Catalyst 9000 스위치의 알 수 없는 프로토콜 삭제 문제 해결

목차

소개

이 문서에서는 Catalyst 9000 Series 스위치에서 알 수 없는 프로토콜 삭제의 일반적인 원인을 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- DTP(Dynamic Trunking Protocol)
- LLDP(Link Layer Discovery Protocol)
- CDP(Cisco Discovery Protocol)
- 캡슐화 802.1Q

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Catalyst 9000 시리즈 스위치

- Cisco IOS® XE

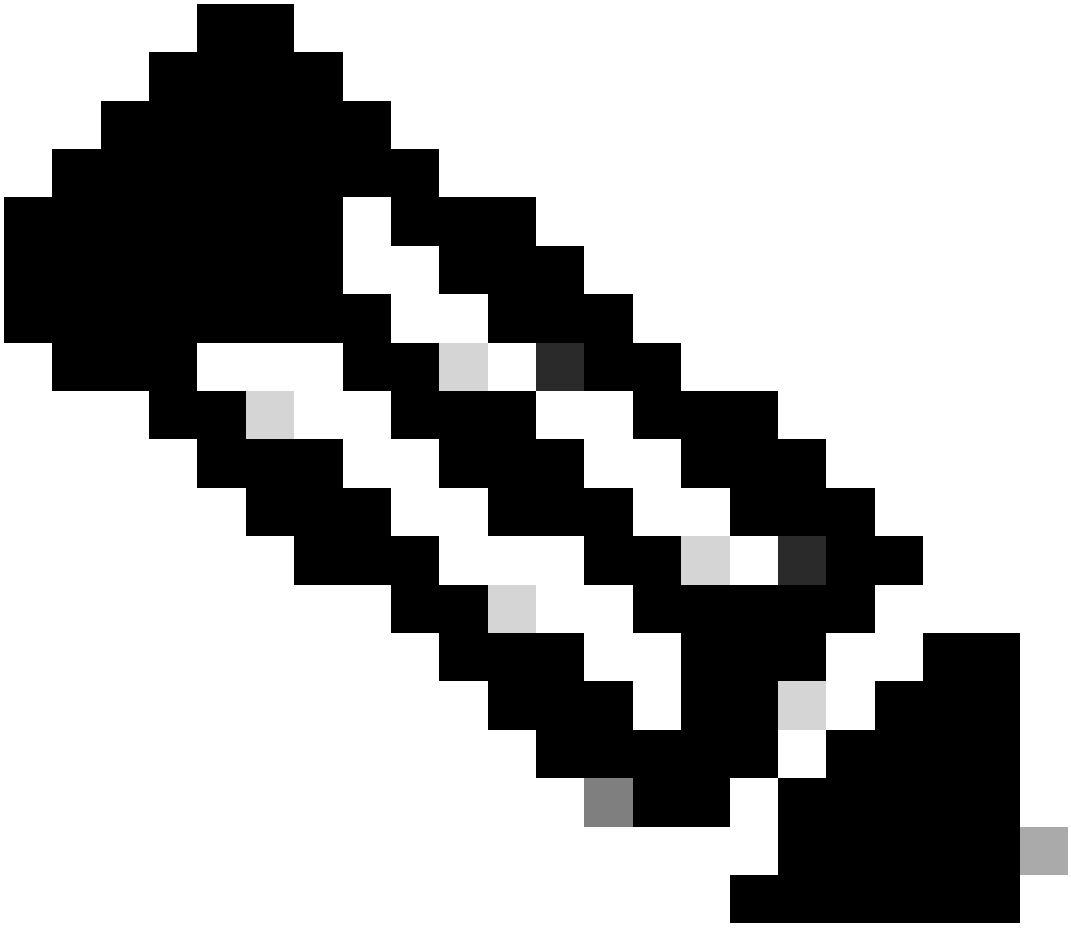
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

알 수 없는 프로토콜 삭제는 프레임의 이더 타입이 인식되지 않을 때 발생합니다. 즉, 캡슐화된 프로토콜이 지원되지 않거나 스위치 인터페이스에서 구성되지 않습니다. 또한 프레임의 대상 MAC 주소는 이 명령에 나열된 멀티캐스트 컨트롤 플레인 주소여야 합니다.

<#root>

```
Switch#

show mac address-table | include CPU

 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0180.c200.0000    STATIC      CPU
 All    0180.c200.0001    STATIC      CPU
 All    0180.c200.0002    STATIC      CPU
 All    0180.c200.0003    STATIC      CPU
 All    0180.c200.0004    STATIC      CPU
 All    0180.c200.0005    STATIC      CPU
 All    0180.c200.0006    STATIC      CPU
 All    0180.c200.0007    STATIC      CPU
 All    0180.c200.0008    STATIC      CPU
 All    0180.c200.0009    STATIC      CPU
 All    0180.c200.000a    STATIC      CPU
 All    0180.c200.000b    STATIC      CPU
 All    0180.c200.000c    STATIC      CPU
 All    0180.c200.000d    STATIC      CPU
 All    0180.c200.000e    STATIC      CPU
 All    0180.c200.000f    STATIC      CPU
 All    0180.c200.0010    STATIC      CPU
 All    0180.c200.0021    STATIC      CPU
 All    ffff.ffff.ffff    STATIC      CPU
```



참고: 목적지 MAC 주소가 브로드캐스트될 때 알 수 없는 프로토콜 삭제는 증가하지 않습니다.

문제 해결

1단계. 알 수 없는 프로토콜 삭제의 증가 여부를 확인합니다.

<#root>

Switch#

show interface ten1/0/5 | include protocol

TenGigabitEthernet1/0/5 is up, line protocol is up (connected)

85 unknown protocol drops

Switch#

```
show interface ten1/0/5 | include protocol

TenGigabitEthernet1/0/5 is up, line protocol is up (connected)

90 unknown protocol drops
```

2단계. 영향을 받는 인터페이스에서 패킷 캡처를 구성하고 01부터 대상 MAC 주소를 확인합니다.

```
<#root>

Switch#

monitor capture port5 interface ten1/0/5 in

Switch#

monitor capture port5 match mac any 0100.0000.0000 00ff.ffff.ffff

Switch#

monitor capture port5 buffer size 100
```

3단계. 패킷 캡처를 시작하고 unknown-protocol-drops 카운터를 확인합니다.

```
<#root>

Switch#

monitor capture port5 start

Started capture point : port5

Switch#

show interface ten1/0/5 | include protocol

TenGigabitEthernet1/0/5 is up, line protocol is up (connected)
     541 unknown protocol drops
```

4단계. 몇 가지 알 수 없는 프로토콜이 삭제된 후 패킷 캡처를 중지합니다.

```
<#root>

Switch#

show interface ten1/0/5 | include protocol

TenGigabitEthernet1/0/5 is up, line protocol is up (connected)
     544 unknown protocol drops
```

```
Switch#

monitor capture port5 stop

Capture statistics collected at software:
        Capture duration - 68 seconds
        Packets received - 38
        Packets dropped - 0
        Packets oversized - 0

Bytes dropped in asic - 0

Capture buffer will exists till exported or cleared

Stopped capture point : port5
```

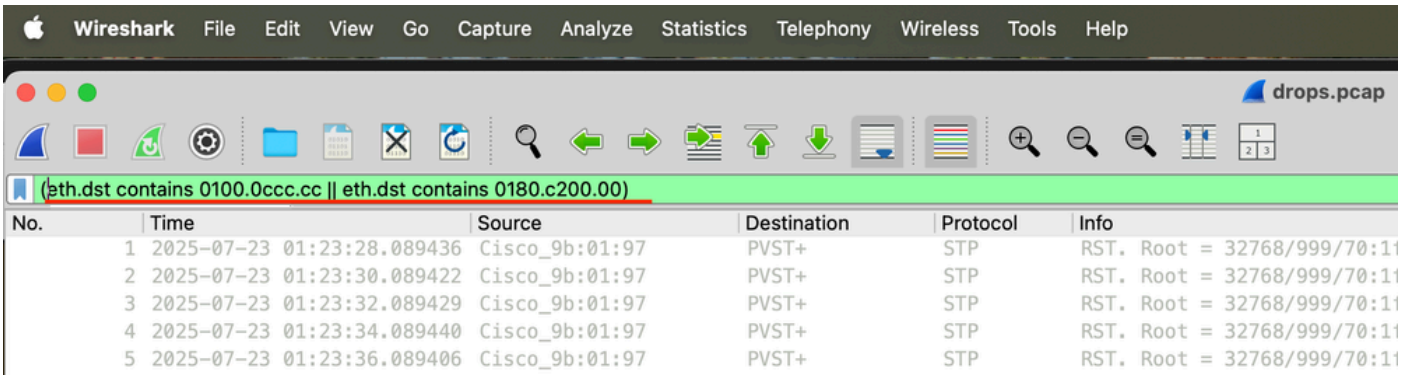
5단계. 패킷 캡처 콘텐츠를 내보냅니다.

```
<#root>

Switch#

monitor capture port5 export location flash:drops.pcap

Export Started Successfully

Switch#
Export completed for capture point port5
```

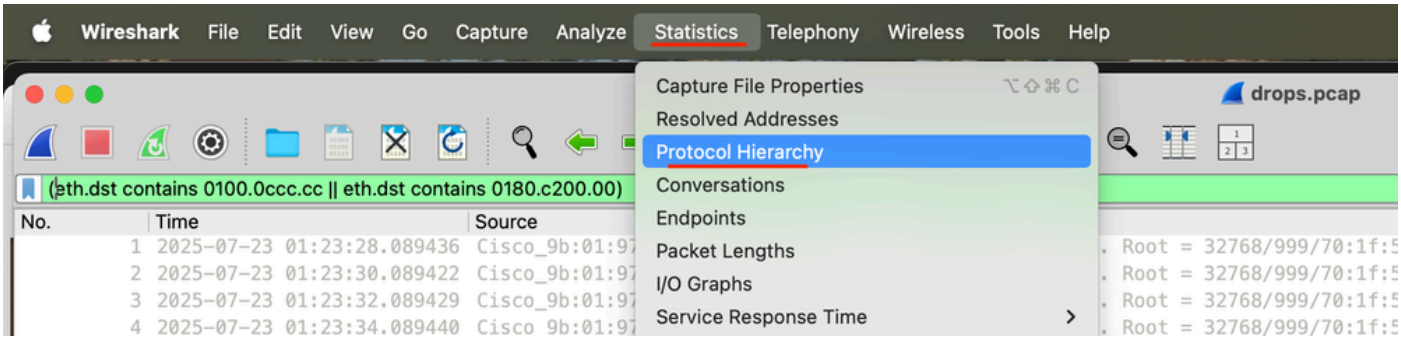
6단계. 패킷 캡처를 컴퓨터로 전송합니다.

```
<#root>

Switch#

copy flash: ftp: vrf Mgmt-vrf

Source filename [drops.pcap]?
Address or name of remote host []? 10.10.10.254
Destination filename [drops.pcap]?
Writing drops.pcap !
4024 bytes copied in 0.026 secs (154769 bytes/sec)
```

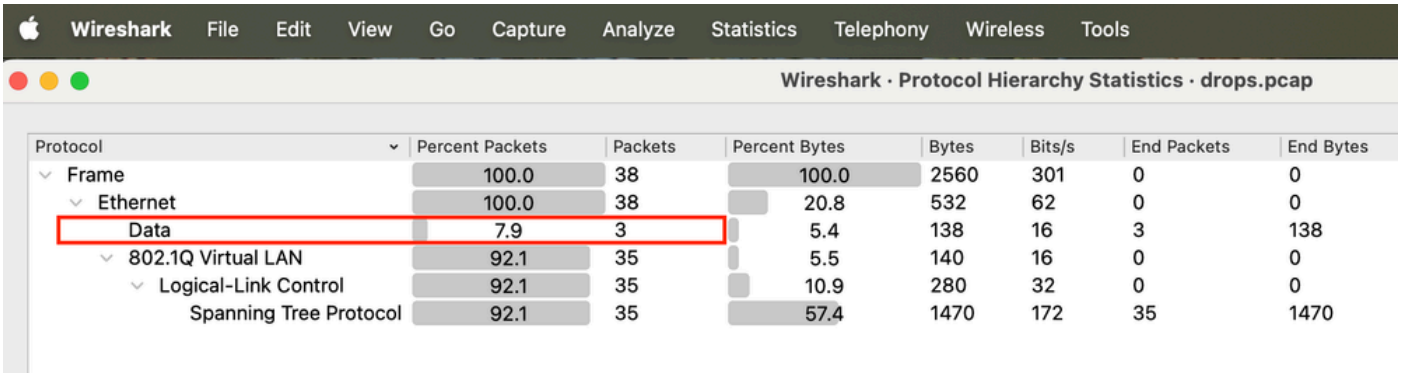
7단계. Wireshark에서 패킷 캡처를 열고 이 필터를 사용합니다(eth.dst contains 0100.0ccc.cc) | eth.dst에는 CPU 멀티캐스트 주소에 주력할 0180.c200.00이 포함되어 있습니다.



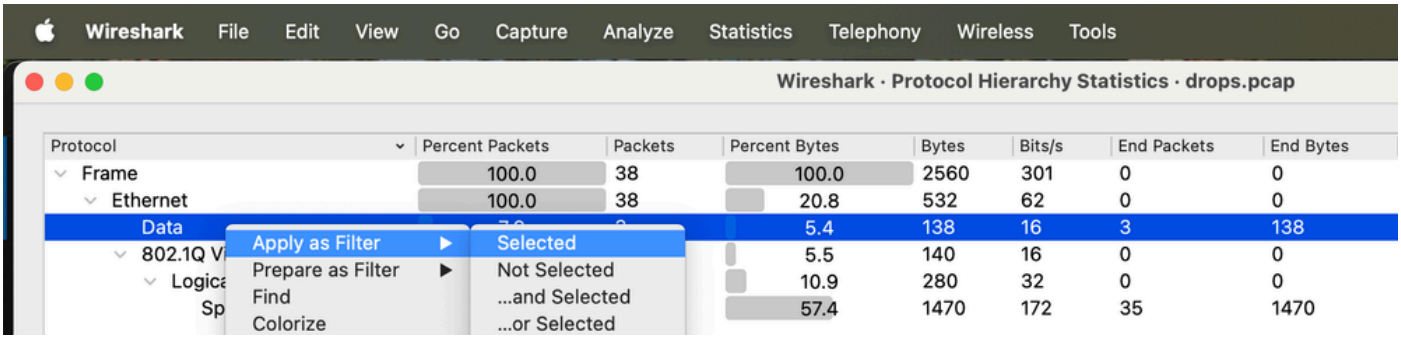
8단계. Statistics(통계)로 이동한 다음 Protocol Hierarchy(프로토콜 계층)를 클릭합니다.



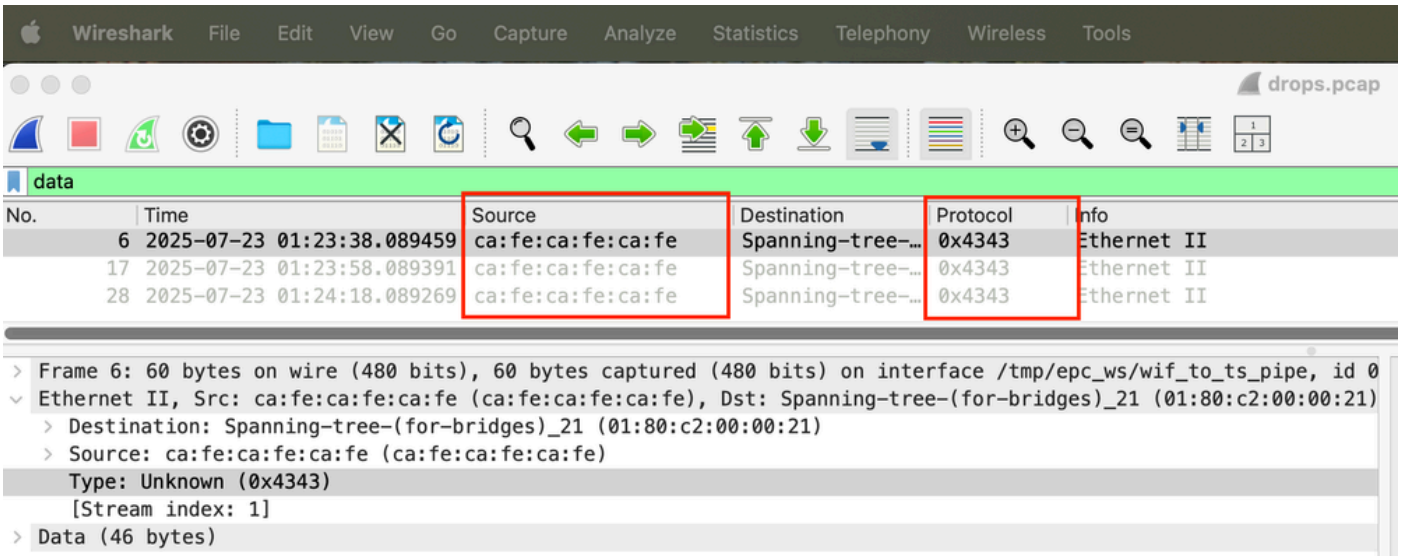
9단계. 프로토콜 트리를 확장하고 스위치 인터페이스가 이러한 프로토콜에 대해 구성되어 있는지 확인합니다. 이더 타입을 알 수 없기 때문에 Data로 레이블이 지정된 모든 프로토콜이 손실됩니다.



10단계. Data(데이터)를 마우스 오른쪽 버튼으로 클릭하고 Apply as Filter(필터로 적용)로 이동한 다음 Selected(선택)를 클릭하여 알 수 없는 프로토콜 프레임을 필터링합니다.



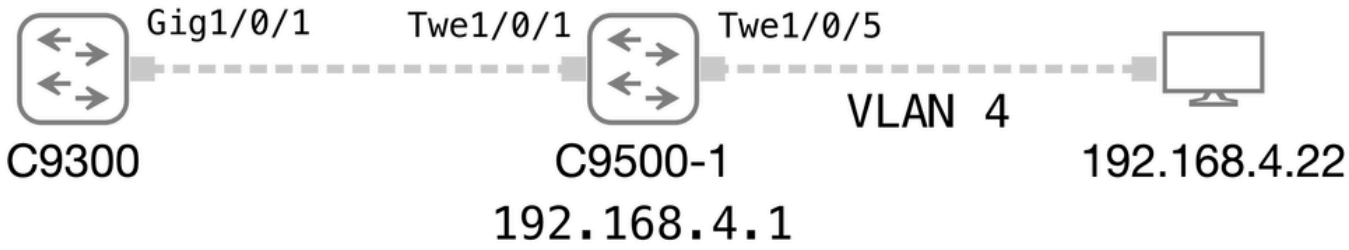
11단계. Wireshark의 주 창으로 돌아가 알 수 없는 프로토콜에 대한 소스 MAC 주소 및 이더 타입을 확인합니다.



이 경우 이더 타입 0x4343이 지원되지 않으므로 소스 MAC 주소 CAFE.CAFE.CAFE에서 알 수 없는 프로토콜 삭제를 발생시킵니다.

일반적인 문제

이 섹션의 예는 이 네트워크 토폴로지 다이어그램을 기반으로 합니다.



DTP(Dynamic Trunking Protocol)

DTP 메시지는 DTP가 비활성화된 포트에서 수신된 경우 알 수 없는 프로토콜 삭제를 유발할 수 있습니다. 인터페이스 컨피그레이션 모드에서 no switchport nonegotiate 명령을 사용하여 DTP를 활성화할 수 있습니다.

<#root>

C9500-1#

show running-config interface Twe1/0/1

```
interface TwentyFiveGigE1/0/1
 description C9300
 switchport mode trunk
end

C9300#
```

```
show running-config interface Gi1/0/1

interface GigabitEthernet1/0/1
 description C9500-1
 switchport mode trunk
 switchport nonegotiate
end

C9300#

show interface gi1/0/1 | include unknown

     350 unknown protocol drops
```

LLDP(Link Layer Discovery Protocol)

LLDP 메시지는 LLDP가 비활성화된 포트에서 수신된 경우 알 수 없는 프로토콜 삭제를 일으킬 수도 있습니다. 글로벌 컨피그레이션 모드에서 실행되는 lldp 명령을 사용하여 LLDP를 활성화할 수 있습니다.

```
<#root>

C9500-1#

show lldp

Global LLDP Information:
    Status: ACTIVE
    LLDP advertisements are sent every 30 seconds
    LLDP hold time advertised is 120 seconds
    LLDP interface reinitialisation delay is 2 seconds

C9300#

show lldp

% LLDP is not enabled

C9300#

show interface gi1/0/1 | include unknown

     423 unknown protocol drops
```

CDP(Cisco Discovery Protocol)

마찬가지로 CDP 메시지가 CDP가 비활성화된 포트에서 수신된 경우 알 수 없는 프로토콜 삭제는 증가할 수 있습니다. 글로벌 컨피그레이션 모드에서 cdp run 명령을 사용하여 CDP를 활성화할 수 있습니다.

```
<#root>

C9500-1#
```

```
show cdp


Global CDP information:
        Sending CDP packets every 60 seconds
        Sending a holdtime value of 180 seconds
        Sending CDPv2 advertisements is  enabled

C9300#

show cdp

% CDP is not enabled

C9300#

show interface gi1/0/1 | include unknown

     434 unknown protocol drops
```

802.1Q 헤더의 All-Zero VLAN 식별자

또한 Catalyst 9000 Series 스위치는 VLAN ID가 0인 802.1Q 프레임이 액세스 포트에서 수신될 때 이를 삭제합니다. 그러나 이러한 패킷은 알 수 없는 프로토콜 삭제 카운터를 증가시키지 않습니다. 이 예에서는 Catalyst 9500 스위치가 호스트 192.168.4.22에 대한 ARP 항목을 가져올 수 없는 이유를 알아보겠습니다.

```
<#root>

C9500-1#

ping 192.168.4.22

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.22, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

C9500-1#

show ip arp vlan 4

Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.4.1              -   ecc0.18a4.b1bf  ARPA   Vlan4
C9500-1#

C9500-1#

show running-config interface Twe1/0/5

interface TwentyFiveGigE1/0/5
 switchport access vlan 4
 switchport mode access
 load-interval 30
end
```

1단계. 최종 디바이스에 연결된 인터페이스에서 패킷 캡처를 시작합니다.

<#root>

```
C9500-1#

show monitor capture TAC parameter

   monitor capture TAC interface TwentyFiveGigE1/0/5 both
   monitor capture TAC match any
   monitor capture TAC buffer size 100 circular
   monitor capture TAC limit pps 1000

C9500-1#

monitor capture TAC start

Started capture point : TAC
```

2단계. 일부 ARP 트래픽을 생성하기 위해 최종 디바이스를 ping해 봅니다.

<#root>

```
C9500-1#

ping 192.168.4.22

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.22, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

3단계. 패킷 캡처를 중지합니다.

<#root>

```
C9500-1#

monitor capture TAC stop

Capture statistics collected at software:
        Capture duration - 35 seconds
        Packets received - 28
        Packets dropped - 0
        Packets oversized - 0

Bytes dropped in asic - 0

Capture buffer will exists till exported or cleared

Stopped capture point : TAC
```

4단계. 엔드 디바이스가 ARP 응답을 전송하며, 이 경우 프레임 17입니다.

```
<#root>

C9500-1#

show monitor capture TAC buff brief | include ARP

   15  19.402191 ec:c0:18:a4:b1:bf b^F^R ff:ff:ff:ff:ff:ff ARP 60 Who has 192.168.4.22? Tell 192.168.4.
   17  21.347022 fe:af:ea:fe:af:ea b^F^R ec:c0:18:a4:b1:bf ARP 60 192.168.4.22 is at fe:af:ea:fe:af:ea
```

5단계. ARP 회신은 VLAN ID 0을 사용하여 802.1Q 헤더에 캡슐화됩니다.

```
<#root>

C9500-1#

show monitor capture TAC buff detailed | begin Frame 17

Frame 17: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
<output omitted>
Ethernet II, Src: fe:af:ea:fe:af:ea (fe:af:ea:fe:af:ea), Dst: ec:c0:18:a4:b1:bf (ec:c0:18:a4:b1:bf)
    Destination: ec:c0:18:a4:b1:bf (ec:c0:18:a4:b1:bf)
        Address: ec:c0:18:a4:b1:bf (ec:c0:18:a4:b1:bf)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: fe:af:ea:fe:af:ea (fe:af:ea:fe:af:ea)
        Address: fe:af:ea:fe:af:ea (fe:af:ea:fe:af:ea)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: 802.1Q Virtual LAN (0x8100)

802.1Q Virtual LAN

, PRI: 0, DEI: 0, ID: 0
    000. .... .... .... = Priority: Best Effort (default) (0)
    ...0 .... .... .... = DEI: Ineligible
    ....

0000 0000 0000 = ID: 0

    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: fe:af:ea:fe:af:ea (fe:af:ea:fe:af:ea)
    Sender IP address: 192.168.4.22
    Target MAC address: ec:c0:18:a4:b1:bf (ec:c0:18:a4:b1:bf)
    Target IP address: 192.168.4.1
```

6단계. 패킷 캡처 콘텐츠를 내보냅니다.

<#root>

```
C9500-1#

monitor capture TAC export location flash:ARP.pcap

Export Started Successfully
```

7단계. 패킷 추적기 도구를 사용하여 스위치에서 패킷 17에 대해 수행하는 작업을 확인합니다.

<#root>

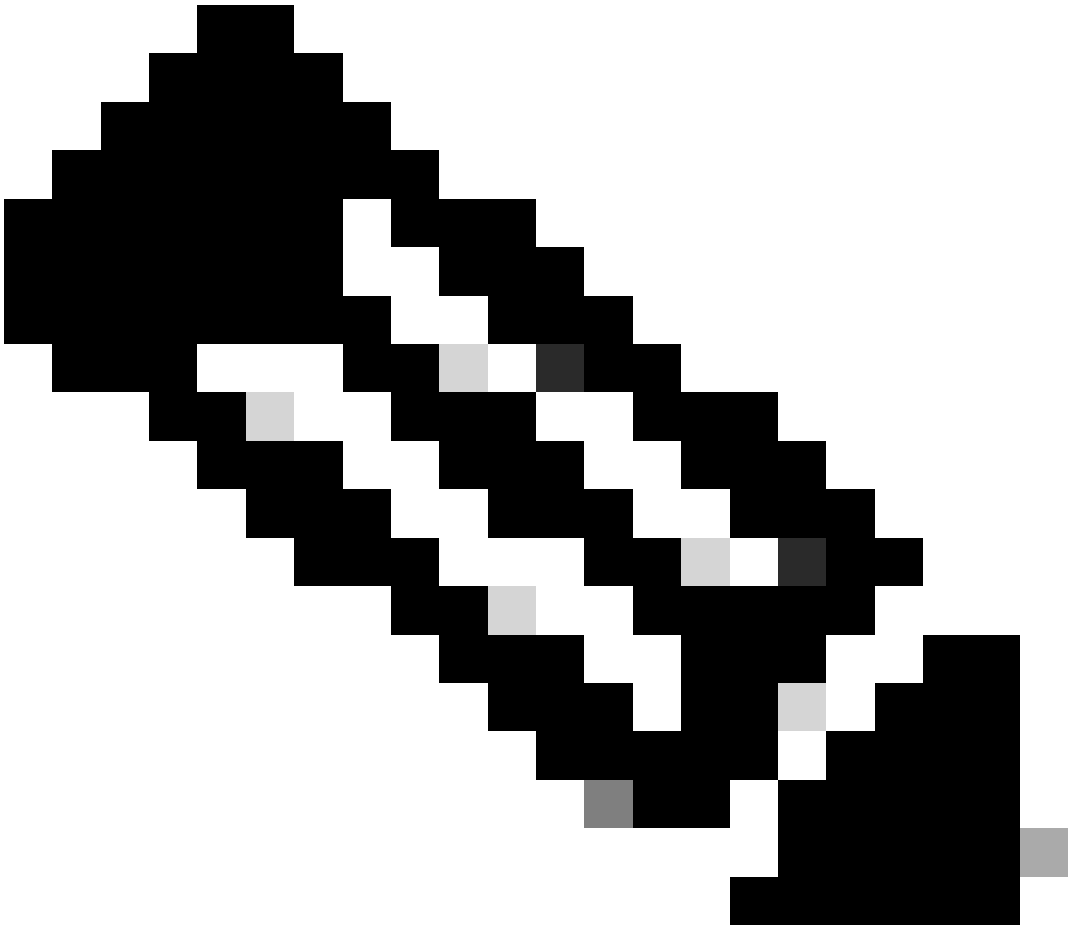
```
C9500-1#

show platform hardware fed active forward interface Twe1/0/5 pcap flash:ARP.pcap number 17 data

Show forward is running in the background. After completion, syslog will be generated.

C9500-1#
*Sep 29 17:45:29.091: %SHFWD-6-PACKET_TRACE_DONE: R0/0: fed: Packet Trace Complete:  Execute (show plat
*Sep 29 17:45:29.091: %SHFWD-6-PACKET_TRACE_FLOW_ID: R0/0: fed: Packet Trace Flow id is 6881284
```

8단계. 패킷 추적기 결과를 표시합니다.

<#root>

```
C9500-1#

show platform hardware fed active forward last summary


Input Packet Details:
###[ Ethernet ]###
  dst       = ec:c0:18:a4:b1:bf
  src=fe:af:ea:fe:af:ea
  type      = 0x8100
###[ 802.1Q ]###
     prio      = 0
     id        = 0
     vlan      = 0
     type      = 0x806
###[ ARP ]###
        hwtype    = 0x1
        ptype     = 0x800
        hwlen     = 6
        plen      = 4
        op        = is-at
        hwsrc=fe:af:ea:fe:af:ea
        psrc=192.168.4.22
        hwdst     = ec:c0:18:a4:b1:bf
        pdst      = 192.168.4.1
###[ Padding ]###
           load      = '00 00 00 00 00 00 00 00 00 00 00 00 00 00'
<output omitted>

Packet DROPPED
```

```
 Catch-all for phf.finalFdPresent==1.
```



참고: 패킷은 VLAN ID 0을 포함하므로 삭제됩니다.

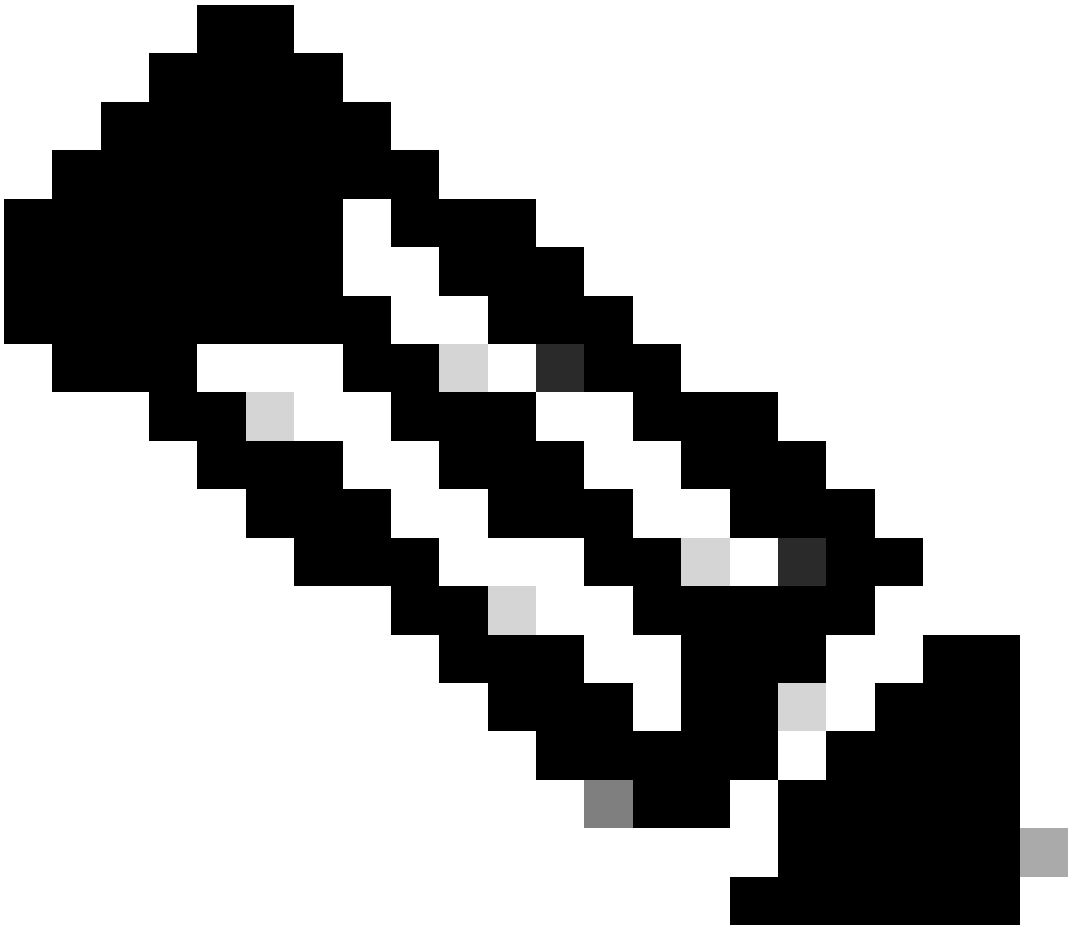
이러한 유형의 삭제를 방지하는 두 가지 옵션이 있습니다.

옵션 1: switchport voice vlan dot1p 명령을 사용합니다. 이렇게 VLAN 0으로 수신된 프레임은 액세스 VLAN에 할당됩니다.

```
interface TwentyFiveGigE1/0/5
 switchport access vlan 4
 switchport mode access
 switchport voice vlan dot1p
 load-interval 30
```

옵션 2: 인터페이스를 트렁크 포트로 구성합니다. 이렇게 하면 vlan 0과 함께 수신된 프레임이 네이티브 vlan에 할당됩니다.

```
interface TwentyFiveGigE1/0/5
 switchport trunk native vlan 4
 switchport mode trunk
 load-interval 30
end
```



참고: 이는 Profinet 디바이스에서 흔히 볼 수 있는 현상입니다.

관련 결함

- 자세한 내용은 Cisco 버그 ID CSCwe88812를 참조하십시오.

관련 정보

- VLAN 0 우선순위 태깅 지원

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.