

Configurazione e verifica della risoluzione dei problemi QinQ e L2PT sugli switch Catalyst 9000

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Comandi di debug aggiuntivi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare, verificare e risolvere i problemi relativi ai tunnel 802.1Q (QinQ) e al tunneling del protocollo di layer 2 (L2PT) sulla famiglia di switch Catalyst 9000 con software Cisco IOS® XE.

Fare riferimento alle Note ufficiali sulla versione e alle Guide alla configurazione Cisco per informazioni aggiornate su limitazioni, restrizioni, opzioni di configurazione e avvertenze, nonché su altri dettagli relativi a questa funzione.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Catalyst serie 9000 Switch Architettura
- Architettura software Cisco IOS XE
- VLAN (Virtual Local Area Network), trunk VLAN e incapsulamento IEEE 802.1Q
- Protocolli di layer 2, ad esempio Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP), Spanning Tree Protocol (STP), Link Aggregation Control Protocol (LACP) e Port Aggregation Protocol (PAgP).
- Conoscenze base di tunnel QinQ, tunnel QinQ selettivi e tunnel di protocollo di livello 2 (L2PT)
- SPAN (Switched Port Analyzer) e EPC (Embedded Packet Capture)

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni hardware e software:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Il presente documento può essere utilizzato anche per le seguenti versioni hardware e software:

- Switch Catalyst serie 3650 e 3850 con software Cisco IOS XE
- Catalyst serie 9200, 9300, 9400 e 9600 switch con software Cisco IOS XE

Configurazione

In questa sezione viene presentata una topologia di base per l'implementazione dei tunnel IEEE 802.1Q (QinQ) sugli switch Catalyst 9000 e alcuni esempi di configurazione per ciascuno switch Catalyst.

Esempio di rete

Nella topologia presentata sono presenti due siti, il sito A e il sito B, fisicamente separati da una rete a commutazione di provider di servizi in cui viene utilizzata la LAN virtuale di servizio (SVLAN) 1010. Gli switch Provider Edge (PE) ProvSwitchA e ProvSwitchB concedono l'accesso rispettivamente al Sito A e al Sito B alla rete del provider. La sede A e la sede B usano le VLAN del cliente (CVLAN) 10, 20 e 30 e richiedono l'estensione di queste VLAN sul layer 2 (L2). Il sito A si connette alla rete del provider tramite lo switch CusSwitchA Customer Edge (CE) e il sito B tramite lo switch CE CusSwitchB.

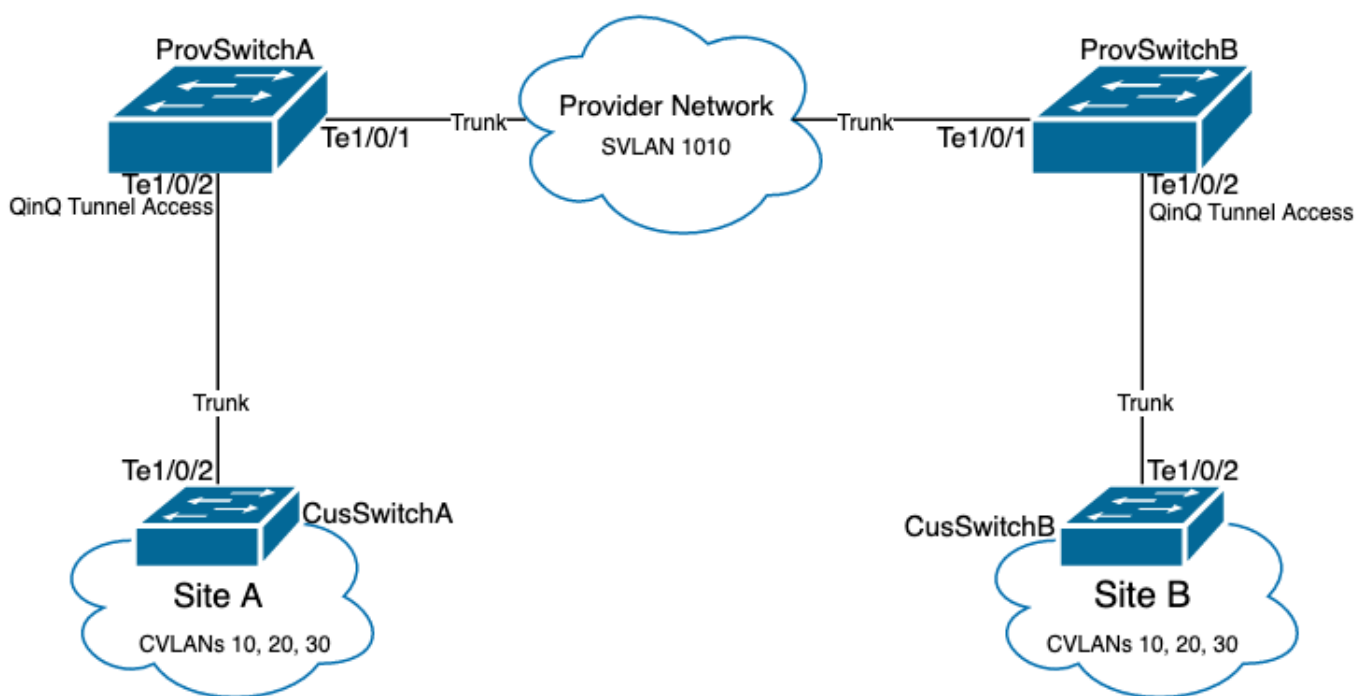
Il sito A invia il traffico con il tag IEEE 802.1Q della CVLAN utilizzata, o tag interno, allo switch PE ProvSwitchA, che agisce da accesso tunnel QinQ. ProvSwitchA inoltra il traffico ricevuto alla rete a commutazione di provider con il secondo tag IEEE 802.1Q della SVLAN, detto anche tag esterno o tag Metro, aggiunto sopra il tag CVLAN 802.1Q. Questo processo è noto anche come stack VLAN e nell'esempio riportato viene presentato uno stack VLAN a 2 tag. Il traffico con doppio tag viene inoltrato da L2 nella rete del provider solo in base alle informazioni della tabella SVLAN Media Access Control (MAC). Quando il traffico con doppio tag arriva all'estremità remota del tunnel QinQ, lo switch PE remoto ProvSwitchB, che agisce anche come accesso al tunnel QinQ, rimuove il tag SVLAN dal traffico e lo inoltra al sito B contrassegnato solo con il tag CVLAN 802.1Q, ottenendo l'estensione di layer 2 delle VLAN sui siti remoti. Il tunneling dei protocolli L2 è implementato anche per scambiare i frame Cisco Discovery Protocol (CDP) tra gli switch CE CusSwitchA e CusSwitchB.

Lo stesso processo si verifica quando il traffico viene inoltrato dal Sito B al Sito A e la stessa configurazione, verifica e procedura di risoluzione dei problemi sono valide per lo switch PE ProvSwitchB. Si supponga che tutti gli altri dispositivi all'interno della rete dello switch del provider e le sedi del Cliente siano configurati solo con comandi di accesso/trunk e non eseguano alcuna funzione QinQ.

Nell'esempio si presume che gli switch di accesso al tunnel QinQ ricevano solo un tag 802.1Q, ma il traffico ricevuto può avere zero o più tag 802.1Q. Il tag SVLAN viene aggiunto allo stack di VLAN ricevuto. Non sono necessarie ulteriori configurazioni QinQ, VLAN e trunk nei dispositivi per supportare il traffico con zero o più tag 802.1Q. Tuttavia, è necessario modificare l'MTU (Maximum Transmission Unit) nei dispositivi per supportare i byte aggiuntivi aggiunti al traffico (ulteriori dettagli descritti nella sezione Risoluzione dei problemi).

Per ulteriori informazioni sui tunnel IEEE 802.1Q, consultare il documento sulla guida alla configurazione di layer 2 per 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



Configurazione su dispositivo 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
!
```

Configurazione su ProvSwitchB (dispositivo QinQ tunnel PE):

```
<#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
!
!
```

Configurazione su 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  
!
```

Configurazione su 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  
!
```

Si noti che le CVLAN non sono definite nei dispositivi del provider e che la SVLAN non è definita sugli switch CE. I dispositivi del provider inoltrano il traffico solo in base alla SVLAN e non prendono in considerazione le informazioni CVLAN per prendere una decisione in avanti, quindi non è necessario per i dispositivi del provider sapere quali VLAN sono state ricevute in un accesso al tunnel QinQ (a meno che non si utilizzi QinQ selettivo). Ciò significa anche che gli stessi ID VLAN utilizzati per i tag CVLAN possono essere utilizzati per il traffico all'interno della rete a commutazione del provider e viceversa. In questo caso, si consiglia di configurare il tag vlan dot1q in modo nativo sulla modalità di configurazione globale per evitare perdite di pacchetti o problemi di perdita di traffico. Per impostazione predefinita, la vlan dot1q tag native consente di

contrassegnare la VLAN nativa 802.1Q su tutte le interfacce trunk, ma questa opzione può essere disabilitata a livello di interfaccia senza la configurazione switchport trunk native vlan tag.

Verifica

La configurazione delle porte per i tunnel QinQ e L2PT può essere verificata dalla prospettiva Cisco IOS XE alla prospettiva FWD-ASIC (Forwarding Application-Specific Integrated Circuit), con le decisioni di inoltro su uno switch Catalyst. I comandi di base per la verifica di Cisco IOS XE sono:

- `show dot1q-tunnel`: elenca le interfacce configurate come accesso al tunnel QinQ.

<#root>

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

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

```
-----
```

```
Te1/0/2
```

- `show vlan id {svlan-number}`: visualizza le interfacce assegnate alla VLAN specificata.

<#root>

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

```
VLAN
```

```
Name Status
```

```
Ports
```

```
-----
```

```
1010
```

```
QinQ-VLAN active
```

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

- `show interfaces trunk`: elenca le interfacce configurate in modalità 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: elenca lo stato globale del tag VLAN nativo 802.1Q e le interfacce trunk configurate per contrassegnare la 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}: visualizza gli indirizzi MAC appresi nella SVLAN. Gli indirizzi MAC dei dispositivi LAN vengono appresi nella SVLAN indipendentemente dalla CVLAN usata.

<#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: visualizza l'interfaccia abilitata per L2PT e i contatori per ciascuno dei protocolli L2 abilitati.

<#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 neighbors - Può essere eseguito sugli switch CE per verificare che possano vedersi tramite 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 un'interfaccia è configurata come accesso al tunnel QinQ tramite interfacce della riga di comando (CLI), Cisco IOS XE avvia il processo Port Manager (PM) per configurare le porte dello switch con la modalità e la VLAN specificate. Le informazioni sulla porta di commutazione possono essere verificate in PM con il comando `show pm port interface {interface-name}`.

 Nota: per eseguire i comandi PM, è necessario configurare il servizio interno in modalità di configurazione globale. Questa configurazione consente di eseguire sulla CLI altri comandi di piattaforma e debug e non ha alcun impatto funzionale sulla rete. Si consiglia di rimuovere questo comando una volta completata la verifica del PM.

```
<#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
```

All'interfaccia Te1/0/2 è assegnato il numero di interfaccia (if_number) 2. Si tratta dell'identificatore di interfaccia (IF-ID), il valore interno che identifica una porta specifica. La configurazione di switchport può essere verificata anche su PM con il 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

```

Una volta applicata la configurazione switchport, PM inoltra le informazioni sulla porta al driver del motore di inoltra (FED) per programmare di conseguenza i circuiti integrati specifici dell'applicazione (ASIC, Application-Specific Integrated Circuits).

Nel feed, è possibile controllare le porte con il comando `show platform software fed switch {switch-number} porta if_id {IF-ID}` per verificare che siano programmate come porte di accesso al tunnel 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
```

A differenza delle switchport in modalità di accesso, che si aspettano di ricevere solo traffico senza tag, una switchport configurata in modalità tunnel 802.1Q accetta il traffico anche con tag 802.1Q. FED consente questa funzionalità sulla porta per le porte di accesso al tunnel QinQ, come può essere confermato con il comando `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]
```

FED fornisce inoltre un valore di handle in un formato esadecimale denominato Port Logical Entity (Port LE). Port LE è un puntatore alle informazioni sulla porta programmate nell'ASIC Forwarding (fwd-asic). Il comando `show platform hardware fed switch 1 fwd-asic abstraction print-resource-handle {Port-LE-handle} 1` visualizza le diverse funzionalità abilitate sulla porta a livello 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  
=====
```

Questo output conferma a livello ASIC che la porta dello switch di accesso al tunnel QinQ è configurata per consentire il traffico senza tag e con tag 802.1Q proveniente dalla LAN, quindi assegna la SVLAN 1010 da inoltrare sulla rete a commutazione di provider. Il campo LEAD_PORT_SEL_QINQ_ENABLED non è impostato. Questo bit è impostato solo per la configurazione QinQ selettiva, non per la configurazione dei tunnel QinQ tradizionali, come mostrato in questo documento.

Risoluzione dei problemi

In questa sezione viene descritto come risolvere i problemi relativi alla configurazione. Lo strumento più utile per risolvere i problemi relativi al traffico in un tunnel 802.1Q è SPAN (Switched Port Analyzer). Le clip SPAN possono essere usate per verificare il tag 802.1Q della CVLAN ricevuta dalla LAN e la SVLAN aggiunta al dispositivo di accesso al tunnel QinQ.

 Nota: l'EPC (Embedded Packet Capture) può essere utilizzata anche per acquisire il traffico in un ambiente tunnel 802.1Q. Tuttavia, le acquisizioni dei pacchetti in uscita con EPC avvengono prima che il traffico venga etichettato con IEEE 802.1Q (l'inserimento di tag 802.1Q avviene a livello di porta nella direzione di uscita). Di conseguenza, l'EPC in uscita sul trunk uplink del dispositivo sul lato del provider non è in grado di visualizzare il tag SVLAN utilizzato nella rete a commutazione di provider. Un'opzione per raccogliere il traffico con doppio tag con EPC consiste nell'acquisire il traffico con EPC in entrata sul dispositivo del provider adiacente.

Per ulteriori informazioni sull'EPC, consultare la guida alla configurazione della gestione della rete per gli switch 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_packet_capture.html

Per configurare SPAN per l'acquisizione del traffico con tag 802.1Q, è importante configurare il comando di replica dell'interfaccia di destinazione {interface-name} dell'incapsulamento della sessione di monitoraggio {session-number}. Se la parola chiave encapsulation replicate non è

configurata, il traffico con mirroring con SPAN potrebbe contenere informazioni sui tag 802.1Q errate. Per un esempio della configurazione SPAN, consultare la sezione Configure.

Per ulteriori informazioni su SPAN, consultare la guida alla configurazione della gestione di rete per gli switch 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

Esempio di configurazione SPAN su ProvSwitchA:


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

Nel dispositivo Network Analyzer, il traffico con mirroring ricevuto può essere esaminato per confermare la presenza di CVLAN 10 nell'ingresso del tunnel 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
```

Analogamente, è possibile confermare la presenza di CVLAN 10 e SVLAN 1010 in direzione di uscita nel trunk di interfaccia collegato alla rete a commutazione di 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
```

 Nota: alcune schede di interfaccia di rete (NIC, Network Interface Card) sugli analizzatori di rete possono rimuovere i tag 802.1Q sul traffico con tag ricevuto. Per informazioni specifiche su come mantenere i tag 802.1Q sui frame ricevuti, contattare il fornitore della scheda NIC.

Se si sospetta una perdita di traffico nella rete a commutazione QinQ, prendere in considerazione i seguenti elementi:

- L'MTU (Maximum Transmission Unit) predefinita su un'interfaccia trunking è 1522 byte. In questo modo viene calcolata l'MTU IP di 1500, il frame dell'intestazione Ethernet di 18 byte e un tag 802.1Q di 4 byte. L'MTU configurata in tutti i dispositivi periferici del provider e del provider deve avere 4 byte aggiuntivi per tag 802.1Q aggiunti nello stack VLAN. Ad esempio, per uno stack di VLAN a 2 tag, è necessario configurare un'MTU di 1504. Per uno stack VLAN a 3 tag, è necessario configurare un'MTU di 1508 e così via. Per i dettagli sulla configurazione dell'MTU, consultare la guida alla configurazione dei componenti di interfaccia e hardware per 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/int_hw/b_173_int_and_hw_9500_cg/configuring_system_mtu.html
- Il traffico diretto alla CPU sui dispositivi all'interno di un tunnel 802.1Q non è supportato. Le funzionalità che richiedono un'ispezione del traffico possono causare la perdita o la perdita di pacchetti in un ambiente 802.1Q. Esempi di queste funzionalità sono lo snooping DHCP per il traffico DHCP, lo snooping IGMP per il traffico IGMP, lo snooping MLD per il traffico MLD e l'ispezione ARP dinamica per il traffico ARP. Si consiglia di disabilitare queste funzionalità sulla SVLAN utilizzata per trasportare il traffico attraverso la rete a commutazione del provider.

Comandi di debug aggiuntivi

 Nota: consultare le [informazioni importanti sui comandi di debug](#) prima di usare i comandi di debug.

- debug pm port - Visualizza le transizioni delle porte di Port Manager (PM) e la modalità programmata. Utile per eseguire il debug dello stato di configurazione della porta QinQ.

Informazioni correlate

- [Switch Catalyst 9300 - Configurazione del tunneling IEEE 802.1Q](#)
- [Switch Catalyst 9300 - Configurazione del tunneling del protocollo di layer 2](#)
- [Switch Catalyst 9300 - Configurazione di EtherChannel](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).