Konfiguration der Verifizierung zur Fehlerbehebung für QinQ und L2PT auf Catalyst Switches der Serie 9000

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration, Überprüfung und Fehlerbehebung von 802.1Q-Tunneln (QinQ) und Layer 2 Protocol Tunneling (L2PT) auf den Catalyst Switches der Serie 9000 mit Cisco IOS® XE Software beschrieben.

In den offiziellen Versionshinweisen und Konfigurationsleitfäden von Cisco finden Sie aktuelle Informationen zu den Einschränkungen, Einschränkungen, Konfigurationsoptionen und Einschränkungen sowie alle weiteren relevanten Details zu dieser Funktion.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Architektur der Catalyst Switches der Serie 9000
- Cisco IOS XE Software-Architektur
- Virtual Local Area Networks (VLAN), VLAN-Trunks und IEEE 802.1Q-Kapselung
- Layer-2-Protokolle wie Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP), Spanning Tree Protocol (STP), Link Aggregation Control Protocol (LACP) und Port Aggregation Protocol (PAgP).
- Grundkenntnisse von QinQ Tunnels, Selective QinQ Tunnels und Layer 2 Protocol Tunneling (L2PT)
- Switched Port Analyzer (SPAN) und Embedded Packet Captures (EPC)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Hardware- und Software-Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Verwandte Produkte

Dieses Dokument kann auch mit folgenden Hardware- und Softwareversionen verwendet werden:

- Catalyst Switches der Serien 3650 und 3850 mit Cisco IOS XE Software
- Catalyst Switches der Serien 9200, 9300, 9400 und 9600 mit Cisco IOS XE Software

Konfigurieren

Dieser Abschnitt enthält eine grundlegende Topologie für die IEEE 802.1Q-Tunnelbereitstellung (QinQ) auf Catalyst 9000-Switches sowie Konfigurationsbeispiele für jeden Catalyst-Switch.

Netzwerkdiagramm

In der dargestellten Topologie gibt es zwei Standorte, Standort A und Standort B, die physisch durch ein vom Service Provider geschaltetes Netzwerk getrennt sind, in dem Service Virtual LAN (SVLAN) 1010 verwendet wird. Die Provider Edge (PE)-Switches ProvSwitchA und ProvSwitchB gewähren Zugriff auf Standort A bzw. Standort B für das Anbieternetzwerk. Standort A und B verwenden Kunden-VLANs (CVLAN) 10, 20 und 30 und erfordern eine Erweiterung dieser VLANs auf Layer 2 (L2). Standort A ist über Customer Edge (CE)-Switch CusSwitchA und Standort B über CE-Switch CusSwitchB mit dem Anbieternetzwerk verbunden.

Standort A sendet Datenverkehr mit dem IEEE 802.1Q-Tag des verwendeten CVLAN, auch als inneres Tag bezeichnet, an den ProvSwitchA des PE-Switches, der als QinQ-Tunnelzugriff fungiert. ProvSwitchA leitet den empfangenen Datenverkehr mit dem zweiten IEEE 802.1Q-Tag des SVLAN, das dem CVLAN 802.1Q-Tag hinzugefügt wird, an das Provider Switched Network weiter. Dieser Prozess wird auch als VLAN-Stacks bezeichnet. In diesem Beispiel wird ein 2-Tag-VLAN-Stack vorgestellt. Der doppelt gekennzeichnete Datenverkehr wird von L2 im Anbieternetzwerk weitergeleitet, wobei nur die Informationen der SVLAN Media Access Control (MAC)-Tabelle berücksichtigt werden. Sobald der doppelt gekennzeichnete Datenverkehr am Remote-Ende des QinQ-Tunnels ankommt, entfernt der Remote-PE-Switch ProvSwitchB, der auch als QinQ-Tunnelzugriff fungiert, den SVLAN-Tag aus dem Datenverkehr und leitet ihn nur mit dem CVLAN 802.1Q-Tag an den Standort B weiter, sodass die Layer-2-Erweiterung der VLANs über die Remote-Standorte erreicht wird. L2 Protocols Tunneling wird auch implementiert, um Cisco Discovery Protocol (CDP)-Frames zwischen den CE-Switches CusSwitchA und CusSwitchB auszutauschen.

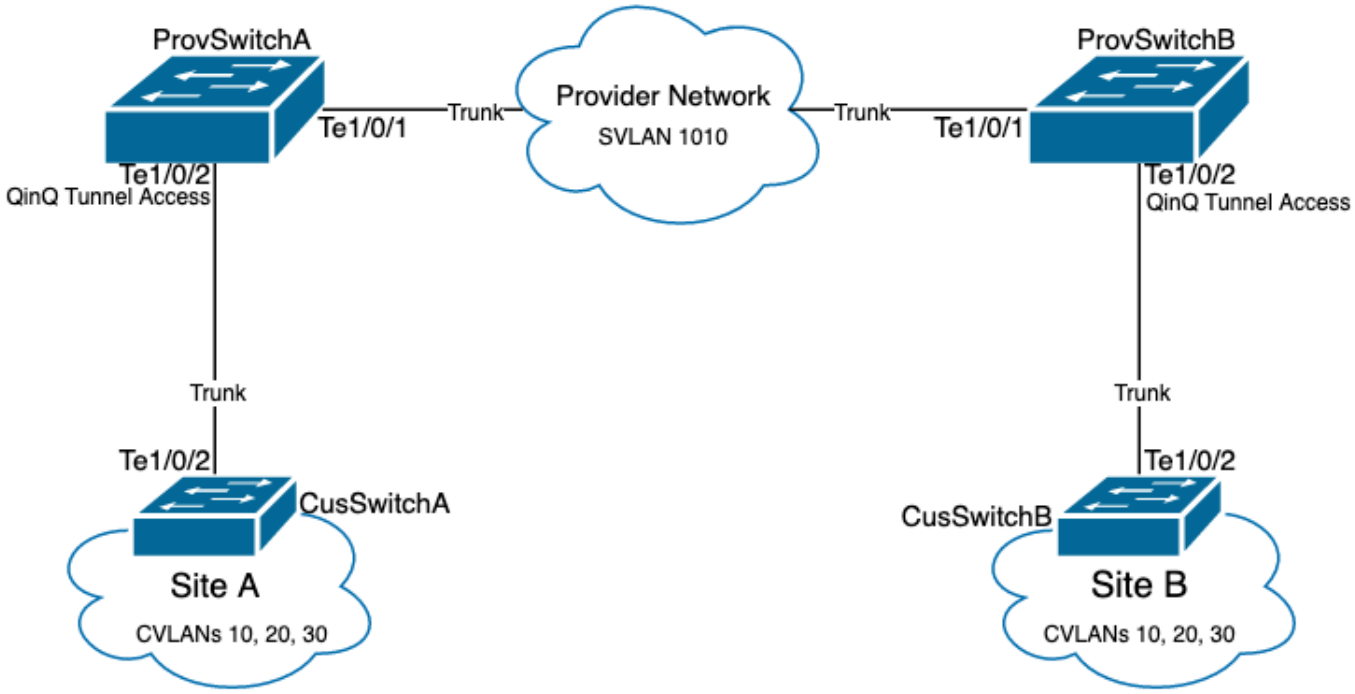
Derselbe Prozess findet statt, wenn Datenverkehr von Standort B an Standort A weitergeleitet wird. Für den ProvSwitch B des PE-Switches gelten die gleichen Konfigurations-, Verifizierungs- und Schritte zur Fehlerbehebung. Angenommen, alle anderen Geräte innerhalb des Provider Switch-Netzwerks und die Kundenstandorte sind nur mit Zugriffs-/Trunk-Befehlen konfiguriert und

führen keine QinQ-Funktion aus.

Im vorliegenden Beispiel wird davon ausgegangen, dass Datenverkehr mit nur einem 802.1Q-Tag in den QinQ Tunnel Access Switches empfangen wird. Der empfangene Datenverkehr kann jedoch null oder mehr 802.1Q-Tags aufweisen. Der SVLAN-Tag wird dem empfangenen VLAN-Stack hinzugefügt. Es sind keine zusätzlichen QinQ-, VLAN- und Trunk-Konfigurationen auf den Geräten erforderlich, um Datenverkehr mit 0 oder mehr 802.1Q-Tags zu unterstützen. Die Maximum Transmission Unit (MTU) auf den Geräten muss jedoch geändert werden, um die zusätzlichen Bytes zu unterstützen, die dem Datenverkehr hinzugefügt werden (weitere Details werden im Abschnitt "Fehlerbehebung" beschrieben).

Weitere Informationen zu IEEE 802.1Q-Tunneln finden Sie im Layer-2-Konfigurationsleitfaden für Catalyst 9500 mit 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



Konfiguration auf ProvSwitchA (QinQ Tunnel PE Gerät):

```
!
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
!
```

Konfiguration auf ProvSwitchB (QinQ Tunnel PE-Gerät):

```
!
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
!
```

Konfiguration auf CusSwitchA (CE-Gerät):

```
!
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
!
```

Konfiguration auf CusSwitchB (CE-Gerät):

```
!
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
!
```

Beachten Sie, dass die CVLANs nicht in den Anbietergeräten und SVLANs nicht in den CE-Switches definiert sind. Die Provider-Geräte leiten den Datenverkehr ausschließlich SVLAN-basiert weiter und berücksichtigen die CVLAN-Informationen nicht für Weiterleitungsentscheidungen. Daher ist es nicht erforderlich, dass ein Provider-Gerät weiß, welche VLANs in einem QinQ-Tunnelzugriff empfangen werden (es sei denn, Selective QinQ wird verwendet). Dies bedeutet auch, dass dieselben VLAN-IDs, die für die CVLAN-Tags verwendet werden, für den Datenverkehr innerhalb des Provider Switched Network und umgekehrt verwendet werden können. In diesem Fall wird empfohlen, **vlan dot1q tag im** globalen Konfigurationsmodus **nativ** zu konfigurieren, um Paketverluste oder Datenlecks zu vermeiden. Mit dem **nativen VLAN dot1q-Tag** kann natives 802.1Q-VLAN standardmäßig an allen Trunk-Schnittstellen markiert werden. Dies kann jedoch auf Schnittstellenebene deaktiviert werden, wenn **keine** Konfiguration für **native VLAN-Tags für Switchport-Trunks vorliegt**.

Überprüfung

Die Port-Konfiguration für QinQ-Tunnel und L2PT kann aus der Perspektive von Cisco IOS XE bis hin zur Perspektive von Forwarding Application-Specific Integrated Circuit (FWD-ASIC) überprüft werden, bei der die Weiterleitungsentscheidungen für einen Catalyst Switch getroffen werden. Die Cisco IOS XE-Verifizierungsbefehle lauten wie folgt:

- **show dot1q-tunnel**: Listet die als QinQ-Tunnelzugriff konfigurierten Schnittstellen auf.

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

- **show vlan id {svlan-number}** - Zeigt die Schnittstellen an, die dem angegebenen VLAN zugewiesen sind.

```
ProvSwitchA# show vlan id 1010
VLAN Name                             Status    Ports
```

```
---- ------------------------------ --------- --------------------------------
1010 QinQ-VLAN                      active    Te1/0/1, Te1/0/2
```

- **show interfaces trunk**: Listet die im Trunk-Modus konfigurierten Schnittstellen auf.

```
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**: Gibt den globalen Status des nativen 802.1Q-VLAN-Tags und der Trunk-Schnittstellen an, die für das Tagging des nativen 802.1Q-VLAN konfiguriert wurden.

```
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}** - Zeigt die im SVLAN ermittelten MAC-Adressen an. MAC-Adressen von LAN-Geräten werden unabhängig vom verwendeten CVLAN im SVLAN erfasst.

```
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**: Zeigt die für L2PT aktivierte Schnittstelle und die Zähler für jedes aktivierte L2-Protokoll an.

```
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** - Kann auf CE-Switches ausgeführt werden, um sicherzustellen, dass sie sich über CDP sehen können.

```
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
```

Wenn eine Schnittstelle als QinQ-Tunnelzugriff über Befehlszeilenschnittstellen (CLI) konfiguriert ist, löst Cisco IOS XE den Port Manager (PM)-Prozess aus, um die Switch-Ports mit dem angegebenen Modus und VLAN zu konfigurieren. Switchport-Informationen können in PM mit dem Befehl **show pm port interface {interface-name} überprüft werden**.

> **Hinweis**: Zum Ausführen von PM-Befehlen muss der **Dienst intern** im globalen Konfigurationsmodus konfiguriert werden. Diese Konfiguration ermöglicht die Ausführung zusätzlicher Plattform- und Debugbefehle über die CLI und hat keine funktionalen Auswirkungen auf das Netzwerk. Es wird empfohlen, diesen Befehl nach Abschluss der PM-Überprüfung zu entfernen.

```
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
```

Der Schnittstelle Te1/0/2 wird die Schnittstellennummer (if_number) 2 zugewiesen. Dies ist der Interface Identifier (IF-ID), der interne Wert, der einen bestimmten Port identifiziert. Die Switch-Port-Konfiguration kann auch mithilfe des Befehls **show platform software pm-port switch 1 R0 interface {IF-ID} auf** PM überprüft werden.

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

IntfPORTDEFAULTNATIVEALLOWMODEPORTPORT
IDENABLEVLANVLANNATIVEDUPLEXSPEED
------------------------------------------------------------
2TRUE1010 1010TRUEtunnelfullunknown
```

Sobald PM die Switch-Port-Konfiguration anwendet, leitet PM die Port-Informationen an den Forwarding Engine Driver (FED) weiter, um die anwendungsspezifischen integrierten Schaltungen (ASIC) entsprechend zu programmieren.

In FED können Ports mit dem **Befehl show platform software fed switch {switch-number} port if_id {IF-ID}** überprüft werden, um zu bestätigen, dass sie als QinQ Tunnel Access Ports programmiert sind:

```
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
```

Im Gegensatz zu Switch-Ports im Zugriffsmodus, die nur nicht gekennzeichneten Datenverkehr empfangen, akzeptiert ein im 802.1Q-Tunnelmodus konfigurierter Switch-Port auch Datenverkehr mit 802.1Q-Tags. FED ermöglicht diese Funktion auf dem Port für QinQ Tunnel Access Ports, wie mit dem **show platform software feed switch {switch-number} ifm if-id {IF-ID} bestätigt** werden kann:

```
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 stellt auch einen Handlewert im Hexadezimalformat mit der Bezeichnung Port Logical Entity (Port LE) bereit. Der Port LE ist ein Zeiger auf die im Forwarding ASIC programmierten Port-Informationen (fwd-asic). Der Befehl **show platform hardware fed switch 1 fwd-asic abstraction print-resource-handle {Port-LE-handle} 1** zeigt die verschiedenen auf dem Port aktivierten Funktionen auf ASIC-Ebene an:

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

Diese Ausgabe bestätigt auf ASIC-Ebene, dass der QinQ-Tunnel-Access-Switch-Port so

konfiguriert ist, dass unmarkierter und 802.1Q-markierter Datenverkehr aus dem LAN zugelassen wird, und weist SVLAN 1010 die Weiterleitung über das Provider Switched Network zu. Beachten Sie, dass das Feld LEAD_PORT_SEL_QINQ_ENABLED nicht gesetzt ist. Dieses Bit wird nur für die selektive QinQ-Konfiguration festgelegt, nicht für die herkömmliche QinQ-Tunnelkonfiguration, wie in diesem Dokument beschrieben.

Fehlerbehebung

In diesem Abschnitt finden Sie die Schritte, die Sie zur Fehlerbehebung bei Ihrer Konfiguration durchführen können. Das hilfreichste Tool zur Behebung von Datenverkehrsproblemen in einem 802.1Q-Tunnel ist der Switched Port Analyzer (SPAN). Mithilfe von SPAN-Erfassungen kann das 802.1Q-Tag des vom LAN empfangenen CVLAN und des im QinQ-Tunnelzugangsgerät hinzugefügten SVLAN überprüft werden.

> **Hinweis**: Embedded Packet Captures (EPC) kann auch verwendet werden, um Datenverkehr in einer 802.1Q-Tunnelumgebung zu erfassen. Egress-Paketerfassungen mit EPC erfolgen jedoch vor der Kennzeichnung des Datenverkehrs mit IEEE 802.1Q (802.1Q-Tags werden auf Portebene in Egress-Richtung eingefügt). Daher kann der Egress-EPC auf dem Uplink-Trunk des Provider-Edge-Geräts den im Switch-Netzwerk des Anbieters verwendeten SVLAN-Tag nicht anzeigen. Eine Option zum Sammeln des doppelt gekennzeichneten Datenverkehrs mit EPC besteht darin, den Datenverkehr mit dem Eingangs-EPC auf dem benachbarten Anbietergerät zu erfassen.
> Weitere Informationen zu EPC finden Sie im Konfigurationsleitfaden für die Netzwerkverwaltung mit Catalyst 9500 Switches mit 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

Um SPAN so zu konfigurieren, dass der Datenverkehr mit 802.1Q-Tags erfasst wird, muss der Befehl **zur Kapselungsreplikation für** die **{session-number}-Zielschnittstelle {interface-name} der Überwachungssitzung** konfiguriert werden. Wenn das Schlüsselwort **encapsulation replicate** nicht konfiguriert ist, enthält der mit SPAN gespiegelte Datenverkehr möglicherweise falsche 802.1Q-Tags-Informationen. Im Abschnitt "Configure" (Konfigurieren) finden Sie ein Beispiel für die SPAN-Konfiguration.

Weitere Informationen zu SPAN finden Sie im Network Management Configuration Guide for Catalyst 9500 switches 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/nmgmt/b_173_nmgmt_9500_cg/configuring_span_and_rspan.html

SPAN-Konfigurationsbeispiel für ProvSwitchA:

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

Im Network Analyzer-Gerät kann der empfangene gespiegelte Datenverkehr überprüft werden, um das Vorhandensein von CVLAN 10 im QinQ-Tunnelzugang zu bestätigen:

```
> 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
```

Ebenso kann das Vorhandensein von CVLAN 10 und SVLAN 1010 in Ausgangsrichtung in dem mit dem Provider Switched Network verbundenen Schnittstellen-Trunk bestätigt werden.

```
> 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
```

> **Hinweis**: Bestimmte Netzwerkschnittstellenkarten (NICs) in Network Analyzers können 802.1Q-Tags für empfangenen getaggten Datenverkehr entfernen. Wenden Sie sich an den Support-Anbieter für Netzwerkkarten, um spezifische Informationen zur Verwaltung der 802.1Q-Tags für empfangene Frames zu erhalten.

Bei Verdacht auf Datenverlust im QinQ-Switched-Netzwerk sollten folgende Punkte überprüft werden:

- Die standardmäßige Maximum Transmission Unit (MTU) für eine Trunk-Schnittstelle beträgt 1.522 Byte. Dies berücksichtigt die IP-MTU von 1500, den Ethernet-Header-Frame von 18 Byte und ein 802.1Q-Tag von 4 Byte. Die konfigurierte MTU in allen Provider- und Provider-Edge-Geräten muss 4 zusätzliche Bytes pro 802.1Q-Tag im VLAN-Stack enthalten. Beispiel: Für einen VLAN-Stack mit 2 Tags muss eine MTU von 1504 konfiguriert werden. Für einen VLAN-Stack mit 3 Tags muss eine MTU von 1508 konfiguriert werden usw. Einzelheiten zur MTU-Konfiguration finden Sie im Konfigurationsleitfaden für Schnittstellen- und Hardwarekomponenten für Catalyst 9500 mit 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
- Datenverkehr-Punt zur CPU auf Geräten in einem 802.1Q-Tunnel wird nicht unterstützt. Funktionen, die eine Überprüfung des Datenverkehrs erfordern, können in einer 802.1Q-

Umgebung zu Paketverlusten oder Paketlecks führen. Beispiele für diese Funktionen sind DHCP-Snooping für DHCP-Verkehr, IGMP-Snooping für IGMP-Verkehr, MLD-Snooping für MLD-Verkehr und dynamische ARP-Inspektion für ARP-Verkehr. Es wird empfohlen, diese Funktionen für das SVLAN zu deaktivieren, das für den Transport des Datenverkehrs durch das Provider Switched Network verwendet wird.

Zusätzliche Debug-Befehle

Hinweis: Lesen Sie Wichtige Informationen zu Debug-Befehlen, bevor Sie **Debug-**Befehle verwenden.

- **debug pm port** - Zeigt Port-Manager-Portübergänge und den programmierten Modus an. Hilfreich zum Debuggen des QinQ-Port-Konfigurationsstatus.

Zugehörige Informationen

- Catalyst 9300-Switches - Konfigurieren von IEEE 802.1Q Tunneling
- Catalyst 9300-Switches - Konfiguration von Layer-2-Protokoll-Tunneling
- Catalyst 9300-Switches - Konfigurieren von EtherChannels
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.