Configure Verify Troubleshoot QinQ and L2PT on Catalyst 9000 Switches

Contenido

Introducción

Este documento describe cómo configurar. verificar y resolver problemas de túneles 802.1Q (QinQ) y tunelación de protocolo de capa 2 (L2PT) en la familia de switches Catalyst 9000 que ejecutan el software Cisco IOS® XE.

Consulte las Notas de la versión oficiales de Cisco y las Guías de configuración para obtener información actualizada sobre las limitaciones, restricciones, opciones de configuración y advertencias, así como cualquier otro detalle relevante sobre esta función.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Arquitectura de switches Catalyst serie 9000
- Arquitectura de software Cisco IOS XE
- Redes de área local virtuales (VLAN), VLAN troncales y encapsulación IEEE 802.1Q
- Protocolos de capa 2, como Cisco Discovery Protocol (CDP), protocolo de descubrimiento de la capa de enlace (LLDP), protocolo de árbol de extensión (STP), protocolo de control de agregación de enlaces (LACP) y protocolo de agregación de puertos (PAgP).
- Conocimientos básicos de túneles QinQ, túneles QinQ selectivos y tunelación de protocolo de capa 2 (L2PT)
- Analizador de puertos conmutados (SPAN) y captura de paquetes integrada (EPC)

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software y hardware.

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Productos Relacionados

Este documento también puede utilizarse con estas versiones de software y hardware:

- Catalyst 3650 y 3850 Series Switches con el software Cisco IOS XE
- Switches Catalyst series 9200, 9300, 9400 y 9600 con el software Cisco IOS XE

Configurar

Esta sección presenta una topología básica para la implementación de túneles IEEE 802.1Q (QinQ) en switches Catalyst 9000, así como ejemplos de configuración para cada switch Catalyst.

Diagrama de la red

En la topología presentada hay dos sitios, el sitio A y el sitio B, que están separados físicamente por una red conmutada de proveedor de servicios en la que se utiliza la LAN virtual de servicio (SVLAN) 1010. Los switches Provider Edge (PE) ProvSwitchA y ProvSwitchB conceden acceso al sitio A y al sitio B, respectivamente, a la red del proveedor. El sitio A y el sitio B utilizan las VLAN del cliente (CVLAN) 10, 20 y 30, y requieren que estas VLAN se amplíen a la capa 2 (L2). El sitio A se conecta a la red del proveedor a través del switch de extremo del cliente (CE) CusSwitchA y el sitio B a través del switch CE CusSwitchB.

El sitio A envía el tráfico con la etiqueta IEEE 802.1Q de la CVLAN utilizada, también denominada etiqueta interna, al switch PE ProvSwitchA, que actúa como un acceso de túnel QinQ. ProvSwitchA reenvía el tráfico recibido a la red conmutada del proveedor con la segunda etiqueta IEEE 802.1Q de la SVLAN, también conocida como etiqueta externa o etiqueta Metro, agregada sobre la etiqueta CVLAN 802.1Q. Este proceso también se conoce como pilas de VLAN y este ejemplo presenta una pila de VLAN de 2 etiquetas. L2 reenvía el tráfico con doble etiqueta en la red del proveedor basándose únicamente en la información de la tabla de control de acceso a medios (MAC) de SVLAN. Una vez que el tráfico con doble etiqueta llega al extremo remoto del túnel QinQ, el switch PE remoto ProvSwitchB, que también actúa como acceso de túnel QinQ, elimina la etiqueta SVLAN del tráfico y la reenvía al sitio B etiquetado solo con la etiqueta CVLAN 802.1Q, con lo que se logra la extensión de capa 2 de las VLAN a través de los sitios remotos. La tunelización de protocolos L2 también se implementa para intercambiar tramas de Cisco Discovery Protocol (CDP) entre los switches CE CusSwitchA y CusSwitchB.

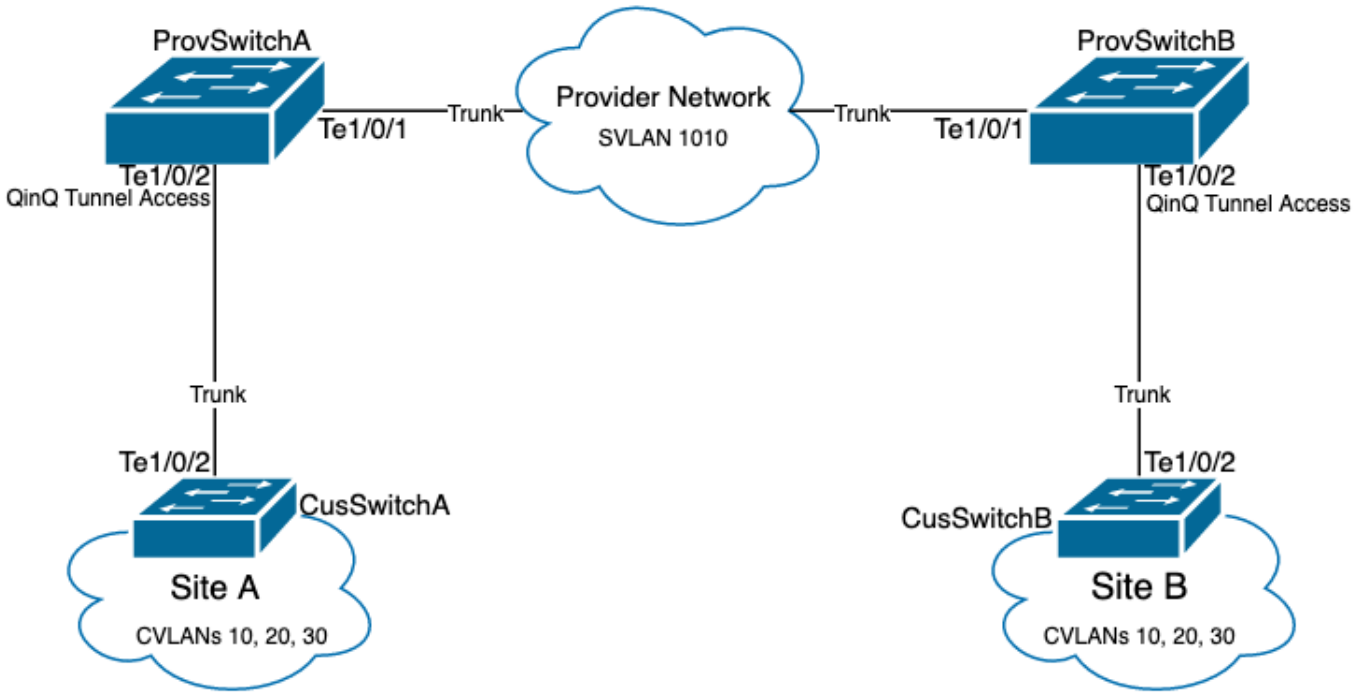
Este mismo proceso ocurre cuando el tráfico se reenvía del Sitio B al Sitio A, y la misma configuración, verificación y pasos para resolver problemas se aplican para el switch PE ProvSwitchB. Supongamos que todos los demás dispositivos dentro de la red del switch del proveedor y los sitios del cliente solo se configuran con comandos de acceso/trunk y no realizan ninguna función QinQ.

El ejemplo presentado supone que el tráfico con una sola etiqueta 802.1Q se recibe en los switches de acceso de túnel QinQ; sin embargo, el tráfico recibido puede tener cero o más

etiquetas 802.1Q. La etiqueta SVLAN se agrega a la pila de VLAN recibida. No se requieren configuraciones QinQ, VLAN y troncales adicionales en los dispositivos para admitir el tráfico con cero o más etiquetas 802.1Q; sin embargo, la unidad de transmisión máxima (MTU) en los dispositivos debe cambiarse para admitir los bytes adicionales agregados al tráfico (se describen detalles adicionales en la sección Solución de problemas).

Se presenta información adicional sobre los túneles IEEE 802.1Q en el documento Layer 2 Configuration Guide Document para Catalyst 9500 con 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



Configuración en 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
```

```
!
```

Configuración en ProvSwitchB (dispositivo PE de túnel QinQ):

```
!
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
!
```

Configuración en 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
!
```

Configuración en 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 las CVLAN no están definidas en los dispositivos del proveedor y que la SVLAN no está definida en los switches CE. Los dispositivos del proveedor reenvían tráfico basado solamente en SVLAN y no tienen en cuenta la información de CVLAN para ninguna decisión de reenvío, por lo tanto no es necesario que un dispositivo del proveedor sepa qué VLAN se reciben en un acceso de túnel QinQ (a menos que se utilice QinQ selectivo). Esto también significa que los mismos ID de VLAN utilizados para las etiquetas CVLAN se pueden utilizar para el tráfico dentro de la red conmutada del proveedor y viceversa. Si este es el caso, se recomienda configurar la **etiqueta vlan dot1q nativa** en el modo de configuración global para evitar cualquier pérdida de paquetes o problema de fuga de tráfico. El **vlan dot1q tag native** habilita la VLAN nativa 802.1Q para ser etiquetada en todas las interfaces trunk de forma predeterminada, pero esto se puede inhabilitar en el nivel de interfaz sin la configuración de la **etiqueta vlan nativa trunk switchport**.

Verificación

La configuración de puertos para túneles QinQ y L2PT se puede verificar desde la perspectiva de Cisco IOS XE a la perspectiva de circuito integrado de aplicación específica de reenvío (FWD-ASIC), donde se producen las decisiones de reenvío en un switch Catalyst. Los comandos básicos de verificación de Cisco IOS XE son:

- **show dot1q-tunnel** - Enumera las interfaces configuradas como acceso al túnel QinQ.

```
ProvSwitchA# show dot1q-tunnel
dot1q-tunnel mode LAN Port(s)
------------------------------
Te1/0/2
```

- **show vlan id {svlan-number}** - Muestra las interfaces asignadas a la VLAN especificada.

```
ProvSwitchA# show vlan id 1010
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1010 QinQ-VLAN                        active    Te1/0/1, Te1/0/2
```

- **show interfaces trunk** - Enumera las interfaces configuradas en el modo trunk.

```
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** - Enumera el estado global de la etiqueta de VLAN nativa 802.1Q y las interfaces troncales configuradas para etiquetar la VLAN nativa 802.1Q.

```
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}** - Muestra las direcciones MAC aprendidas en la SVLAN. Las direcciones MAC de los dispositivos LAN se aprenden en la SVLAN independientemente de la CVLAN utilizada.

```
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** - Muestra la interfaz habilitada para L2PT y los contadores para cada uno de los protocolos L2 habilitados.

```
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** - Se puede ejecutar en los switches CE para confirmar que pueden verse entre sí a través de 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
```

Cuando una interfaz se configura como un acceso de túnel QinQ a través de las interfaces de línea de comandos (CLI), Cisco IOS XE activa el proceso del administrador de puertos (PM) para configurar los puertos de switch con el modo y la VLAN especificados. La información del puerto de switch se puede verificar en PM con el comando **show pm port interface {interface-name}**.

Nota: Para ejecutar los comandos PM, es necesario configurar el servicio interno en el modo de configuración global. Esta configuración permite que se ejecuten comandos adicionales de plataforma y depuración en la CLI, y no tiene impacto funcional en la red. Se recomienda quitar este comando una vez que se haya completado la verificación de PM.

```
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
```

La interfaz Te1/0/2 tiene asignado el número de interfaz (if_number) de 2. Este es el identificador de interfaz (IF-ID), el valor interno que identifica un puerto específico. La configuración del puerto de switch también se puede verificar en el PM con el comando show platform software pm-port switch 1 R0 interface {IF-ID}.

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

IntfPORTDEFAULTNATIVEALLOWMODEPORTPORT
IDENABLEVLANVLANNATIVEDUPLEXSPEED
-------------------------------------------------------------
2TRUE1010101OTRUEtunnelfullunknown
```

Una vez que PM aplica la configuración del puerto de switch, PM retransmite la información del puerto al controlador del motor de reenvío (FED) para programar los circuitos integrados específicos de la aplicación (ASIC) en consecuencia.

En FED, los puertos se pueden verificar con el comando show platform software fed switch {switch-number} port if_id {IF-ID} para confirmar que están programados como puertos de acceso de túnel QinQ:

```
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
```

A diferencia de los puertos de switch en el modo de acceso, que esperan recibir solamente tráfico sin etiqueta, un puerto de switch configurado en el modo de túnel 802.1Q también acepta tráfico con etiquetas 802.1Q. FED permite esta función en el puerto para los puertos de acceso de túnel

QinQ, como se puede confirmar con el **show platform software fed switch {switch-number} ifm if-id {IF-ID}**:

```
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]
```

FED también proporciona un valor de identificador en un formato hexadecimal denominado Entidad lógica de puerto (Port LE). El LE de puerto es un puntero a la información de puerto programada en el ASIC de reenvío (fwd-asic). El comando **show platform hardware fed switch 1 fwd-asic abstraction print-resource-handle {Port-LE-handle} 1** muestra las diferentes funciones habilitadas en el puerto en el nivel ASIC:

```
C9500-12Q-PE1# show platform hardware fed switch 1 fwd-asic abstraction print-resource-handle
0x7f79548c3718 1

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
================================================================
```

Este resultado confirma en el nivel ASIC que el puerto de switch de acceso al túnel QinQ está configurado para permitir el tráfico sin etiqueta y con etiqueta 802.1Q desde la LAN, y asignar la SVLAN 1010 para ser reenviada a través de la red conmutada del proveedor. Observe que el campo LEAD_PORT_SEL_QINQ_ENABLED no está definido. Este bit está configurado sólo para la configuración QinQ selectiva, no para la configuración de túneles QinQ tradicionales como se presenta en este documento.

Troubleshoot

Esta sección proporciona los pasos que puede seguir para resolver problemas de su configuración. La herramienta más útil para resolver problemas de tráfico en un túnel 802.1Q es el analizador de puerto conmutado (SPAN). Las capturas de SPAN se pueden utilizar para verificar la etiqueta 802.1Q de la CVLAN recibida de la LAN y la SVLAN agregadas en el dispositivo de acceso de túnel QinQ.

> **Nota**: las capturas de paquetes integradas (EPC) también se pueden utilizar para capturar el tráfico en un entorno de túnel 802.1Q. Sin embargo, las capturas de paquetes de salida con EPC se producen antes de que el tráfico se etiquete con IEEE 802.1Q (la inserción de etiquetas 802.1Q se produce en el nivel del puerto en la dirección de salida). En consecuencia, el EPC de salida en el troncal de enlace ascendente del dispositivo de borde del proveedor no puede mostrar la etiqueta SVLAN utilizada en la red conmutada del proveedor. Una opción para recopilar el tráfico de doble etiqueta con EPC es capturar el tráfico con EPC de entrada en el dispositivo del proveedor vecino.
> Consulte la Guía de configuración de administración de red para switches Catalyst 9500 con Cisco IOS XE Amsterdam-17.3.x para obtener información adicional 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 SPAN para capturar el tráfico con etiquetas 802.1Q, es importante configurar el comando **monitor session {session-number} destination interface {interface-name} encapsulation replicate**. Si la palabra clave **encapsulation replicate** no se configura, el tráfico reflejado con SPAN podría contener información de etiquetas 802.1Q incorrecta. Consulte la sección Configuración para ver un ejemplo de la configuración de SPAN.

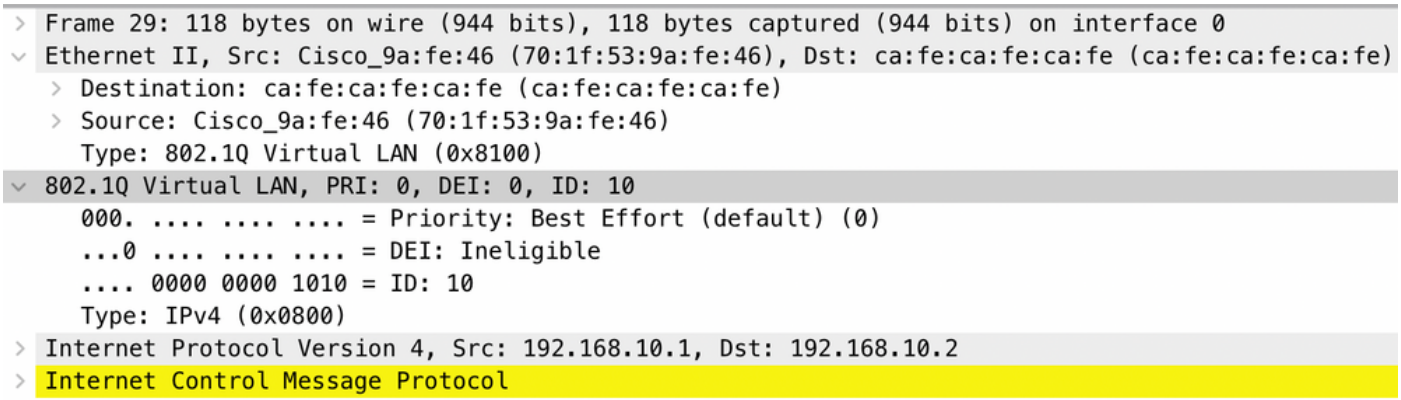
Para obtener información adicional sobre SPAN, consulte la Guía de configuración de administración de red para switches Catalyst 9500 con Cisco IOS XE Amsterdam-17.3.x

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

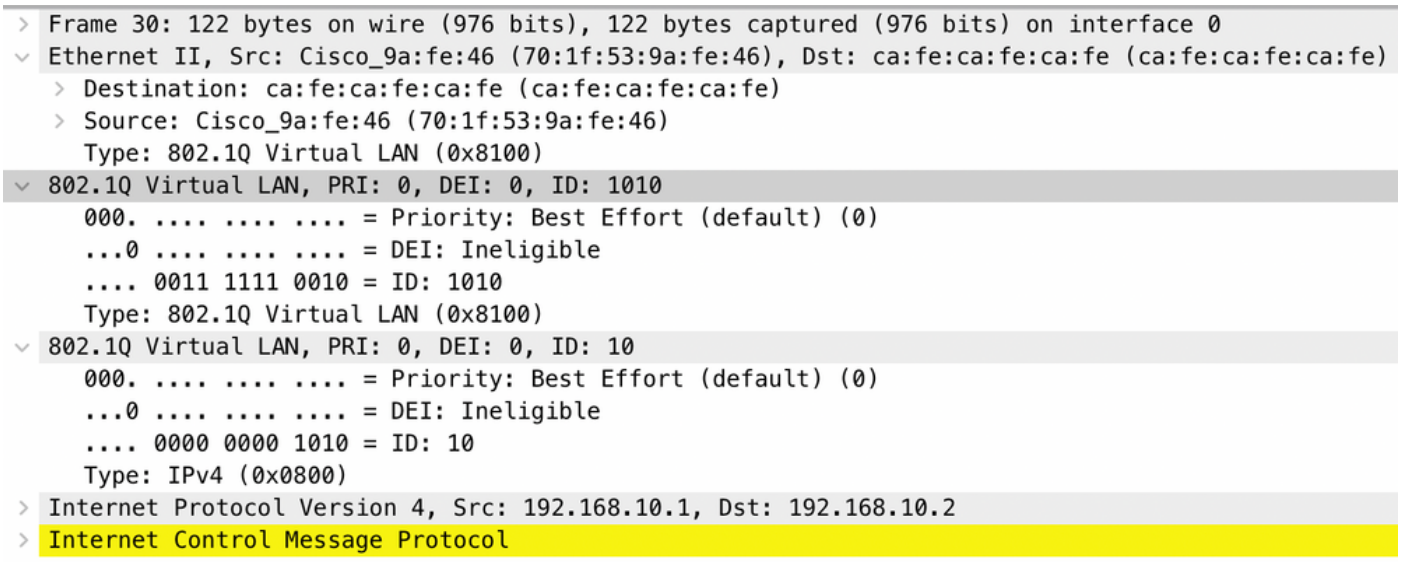
Ejemplo de configuración de SPAN en ProvSwitchA:

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

En el dispositivo Network Analyzer, el tráfico reflejado recibido se puede revisar para confirmar la presencia de la CVLAN 10 en el ingreso de acceso al túnel QinQ:



De manera similar, la presencia de CVLAN 10 y SVLAN 1010 se puede confirmar en la dirección de salida en el troncal de interfaz conectado a la red conmutada del proveedor.



> **Nota**: algunas tarjetas de interfaz de red (NIC) de los analizadores de red pueden eliminar etiquetas 802.1Q del tráfico etiquetado recibido. Póngase en contacto con el proveedor de NIC para obtener información específica sobre cómo mantener las etiquetas 802.1Q en las tramas recibidas.

Si se sospecha una pérdida de tráfico en la red conmutada QinQ, tenga en cuenta estos elementos para revisar:

- La unidad de transmisión máxima (MTU) predeterminada en una interfaz troncal es de 1522 bytes. Esto explica la MTU IP de 1500, la trama de encabezado Ethernet de 18 bytes y una etiqueta 802.1Q de 4 bytes. La MTU configurada en todos los dispositivos de borde de proveedor y proveedor debe tener 4 bytes adicionales por etiqueta 802.1Q agregada en la pila de VLAN. Por ejemplo, para una pila VLAN de 2 etiquetas, se debe configurar una MTU de 1504. Para una pila VLAN de 3 etiquetas, se debe configurar una MTU de 1508, y así sucesivamente. Consulte la Guía de Configuración de Componentes de Hardware e Interfaz para Catalyst 9500 con Cisco IOS XE Amsterdam-17.3.x para obtener detalles de la configuración 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
- No se admite el tráfico dirigido a la CPU en dispositivos dentro de un túnel 802.1Q. Las funciones que requieren inspección de tráfico pueden causar pérdida de paquetes o fugas de paquetes en un entorno 802.1Q. Algunos ejemplos de estas funciones son la indagación DHCP para tráfico DHCP, la indagación IGMP para tráfico IGMP, la indagación MLD para tráfico MLD y la inspección dinámica ARP para tráfico ARP. Se recomienda inhabilitar estas funciones en la SVLAN utilizada para transportar tráfico a través de la red conmutada del proveedor.

Comandos debug adicionales

> **Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los**

comandos debug.

- **debug pm port** - Muestra las transiciones de puerto del Administrador de puertos (PM) y el modo programado. Útil para depurar el estado de configuración del puerto QinQ.

Información Relacionada

- Switches Catalyst 9300 - Configuración de la tunelización IEEE 802.1Q
- Switches Catalyst 9300 - Configuración de tunelación de protocolo de capa 2
- Switches Catalyst 9300 - Configuración de EtherChannels
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).