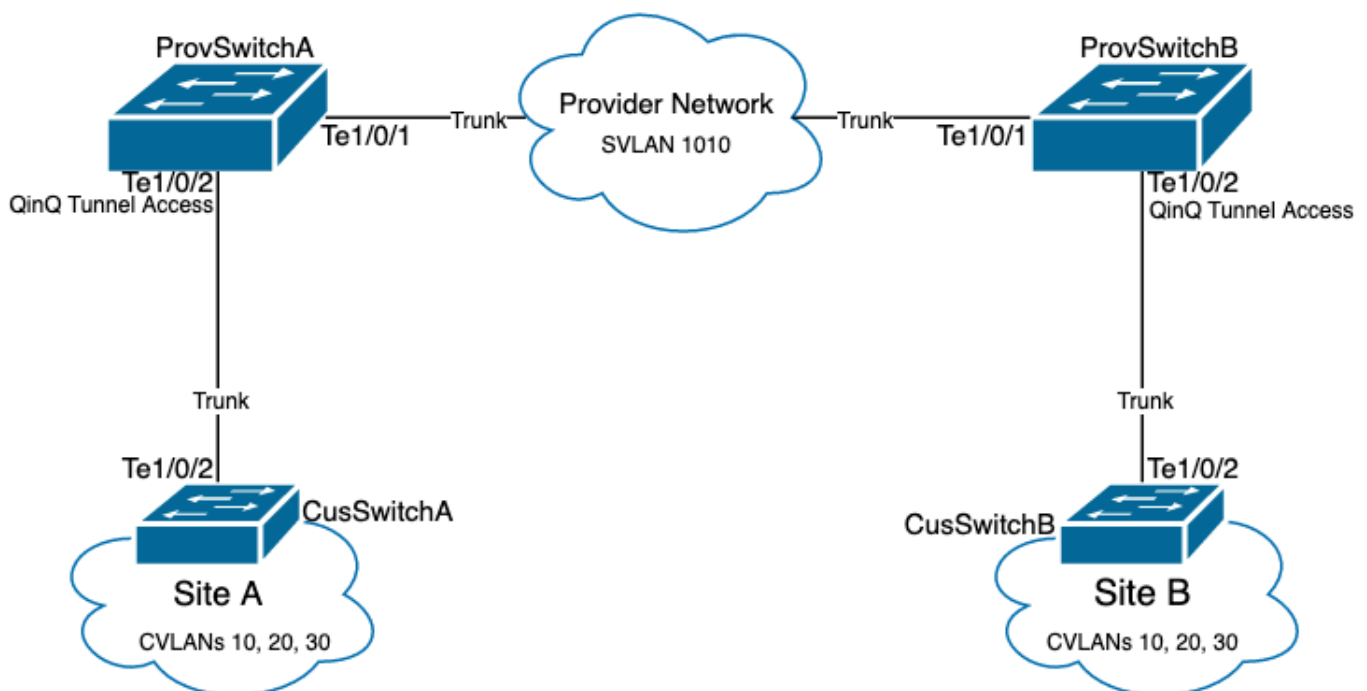
O site A envia tráfego com a marca IEEE 802.1Q da CVLAN usada, também conhecida como marca interna, para o switch PE ProvSwitchA, que atua como um acesso de túnel QinQ. ProvSwitchA encaminha o tráfego recebido para a rede comutada do provedor com a segunda marca IEEE 802.1Q da SVLAN, também conhecida como marca externa ou marca Metro, adicionada sobre a marca CVLAN 802.1Q. Esse processo também é conhecido como pilhas de VLAN e este exemplo apresenta uma pilha de VLAN de 2 marcas. O tráfego com marcação dupla é encaminhado por L2 na rede do provedor com base apenas nas informações da tabela de Controle de Acesso ao Meio (MAC - Media Access Control) da SVLAN. Quando o tráfego com marcação dupla chega à extremidade remota do túnel QinQ, o switch PE remoto ProvSwitchB, que também atua como QinQ Tunnel Access, retira a marca SVLAN do tráfego e a encaminha para o Site B marcado apenas com a marca CVLAN 802.1Q, assim, a extensão de Camada 2 das VLANs através dos sites remotos é alcançada. O L2 Protocols Tunneling também é implementado para trocar quadros do Cisco Discovery Protocol (CDP) entre os switches CE CusSwitchA e CusSwitchB.

Esse mesmo processo acontece quando o tráfego é encaminhado do Site B para o Site A, e a mesma configuração, verificação e etapas para solucionar problemas se aplicam ao switch ProvSwitchB do PE. Suponha que todos os outros dispositivos dentro da rede do switch do provedor e os locais do cliente sejam configurados apenas com comandos de acesso/tronco e não executem nenhuma função QinQ.

O exemplo apresentado assume que o tráfego com apenas uma marca 802.1Q é recebido nos switches de acesso de túnel QinQ, no entanto, o tráfego recebido pode ter zero ou mais marcas 802.1Q. A marca SVLAN é adicionada à pilha VLAN recebida. Nenhuma configuração adicional de QinQ, VLAN e tronco é necessária nos dispositivos para suportar o tráfego com zero ou mais marcas 802.1Q, no entanto, a Unidade máxima de transmissão (MTU) nos dispositivos deve ser alterada para suportar os bytes adicionais adicionados ao tráfego (detalhes adicionais descritos na seção Solução de problemas).

Informações adicionais sobre túneis IEEE 802.1Q são apresentadas no Documento do Guia de Configuração da Camada 2 do Catalyst 9500 com Cisco IOS XE Amsterdam-17.3.x:

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-3/configuration_guide/lyr2/b_173_lyr2_9500_cg/configuring_ieee_802_1q_tunneling.html



Configuração em ProvSwitchA (dispositivo PE de túnel QinQ):

```
!  
version 17.3  
!  
hostname ProvSwitchA  
!  
vtp domain QinQ  
vtp mode transparent  
!  
vlan dot1q tag native
```

```
!  
vlan 1010  
  name QinQ-VLAN  
!  
interface TenGigabitEthernet1/0/1  
  switchport trunk allowed vlan 1010  
  switchport mode trunk  
!  
interface TenGigabitEthernet1/0/2  
  switchport access vlan 1010  
  switchport mode dot1q-tunnel  
  no cdp enable  
  l2protocol-tunnel cdp  
!
```

Configuração em ProvSwitchB (dispositivo PE de túnel QinQ):

<#root>

```
!  
version 17.3  
!  
hostname ProvSwitchB  
!  
vtp domain QinQ  
vtp mode transparent  
!  
vlan dot1q tag native  
!  
vlan 1010  
  name QinQ-VLAN  
!  
interface TeGigabitEthernet1/0/1  
  switchport trunk allowed vlan 1010  
  switchport mode trunk  
!  
interface TeGigabitEthernet1/0/2  
  switchport access vlan 1010  
  switchport mode dot1q-tunnel  
  no cdp enable  
  l2protocol-tunnel cdp  
!  
!
```

Configuração no CusSwitchA (dispositivo CE):

```
!  
version 17.3  
!  
hostname CusSwitchA  
!  
vtp domain SiteA
```

```
vtp mode transparent
!  
vlan dot1q tag native
!  
vlan 10
  name Data
!  
vlan 20
  name Voice
!  
vlan 30
  name Mgmt
!  
interface TenGigabitEthernet1/0/2
  switchport trunk allowed vlan 10,20,30
  switchport mode trunk
!
```

Configuração em CusSwitchB (dispositivo CE):

```
!  
version 17.3
!  
hostname CusSwitchB
!  
vtp domain SiteB
vtp mode transparent
!  
vlan dot1q tag native
!  
vlan 10
  name Data
!  
vlan 20
  name Voice
!  
vlan 30
  name Mgmt
!  
interface TenGigabitEthernet1/0/2
  switchport trunk allowed vlan 10,20,30
  switchport mode trunk
!
```

Observe que as CVLANs não estão definidas nos dispositivos do provedor e a SVLAN não está definida nos switches CE. Os dispositivos do provedor encaminham o tráfego com base apenas em SVLAN e não consideram as informações de CVLAN para qualquer decisão de encaminhamento, portanto, não é necessário que um dispositivo do provedor saiba quais VLANs são recebidas em um acesso de túnel QinQ (a menos que QinQ Seletivo seja usado). Isso também significa que os mesmos IDs de VLAN usados para as marcas CVLAN podem ser usados para o tráfego dentro da rede comutada do provedor e vice-versa. Se esse for o caso, a recomendação é configurar a vlan dot1q tag native no modo de Configuração Global para evitar

qualquer perda de pacotes ou problema de vazamento de tráfego. A vlan dot1q tag native permite que a VLAN nativa 802.1Q seja marcada em todas as interfaces de tronco por padrão, mas isso pode ser desabilitado no nível da interface com nenhuma configuração de switchport trunk native vlan tag.

Verificar

A configuração de porta para túneis QinQ e L2PT pode ser verificada da perspectiva do Cisco IOS XE para a perspectiva do Circuito Integrado Específico de Aplicação de Encaminhamento (FWD-ASIC), onde ocorrem as decisões de encaminhamento em um switch Catalyst. Os comandos básicos de verificação do Cisco IOS XE são:

- show dot1q-tunnel - Lista as interfaces configuradas como acesso ao túnel QinQ.

<#root>

```
ProvSwitchA# show dot1q-tunnel
```

```
dot1q-tunnel mode LAN Port(s)
```

```
-----  
Te1/0/2
```

- show vlan id {svlan-number} - Exibe as interfaces atribuídas à VLAN especificada.

<#root>

```
ProvSwitchA# show vlan id 1010
```

```
VLAN
```

```
Name Status
```

```
Ports
```

```
-----  
1010
```

```
QinQ-VLAN active
```

```
Te1/0/1, Te1/0/2
```

- show interfaces trunk - Lista as interfaces configuradas no modo trunk.

<#root>

```
ProvSwitchA# show interfaces trunk
```

```
Port Mode Encapsulation Status Native vlan  
Te1/0/1 on 802.1q trunking 1
```

Port

Vlans allowed on trunk

Te1/0/1

1010

- show vlan dot1q tag native - Lista o status global da marca de VLAN nativa 802.1Q e as interfaces de tronco configuradas para marcar a VLAN nativa 802.1Q.

<#root>

```
ProvSwitchA# show vlan dot1q tag native
```

```
dot1q native vlan tagging is enabled globally
```

```
Per Port Native Vlan Tagging State
```

```
-----
```

```
Port
```

```
Operational
```

```
Native VLAN
```

```
Mode
```

```
Tagging State
```

```
-----
```

```
Te1/0/1
```

```
trunk
```

```
enabled
```

- show mac address-table vlan {svlan-number} - Mostra os endereços MAC aprendidos na SVLAN. Os endereços MAC dos dispositivos de LAN são aprendidos na SVLAN, independentemente da CVLAN usada.

<#root>

```
ProvSwitchA#show mac address-table vlan 1010
```

```
Mac Address Table
```

```
-----
```

```
Vlan
```

```
Mac Address
```

```

Type
Ports
-----
1010    701f.539a.fe46
DYNAMIC
Te1/0/2
Total Mac Addresses for this criterion: 3

```

- show l2-protocol tunnel - Mostra a interface habilitada para L2PT e os contadores para cada um dos protocolos L2 habilitados.

<#root>

```

ProvSwitchA#show l2protocol-tunnel
COS for Encapsulated Packets: 5
Drop Threshold for Encapsulated Packets: 0

```

```

Port          Protocol
Shutdown Drop
Encaps
Decaps
Drop          Threshold Threshold
Counter
Counter
Counter
-----
Te1/0/2      cdp
-----
90
97
0
-----

```


- show cdp neighbor - Pode ser executado em switches CE para confirmar se eles podem ver

um ao outro via CDP.

```
CusSwitcha#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID Local      Intrfce  Holdtme Capability Platform  Port ID
CusSwitchB.cisco.com Ten 1/0/2 145      S I       C9500-12  Ten 1/0/2
```

Quando uma interface é configurada como um acesso de túnel QinQ através de Interfaces de Linha de Comando (CLI - Command Line Interfaces), o Cisco IOS XE aciona o processo do Gerenciador de Portas (PM - Port Manager) para configurar as portas do switch com o modo e a VLAN especificados. As informações da porta do switch podem ser verificadas no PM com o comando `show pm port interface {interface-name}`.

 Observação: para executar comandos PM, é necessário configurar o serviço interno no modo de Configuração Global. Essa configuração permite que comandos adicionais de plataforma e depuração sejam executados na CLI e não tem nenhum impacto funcional na rede. Recomenda-se remover esse comando assim que a verificação de PM estiver concluída.

<#root>

```
ProvSwitchA# show pm port interface TenGigabitEthernet1/0/2
port 1/2  pd 0x7F9E317C3A48 swidb 0x7F9E30851320(switch)  sb 0x7F9E30852FE8

if_number = 2

  hw_if_index = 1 snmp_if_index = 2(2) ptrunkgroup = 0(port)
  admin up(up)  line up(up)  operErr none
  port assigned mac address 00a3.d144.200a
  idb

port vlan id 1010

  default vlan id 1010
  speed: 10G  duplex: full  mode: tunnel  encap: native
  flowcontrol receive: on  flowcontrol send: off

sm(pm_port 1/2), running yes,

state dot1qtunnel
```

À interface Te1/0/2 é atribuído o número de interface (if_number) de 2. Este é o Identificador de Interface (IF-ID), o valor interno que identifica uma porta específica. A configuração de switchport também pode ser verificada no PM com o comando `show platform software pm-port switch 1 R0 interface {IF-ID}`.

<#root>

```
ProvSwitchA# show platform software pm-port switch 1 R0 interface 2
PM PORT Data:
```

```
Intf
  PORT
DEFAULT
  NATIVE    ALLOW
MODE
  PORT     PORT
ID
  ENABLE
VLAN
  VLAN     NATIVE     DUPLEX     SPEED
-----
2
  TRUE
1010
  1010    TRUE
tunnel
  full    unknown
```

Quando o PM aplica a configuração da porta do switch, ele retransmite as informações da porta para o FED (Forwarding Engine Driver) para programar os ASICs (Application-specific Integrated Circuits) de acordo.

No FED, as portas podem ser verificadas com o comando `show platform software fed switch {switch-number} port if_id {IF-ID}` para confirmar se estão programadas como portas de acesso de túnel QinQ:

<#root>

```
ProvSwitchA# show platform software fed switch 1 port if_id 2
FED PM SUB PORT Data :
```

```
if_id = 2
```

```
if_name = TenGigabitEthernet1/0/2
```

```
enable: true
speed: 10Gbps
operational speed: 10Gbps
```

```
duplex: full
operational duplex: full
flowctrl: on
link state: UP

defaultvlan: 1010
```

```
port_state: Fed PM port ready
```

```
mode: tunnel
```

Ao contrário das portas de switch no modo de acesso, que esperam receber apenas tráfego não marcado, uma porta de switch configurada no modo de túnel 802.1Q também aceita tráfego com marcas 802.1Q. O FED permite este recurso na porta para portas de acesso de túnel QinQ, como pode ser confirmado com o `show platform software fed switch {switch-number} ifm if-id {IF-ID}`:

```
<#root>
```

```
C9500-12Q-PE1# show platform software fed switch 1 ifm if-id 2
```

```
Interface Name      :
```

```
TenGigabitEthernet1/0/2
```

```
Interface State      : Enabled
Interface Type       : ETHER
  Port Type          : SWITCH PORT
  Port Location      : LOCAL
  Port Information
  Type ..... [Layer2]
  Identifier ..... [0x9]
  Slot ..... [1]
  Port Physical Subblock
    Asic Instance .... [0 (A:0,C:0)]
    Speed ..... [10GB]
```

```
PORT_LE ..... [0x7fa164777618]
```

```
  Port L2 Subblock
    Enabled ..... [Yes]
```

```
  Allow dot1q ..... [Yes]
```

```
    Allow native ..... [Yes]
```

```
  Default VLAN ..... [1010]
```

```
    Allow priority tag ... [Yes]
    Allow unknown unicast [Yes]
    Allow unknown multicast[Yes]
    Allow unknown broadcast[Yes]
```

O FED também fornece um valor de identificador em formato hexadecimal chamado Entidade lógica da porta (Porta LE). A porta LE é um ponteiro para as informações de porta programadas no ASIC de encaminhamento (fwd-asic). O comando `show platform hardware fed switch 1 fwd-asic abstraction print-resource-handle {Port-LE-handle} 1` exibe os diferentes recursos habilitados na porta no nível ASIC:

```
<#root>
```

```
C9500-12Q-PE1# show platform hardware fed switch 1 fwd-asic abstraction print-resource-handle 0x7f79548
```

```
Detailed Resource Information (ASIC_INSTANCE# 0)
```

```
-----  
LEAD_PORT_ALLOW_BROADCAST value 1 Pass
```

```
LEAD_PORT_ALLOW_DOT1Q_TAGGED value 1 Pass
```

```
LEAD_PORT_ALLOW_MULTICAST value 1 Pass
```

```
LEAD_PORT_ALLOW_NATIVE value 1 Pass
```

```
LEAD_PORT_ALLOW_UNICAST value 1 Pass
```

```
LEAD_PORT_ALLOW_UNKNOWN_UNICAST value 1 Pass;
```


```
LEAD_PORT_SEL_QINQ_ENABLED value 0 Pass
```


```
LEAD_PORT_DEFAULT_VLAN value 1010 Pass  
=====
```

Essa saída confirma, no nível ASIC, que a porta de switch de acesso ao túnel QinQ está configurada para permitir tráfego não marcado e marcado 802.1Q da LAN e atribuir a SVLAN 1010 para ser encaminhado através da rede comutada do provedor. Observe que o campo `LEAD_PORT_SEL_QINQ_ENABLED` não está definido. Esse bit é definido somente para a configuração QinQ seletiva, não para a configuração de túneis QinQ tradicional conforme apresentado neste documento.

Troubleshooting

Esta seção fornece as etapas que você pode seguir para solucionar problemas da sua configuração. A ferramenta mais útil para solucionar problemas de tráfego em um túnel 802.1Q é o Switched Port Analyzer (SPAN). As capturas de SPAN podem ser usadas para verificar a marca 802.1Q do CVLAN recebido da LAN e do SVLAN adicionado ao dispositivo de acesso de túnel QinQ.

 **Observação:** o EPC (Embedded Packet Captures) também pode ser usado para capturar o tráfego em um ambiente de túnel 802.1Q. No entanto, as capturas de pacotes de saída com EPC ocorrem antes que o tráfego seja marcado com IEEE 802.1Q (a inserção de marca 802.1Q ocorre no nível de porta na direção de saída). Consequentemente, o EPC de saída no tronco de uplink do dispositivo de borda do provedor não pode exibir a marca SVLAN usada na rede comutada do provedor. Uma opção para coletar o tráfego com marcação dupla com EPC é capturar o tráfego com EPC de entrada no dispositivo do provedor vizinho.

 Consulte o Guia de Configuração de Gerenciamento de Rede para Catalyst 9500 Switches com Cisco IOS XE Amsterdam-17.3.x para obter informações adicionais sobre EPC:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-3/configuration_guide/nmgmt/b_173_nmgmt_9500_cg/configuring_packet_capture.html

Para configurar o SPAN para capturar o tráfego com marcas 802.1Q, é importante configurar o comando `monitor session {session-number} destination interface {interface-name} encapsulation replicate`. Se a palavra-chave `encapsulation replicate` não estiver configurada, o tráfego espelhado com o SPAN pode conter informações de marcas 802.1Q incorretas. Consulte a seção Configurar para obter um exemplo da configuração de SPAN.

Para obter informações adicionais sobre SPAN, consulte o Guia de Configuração de Gerenciamento de Rede para Catalyst 9500 Switches com Cisco IOS XE Amsterdam-17.3.x

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-3/configuration_guide/nmgmt/b_173_nmgmt_9500_cg/configuring_span_and_rspan.html

Exemplo de configuração de SPAN em ProvSwitchA:

```
!  
monitor session 1 source interface Te1/0/1 , Te1/0/2  
monitor session 1 destination interface Te1/0/3 encapsulation replicate  
!
```

No dispositivo Network Analyzer, o tráfego espelhado recebido pode ser analisado para confirmar a presença de CVLAN 10 no ingresso de acesso ao túnel QinQ:


```
> Frame 29: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface 0  
v Ethernet II, Src: Cisco_9a:fe:46 (70:1f:53:9a:fe:46), Dst: ca:fe:ca:fe:ca:fe (ca:fe:ca:fe:ca:fe)  
  > Destination: ca:fe:ca:fe:ca:fe (ca:fe:ca:fe:ca:fe)  
  > Source: Cisco_9a:fe:46 (70:1f:53:9a:fe:46)  
    Type: 802.1Q Virtual LAN (0x8100)  
v 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 10  
  000. .... .... = Priority: Best Effort (default) (0)  
  ...0 .... .... = DEI: Ineligible  
  .... 0000 0000 1010 = ID: 10  
    Type: IPv4 (0x0800)  
> Internet Protocol Version 4, Src: 192.168.10.1, Dst: 192.168.10.2  
> Internet Control Message Protocol
```

Da mesma forma, a presença de CVLAN 10 e SVLAN 1010 pode ser confirmada na direção de saída no tronco de interface conectado à rede comutada do provedor.

```

> Frame 30: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface 0
v Ethernet II, Src: Cisco_9a:fe:46 (70:1f:53:9a:fe:46), Dst: ca:fe:ca:fe:ca:fe (ca:fe:ca:fe:ca:fe)
  > Destination: ca:fe:ca:fe:ca:fe (ca:fe:ca:fe:ca:fe)
  > Source: Cisco_9a:fe:46 (70:1f:53:9a:fe:46)
  Type: 802.1Q Virtual LAN (0x8100)
v 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1010
  000. .... .... = Priority: Best Effort (default) (0)
  ...0 .... .... = DEI: Ineligible
  .... 0011 1111 0010 = ID: 1010
  Type: 802.1Q Virtual LAN (0x8100)
v 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 10
  000. .... .... = Priority: Best Effort (default) (0)
  ...0 .... .... = DEI: Ineligible
  .... 0000 0000 1010 = ID: 10
  Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.10.1, Dst: 192.168.10.2
> Internet Control Message Protocol


```

 **Observação:** determinadas placas de interface de rede (NICs) em analisadores de rede podem remover marcas 802.1Q no tráfego marcado recebido. Entre em contato com o suporte do fornecedor da placa de rede para obter informações específicas sobre como manter as marcas 802.1Q nos quadros recebidos.

Se houver suspeita de perda de tráfego na rede comutada QinQ, considere estes itens para revisar:

- A Unidade de Transmissão Máxima (MTU - Maximum Transmission Unit) padrão em uma interface de tronco é de 1522 bytes. Isso responde pela MTU IP de 1500, o quadro do cabeçalho Ethernet de 18 bytes e uma marca 802.1Q de 4 bytes. O MTU configurado em todos os dispositivos de borda do provedor e do provedor deve ter 4 bytes adicionais por marca 802.1Q adicionados à pilha de VLANs. Por exemplo, para uma pilha de VLAN de 2 marcas, um MTU de 1504 deve ser configurado. Para uma pilha de VLAN de 3 marcas, uma MTU de 1508 deve ser configurada e assim por diante. Consulte o Guia de Configuração de Componentes de Hardware e Interface para o Catalyst 9500 com Cisco IOS XE Amsterdam 17.3.x para obter detalhes de configuração de MTU:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-3/configuration_guide/int_hw/b_173_int_and_hw_9500_cg/configuring_system_mtu.html
- Não há suporte para o tráfego enviado para a CPU em dispositivos dentro de um túnel 802.1Q. Os recursos que requerem inspeção de tráfego podem causar perda de pacotes ou vazamentos de pacotes em um ambiente 802.1Q. Exemplos desses recursos são o DHCP Snooping para tráfego DHCP, o IGMP Snooping para tráfego IGMP, o MLD Snooping para tráfego MLD e o Dynamic ARP Inspection para tráfego ARP. É recomendável desativar esses recursos na SVLAN usada para transportar o tráfego através da rede comutada do provedor.

Comandos de depuração adicionais

 **Nota:** Consulte Informações Importantes sobre Comandos de Depuração antes de usar

 comandos debug.

- debug pm port - Exibe as transições de porta do Gerenciador de Portas (PM) e o modo programado. Útil para depurar o status de configuração da porta QinQ.

Informações Relacionadas

- [Switches Catalyst 9300 - Configuração de encapsulamento IEEE 802.1Q](#)
- [Switches Catalyst 9300 - Configurando o tunelamento de protocolo de camada 2](#)
- [Switches Catalyst 9300 - Configuração de EtherChannels](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.