

Catalyst 9000 스위치에서 QinQ 및 L2PT 문제 해결 확인 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[네트워크 다이어그램](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[추가 debug 명령](#)

[관련 정보](#)

소개

이 문서에서는 Cisco IOS® XE 소프트웨어를 실행하는 Catalyst 9000 스위치 제품군에서 802.1Q 터널(QinQ) 및 L2PT(Layer 2 Protocol Tunneling)를 구성하고 문제를 해결하는 방법을 설명합니다.

제한 사항, 제한 사항, 컨피그레이션 옵션, 주의 사항 및 이 기능에 대한 기타 관련 세부 사항에 대한 최신 정보는 Cisco 공식 릴리스 노트 및 컨피그레이션 가이드를 참조하십시오.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Catalyst 9000 Series 스위치 아키텍처
- Cisco IOS XE 소프트웨어 아키텍처
- VLAN(Virtual Local Area Network), VLAN 트렁크 및 IEEE 802.1Q 캡슐화
- CDP(Cisco Discovery Protocol), LLDP(Link Layer Discovery Protocol), STP(Spanning Tree Protocol), LACP(Link Aggregation Control Protocol) 및 PAgP(Port Aggregation Protocol)와 같은 레이어 2 프로토콜.
- QinQ 터널, 선택적 QinQ 터널 및 L2PT(Layer 2 Protocol Tunneling)에 대한 기본 지식
- SPAN(Switched Port Analyzer) 및 EPC(Embedded Packet Captures)

사용되는 구성 요소

이 문서의 정보는 다음 하드웨어 및 소프트웨어 버전을 기반으로 합니다.

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

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

관련 제품

이 문서는 다음과 같은 하드웨어 및 소프트웨어 버전에서도 사용할 수 있습니다.

- Cisco IOS XE 소프트웨어를 사용하는 Catalyst 3650 및 3850 Series 스위치
- Cisco IOS XE 소프트웨어를 사용하는 Catalyst 9200, 9300, 9400 및 9600 Series 스위치

구성

이 섹션에서는 Catalyst 9000 스위치에서 IEEE 802.1Q 터널(QinQ) 구축을 위한 기본 토폴로지와 각 Catalyst 스위치의 컨피그레이션 예를 소개합니다.

네트워크 다이어그램

제시된 토폴로지에는 사이트 A와 사이트 B의 두 사이트가 있습니다. 이 사이트는 SVLAN(Service Virtual LAN) 1010이 사용되는 통신 사업자 전환 네트워크에 의해 물리적으로 분리되어 있습니다. PE(Provider Edge) 스위치인 ProvSwitchA와 ProvSwitchB는 각각 사이트 A와 사이트 B에 대한 액세스 권한을 제공자 네트워크에 부여합니다. 사이트 A와 사이트 B는 CVLAN(Customer VLAN) 10, 20, 30을 사용하므로 이러한 VLAN을 레이어 2(L2)에서 확장해야 합니다. 사이트 A는 CE(Customer Edge) 스위치 CusSwitchA를 통해 사업자 네트워크에, 사이트 B는 CE 스위치 CusSwitchB를 통해 사업자 네트워크에 연결됩니다.

사이트 A는 사용된 CVLAN의 IEEE 802.1Q 태그(내부 태그라고도 함)를 사용하여 트래픽을 PE 스위치 ProvSwitchA로 보냅니다. 이 스위치는 QinQ 터널 액세스 역할을 합니다. ProvSwitchA는 수신된 트래픽을 SVLAN의 두 번째 IEEE 802.1Q 태그(외부 태그 또는 메트로 태그라고도 함)를 CVLAN 802.1Q 태그 위에 추가하여 사업자 스위치 네트워크로 전달합니다. 이 프로세스를 VLAN 스택이라고도 하며 이 예에서는 2태그 VLAN 스택을 나타냅니다. 이중 태그 트래픽은 SVLAN MAC(Media Access Control) 테이블 정보만을 기반으로 사업자 네트워크의 L2에 의해 전달됩니다. 이중 태그가 지정된 트래픽이 QinQ 터널의 원격 끝에 도착하면, QinQ 터널 액세스 역할을 하는 원격 PE 스위치 ProvSwitchB는 트래픽에서 SVLAN 태그를 제거하고 CVLAN 802.1Q 태그만 있는 사이트 B로 전달합니다. 따라서 원격 사이트 전체에서 VLAN의 레이어 2 확장이 이루어집니다. 또한 L2 프로토콜 터널링은 CE 스위치 CusSwitchA 및 CusSwitchB 간에 CDP(Cisco Discovery Protocol) 프레임을 교환하도록 구현됩니다.

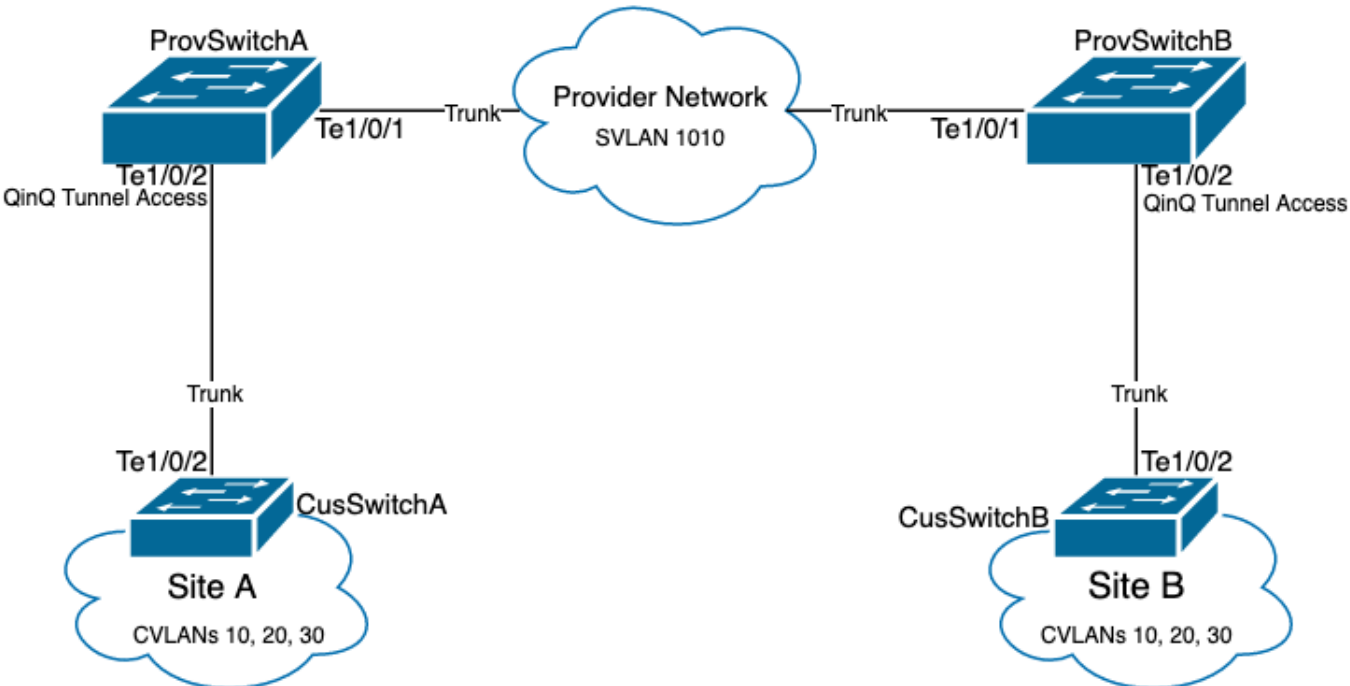
이 프로세스는 사이트 B에서 사이트 A로 트래픽이 전달될 때 발생하며, 동일한 컨피그레이션, 확인 및 문제 해결 단계가 PE 스위치 ProvSwitchB에 적용됩니다. 제공자 스위치 네트워크 및 고객 사이트 내의 다른 모든 장치가 access/trunk 명령으로만 구성되어 있고 QinQ 기능을 수행하지 않는다고 가정합니다.

제시된 예에서는 하나의 802.1Q 태그가 있는 트래픽만 QinQ 터널 액세스 스위치에서 수신된다고 가정합니다. 그러나 수신된 트래픽에는 0개 이상의 802.1Q 태그가 있을 수 있습니다. SVLAN 태그

가 수신된 VLAN 스택에 추가됩니다. 0개 이상의 802.1Q 태그가 있는 트래픽을 지원하기 위해 디바이스에서 추가 QinQ, VLAN 및 트렁크 컨피그레이션이 필요하지 않습니다. 그러나 트래픽에 추가된 추가 바이트를 지원하도록 디바이스의 MTU(Maximum Transmission Unit)를 변경해야 합니다 (Troubleshoot(문제 해결) 섹션에 설명된 추가 세부 사항).

IEEE 802.1Q 터널에 대한 추가 정보는 Catalyst 9500 with Cisco IOS XE Amsterdam-17.3.x용 레이어 2 컨피그레이션 가이드 문서에 나와 있습니다.

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 터널 PE 디바이스)의 컨피그레이션:

```

!
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 터널 PE 디바이스)의 컨피그레이션:

```
<#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 디바이스)의 컨피그레이션:

```
!
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 장치)의 구성:

```
!
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
!
```

CVLAN은 사업자 디바이스에 정의되어 있지 않으며 SVLAN은 CE 스위치에 정의되어 있지 않습니다. 사업자 디바이스는 SVLAN만을 기반으로 트래픽을 포워딩하고 어떤 순방향 결정을 위한 CVLAN 정보도 고려하지 않으므로, 사업자 디바이스가 어떤 VLAN이 QinQ 터널 액세스에서 수신되는지 알 필요가 없습니다(선택적 QinQ가 사용되지 않는 경우). 이는 CVLAN 태그에 사용되는 것과 동일한 VLAN ID를 사업자 스위치 네트워크 및 viceversa 내의 트래픽에 사용할 수 있음을 의미합니다. 이 경우 패킷 손실 또는 트래픽 유출 문제를 방지하기 위해 전역 컨피그레이션 모드에서 vlan dot1q 태그 네이티브를 구성하는 것이 좋습니다. vlan dot1q tag native는 기본적으로 모든 트렁크 인터페이스에서 802.1Q 네이티브 VLAN에 태그를 지정할 수 있지만, 스위치포트 트렁크 네이티브 vlan 태그 컨피그레이션이 없는 인터페이스 레벨에서 비활성화할 수 있습니다.

다음을 확인합니다.

QinQ 터널 및 L2PT에 대한 포트 컨피그레이션은 Cisco IOS XE 관점에서 Catalyst 스위치의 전달 결정이 발생하는 FWD-ASIC(Forwarding Application-Specific Integrated Circuit) 관점에서 확인할 수 있습니다. 기본 Cisco IOS XE 확인 명령은 다음과 같습니다.

- show dot1q-tunnel - QinQ 터널 액세스로 구성된 인터페이스를 나열합니다.

<#root>

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

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

```
-----
```

```
Te1/0/2
```

- show vlan id {svlan-number} - 지정된 VLAN에 할당된 인터페이스를 표시합니다.

<#root>

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

```
VLAN
```

```
Name Status
```

```
Ports
```

```
-----
```

```
1010
```

```
QinQ-VLAN active
```

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

- show interfaces trunk - 트렁크 모드에서 구성된 인터페이스를 나열합니다.

<#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 네이티브 VLAN 태그 전역 상태 및 802.1Q 네이티브

VLAN에 태그를 지정하도록 구성된 트렁크 인터페이스를 나열합니다.

<#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} - SVLAN에서 학습한 MAC 주소를 표시합니다. LAN 디바이스의 MAC 주소는 사용된 CVLAN과 상관없이 SVLAN에서 학습됩니다.

<#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 - L2PT에 대해 활성화된 인터페이스 및 활성화된 각 L2 프로토콜에 대한 카운터를 표시합니다.

<#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
Ten1/0/2	cdp			90	97	0					

- show cdp neighbor - CE 스위치에서 실행하여 CDP를 통해 서로를 볼 수 있는지 확인할 수 있습니다.

```
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
```


인터페이스가 CLI(Command Line Interfaces)를 통한 QinQ 터널 액세스로 구성된 경우 Cisco IOS XE는 PM(Port Manager) 프로세스를 트리거하여 지정된 모드 및 VLAN으로 스위치 포트를 구성합니다. Switchport 정보는 PM에 show pm port interface {interface-name} 명령을 사용하여 확인할 수 있습니다.

 참고: PM 명령을 실행하려면 글로벌 컨피그레이션 모드에서 서비스 내부를 구성해야 합니다. 이 컨피그레이션을 사용하면 추가 플랫폼 및 디버그 명령을 CLI에서 실행할 수 있으며 네트워크에 아무런 영향을 미치지 않습니다. PM 검증이 완료되면 이 명령을 제거하는 것이 좋습니다.

<#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
```

인터페이스 Te1/0/2에는 인터페이스 번호(if_number)인 2가 할당됩니다. 특정 포트를 식별하는 내부 값인 인터페이스 식별자(IF-ID)입니다. switchport 컨피그레이션은 PM에서 show platform software pm-port switch 1 R0 interface {IF-ID} 명령을 사용하여 확인할 수도 있습니다.

<#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	

PM이 스위치 포트 컨피그레이션을 적용하면 PM은 ASIC(Application-specific Integrated Circuits)를 프로그래밍하기 위해 포트 정보를 FED(Forwarding Engine Driver)에 릴레이합니다.

FED에서 포트는 show platform software fed switch {switch-number} port if_id {IF-ID} 명령으로 확인하여 QinQ 터널 액세스 포트에 프로그래밍되었는지 확인할 수 있습니다.

<#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
```

태그가 지정되지 않은 트래픽만 수신해야 하는 액세스 모드의 switchport와 달리, 802.1Q 터널 모드로 구성된 switchport는 802.1Q 태그가 있는 트래픽도 수용합니다. FED는 show platform software fed switch {switch-number} ifm if-id {IF-ID}에서 확인할 수 있는 것처럼 QinQ 터널 액세스 포트에 대

해 이 기능을 허용합니다.

<#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]
```

FED는 또한 Port Logical Entity(Port LE)라는 16진수 형식의 핸들 값을 제공합니다. 포트 LE는 포워딩 ASIC(fwd-asic)에 프로그래밍된 포트 정보에 대한 포인터이다. show platform hardware fed switch 1 fwd-asic 추상화 print-resource-handle {Port-LE-handle} 1 명령은 ASIC 레벨에서 포트에 활성화된 다양한 기능을 표시합니다.

<#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
```

이 출력은 ASIC 레벨에서 QinQ 터널 액세스 스위치 포트가 LAN에서 오는 태그되지 않은 802.1Q 태그된 트래픽을 허용하도록 구성되어 있으며 SVLAN 1010이 사업자 스위치 네트워크를 통해 전달 되도록 지정되었음을 확인합니다. LEAD_PORT_SEL_QINQ_ENABLED 필드가 설정되지 않았습니 다. 이 비트는 Selective QinQ 컨피그레이션에만 설정되며 이 문서에 제시된 기존 QinQ 터널 컨피 그레이션에는 설정되지 않습니다.

문제 해결

이 섹션에서는 컨피그레이션 트러블슈팅을 위해 수행할 수 있는 단계를 제공합니다. 802.1Q 터널 에서 트래픽 문제를 해결하는 데 가장 유용한 툴은 SPAN(Switched Port Analyzer)입니다. SPAN 캡 처는 QinQ 터널 액세스 디바이스에 추가된 LAN 및 SVLAN에서 수신한 CVLAN의 802.1Q 태그를 확인하는 데 사용할 수 있습니다.

 참고: EPC(Embedded Packet Captures)는 802.1Q 터널 환경에서 트래픽을 캡처하는 데에도 사용할 수 있습니다. 그러나 EPC를 통한 이그레스 패킷 캡처는 트래픽이 IEEE 802.1Q로 태 그되기 전에 발생합니다(802.1Q 태그 삽입은 이그레스 방향의 포트 레벨에서 발생함). 따라서 공급자 에지 장치의 업링크 트렁크에 있는 이그레스 EPC는 공급자 스위치 네트워크에서 사 용되는 SVLAN 태그를 표시할 수 없습니다. EPC를 사용하여 이중 태그 트래픽을 수집하는 옵션은 인접 디바이스 제공자 디바이스에서 인그레스 EPC를 사용하여 트래픽을 캡처하는 것입 니다.

EPC에 대한 자세한 내용은 Cisco IOS XE Amsterdam-17.3.x를 사용하는 Catalyst 9500 스위 치의 네트워크 관리 컨피그레이션 가이드를 참조하십시오.

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 태그로 트래픽을 캡처하도록 SPAN을 구성하려면 monitor session {session-number} destination interface {interface-name} encapsulation replicate 명령을 구성해야 합니다. encapsulation replicate 키워드가 구성되지 않은 경우 SPAN으로 미러링된 트래픽에 잘못된 802.1Q 태그 정보가 포함될 수 있습니다. SPAN 컨피그레이션의 예는 Configure 섹션을 참조하십 시오.

SPAN에 대한 자세한 내용은 Cisco IOS XE Amsterdam-17.3.x를 사용하는 Catalyst 9500 스위치의 네트워크 관리 컨피그레이션 가이드를 참조하십시오

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

ProvSwitchA의 SPAN 컨피그레이션 예:


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

네트워크 분석기 디바이스에서 수신된 미러링된 트래픽을 검토하여 QinQ 터널 액세스 인그레스 (ingress)에 CVLAN 10이 있는지 확인할 수 있습니다.

```
> Frame 29: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface 0  
> 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)  
> 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
```

마찬가지로 CVLAN 10 및 SVLAN 1010의 존재는 사업자 스위치 네트워크에 연결된 인터페이스 트렁크에서 이그레스 방향으로 확인할 수 있습니다.

```
> Frame 30: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface 0  
> 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)  
> 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)  
> 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
```

 참고: 네트워크 분석기의 특정 NIC(Network Interface Card)는 수신된 태그 트래픽에서 802.1Q 태그를 제거할 수 있습니다. 수신된 프레임에서 802.1Q 태그를 유지 관리하는 방법에 대한 자세한 내용은 NIC 공급업체에 문의하십시오.

QinQ 스위치 네트워크에서 트래픽 손실이 의심되는 경우 다음 항목을 검토하십시오.


- 트렁크 인터페이스의 기본 MTU(Maximum Transmission Unit)는 1522바이트입니다. 이는 IP MTU 1500, 이더넷 헤더 프레임 18바이트, 802.1Q 태그 1개(4바이트)를 차지합니다. 모든 사업자 및 사업자 에지 디바이스에서 구성된 MTU는 VLAN 스택에 추가된 802.1Q 태그당 4바이트가 더 있어야 합니다. 예를 들어, 2태그 VLAN 스택의 경우 MTU 1504를 구성해야 합니다.

3태그 VLAN 스택의 경우 MTU 1508을 구성해야 합니다. MTU 컨피그레이션 세부사항은 Cisco IOS XE Amsterdam-17.3.x를 사용하는 Catalyst 9500용 인터페이스 및 하드웨어 구성 요소 컨피그레이션 설명서를 참조하십시오.

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 터널 내 디바이스의 CPU에 대한 트래픽은 지원되지 않습니다. 트래픽 검사가 필요한 기능은 802.1Q 환경에서 패킷 손실 또는 패킷 유출을 일으킬 수 있습니다. 이러한 기능의 예로는 DHCP 트래픽용 DHCP 스누핑, IGMP 트래픽용 IGMP 스누핑, MLD 트래픽용 MLD 스누핑 및 ARP 트래픽용 동적 ARP 검사가 있습니다. 사업자 전환 네트워크를 통해 트래픽을 전송하는 데 사용되는 SVLAN에서 이러한 기능을 비활성화하는 것이 좋습니다.

추가 debug 명령

 참고: debug 명령을 사용하기 [전에 Debug 명령](#)에 대한 중요 정보를 참조하십시오.

- debug pm port - 포트 관리자(PM) 포트 전환 및 프로그래밍된 모드를 표시합니다. QinQ 포트 컨피그레이션 상태를 디버깅하는 데 유용합니다.

관련 정보

- [Catalyst 9300 스위치 - IEEE 802.1Q 터널링 구성](#)
- [Catalyst 9300 스위치 - 레이어 2 프로토콜 터널링 구성](#)
- [Catalyst 9300 스위치 - EtherChannel 구성](#)
- [기술 지원 및 문서 - Cisco Systems](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.