設定確認Catalyst 9000スイッチのQinQおよびL2PTのトラブルシューティング

内容

概要

このドキュメントでは、Cisco IOS® XEソフトウェアを実行するCatalyst 9000ファミリスイッチで802.1Qトンネル(QinQ)およびレイヤ2プロトコルトンネリング(L2PT)を設定し、トラブルシューティングする方法について説明します。

この機能に関する制限事項、制限事項、設定オプション、注意事項、およびその他の関連情報の最新情報については、シスコの公式リリースノートと設定ガイドを参照してください。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Catalyst 9000シリーズスイッチのアーキテクチャ
- Cisco IOS XEソフトウェアアーキテクチャ
- 仮想ローカルエリアネットワーク(VLAN)、VLANトランク、およびIEEE 802.1Qカプセル化
- Cisco Discovery Protocol(CDP)、Link Layer Discovery Protocol(LLDP)、Spanning Tree Protocol(STP)、Link Aggregation Control Protocol(LACP)、Port Aggregation Protocol(PAgP)などのレイヤ2プロトコル。
- QinQトンネル、選択的QinQトンネル、およびレイヤ2プロトコルトンネリング(L2PT)に関する基礎知識
- スイッチドポートアナライザ(SPAN)および組み込みパケットキャプチャ(EPC)

使用するコンポーネント

このドキュメントの情報は、次のハードウェアとソフトウェアのバージョンに基づいています。

- Cisco Catalyst C9500-12Q（Cisco IOS XE 17.3.3搭載）

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

関連製品

このドキュメントは、次のバージョンのハードウェアとソフトウェアにも使用できます。

- Cisco IOS XEソフトウェアを搭載したCatalyst 3650および3850シリーズスイッチ
- Cisco IOS XEソフトウェアを搭載したCatalyst 9200、9300、9400、および9600シリーズスイッチ

設定

このセクションでは、Catalyst 9000スイッチにIEEE 802.1Qトンネル(QinQ)を導入するための基本的なトポロジと、各Catalystスイッチの設定例を紹介します。

ネットワーク図

このトポロジでは、サイトAとサイトBの2つのサイトがあり、これらはサービスプロバイダーのスイッチドネットワークによって物理的に分離されており、サービス仮想LAN(SVLAN)1010が使用されています。プロバイダーエッジ(PE)スイッチのProvSwitchAとProvSwitchBは、プロバイダーネットワークへのサイトAとサイトBへのアクセスをそれぞれ許可します。サイトAとサイトBはカスタマーVLAN(CVLAN)10、20、および30を使用し、これらのVLANをレイヤ2(L2)で拡張する必要があります。サイトAはカスタマーエッジ(CE)スイッチCusSwitchAを介してプロバイダーネットワークに接続し、サイトBはCEスイッチCusSwitchBを介してプロバイダーネットワークに接続します。

サイトAは、内部タグとも呼ばれるCVLANのIEEE 802.1Qタグを使用して、QinQトンネルアクセスとして機能するPEスイッチProvSwitchAにトラフィックを送信します。ProvSwitchAは、受信したトラフィックを、CVLAN 802.1Qタグの上に追加されたSVLANの2番目のIEEE 802.1Qタグ（外部タグまたはメトロタグとも呼ばれる）を使用して、プロバイダースイッチドネットワークに転送します。このプロセスはVLANスタックとも呼ばれ、この例では2タグのVLANスタックを示します。二重タグ付きトラフィックは、SVLAN Media Access Control(MAC)テーブル情報のみに基づいて、プロバイダーネットワークのL2によって転送されます。二重タグ付きトラフィックがQinQトンネルのリモートエンドに到達すると、QinQトンネルアクセスとしても機能するリモートPEスイッチProvSwitchBは、トラフィックからSVLANタグを除去し、CVLAN 802.1Qタグのみがタグ付けされたサイトBに転送します。このようにして、リモートサイトを介したVLANのレイヤ2拡張が実現されます。L2プロトコルトンネリングは、CEスイッチCusSwitchAとCusSwitchBの間でCisco Discovery Protocol(CDP)フレームを交換するためにも実装されます。

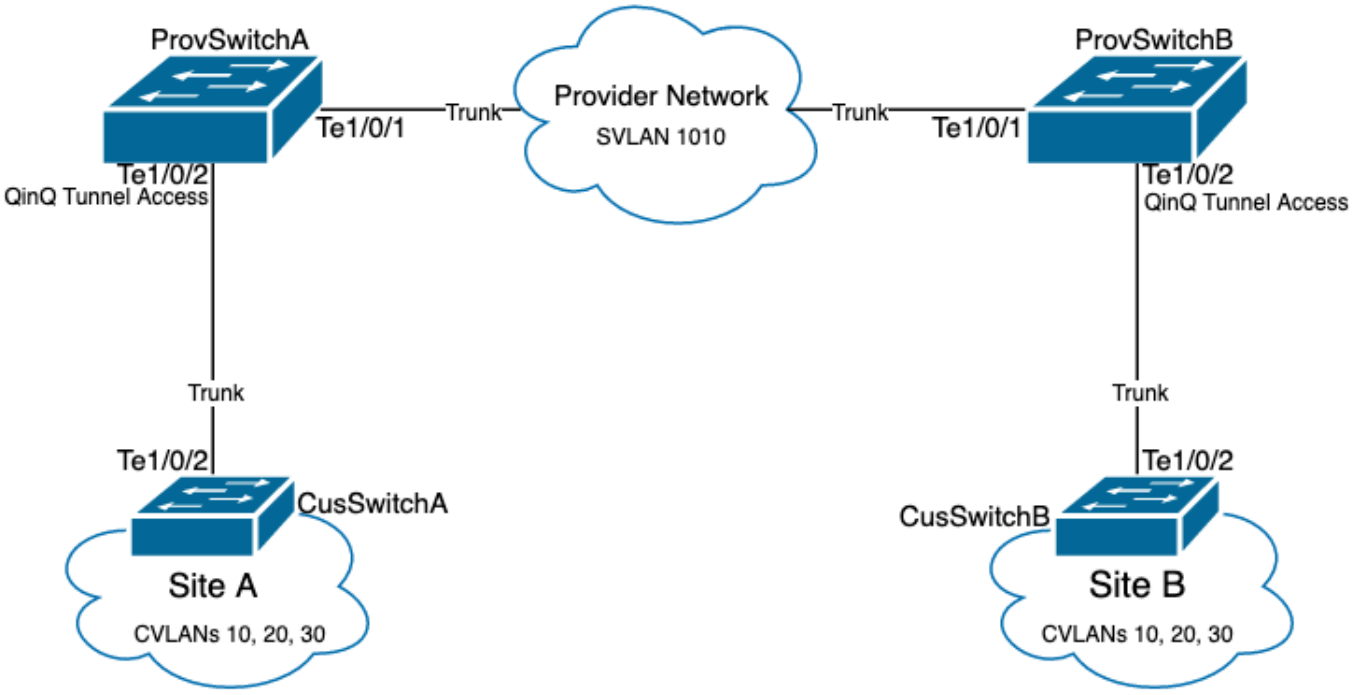
この同じプロセスは、トラフィックがサイトBからサイトAに転送されるときに発生し、同じ設定

、検証、およびトラブルシューティング手順がPEスイッチProvSwitchBにも適用されます。プロバイダースイッチネットワーク内の他のすべてのデバイスとカスタマーサイトは、access/trunkコマンドでのみ設定され、QinQ機能は実行しないものとします。

この例では、QinQトンネルアクセススイッチで受信される802.1Qタグが1つだけであると仮定していますが、受信されるトラフィックには、0個以上の802.1Qタグを含めることができます。SVLANタグは、受信したVLANスタックに追加されます。デバイスでゼロ以上の802.1Qタグを持つトラフィックをサポートするために追加のQinQ、VLAN、およびトランク設定は必要ありませんが、トラフィックに追加される追加のバイト数をサポートするには、デバイスの最大伝送ユニット(MTU)を変更する必要があります（「トラブルシューティング」セクションで説明する詳細）。

IEEE 802.1Qトンネルの詳細は、『Cisco IOS XE Amsterdam-17.3.xを搭載したCatalyst 9500用のレイヤ2設定ガイド』に記載されています。

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



ProvSwitchA（QinQトンネルPEデバイス）の設定：

```
!
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
!
```

ProvSwitchB（QinQトンネルPEデバイス）の設定：

<#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


!
```

CusSwitchA（CEデバイス）の設定：

```
!
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
!
```

CusSwitchB（CEデバイス）の設定：

```
!
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
!
```

CVLANはプロバイダーデバイスで定義されておらず、SVLANはCEスイッチで定義されていないことに注意してください。プロバイダーデバイスはSVLANのみに基づいてトラフィックを転送し、転送決定にCVLAN情報を考慮しないため、QinQトンネルアクセスでどのVLANが受信されたかをプロバイダーデバイスが知る必要はありません（選択的QinQが使用されていない場合）。これは、CVLANタグに使用されているのと同じVLAN IDを、プロバイダースイッチドネットワーク内のトラフィックにも使用できることを意味します。この場合は、パケット損失やトラフィックリークの問題を防ぐために、グローバルコンフィギュレーションモードでvlan dot1q tag nativeを設定することを推奨します。vlan dot1q tag nativeは、デフォルトですべてのトランクインターフェイスで802.1Qネイティブ VLANにタグを付けることを有効にします。ただし、インターフェイスレベルでno switchport trunk native vlan tagを設定して、これを無効にすることができます。

確認

QinQトンネルおよびL2PTのポート設定は、Cisco IOS XEの観点から、Catalystスイッチでの転送決定が行われる転送特定用途向け集積回路(FWD-ASIC)の観点まで検証できます。Cisco IOS XEの基本的な検証コマンドは次のとおりです。

- show dot1q-tunnel:QinQトンネルアクセスとして設定されているインターフェイスをリストします。

<#root>

```
ProvSwitchA# show dot1q-tunnel

dot1q-tunnel mode LAN Port(s)

-----------------------------

Te1/0/2
```

- show vlan id {svlan-number}：指定したVLANに割り当てられたインターフェイスを表示します。

<#root>

```
ProvSwitchA# show vlan id 1010

VLAN

 Name                             Status

Ports

---- -------------------------------- --------- -------------------------------

1010

 QinQ-VLAN                        active

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

- show interfaces trunk：トランクモードで設定されたインターフェイスのリストを表示します。

<#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:802.1QネイティブVLANタグのグローバルステータスと、802.1QネイティブVLANにタグを付けるように設定されたトランクインターフェイスをリストします。

<#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}:SVLANで学習されたMACアドレスを表示します。LANデバイスからのMACアドレスは、使用されるCVLANに関係なく、SVLANで学習されます。

<#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:L2PTが有効になっているインターフェイスと、有効になっている各L2プロトコルのカウンタを表示します。

<#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:CEスイッチ上で実行して、CDPを介して相互に認識できることを確認できます。

```
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
```

コマンドラインインターフェイス(CLI)を介してインターフェイスがQinQトンネルアクセスとして設定されている場合、Cisco IOS XEはポートマネージャ(PM)プロセスをトリガーし、指定されたモードとVLANでスイッチポートを設定します。PMのスイッチポート情報を確認するには、show pm port interface {interface-name}コマンドを使用します。

注:PMコマンドを実行するには、グローバルコンフィギュレーションモードでservice internalを設定する必要があります。この設定により、追加のプラットフォームとdebugコマンドをCLIで実行することが可能になり、ネットワークの機能への影響はありません。PMの検証が完了したら、このコマンドを削除することをお勧めします。

<#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
```

インターフェイスTe1/0/2には、2のインターフェイス番号(if_number)が割り当てられます。これは、特定のポートを識別する内部値であるインターフェイスID(IF-ID)です。スイッチポートの設定は、PMでshow platform software pm-port switch 1 R0 interface {IF-ID}コマンドを使用して確認することもできます。

<#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
```

PMがスイッチポート設定を適用すると、PMはポート情報をForwarding Engine Driver(FED)にリレーし、それに応じて特定用途向け集積回路(ASIC)をプログラムします。

FEDでは、show platform software fed switch {switch-number} port if_id {IF-ID}コマンドを使用してポートをチェックし、これらがQinQトンネルアクセスポートとしてプログラムされていることを確認できます。

<#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
```

タグなしのトラフィックだけを受信することを想定しているアクセスモードのスイッチポートとは異なり、802.1Qトンネルモードで設定されたスイッチポートは、802.1Qタグを持つトラフィックも受け入れます。FEDは、QinQトンネルアクセスポートでこの機能を許可します。このことは、show platform software fed switch {switch-number} ifm if-id {IF-ID}で確認できます。

<#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は、ポート論理エンティティ（ポートLE）と呼ばれる16進数形式のハンドル値も提供します。ポートLEは、フォワーディングASIC(fwd-asic)にプログラムされているポート情報へのポインタです。show platform hardware fed switch 1 fwd-asic abstraction print-resource-handle {Port-LE-handle} 1コマンドは、ASICレベルでポートで有効にされている各種機能を表示します。

```
<#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

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

この出力は、ASICレベルで、QinQトンネルアクセススイッチポートが、LANからのタグなしトラフィックと802.1Qタグ付きトラフィックを許可し、プロバイダースイッチドネットワーク経由で転送されるようにSVLAN 1010を割り当てるように設定されていることを確認します。LEAD_PORT_SEL_QINQ_ENABLEDフィールドが設定されていないことに注意してください。このビットは、このドキュメントで説明されているように、従来のQinQトンネル設定ではなく、選択的QinQ設定のみに設定されます。

トラブルシュート

このセクションでは、設定のトラブルシューティングを行うための手順を説明します。802.1Qトンネルのトラフィック問題をトラブルシューティングする最も便利なツールは、スイッチドポートアナライザ(SPAN)です。SPANキャプチャを使用して、LANから受信したCVLANの802.1Qタグと、QinQトンネルアクセスデバイスに追加されたSVLANを確認できます。

注:Embedded Packet Captures(EPC)は、802.1Qトンネル環境でトラフィックをキャプチャするためにも使用できます。ただし、EPCによる出力パケットキャプチャは、トラフィックがIEEE 802.1Qでタグ付けされる前に発生します（802.1Qタグの挿入は、出力方向のポートレベルで発生します）。その結果、プロバイダーエッジデバイスのアップリンクトランク上の出力EPCは、プロバイダースイッチドネットワークで使用されるSVLANタグを表示できません。EPCで二重タグ付きトラフィックを収集するオプションは、隣接するプロバイダーデバイスで入力EPCのトラフィックをキャプチャすることです。
EPCの詳細については、『Cisco IOS XE Amsterdam-17.3.xを搭載したCatalyst 9500スイッチのネットワーク管理設定ガイド』を参照してください。
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

---

802.1Qタグを使用してトラフィックをキャプチャするようにSPANを設定するには、monitor session {session-number} destination interface {interface-name} encapsulation replicateコマンドを設定することが重要です。encapsulation replicateキーワードが設定されていない場合、SPANでミラーリングされたトラフィックに誤った802.1Qタグ情報が含まれている可能性があり

ます。SPAN設定の例については、「設定」セクションを参照してください。

SPANの詳細については、『Cisco IOS XE Amsterdam-17.3.xを搭載したCatalyst 9500スイッチのネットワーク管理設定ガイド』を参照してください

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

ProvSwitchAでのSPANの設定例：

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

ネットワークアナライザデバイスでは、受信したミラー化トラフィックを確認して、QinQトンネルアクセス入力にCVLAN 10が存在することを確認できます。

```
> 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
```

同様に、CVLAN 10とSVLAN 1010の両方が、プロバイダースイッチドネットワークに接続されているインターフェイストランクの出力方向に存在することを確認できます。

```
> 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
```

注：ネットワークアナライザの特定のネットワークインターフェイスカード(NIC)は、受信したタグ付きトラフィックの802.1Qタグを削除できます。受信したフレームで802.1Qタグを維持する方法の詳細については、NICベンダーに問い合わせてください。

QinQスイッチドネットワークでトラフィック損失が疑われる場合は、次の項目を検討して確認してください。

- トランキングされたインターフェイスのデフォルトの最大伝送ユニット(MTU)は1522バイトです。これは、1500バイトのIP MTU、18バイトのイーサネットヘッダーフレーム、および4バイトの802.1Qタグ1つに対応します。すべてのプロバイダーエッジデバイスとプロバイダーエッジデバイスで設定されているMTUは、VLANスタックに追加される802.1Qタグごとに4バイト追加する必要があります。たとえば、2タグのVLANスタックの場合、1504のMTUを設定する必要があります。3タグのVLANスタックの場合は、1508のMTUを設定する必要があります。その他も同様です。MTU設定の詳細については、『Cisco IOS XE Amsterdam-17.3.xを使用したCatalyst 9500のインターフェイスおよびハードウェアコンポーネント設定ガイド』を参照してください。
  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
- 802.1Qトンネル内のデバイス上のCPUへのトラフィックのパントはサポートされていません。トラフィック検査を必要とする機能は、802.1Q環境でパケット損失またはパケットリークを引き起こす可能性があります。これらの機能の例としては、DHCPトラフィックのDHCPスヌーピング、IGMPトラフィックのIGMPスヌーピング、MLDトラフィックのMLDスヌーピング、ARPトラフィックのダイナミックARPインスペクションがあります。プロバイダースイッチドネットワークを介してトラフィックを転送するために使用されるSVLAN上のこれらの機能を無効にすることを推奨します。

追加のデバッグ コマンド

注：debug コマンドを使用する前に、『debug コマンドの重要な情報』を参照してください。

- debug pm port：ポートマネージャ(PM)ポートの遷移とプログラム済みモードを表示します。QinQポート設定ステータスのデバッグに役立ちます。

関連情報

- Catalyst 9300スイッチ：IEEE 802.1Qトンネリングの設定
- Catalyst 9300スイッチ：レイヤ2プロトコルトンネリングの設定
- Catalyst 9300スイッチ：EtherChannelの設定
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。