Catalyst 9000スイッチでの未知のプロトコルドロップのトラブルシューティング

内容

はじめに

前提条件

- 要件
- 使用するコンポーネント

背景説明

トラブルシュート

一般的な問題

- Dynamic Trunking Protocol（DTP; ダイナミック トランキング プロトコル）
- Link Layer Discovery Protocol（LLDP）
- シスコ検出プロトコル（CDP）
- 802.1Qヘッダーですべてゼロ のVLAN識別子

関連する不具合

関連情報

はじめに

このドキュメントでは、Catalyst 9000シリーズスイッチでの未知のプロトコルのドロップの一般的な原因について説明します。

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。

- Dynamic Trunking Protocol（DTP; ダイナミック トランキング プロトコル）
- Link Layer Discovery Protocol（LLDP）
- シスコ検出プロトコル（CDP）
- 802.1Qカプセル化

使用するコンポーネント

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

- Catalyst 9000 シリーズ スイッチ

- Cisco IOS® XE

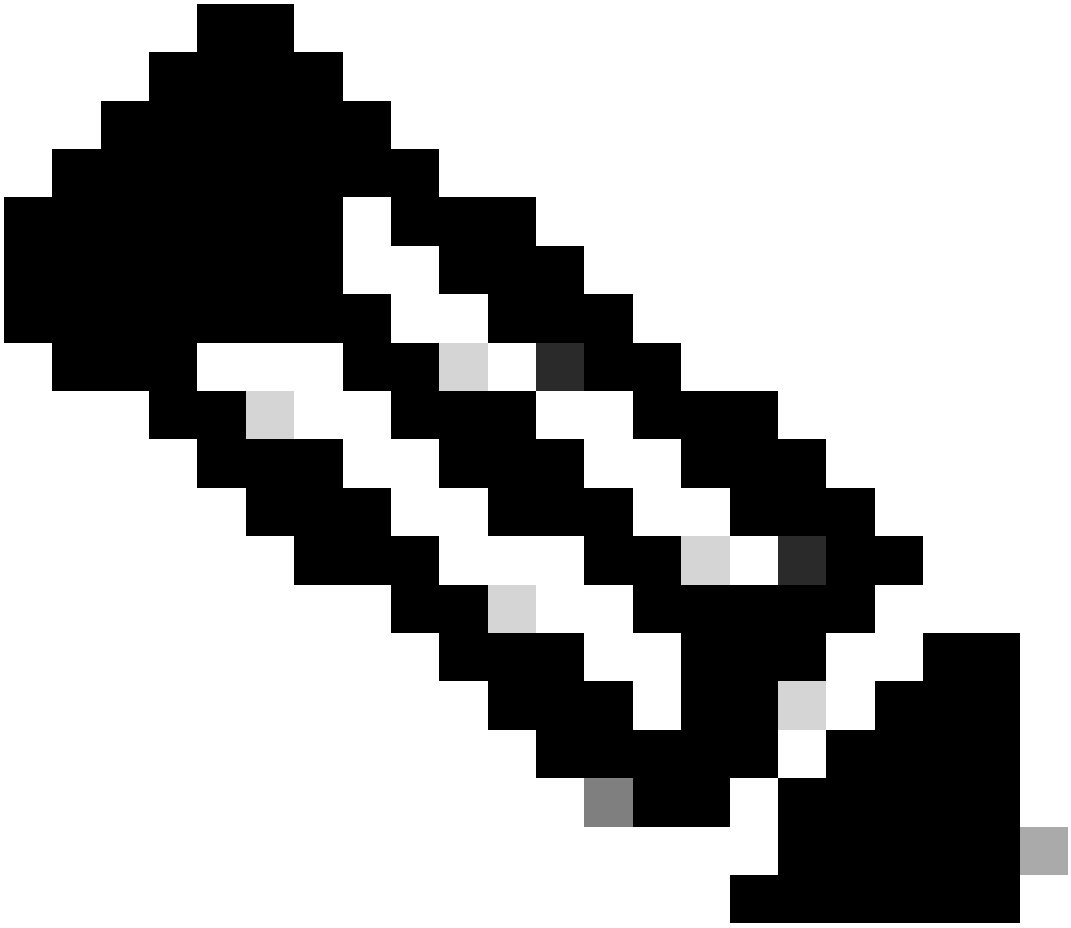
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

不明なプロトコルドロップは、フレームのethertypeが認識されない場合に発生します。これは、カプセル化されたプロトコルがスイッチインターフェイスでサポートされていないか、設定されていないことを意味します。また、フレームの宛先MACアドレスは、このコマンドにリストされているマルチキャストコントロールプレーンアドレスである必要があります。

<#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
```



注：宛先MACアドレスがブロードキャストの場合、未知のプロトコルのドロップは増加しません。

トラブルシュート

ステップ 1：不明なプロトコルの廃棄が増加していることを確認します。

<#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
```

ステップ 2：影響を受けるインターフェイスでパケットキャプチャを設定し、01で始まる宛先MACアドレスを照合します。

```
<#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
```

ステップ 3：パケットキャプチャを開始し、unknown-protocol-dropsカウンタを確認します。

```
<#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
```

ステップ 4：不明なプロトコルが数個廃棄された後、パケットキャプチャを停止します。

```
<#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
```

ステップ 5：パケットキャプチャの内容をエクスポートします。

<#root>

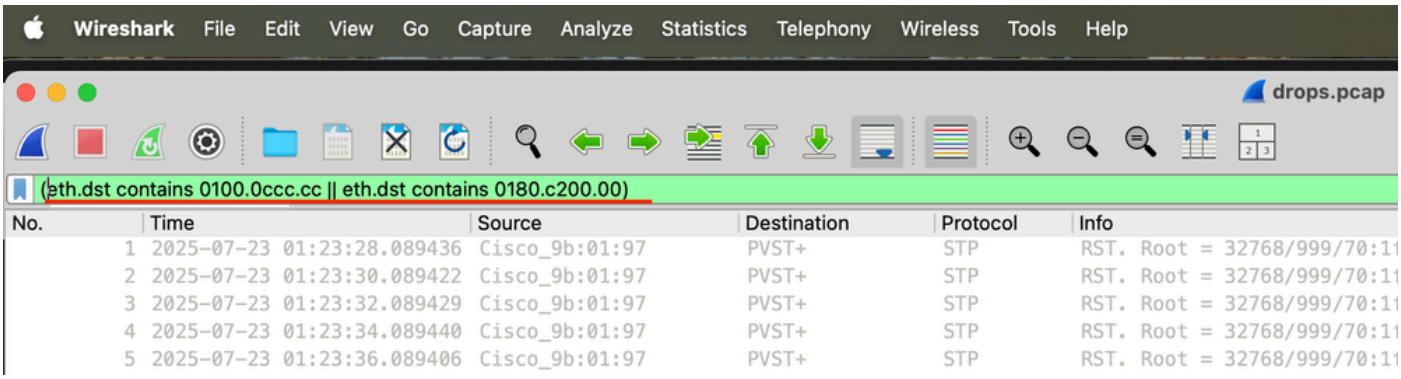
```
Switch#

monitor capture port5 export location flash:drops.pcap

Export Started Successfully

Switch#
Export completed for capture point port5
```

手順 6：パケットキャプチャをコンピュータに転送します。

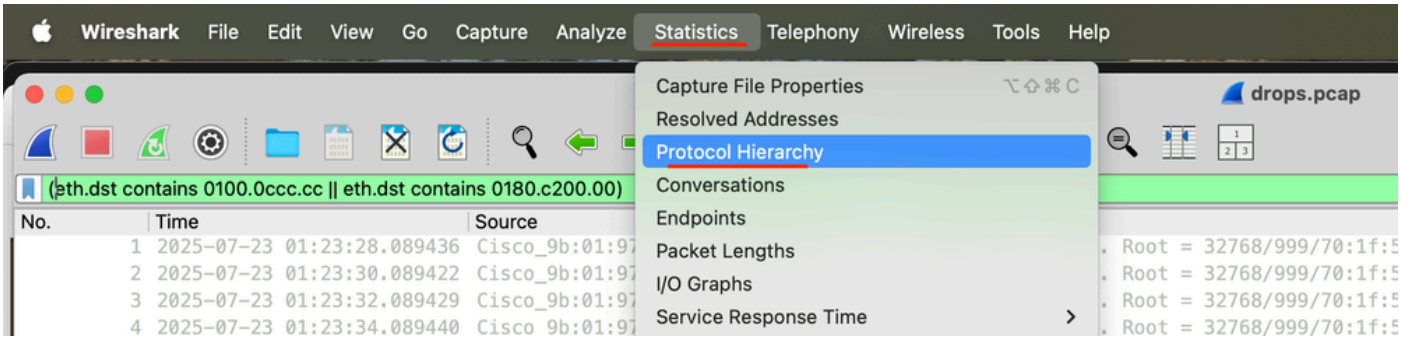
<#root>

```
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)
```

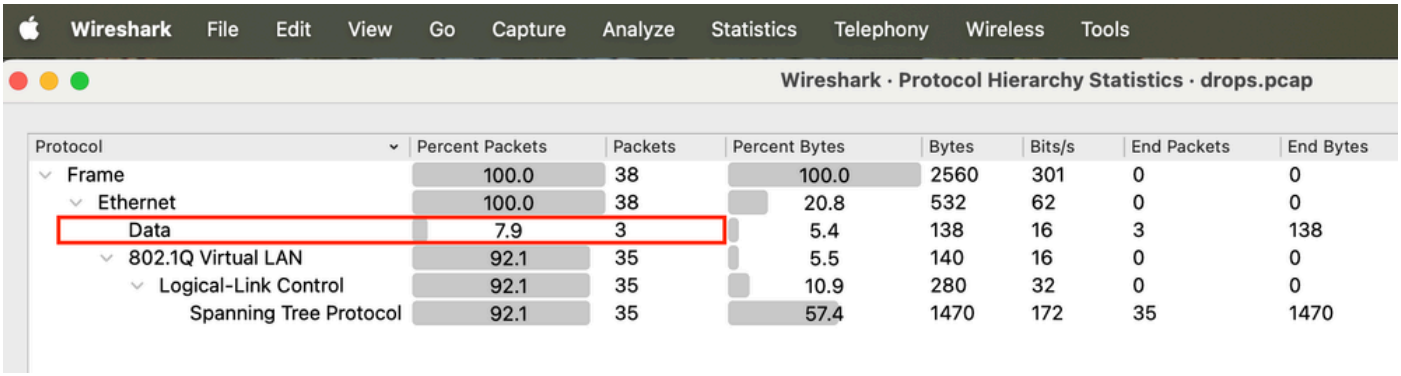
手順 7：Wiresharkでパケットキャプチャを開き、このフィルタ(eth.dst contains 0100.0ccc.cc || eth.dst contains 0180.c200.00)を使用してCPUマルチキャストアドレスに焦点を合わせます。



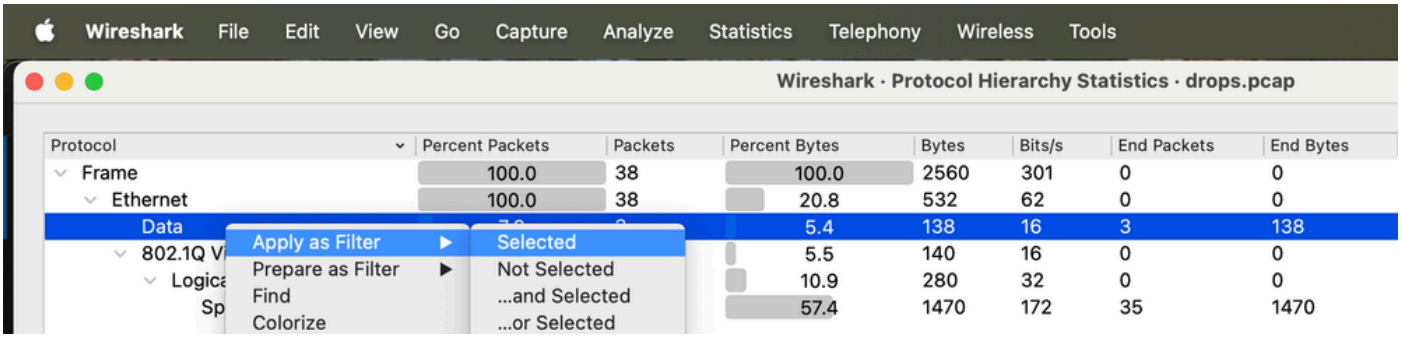
ステップ 8：Statisticsに移動し、次にProtocol Hierarchyをクリックします。



ステップ 9：プロトコルツリーを展開し、スイッチインターフェイスがこれらのプロトコル用に設定されていることを確認します。Dataとラベル付けされているものがあると、EtherTypeが不明になるため、不明なプロトコル廃棄が発生します。

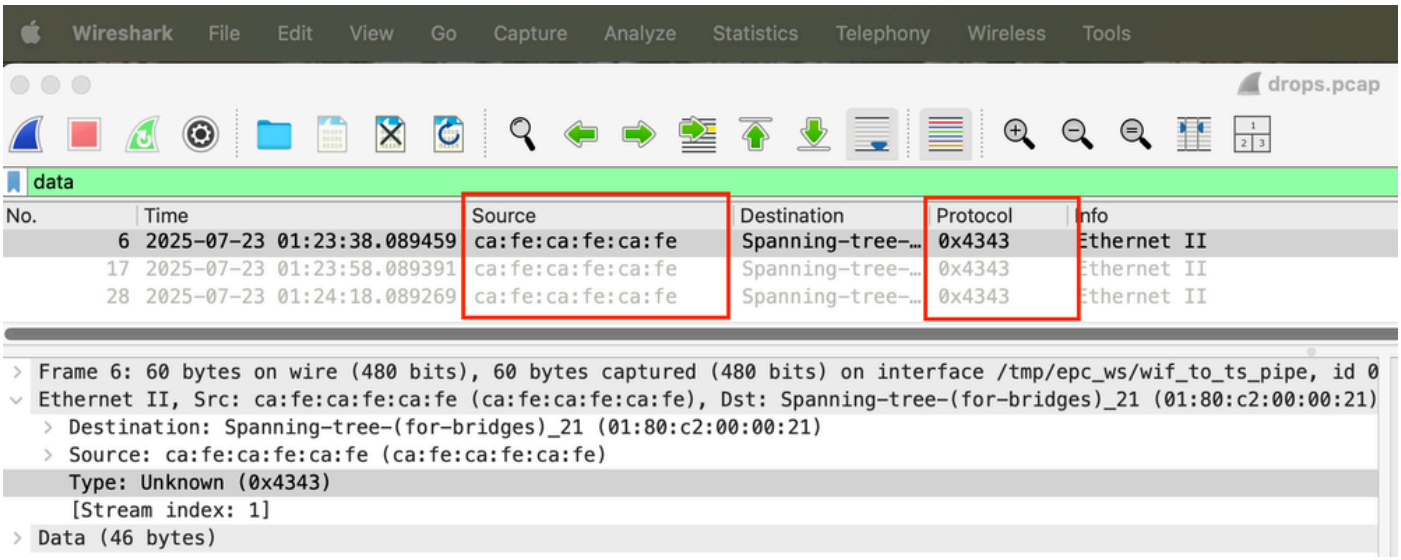


ステップ 10：Dataを右クリックし、Apply as Filterに移動して、Selected をクリックし、不明なプロトコルフレームをフィルタリングします。



ステップ 11Wiresharkのメインウィンドウに戻り、不明なプロトコルの送信元MACアドレスと

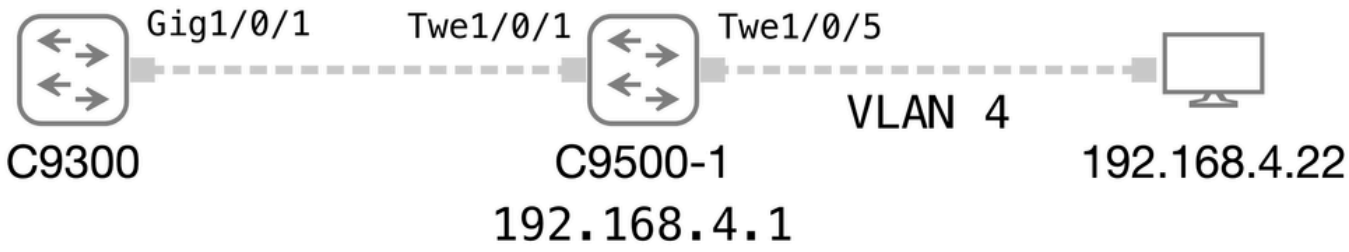
EtherTypeを確認します。



この場合、EtherType 0x4343がサポートされていないため、送信元MACアドレスCAFE.CAFE.CAFEが不明なプロトコルドロップを引き起こしています。

一般的な問題

このセクションの例は、次のネットワークトポロジダイアグラムに基づいています。



Dynamic Trunking Protocol（DTP; ダイナミック トランキング プロトコル）

DTPメッセージは、DTPが無効になっているポートで受信されると、未知のプロトコルのドロップを引き起こす可能性があります。DTPをイネーブルにするには、インターフェイスコンフィギュレーションモードでコマンドno switchport nonegotiateを使用します。

<#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
```

Link Layer Discovery Protocol（LLDP）

LLDPメッセージは、LLDPが無効になっているポートで受信された場合に、未知のプロトコルのドロップを引き起こす可能性もあります。LLDPを有効にするには、グローバルコンフィギュレーションモードでコマンドlldp runを使用します。

```
<#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
```

シスコ検出プロトコル（CDP）

同様に、CDPがディセーブルになっているポートでCDPメッセージが受信されると、不明なプロトコルの廃棄が増加する可能性があります。グローバルコンフィギュレーションモードでコマンドcdp runを使用すると、CDPを有効にできます。

```
<#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ヘッダーですべてゼロ のVLAN識別子

Catalyst 9000シリーズスイッチでも、アクセスポートでの受信時に、VLAN IDが0の802.1Qフレームがドロップされます。ただし、これらのパケットはunknown protocol dropsカウンタを増やしません。この例では、Catalyst 9500スイッチがホスト192.168.4.22のARPエントリを取得できない理由を調べます。

<#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
```

ステップ 1：エンドデバイスに接続しているインターフェイスでパケットキャプチャを開始します。

```
<#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
```

ステップ 2：エンドデバイスにpingを実行して、ARPトラフィックを生成します。

```
<#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)
```

ステップ 3：パケットキャプチャを停止します。

```
<#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
```

ステップ 4：エンドデバイスがARP応答を送信していることに注目してください。この例では、フレーム17です。

```
<#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
```

ステップ 5：VLAN ID 0を使用して、ARP応答が802.1Qヘッダーにカプセル化されていることに注目してください。

```
<#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
```

手順 6：パケットキャプチャの内容をエクスポートします。

```
<#root>

C9500-1#

monitor capture TAC export location flash:ARP.pcap

Export Started Successfully
```

手順 7：パケットトレーサツールを使用して、スイッチがパケット17に対して行う処理を決定します。

```
<#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
```

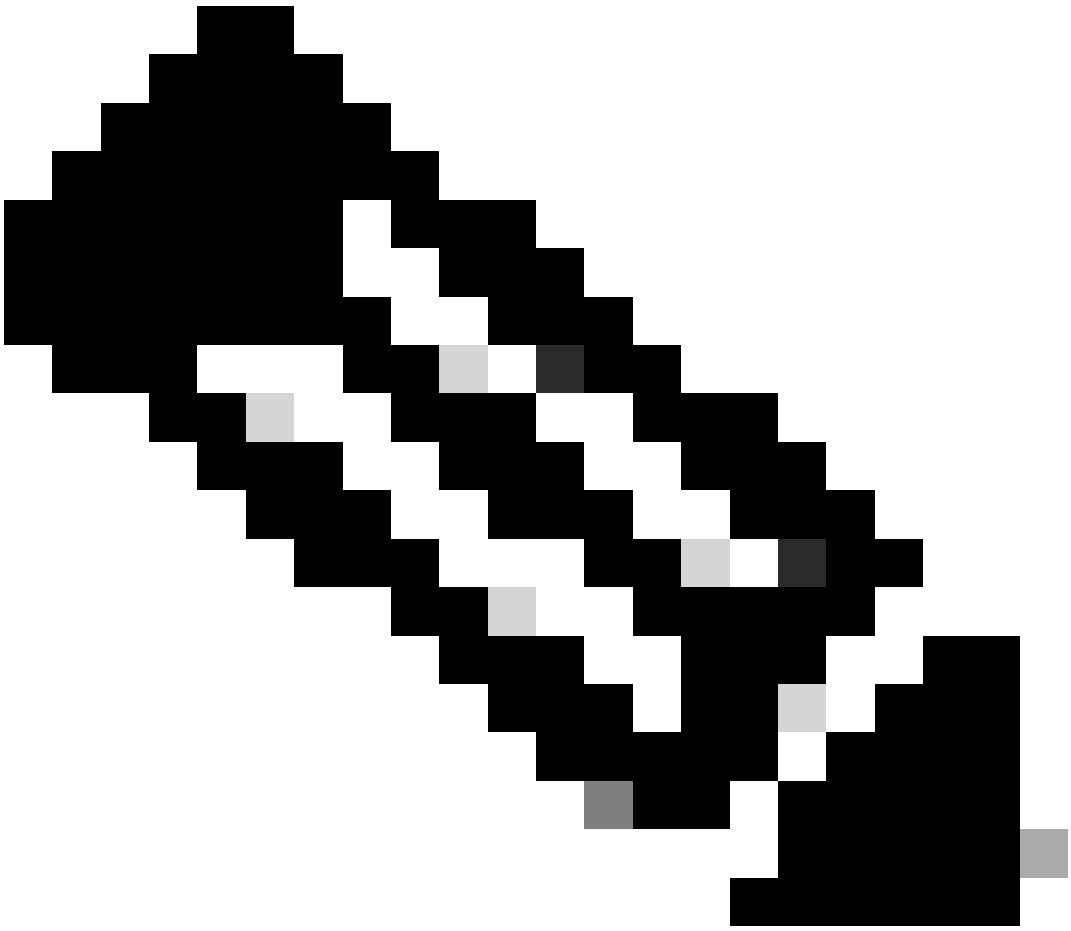
ステップ 8：Packet Tracerの結果を表示します。

```
<#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.
```



注:VLAN ID 0が含まれているため、パケットはドロップされます。

このタイプのドロップを防ぐには2つのオプションがあります。

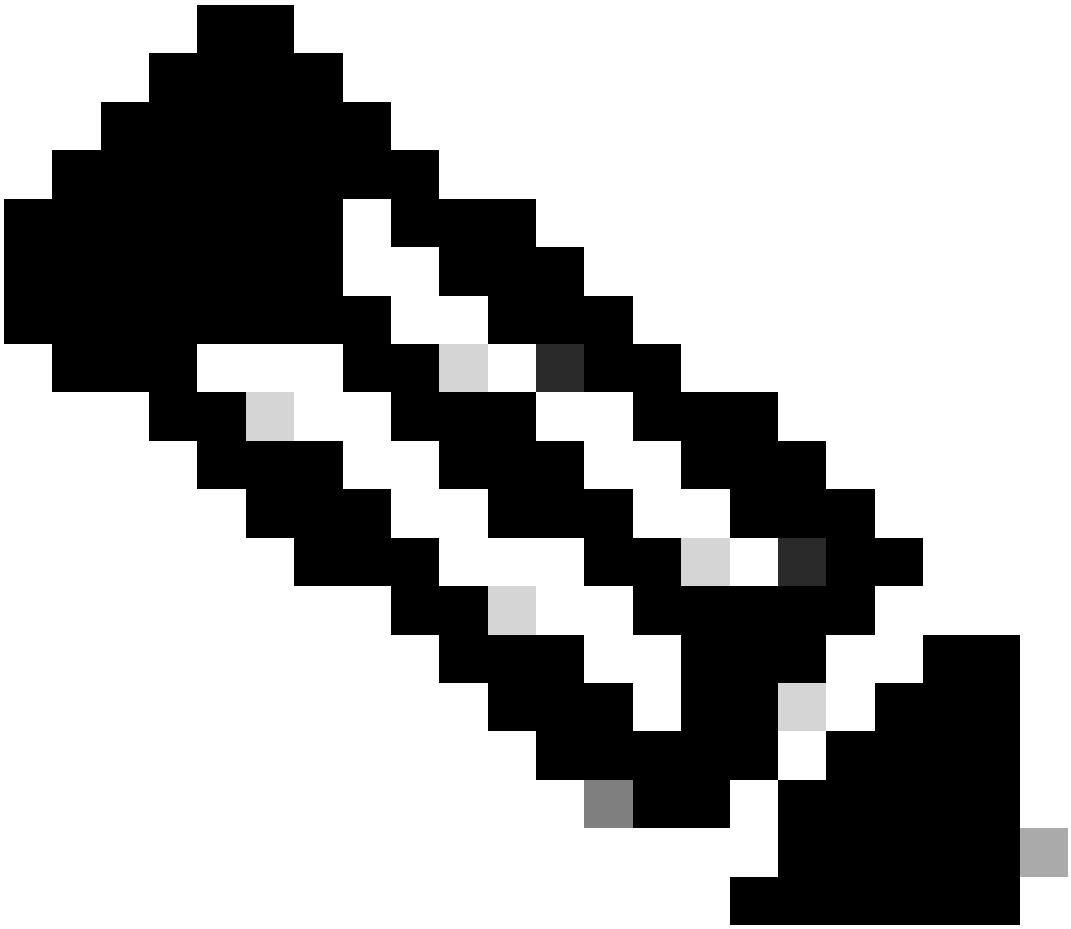
オプション1:switchport voice vlan dot1pコマンドを使用します。このようにして、vlan 0で受信されたフレームはアクセスvlanに割り当てられます。

```
interface TwentyFiveGigE1/0/5
 switchport access vlan 4
 switchport mode access
```

```
 switchport voice vlan dot1p
 load-interval 30
```

オプション2：インターフェイスをトランクポートとして設定します。このようにして、vlan 0で受信されたフレームは、ネイティブvlanに割り当てられます。

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



注：この問題はProfinetデバイスでよく発生します。

関連する不具合

- 詳細は、Cisco Bug ID CSCwe88812（登録ユーザ専用）を参照してください。

関連情報

- VLAN 0プライオリティタギングのサポート

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。