Configureren Controleer probleemoplossing QinQ en L2PT op Catalyst 9000 Switches

Inhoud

Inleiding

Dit document beschrijft hoe u kunt configureren. Controleer en verwerk 802.1Q-tunnels (QinQ) en Layer 2 Protocol Tunneling (L2PT) op de Catalyst 9000-reeks switches waarop Cisco IOS® XE-software wordt uitgevoerd.

Raadpleeg de Officiële Cisco Releaseopmerkingen en Configuratiehandleidingen voor actuele informatie over de beperkingen, beperkingen, configuratieopties en voorbehouden en overige relevante informatie over deze functie.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Catalyst 9000 Series Switches-architectuur
- Cisco IOS XE-softwarearchitectuur
- Virtual Local Area Networks (VLAN), VLAN-trunks en IEEE 802.1Q-insluiting
- Layer 2-protocollen zoals Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP), Spanning Tree Protocol (STP), Link Aggregation Control Protocol (LACS) en Port Aggregation Protocol (PAgP).
- Basiskennis van QinQ-tunnels, selectieve QinQ-tunnels en Layer 2 Protocol-tunneling (L2PT)
- Switched Port Analyzer (SPAN) en ingesloten pakketvastlegging (EPC)

Gebruikte componenten

De informatie in dit document is gebaseerd op deze hardware- en softwareversies:

- Cisco Catalyst C9500-12Q switch met Cisco IOS XE 17.3.3

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Verwante producten

Dit document kan ook worden gebruikt voor de volgende hardware- en softwareversies:

- Catalyst 3650 en 3850 Series switches met Cisco IOS XE-software
- Catalyst 9200, 9300, 9400 en 9600 Series switches met Cisco IOS XE-software

Configureren

In deze sectie wordt een basistopologie voor de implementatie van IEEE 802.1Q-tunnels (QinQ) op Catalyst 9000 switches gepresenteerd, evenals configuratievoorbeelden voor elke Catalyst switch.

Netwerkdiagram

In de gepresenteerde topologie zijn er twee sites, Site A en Site B, die fysiek worden gescheiden door een serviceprovider switched netwerk waar Service Virtual LAN (SVLAN) 1010 wordt gebruikt. Provider Edge (PE) switches ProvSwitchA en ProvSwitchB verleent toegang tot site A respectievelijk site B aan het providernetwerk. Site A en Site B maken gebruik van Customer VLAN's (CVLAN) 10, 20 en 30 en vereisen dat deze VLAN's worden uitgebreid op Layer 2 (L2). Site A verbindt met het netwerk van de provider via Customer Edge (CE) switch CusSwitchA en Site B via CE switch CusSwitchB.

Site A stuurt verkeer met de IEEE 802.1Q-tag van het gebruikte CVLAN, ook wel aangeduid als binnentag, naar de PE-switch ProvSwitchA, die fungeert als een QinQ Tunnel Access. ProvSwitchA stuurt het ontvangen verkeer door naar het provider switched netwerk met de tweede IEEE 802.1Q-tag van het SVLAN, ook wel buitentag of Metro-tag genoemd, toegevoegd bovenop de CVLAN 802.1Q-tag. Dit proces wordt ook wel VLAN-stacks genoemd en dit voorbeeld geeft een 2-tag VLAN-stack weer. Het verkeer met dubbele tags wordt doorgestuurd door L2 in het providernetwerk dat alleen op basis van MAC-tabelinformatie (VLAN Media Access Control) is gebaseerd. Zodra het dubbel-gelabelde verkeer op het verre eind van de QinQ-switch aankomt, ontdoet de externe PE-tunnelprovSwitchB, die ook fungeert als QinQ Tunnel Access, de SVLAN-tag van het verkeer en stuurt het door naar de Site B gelabeld alleen met de CVLAN 802.1Q-tag, waardoor de Layer 2-extensie van de VLAN's over de externe sites wordt bereikt. L2 Protocollen Tunneling is ook geïmplementeerd om Cisco Discovery Protocol (CDP)-frames tussen de CE-switches CusSwitchA en CusSwitchB uit te wisselen.

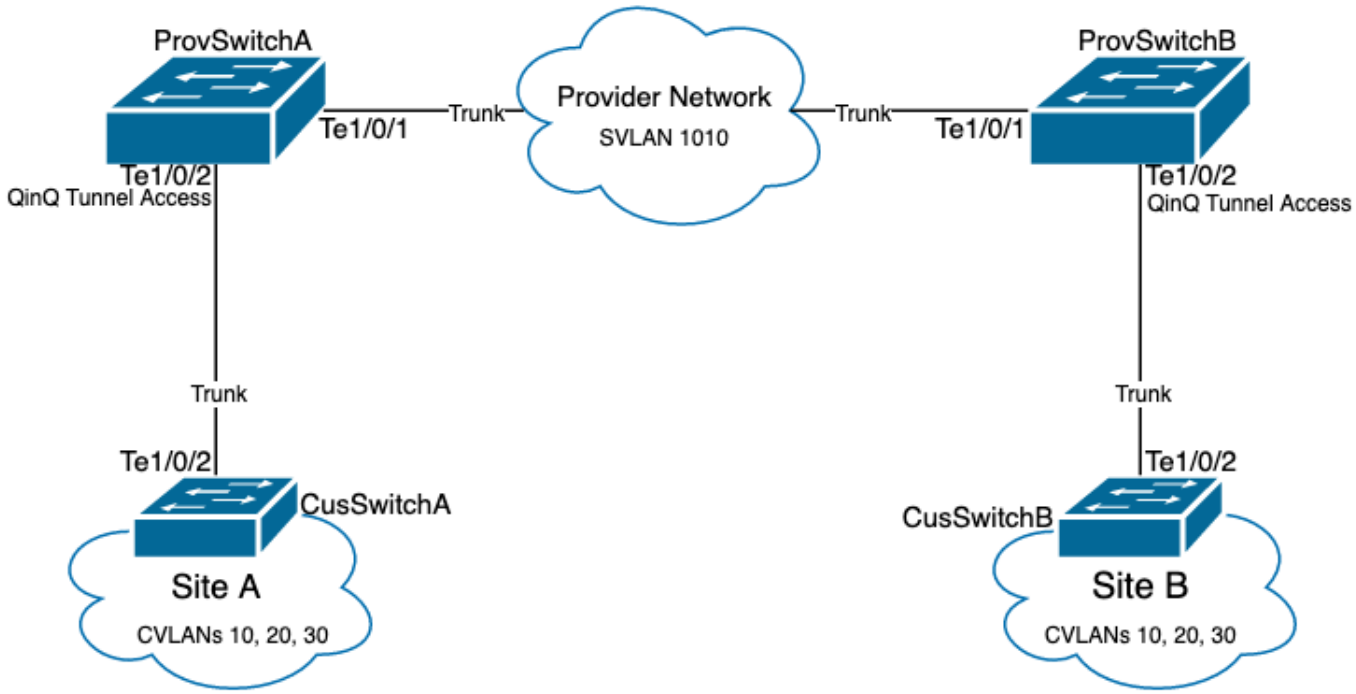
Dit zelfde proces gebeurt wanneer het verkeer van Site B naar Site A wordt doorgestuurd, en dezelfde configuratie, verificatie en stappen om problemen op te lossen van toepassing zijn op PE switch ProvSwitchB. Stel dat alle andere switches in het netwerk van de provider en de locaties van de klant alleen zijn geconfigureerd met toegang/trunkopdrachten en geen QinQ-functie uitvoeren.

In het gepresenteerde voorbeeld wordt ervan uitgegaan dat verkeer met slechts één 802.1Q-tag

wordt ontvangen in de QinQ-switches voor tunneltoegang, maar ontvangen verkeer kan nul of meer 802.1Q-tags hebben. De SVLAN-tag wordt toegevoegd aan de ontvangen VLAN-stack. Er zijn geen extra QinQ-, VLAN- en trunkconfiguraties nodig in de apparaten om verkeer met nul of meer 802.1Q-tags te ondersteunen. De Max Transmission Unit (MTU) op de apparaten moet echter worden gewijzigd om de extra bytes te ondersteunen die aan het verkeer worden toegevoegd (aanvullende details worden beschreven in het gedeelte Probleemoplossing).

Aanvullende informatie over IEEE 802.1Q-tunnels wordt weergegeven in de Layer 2 Configuration Guide Document voor Catalyst 9500 met 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



Configuratie op ProvSwitchA (QinQ tunnel PE):

```
!
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
!
```

Configuratie op ProvSwitchB (QinQ tunnel PE-apparaat):

```
!
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
!
```

Configuratie op Cisco SwitchA (CE-apparaat):

```
!
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
!
```

Configuratie op Cisco SwitchB (CE-apparaat):

```
!
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
!
```

Bericht dat CVLANs niet in de leveranciersapparaten worden bepaald, en SVLAN wordt niet bepaald op de switches van Ce. De provider-apparaten sturen verkeer alleen door op SVLAN en overwegen de CVLAN-informatie niet voor een voorwaarts besluit. Daarom is het niet nodig dat een provider-apparaat weet welke VLAN's worden ontvangen in een QinQ-tunneltoegang (tenzij Selectieve QinQ wordt gebruikt). Dit betekent ook dat dezelfde VLAN-ID's die voor de VLAN-tags worden gebruikt, kunnen worden gebruikt voor verkeer binnen het providerswitched netwerk en de viceversa. Als dit probleem zich voordoet, is het raadzaam om de **VLAN dot1q tag native** te configureren in de Global Configuration-modus om pakketverlies of lekkage van verkeer te voorkomen. De **VLAN dot1q tag native** maakt het mogelijk om 802.1Q native VLAN op alle trunkinterfaces te labelen, maar dit kan worden uitgeschakeld op interfaceniveau zonder **switchport trunk native VLAN-**tagconfiguratie.

Verifiëren

De poortconfiguratie voor QinQ-tunnels en L2PT kan worden geverifieerd vanuit Cisco IOS XE-perspectief naar het Forwarding Application-Specific Integrated Circuit (FWD-ASIC)-perspectief, waar de voorwaartse beslissingen over een Catalyst switch plaatsvinden. De basisopdrachten voor Cisco IOS XE-verificatie zijn:

- **toon dot1q-tunnel** - Toont de interfaces die als QinQ-tunneltoegang zijn geconfigureerd.

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

- **toon VLAN id {svlan-number}** - Toont de interfaces die aan het gespecificeerde VLAN zijn toegewezen.

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

- **toon interfaces trunk** - Toont de interfaces die in trunkmodus zijn geconfigureerd.

```
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
```

- toon VLAN dot1q tag native - Toont de 802.1Q native VLAN-tag globale status en trunkinterfaces die zijn geconfigureerd om 802.1Q native VLAN te labelen.

```
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
```

- toon mac adres-tabel vlan {svlan-number} - toont MAC-adressen die in het SVLAN zijn geleerd. MAC-adressen van LAN-apparaten worden in het SVLAN geleerd, ongeacht het gebruikte VLAN.

```
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
```

- toon l2-protocol tunnel - Toont de interface voor L2PT en tellers voor elk van de ingeschakelde L2 protocollen.

```
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
                    ---         ----      ----      ----      ----      ----
```

- toon cdp buur - Kan op CE switches worden uitgevoerd om te bevestigen dat ze elkaar via CDP kunnen zien.

```
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
```

Wanneer een interface is geconfigureerd als een QinQ-tunneltoegang via Command Line Interfaces (CLI), activeert Cisco IOS XE het Port Manager (PM)-proces om de switchpoorten met de opgegeven modus en VLAN te configureren. De informatie van Switchport kan in PM met het show pm poortinterface {interface-name} bevel worden gecontroleerd.

> **Opmerking**: om PM-opdrachten uit te voeren, moet u de **service intern** configureren in de globale configuratiemodus. Deze configuratie maakt het mogelijk dat extra platform- en debug-opdrachten worden uitgevoerd op de CLI en heeft geen functionele invloed op het netwerk. Het wordt aanbevolen deze opdracht te verwijderen zodra de PM-verificatie is voltooid.

```
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
```

De interface Te1/0/2 krijgt het interfacenummer (if_number) van 2. Dit is de Interface Identifier (IF-ID), de interne waarde die een specifieke poort identificeert. De switchport configuratie kan ook worden geverifieerd op PM met de **show platform software pm-port switch 1 R0 interface {IF-ID}** opdracht.

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

IntfPORTDEFAULTNATIVEALLOWMODEPORTPORT
IDENABLEVLANVLANNATIVEDUPLEXSPEED
-----------------------------------------------------------
2TRUE10101010TRUEtunnelfullunknown
```

Zodra PM de switchpoortconfiguratie toepast, geeft PM de poortinformatie door aan het Forwarding Engine Driver (FED) om de Application-Specific Integrated Circuits (ASIC) dienovereenkomstig te programmeren.

In de FED kunnen poorten worden gecontroleerd met de **show platform software fed switch {switch-number} port if_id {IF-ID}** opdracht om te bevestigen dat ze zijn geprogrammeerd als QinQ tunneltoegangpoorten:

```
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
```

In tegenstelling tot switchports in de toegangsmodus, die alleen verkeer zonder tags verwachten te ontvangen, accepteert een switchport die is geconfigureerd in de 802.1Q-tunnelmodus ook

verkeer met 802.1Q-tags. De FED staat deze functie toe op de poort voor QinQ tunneltoegangpoorten, zoals kan worden bevestigd met de **show platform software fed switch {switch-nummer} 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]
```

De FED levert ook een handvat in een hexadecimaal formaat genaamd Port Logical Entity (Port LE). De poort LE is een aanwijzer naar de poortinformatie die geprogrammeerd is in de Forwarding ASIC (fwd-asic). Het **show platform hardware fed switch 1 fwd-asic abstraction print-resource-handle {Port-LE-handle} 1** commando toont de verschillende functies die op de poort op ASIC-niveau zijn ingeschakeld:

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

Deze uitvoer bevestigt op ASIC-niveau dat de QinQ-tunneltoegangsswitchpoort is geconfigureerd om verkeer zonder tags en 802.1Q-gelabeld verkeer via het LAN toe te staan en SVLAN 1010 toe te wijzen om via het providerswitched netwerk te worden doorgestuurd. Opmerking: het veld LEAD_PORT_SEL_QINQ_ENABLED is verwijderd. Dit bit is alleen ingesteld voor selectieve QinQ-configuratie, niet voor traditionele QinQ-tunnelconfiguratie zoals in dit document wordt weergegeven.

Problemen oplossen

In deze sectie vindt u de stappen die u kunt volgen om problemen met uw configuratie op te lossen. Het nuttigste hulpmiddel om verkeersproblemen in een 802.1Q-tunnel op te lossen is Switched Port Analyzer (SPAN). Met SPAN-opnamen kan de 802.1Q-tag van het VLAN worden geverifieerd die van het LAN is ontvangen en kan VLAN worden toegevoegd aan het QinQ-tunneltoegangsapparaat.

> **Opmerking**: ingesloten pakketvastlegging (EPC) kan ook worden gebruikt om verkeer in een 802.1Q-tunnelomgeving op te nemen. Uitgangspakket wordt echter met EPC opgenomen voordat het verkeer is gelabeld met IEEE 802.1Q (802.1Q tag insertion vindt plaats op poortniveau in uitgangsrichting). Dientengevolge, kan de uitgang EPC op de de opstraalverbindingsboomstam van het leverancier-rand apparaat niet de markering tonen SVLAN die in het leverancier switched netwerk wordt gebruikt. Een optie om het dubbel-gelabelde verkeer met EPC te verzamelen is het verkeer met toegang EPC op het buurprovider apparaat te vangen.
> Raadpleeg de Network Management Configuration Guide voor Catalyst 9500-switches met Cisco IOS XE Amsterdam-17.3.x voor meer informatie over 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

Om SPAN te vormen om verkeer met 802.1Q markeringen op te nemen, is het belangrijk om het bevel van de de **doelinterface van de monitorzitting {zitting-aantal} {interface-naam} inkapselingsherhaling** te vormen. Als het sleutelwoord voor **inkapselingsreplicatie** niet is geconfigureerd, kan het verkeer dat met SPAN wordt gespiegeld onjuiste informatie over 802.1Q-tags bevatten. Raadpleeg de sectie Configureren voor een voorbeeld van de SPAN-configuratie.

Raadpleeg voor aanvullende informatie over SPAN de Network Management Configuration Guide voor Catalyst 9500-switches met 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

Voorbeeld van SPAN-configuratie op ProvSwitchA:

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

In het apparaat van de Analyzer van het Netwerk, kan het ontvangen gespiegelde verkeer worden herzien om de aanwezigheid van CVLAN 10 in de toegang van de QinQ-tunnel te bevestigen:

```
> 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
```

Op dezelfde manier kan de aanwezigheid van zowel CVLAN 10 als SVLAN 1010 worden bevestigd in de uitgangsrichting in de interfacetrunk die is aangesloten op het netwerk van de provider.

```
> 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
```

> **Opmerking**: met bepaalde netwerkinterfacekaarten (NIC) op netwerkanalysatoren kunnen 802.1Q-tags op gelabeld ontvangen verkeer worden verwijderd. Neem contact op met de leverancier van de NIC voor specifieke informatie over het onderhouden van de 802.1Q-tags op ontvangen frames.

Als verkeersverlies in het QinQ switched netwerk wordt vermoed, overweeg deze items om te bekijken:

- Standaard Maximale Transmissie Eenheid (MTU) op een trunked interface is 1522 bytes. Dit verklaart IP MTU van 1500, het Ethernet kopbalkader van 18 bytes, en één markering 802.1Q van 4 bytes. Geconfigureerde MTU in alle provider en provider edge-apparaten moet 4 extra bytes per 802.1Q-tag hebben toegevoegd in de VLAN-stack. Bijvoorbeeld, voor een 2-tag VLAN-stack moet een MTU van 1504 worden geconfigureerd. Voor een 3-tag VLAN-stack moet een MTU van 1508 worden geconfigureerd, enzovoort. Raadpleeg de configuratiehandleiding voor interface- en hardwarecomponenten voor Catalyst 9500 met Cisco IOS XE Amsterdam-17.3.x voor MTU-configuratiedetails: 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
- Traffic point naar de CPU op apparaten binnen een 802.1Q-tunnel wordt niet ondersteund.

Functies die traffic inspection vereisen, kunnen pakketverlies of pakketlekken in een 802.1Q-omgeving veroorzaken. Voorbeelden van deze functies zijn DHCP-controle voor DHCP-verkeer, IGMP-controle voor IGMP-verkeer, MLD-controle voor MLD-verkeer en Dynamische ARP-inspectie voor ARP-verkeer. Het wordt aanbevolen om deze functies op het VLAN uit te schakelen om verkeer te transporteren via het netwerk van de provider.

Aanvullende debug-opdrachten

Opmerking: Raadpleeg Belangrijke informatie over debug commando's voordat u **debug** commando's gebruikt.

- **debug pm poort** - Hier worden poortovergangen en geprogrammeerde modus weergegeven voor Port Manager (PM). Handig om QinQ poortconfiguratiestatus te debuggen.

Gerelateerde informatie

- Catalyst 9300 Switches - IEEE 802.1Q-tunneling configureren
- Catalyst 9300 Switches - Layer 2-protocoltunneling configureren
- Catalyst 9300 Switches - EtherChannel configureren
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.