Problemen met onbekende protocoldruppels in Catalyst 9000-Switches oplossen

Inhoud

Inleiding

Dit document beschrijft veelvoorkomende oorzaken voor onbekende protocoldruppels in switches uit de Catalyst 9000-reeks.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Dynamic Trunking Protocol (DTP)
- Link Layer Discovery Protocol (LLDP)
- Cisco Discovery Protocol (CDP)
- Inkapseling 802.1q

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Catalyst 9000 Series switches

- Cisco IOS® XE

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

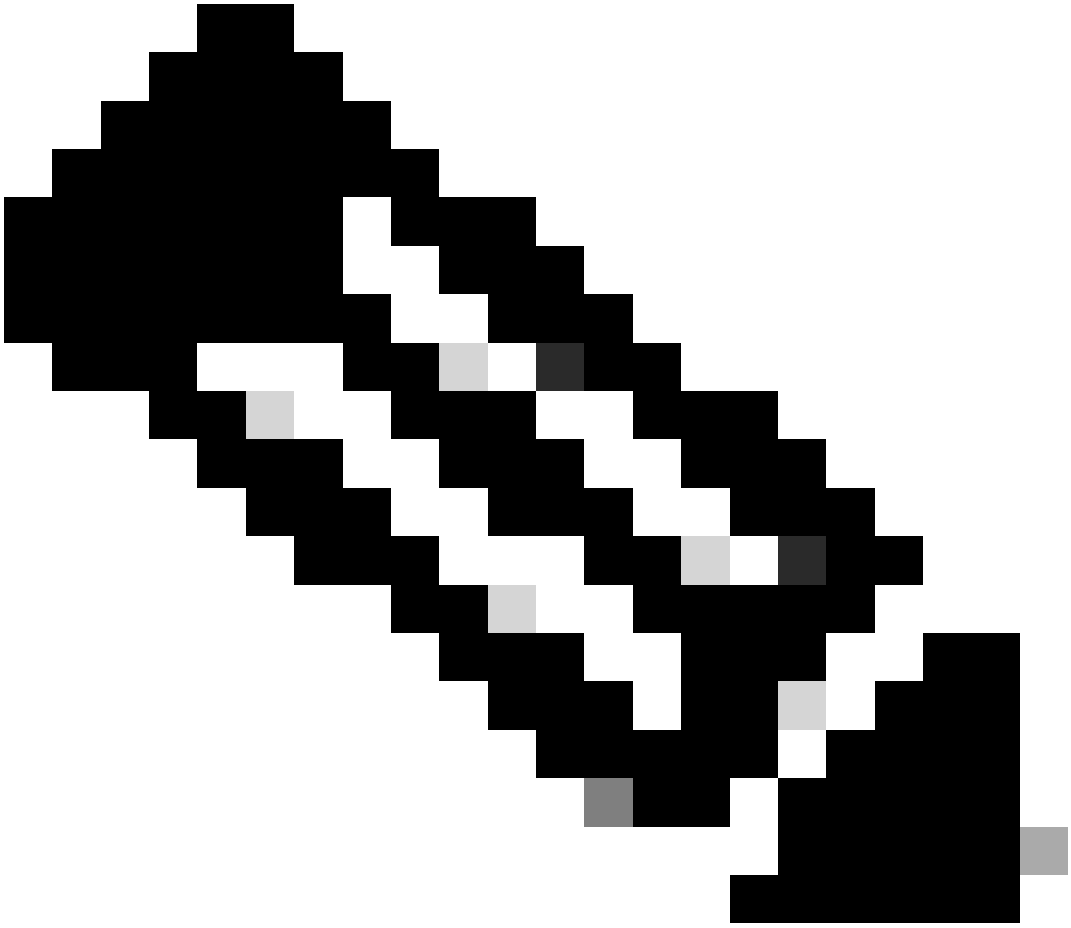
Onbekende protocoldruppels treden op wanneer het ethertype van een frame niet wordt herkend, wat betekent dat het ingekapselde protocol niet wordt ondersteund of niet wordt geconfigureerd via de switch-interface. Ook moet het MAC-adres van de bestemming van het frame een multicast-controlevliegtuigadres zijn, dat in deze opdracht wordt vermeld.

<#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
```



Opmerking: Onbekende protocoldruppels nemen niet toe wanneer het MAC-adres van de bestemming wordt uitgezonden.

Problemen oplossen

Stap 1. Zorg ervoor dat onbekende protocoldruppels toenemen.

<#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
```

Stap 2. Configureer een pakketopname in de betreffende interface en stem MAC-adressen van bestemming af, te beginnen met 01.

```
<#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
```

Stap 3. Start de packet capture en controleer de onbekende-protocol-drops teller.

```
<#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
```

Stap 4. Stop de pakketopname na een paar onbekende protocoldruppels.

```
<#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
```

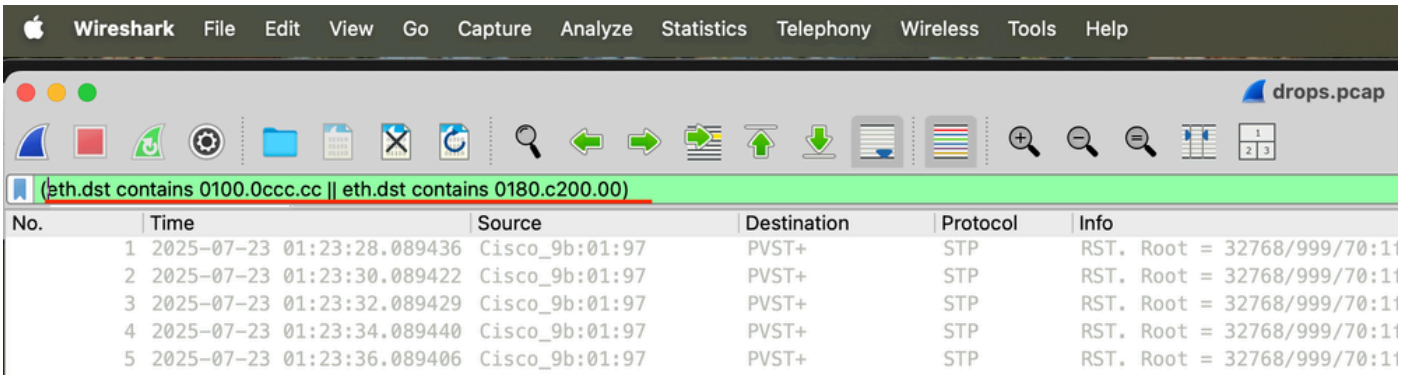
Stap 5. Inhoud pakketopname exporteren.

```
<#root>

Switch#

monitor capture port5 export location flash:drops.pcap

Export Started Successfully

Switch#
Export completed for capture point port5
```

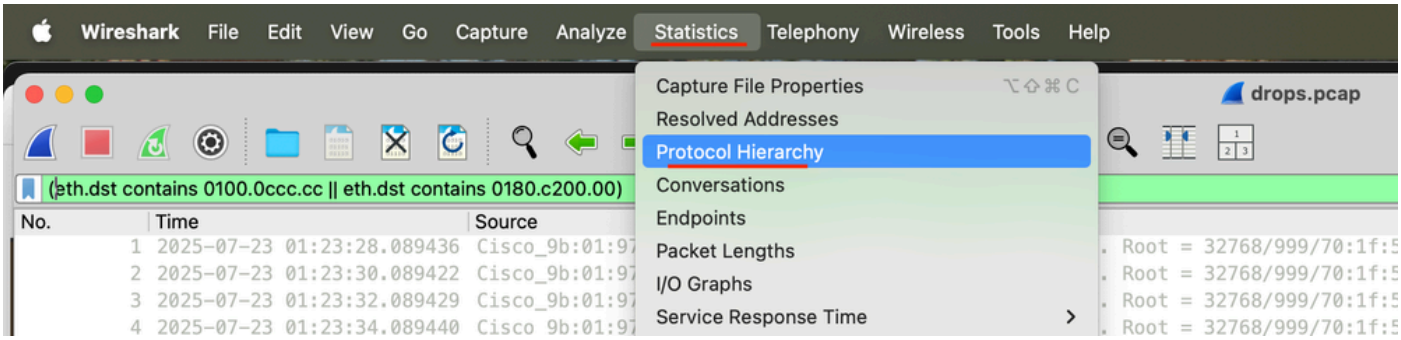
Stap 6. Breng de pakketopname over naar uw computer.

```
<#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)
```

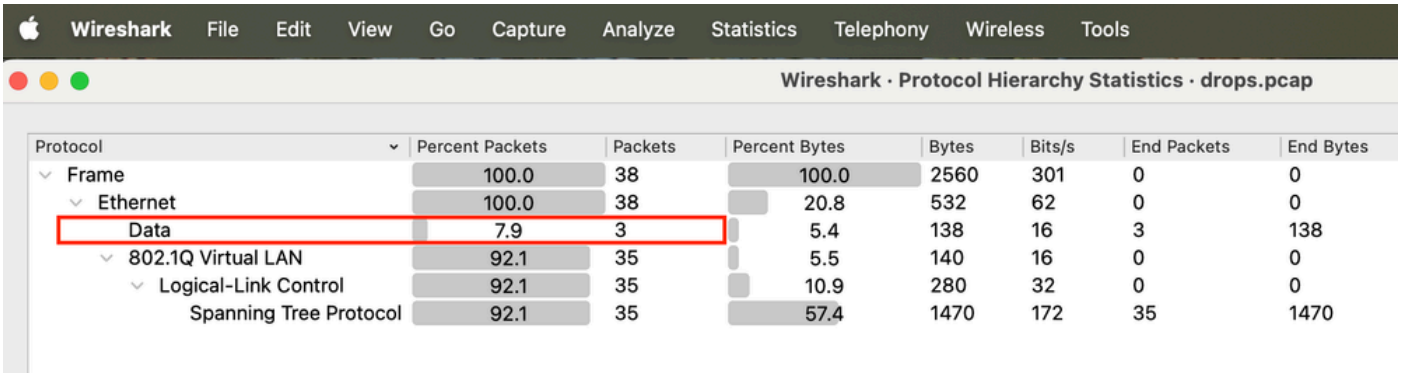
Stap 7. Open de pakketopname in Wireshark en gebruik dit filter (eth.dst bevat 0100.0ccc.cc || eth.dst bevat 0180.c200.00) om u te concentreren op CPU-multicastadressen.



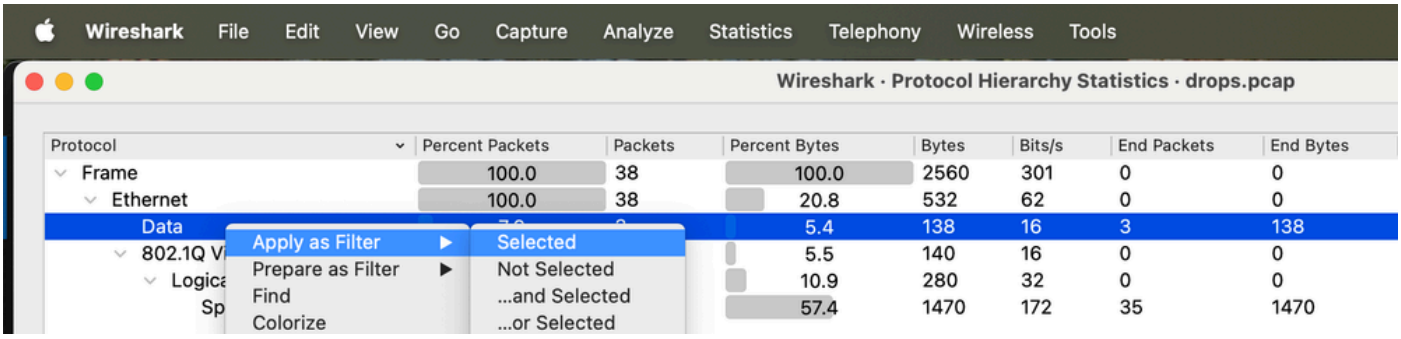
Stap 8. Ga naar Statistieken en klik vervolgens op Protocolhiërarchie.



Stap 9. Vouw de protocolstructuur uit en controleer of de protocolinterface voor deze switches is geconfigureerd. Alles wat als Data wordt bestempeld veroorzaakt een onbekende protocolval omdat het ethertype onbekend is.

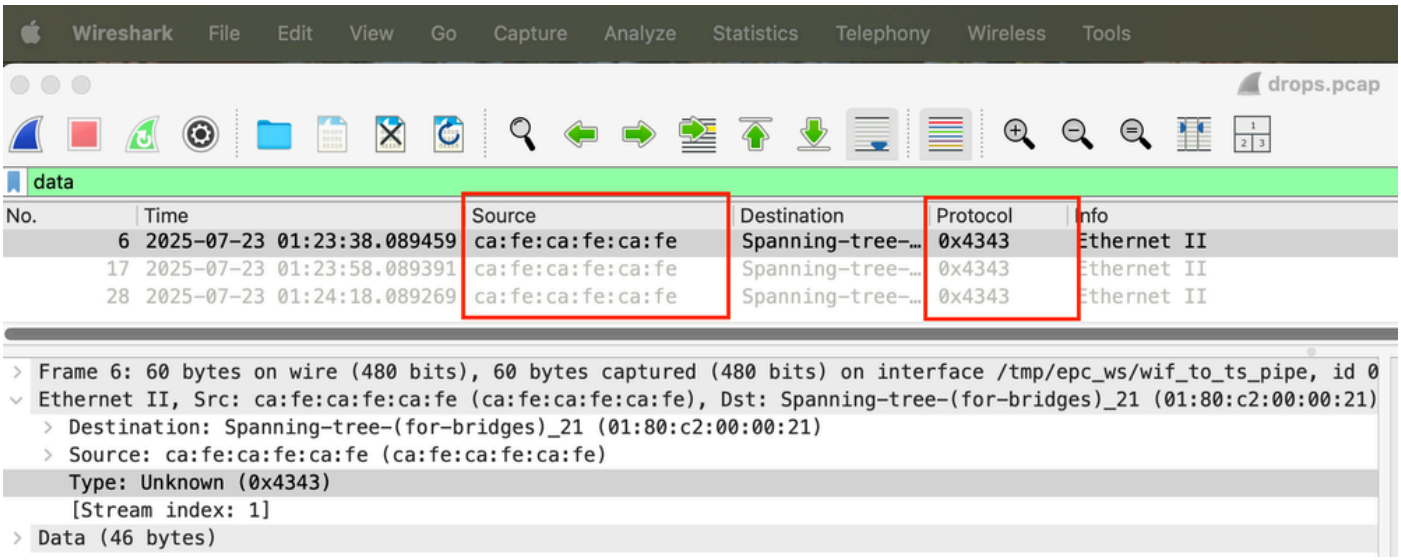


Stap 10. Klik met de rechtermuisknop op Gegevens, blader naar Toepassen als filter en klik op Geselecteerd om onbekende protocolframes te filteren.



Stap 11. Ga terug naar het hoofdvenster van Wireshark om het MAC-adres van de bron en het

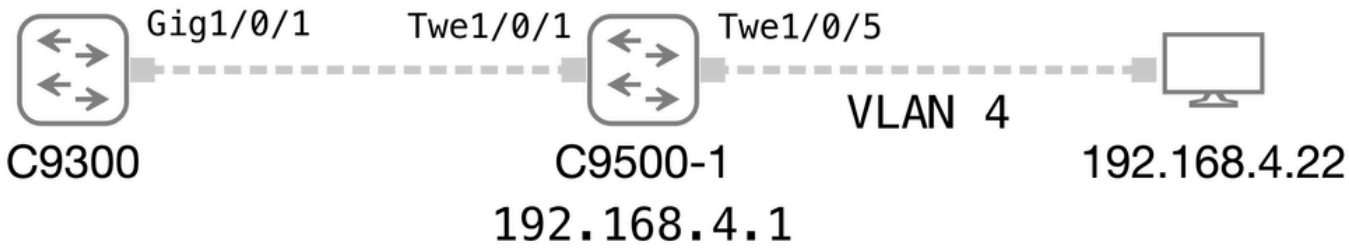
ethertype voor onbekende protocollen te bepalen.



In dit geval veroorzaakt het bron-MAC-adres CAFE.CAFE.CAFE onbekende protocoldalingen omdat ethertype 0x4343 niet wordt ondersteund.

Gemeenschappelijke problemen

De voorbeelden in deze sectie zijn gebaseerd op dit netwerktopologiediagram.



Dynamic Trunking Protocol (DTP)

DTP-berichten kunnen mogelijk leiden tot onbekende protocoldruppels als ze worden ontvangen op een poort waar DTP is uitgeschakeld. U kunt DTP inschakelen met de opdracht geen switchport niet onderhandelen in interface configuratie modus.

```
<#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-berichten kunnen ook leiden tot onbekende protocol vallen als ze worden ontvangen op de poort waar LLDP is uitgeschakeld. U kunt LLDP inschakelen met de opdracht lldp uitvoeren in globale configuratiemodus.

```
<#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
```

Cisco Discovery Protocol (CDP)

Ook kunnen onbekende protocoldruppels toenemen als CDP-berichten worden ontvangen op een poort waarop CDP is uitgeschakeld. U kunt CDP inschakelen door de opdracht cdp in globale configuratiemodus uit te voeren.

```
<#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
```

VLAN-id met alle nullen in 802.1Q-header

Catalyst-switches uit de 9000-reeks laten ook 802.1Q-frames met VLAN-ID 0 vallen wanneer deze op toegangspoorten worden ontvangen. Deze pakketten verhogen echter niet het aantal onbekende protocoldruppels. Laten we in dit voorbeeld onderzoeken waarom de Catalyst 9500-switch geen ARP-vermelding kan krijgen voor host 192.168.4.22.

<#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
```

Stap 1. Start een pakketopname in de interface die verbinding maakt met het eindapparaat.

<#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
```

Stap 2. Probeer het eindapparaat te pingen om wat ARP-verkeer te genereren.

<#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)
```

Stap 3. Stop de pakketvangst.

<#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
```

Stap 4. Merk op dat het eindapparaat een ARP-antwoord verzendt, in dit geval frame 17.

```
<#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 192.168.4.1
   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
```

Stap 5. Het ARP-antwoord is ingekapseld in een 802.1Q-header met VLAN-ID 0.

```
<#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
```

Stap 6. Inhoud pakketopname exporteren.

<#root>

```
C9500-1#

monitor capture TAC export location flash:ARP.pcap

Export Started Successfully
```

Stap 7. Bepaal wat de switch doet met pakket 17 met behulp van de packet tracer tool.

<#root>

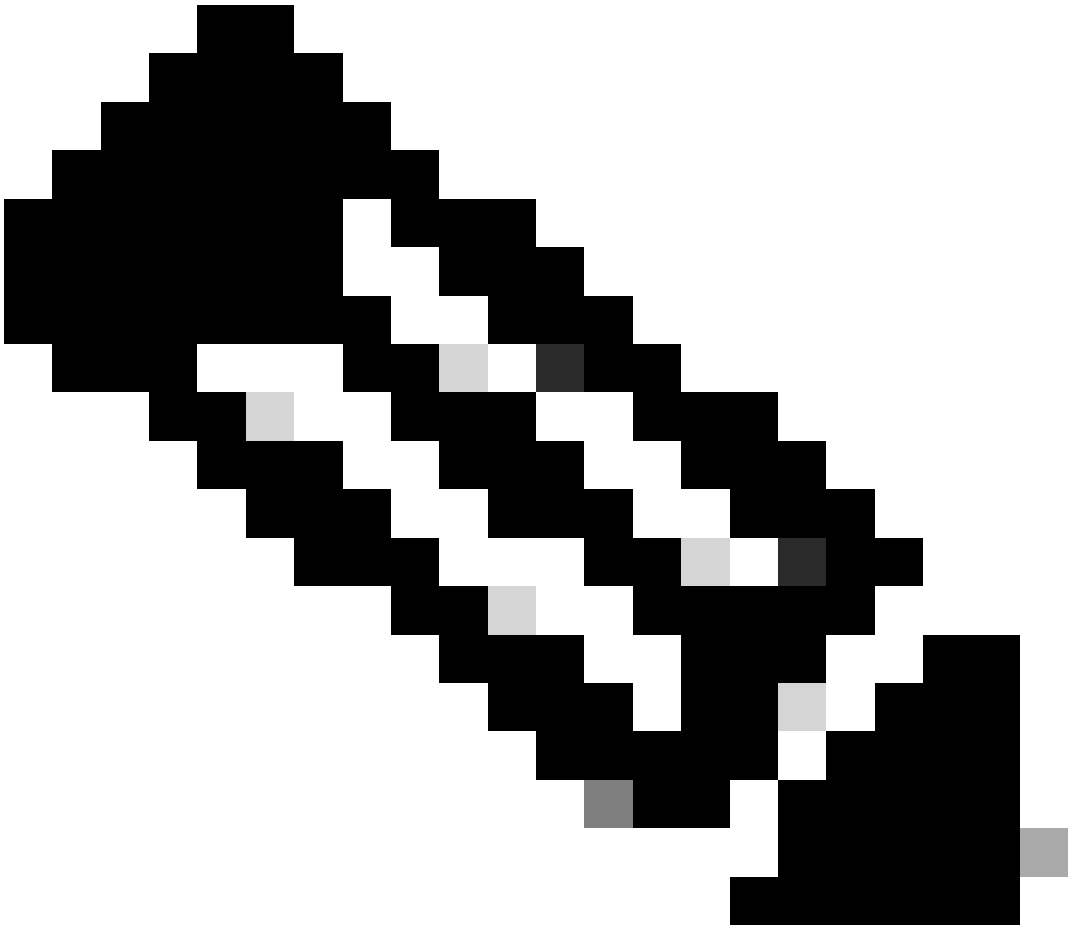
```
C9500-1#

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
```

Stap 8. Resultaten pakkettracer weergeven.

<#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.
```



Opmerking: pakket is verwijderd omdat het VLAN-ID 0 bevat.

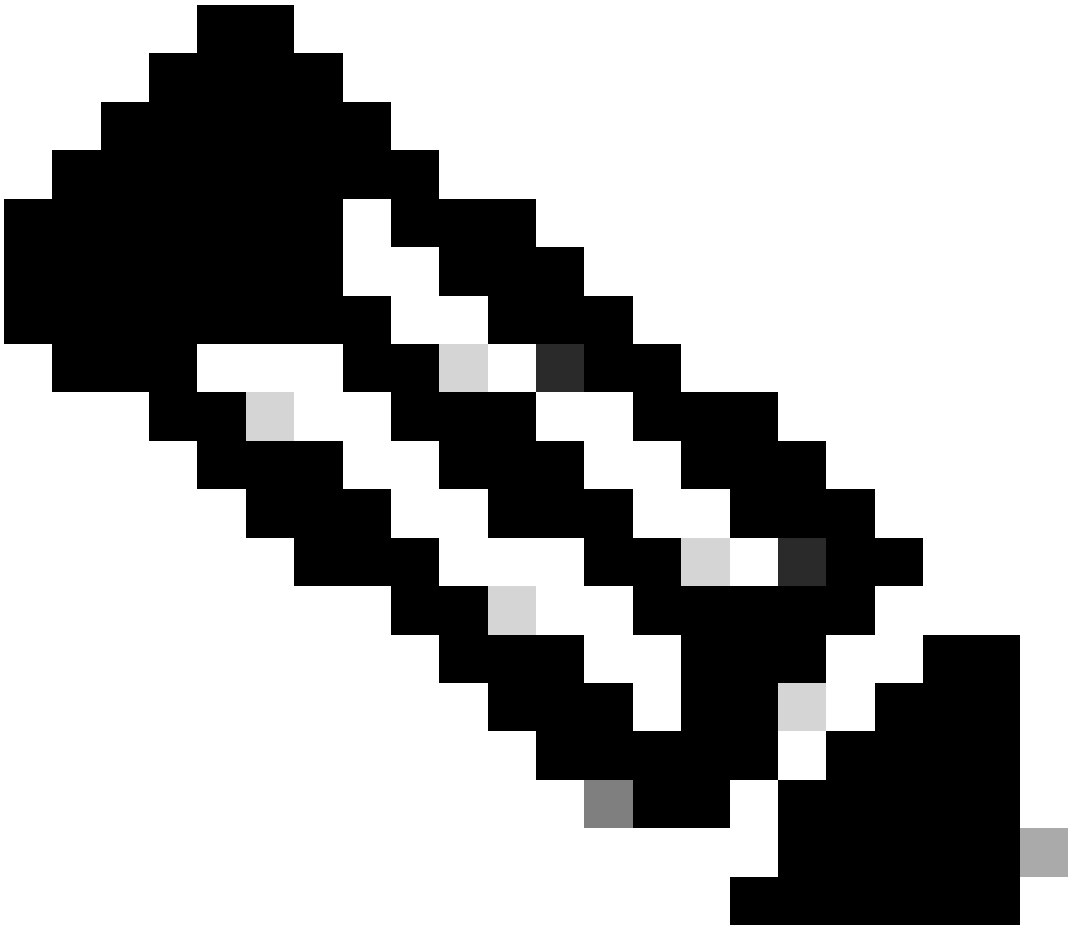
Er zijn twee mogelijkheden om dit soort valpartijen te voorkomen.

Optie 1: gebruik de opdracht switchport voice vlan dot1p. Op deze manier worden frames die met vlan 0 zijn ontvangen, toegewezen aan het toegangs-vlan.

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

Optie 2: configureer de interface als een trunkpoort. Op deze manier worden frames die met vlan 0 zijn ontvangen, toegewezen aan het oorspronkelijke vlan.

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



Opmerking: dit is vaak gezien met Profinet-apparaten.

Gerelateerde gebreken

- Zie Cisco bug ID CSCwe88812 voor meer informatie.

Gerelateerde informatie

- Ondersteuning voor prioriteitscodering van VLAN 0

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.