Configuration Vérification du dépannage de QinQ et L2PT sur les commutateurs Catalyst 9000

Table des matières

Introduction

Ce document décrit comment configurer, vérifier et dépanner les tunnels 802.1Q (QinQ) et le protocole L2PT (Layer 2 Protocol Tunneling) sur la gamme de commutateurs Catalyst 9000 qui exécutent le logiciel Cisco IOS® XE.

Reportez-vous aux notes de version officielles et aux guides de configuration de Cisco pour obtenir des informations à jour sur les limitations, les restrictions, les options de configuration et les mises en garde, ainsi que tout autre détail pertinent sur cette fonctionnalité.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Architecture des commutateurs Catalyst 9000
- Architecture du logiciel Cisco IOS XE
- Réseaux locaux virtuels (VLAN), agrégations VLAN et encapsulation IEEE 802.1Q
- Les protocoles de couche 2 tels que CDP (Cisco Discovery Protocol), LLDP (Link Layer Discovery Protocol), STP (Spanning Tree Protocol), LACP (Link Aggregation Control Protocol) et PAgP (Port Aggregation Protocol).
- Connaissance de base des tunnels QinQ, des tunnels QinQ sélectifs et du protocole L2PT (Layer 2 Protocol Tunneling)

- SPAN (Switched Port Analyzer) et EPC (Embedded Packet Captures)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Produits connexes

Ce document peut également être utilisé avec les versions de matériel et de logiciel suivantes :

- Commutateurs des gammes Catalyst 3650 et 3850 avec logiciel Cisco IOS XE
- Commutateurs des gammes Catalyst 9200, 9300, 9400 et 9600 avec logiciel Cisco IOS XE

Configurer

Cette section présente une topologie de base pour le déploiement des tunnels IEEE 802.1Q (QinQ) sur les commutateurs Catalyst 9000, ainsi que des exemples de configuration pour chaque commutateur Catalyst.

Diagramme du réseau

Dans la topologie présentée, il y a deux sites, le site A et le site B, qui sont physiquement séparés par un réseau commuté de fournisseur de services où le réseau local virtuel de service (SVLAN) 1010 est utilisé. Les commutateurs de périphérie du fournisseur (PE) ProvSwitchA et ProvSwitchB accordent l'accès au site A et au site B, respectivement, au réseau du fournisseur. Le site A et le site B utilisent les VLAN client (CVLAN) 10, 20 et 30 et nécessitent que ces VLAN soient étendus au niveau de la couche 2 (L2). Le site A se connecte au réseau du fournisseur via le commutateur de périphérie client (CE) CusSwitchA et le site B via le commutateur CE CusSwitchB.

Le site A envoie le trafic avec l'étiquette IEEE 802.1Q du CVLAN utilisé, également appelée étiquette interne, au commutateur PE ProvSwitchA, qui agit comme un accès au tunnel QinQ. ProvSwitchA transfère le trafic reçu au réseau commuté du fournisseur avec la deuxième balise IEEE 802.1Q du SVLAN, également appelée balise externe ou balise Metro, ajoutée au-dessus de la balise CVLAN 802.1Q. Ce processus est également appelé pile de VLAN et cet exemple présente une pile de VLAN à 2 balises. Le trafic balisé double est transféré par L2 dans le réseau du fournisseur en fonction uniquement des informations de la table MAC (Media Access Control) du SVLAN. Une fois que le trafic balisé double arrive à l'extrémité distante du tunnel QinQ, le commutateur PE distant ProvSwitchB, qui agit également comme un accès au tunnel QinQ, retire la balise SVLAN du trafic et la transfère au site B balisé uniquement avec la balise CVLAN 802.1Q, ce qui permet d'obtenir l'extension de couche 2 des VLAN sur les sites distants.

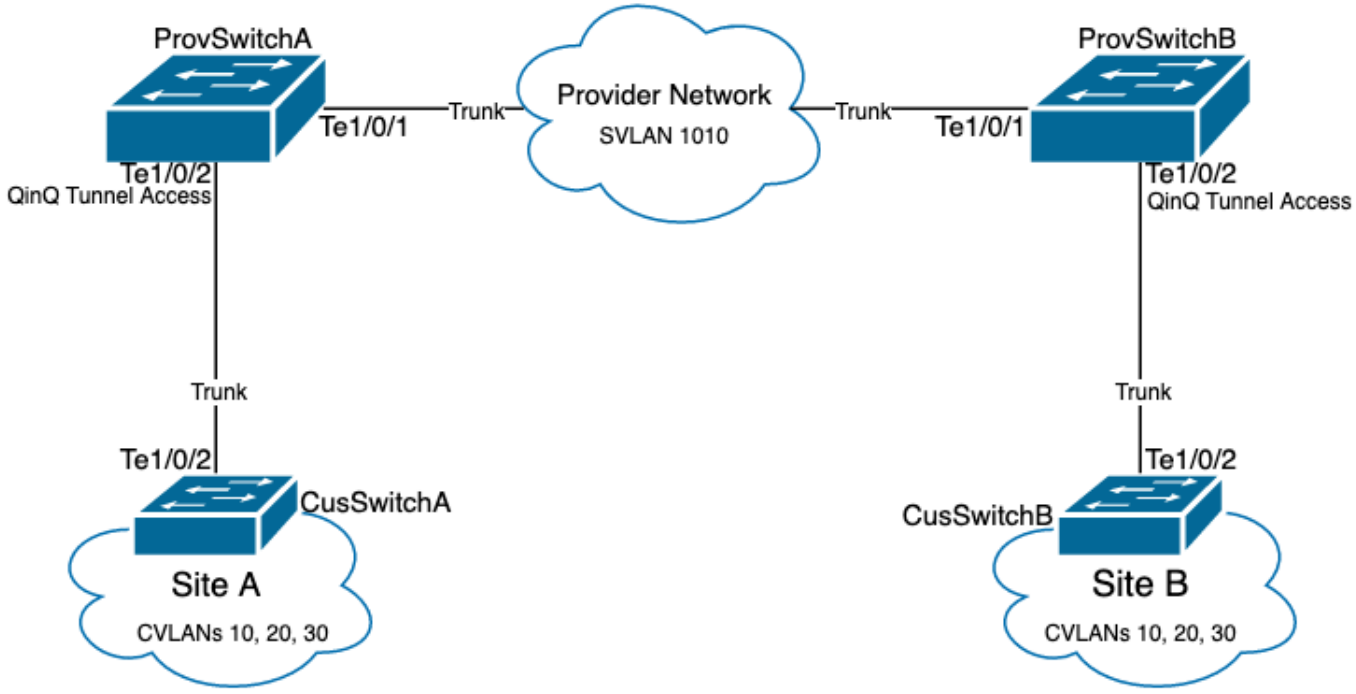
Protocoles L2 La transmission tunnel est également mise en oeuvre pour échanger des trames CDP (Cisco Discovery Protocol) entre les commutateurs CE CusSwitchA et CusSwitchB.

Ce même processus se produit lorsque le trafic est transféré du site B au site A, et la même configuration, la même vérification et les mêmes étapes de dépannage s'appliquent pour le commutateur PE ProvSwitchB. Supposons que tous les autres périphériques du réseau du commutateur du fournisseur et des sites du client sont uniquement configurés avec des commandes d'accès/de liaison et n'exécutent aucune fonction QinQ.

L'exemple présenté suppose que le trafic avec une seule balise 802.1Q est reçu dans les commutateurs d'accès au tunnel QinQ, cependant, le trafic reçu peut avoir zéro ou plusieurs balises 802.1Q. L'étiquette SVLAN est ajoutée à la pile VLAN reçue. Aucune configuration QinQ, VLAN et trunk supplémentaire n'est requise dans les périphériques pour prendre en charge le trafic avec zéro ou plus de balises 802.1Q. Cependant, l'unité de transmission maximale (MTU) sur les périphériques doit être modifiée pour prendre en charge les octets supplémentaires ajoutés au trafic (détails supplémentaires décrits dans la section Dépannage).

Des informations supplémentaires sur les tunnels IEEE 802.1Q sont présentées dans le document Layer 2 Configuration Guide Document for Catalyst 9500 with 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



Configuration sur ProvSwitchA (périphérique PE tunnel 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
!
```

Configuration sur ProvSwitchB (périphérique PE tunnel 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


!
```

Configuration sur CusSwitchA (périphérique 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
!
```

Configuration sur CusSwitchB (périphérique 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
!
```

Notez que les CVLAN ne sont pas définis dans les périphériques du fournisseur et que le SVLAN n'est pas défini sur les commutateurs CE. Les périphériques fournisseurs transfèrent le trafic en fonction de SVLAN uniquement et ne prennent pas en compte les informations CVLAN pour toute décision de transmission. Par conséquent, il n'est pas nécessaire pour un périphérique fournisseur de savoir quels VLAN sont reçus dans un accès de tunnel QinQ (sauf si QinQ sélectif est utilisé).

Cela signifie également que les mêmes ID de VLAN utilisés pour les balises CVLAN peuvent être utilisés pour le trafic au sein du réseau commuté du fournisseur et inversement. Si c'est le cas, la recommandation est de configurer la balise vlan dot1q native sur le mode de configuration globale pour empêcher toute perte de paquets ou problème de fuite de trafic. La balise vlan dot1q native permet par défaut de baliser le VLAN natif 802.1Q sur toutes les interfaces d'agrégation, mais cela peut être désactivé au niveau de l'interface sans configuration de balise vlan native switchport trunk.

Vérifier

La configuration des ports pour les tunnels QinQ et L2PT peut être vérifiée du point de vue de Cisco IOS XE au point de vue de FWD-ASIC (Forwarding Application-Specific Integrated Circuit), où les décisions de transfert sur un commutateur Catalyst se produisent. Les commandes de vérification de base de Cisco IOS XE sont les suivantes :

- show dot1q-tunnel - Répertorie les interfaces configurées comme accès au tunnel QinQ.

<#root>

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

- show vlan id {svlan-number} - Affiche les interfaces attribuées au VLAN spécifié.

<#root>

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

- show interfaces trunk - Répertorie les interfaces configurées en mode 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 - Répertorie l'état global de l'étiquette VLAN native 802.1Q et les interfaces trunk configurées pour étiqueter le VLAN natif 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} - Affiche les adresses MAC apprises dans le SVLAN. Les adresses MAC des périphériques LAN sont acquises dans le SVLAN, quel que soit le CVLAN utilisé.

<#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 - Affiche l'interface activée pour L2PT et les compteurs pour chaque protocole L2 activé.

<#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 - Peut être exécuté sur les commutateurs CE pour confirmer qu'ils peuvent se voir les uns les autres 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
```

Lorsqu'une interface est configurée en tant qu'accès de tunnel QinQ via des interfaces de ligne de commande (CLI), le Cisco IOS XE déclenche le processus Port Manager (PM) pour configurer les ports de commutation avec le mode et le VLAN spécifiés. Les informations de port de commutateur peuvent être vérifiées dans PM avec la commande show pm port interface {interface-name}.

Remarque : pour exécuter les commandes PM, il est nécessaire de configurer le service interne en mode de configuration globale. Cette configuration permet l'exécution de commandes de plate-forme et de débogage supplémentaires sur l'interface de ligne de commande et n'a aucun impact fonctionnel sur le réseau. Il est recommandé de supprimer cette commande une fois la vérification PM terminée.

<#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
```

Le numéro d'interface (if_number) de 2 est attribué à l'interface Te1/0/2. Il s'agit de l'identificateur d'interface (IF-ID), la valeur interne qui identifie un port spécifique. La configuration de switchport peut également être vérifiée sur PM avec la commande 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
```

Une fois que PM applique la configuration de port de commutation, PM relaie les informations de port au pilote de moteur de transfert (FED) afin de programmer les circuits intégrés spécifiques à l'application (ASIC) en conséquence.

Dans FED, les ports peuvent être vérifiés avec la commande show platform software fed switch {switch-number} port if_id {IF-ID} pour confirmer qu'ils sont programmés comme ports d'accès au 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
```

Contrairement aux ports de commutation en mode d'accès, qui ne reçoivent que le trafic non étiqueté, un port de commutation configuré en mode tunnel 802.1Q accepte également le trafic avec des étiquettes 802.1Q. FED autorise cette fonctionnalité sur le port pour les ports d'accès au tunnel QinQ, comme cela peut être confirmé avec le commutateur show platform software fed {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 fournit également une valeur de handle au format hexadécimal appelé Entité logique de port (Port LE). Le port LE est un pointeur vers les informations de port programmées dans l'ASIC de transfert (fwd-asic). La commande show platform hardware fed switch 1 fwd-asic abstraction print-resource-handle {Port-LE-handle} 1 affiche les différentes fonctionnalités activées sur le port au niveau de l'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

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

Ce résultat confirme au niveau de l'ASIC que le port de commutation d'accès au tunnel QinQ est configuré pour autoriser le trafic non étiqueté et étiqueté 802.1Q à partir du LAN, et pour attribuer le SVLAN 1010 à être transféré sur le réseau commuté du fournisseur. Notez que le champ LEAD_PORT_SEL_QINQ_ENABLED n'est pas défini. Ce bit est défini pour la configuration QinQ sélective uniquement, pas pour la configuration de tunnels QinQ traditionnels comme présenté dans ce document.

Dépannage

Cette section décrit les étapes que vous pouvez suivre pour dépanner votre configuration. L'outil le plus utile pour dépanner les problèmes de trafic dans un tunnel 802.1Q est l'analyseur de port commuté (SPAN). Les captures SPAN peuvent être utilisées pour vérifier l'étiquette 802.1Q du CVLAN reçu du LAN et du SVLAN ajouté au périphérique d'accès au tunnel QinQ.

Remarque : les captures de paquets intégrées (EPC) peuvent également être utilisées pour capturer le trafic dans un environnement de tunnel 802.1Q. Cependant, les captures de paquets de sortie avec EPC ont lieu avant que le trafic ne soit étiqueté avec IEEE 802.1Q (l'insertion de l'étiquette 802.1Q a lieu au niveau du port dans le sens de la sortie). Par conséquent, l'EPC de sortie sur la liaison montante du périphérique de périphérie du fournisseur ne peut pas afficher l'étiquette SVLAN utilisée dans le réseau commuté du fournisseur. Une option pour collecter le trafic à double balise avec EPC consiste à capturer le trafic avec EPC d'entrée sur le périphérique du fournisseur voisin.
Référez-vous au Guide de configuration de la gestion du réseau pour les commutateurs

---

Catalyst 9500 avec Cisco IOS XE Amsterdam-17.3.x pour plus d'informations sur 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

Pour configurer la fonctionnalité SPAN afin de capturer le trafic avec des balises 802.1Q, il est important de configurer la commande monitor session {session-number} destination interface {interface-name} encapsulation replicate. Si le mot clé encapsulation replicate n'est pas configuré, le trafic mis en miroir avec la fonctionnalité SPAN peut contenir des informations de balises 802.1Q incorrectes. Reportez-vous à la section Configurer pour obtenir un exemple de configuration de la fonctionnalité SPAN.

Pour plus d'informations sur la fonctionnalité SPAN, reportez-vous au Guide de configuration de la gestion du réseau pour les commutateurs Catalyst 9500 avec 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

Exemple de configuration SPAN sur ProvSwitchA :

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

Dans le périphérique Network Analyzer, le trafic mis en miroir reçu peut être examiné pour confirmer la présence de CVLAN 10 dans l'entrée d'accès au 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
```

De même, la présence de CVLAN 10 et de SVLAN 1010 peut être confirmée dans le sens de la sortie dans l'agrégation d'interface connectée au réseau commuté du fournisseur.

```
> 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
```

Remarque : certaines cartes réseau des analyseurs réseau peuvent supprimer les balises 802.1Q sur le trafic étiqueté reçu. Contactez le support technique du fournisseur de la carte réseau pour obtenir des informations spécifiques sur la façon de gérer les balises 802.1Q sur les trames reçues.

Si vous suspectez une perte de trafic dans le réseau commuté QinQ, prenez en compte les éléments suivants pour les examiner :

- L'unité de transmission maximale (MTU) par défaut sur une interface agrégée est de 1 522 octets. Cela prend en compte le MTU IP de 1500, la trame d'en-tête Ethernet de 18 octets et une balise 802.1Q de 4 octets. Le MTU configuré dans tous les périphériques de périphérie du fournisseur et du fournisseur doit avoir 4 octets supplémentaires par étiquette 802.1Q ajoutée dans la pile VLAN. Par exemple, pour une pile VLAN à 2 balises, une MTU de 1504 doit être configurée. Pour une pile VLAN à 3 balises, une MTU de 1508 doit être configurée, etc. Pour plus d'informations sur la configuration MTU, reportez-vous au Guide de configuration des composants matériels et d'interface pour Catalyst 9500 avec 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

- Le trafic envoyé au processeur sur les périphériques à l'intérieur d'un tunnel 802.1Q n'est pas pris en charge. Les fonctionnalités qui nécessitent une inspection du trafic peuvent entraîner des pertes ou des fuites de paquets dans un environnement 802.1Q. La surveillance DHCP pour le trafic DHCP, la surveillance IGMP pour le trafic IGMP, la surveillance MLD pour le trafic MLD et l'inspection ARP dynamique pour le trafic ARP sont des exemples de ces fonctionnalités. Il est recommandé de désactiver ces fonctionnalités sur le SVLAN utilisé pour transporter le trafic via le réseau commuté du fournisseur.

Commandes de débogage supplémentaires

Remarque : Consulter les renseignements importants sur les commandes de débogage

avant d’utiliser les commandes de débogage.

- debug pm port - Affiche les transitions de port du gestionnaire de ports (PM) et le mode programmé. Utile pour déboguer l'état de configuration des ports QinQ.

Informations connexes

- Commutateurs Catalyst 9300 - Configuration de la transmission tunnel IEEE 802.1Q
- Commutateurs Catalyst 9300 - Configuration de la tunnellisation de protocole de couche 2
- Commutateurs Catalyst 9300 - Configuration des EtherChannels
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.