Resolución de problemas de caídas de protocolo desconocido en switches Catalyst 9000

Contenido

Introducción

Este documento describe las causas comunes de las caídas de protocolos desconocidos en los switches Catalyst de la serie 9000.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Protocolo de concentración de enlaces dinámico (DTP)
- Protocolo de descubrimiento de la capa de enlace (LLDP)
- Protocolo de detección de Cisco (CDP)
- Encapsulación 802.1Q

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Catalyst 9000 Series Switch
- Cisco IOS® XE

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

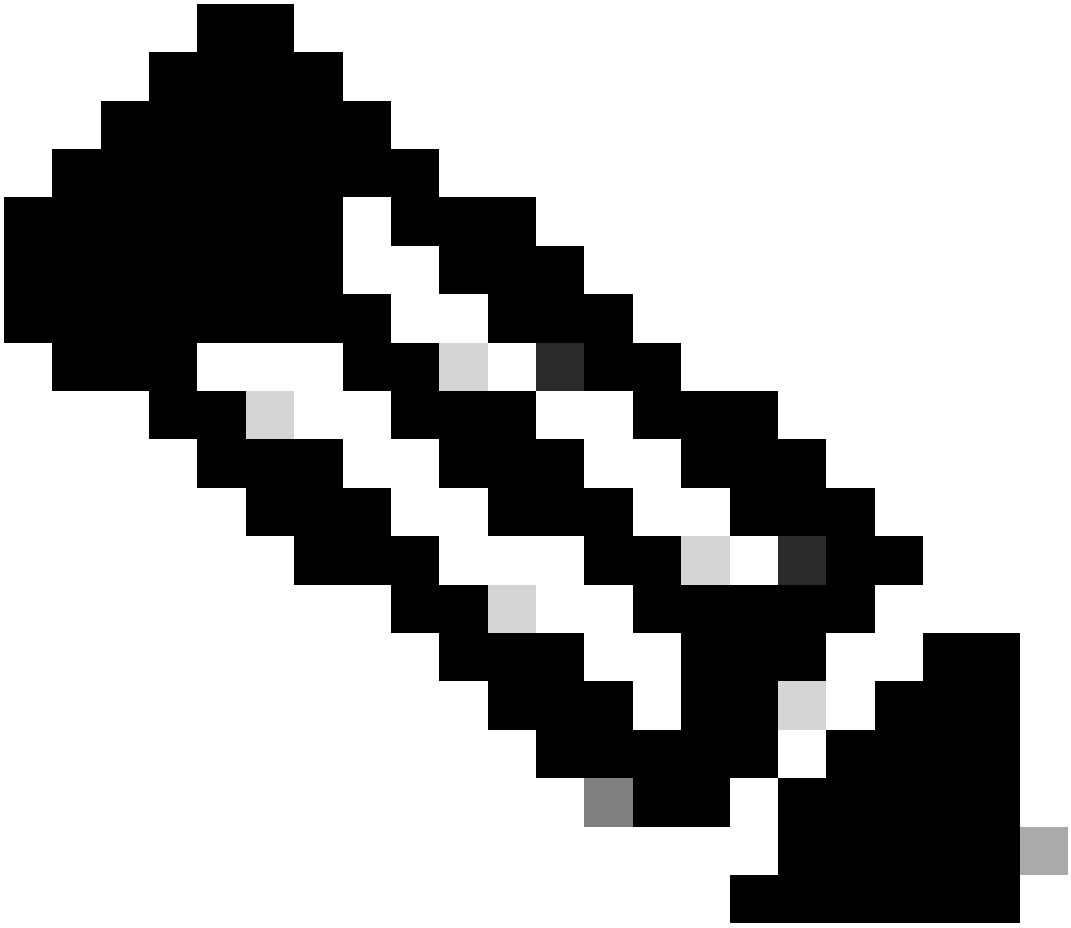
Las caídas de protocolo desconocidas ocurren cuando no se reconoce el ethertype de una trama, lo que significa que el protocolo encapsulado no es compatible o no está configurado en la interfaz del switch. Además, la dirección MAC de destino de la trama debe ser una dirección del plano de control multicast, que se enumeran en este comando.

<#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
```



Nota: Las caídas de protocolo desconocidas no aumentan cuando se difunde la dirección MAC de destino.

Troubleshoot

Paso 1. Asegúrese de que las caídas de protocolos desconocidos estén aumentando.

<#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
```

Paso 2. Configure una captura de paquetes en la interfaz afectada y haga coincidir las direcciones MAC de destino comenzando con 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
```

Paso 3. Inicie la captura de paquetes y verifique el contador unknown-protocol-drops .

<#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
```

Paso 4. Detenga la captura de paquetes después de unas pocas caídas de protocolo desconocidas.

<#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
```

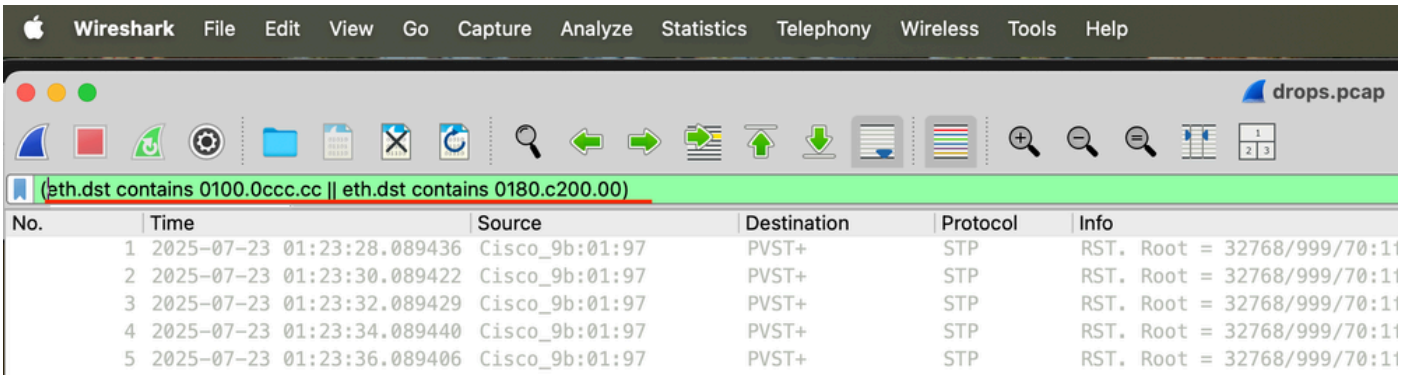
Paso 5. Exportar contenido de captura de paquetes.

```
<#root>

Switch#

monitor capture port5 export location flash:drops.pcap

Export Started Successfully

Switch#
Export completed for capture point port5
```

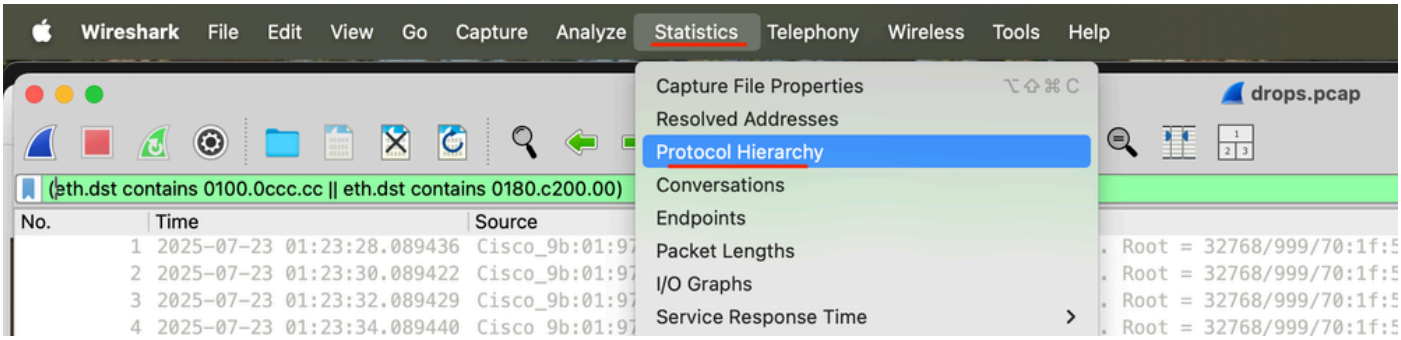
Paso 6. Transfiera la captura de paquetes a su computadora.

```
<#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)
```

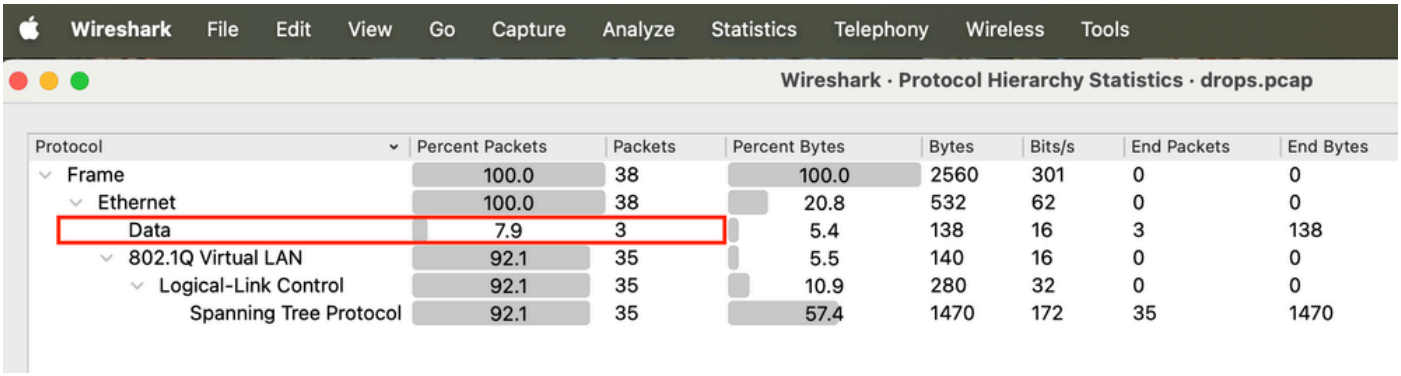
Paso 7. Abra la captura de paquetes en Wireshark y utilice este filtro (eth.dst contiene 0100.0ccc.cc || eth.dst contiene 0180.c200.00) para centrarse en las direcciones de multidifusión de la CPU.



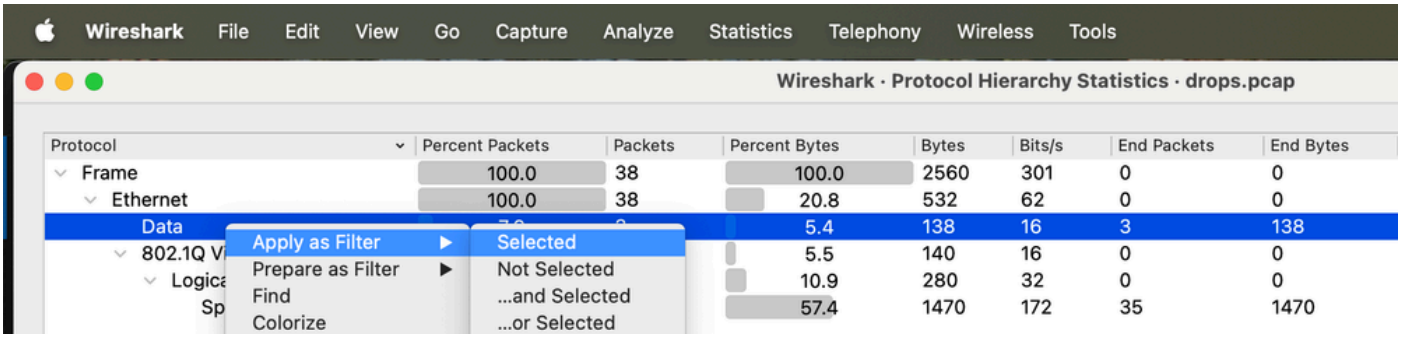
Paso 8. Vaya a Estadísticas y haga clic en Jerarquía de protocolos.



Paso 9. Expanda el árbol de protocolos y verifique que la interfaz del switch esté configurada para estos protocolos. Cualquier cosa etiquetada como Data causa caídas de protocolo desconocidas porque el ethertype es desconocido.

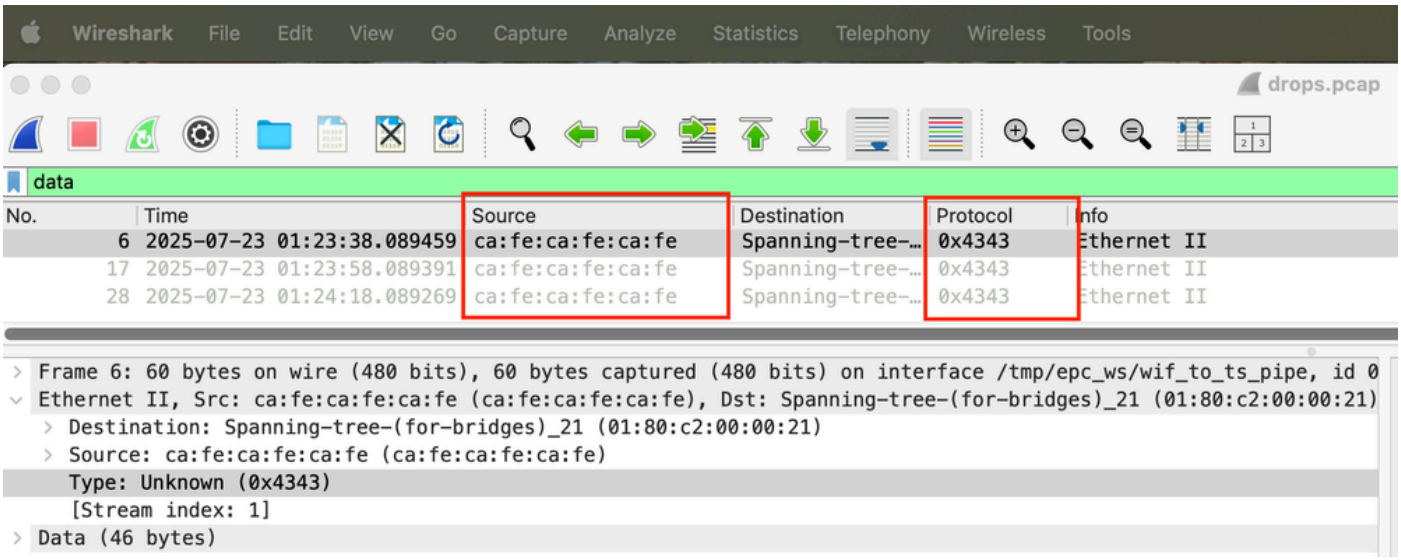


Paso 10. Haga clic con el botón derecho en Data, navegue hasta Apply as Filter y haga clic en Selected para filtrar tramas de protocolo desconocidas.



Paso 11. Vuelva a la ventana principal de Wireshark para determinar la dirección MAC de origen y

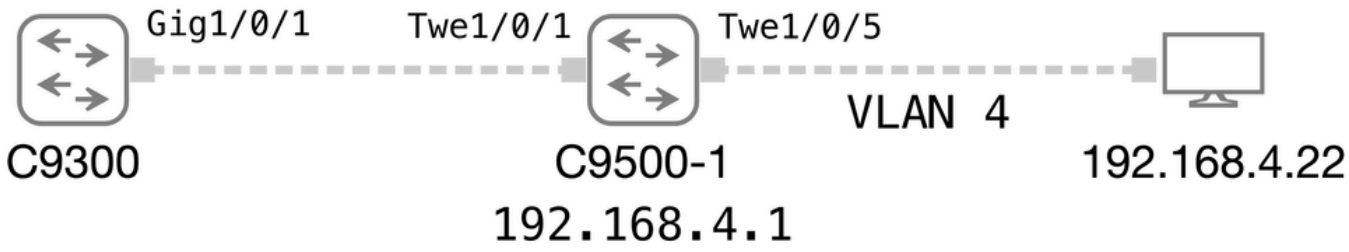
el ethertype para los protocolos desconocidos.



En este caso, la dirección MAC de origen CAFE.CAFE.CAFE está provocando caídas de protocolos desconocidos porque no se admite el ethertype 0x4343.

Problemas Comunes

Los ejemplos de esta sección se basan en este diagrama de topología de red.



Protocolo de concentración de enlaces dinámico (DTP)

Los mensajes DTP podrían potencialmente causar caídas de protocolo desconocidas si se reciben en un puerto donde DTP está inhabilitado. Puede habilitar DTP usando el comando no switchport nonegotiate en el modo de configuración de la interfaz.

```
<#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
```

Protocolo de descubrimiento de la capa de enlace (LLDP)

Los mensajes LLDP también pueden causar caídas de protocolo desconocidas si se reciben en un puerto donde LLDP está inhabilitado. Puede habilitar LLDP usando el comando lldp run en el modo de configuración global.

```
<#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
```

Protocolo de detección de Cisco (CDP)

De manera similar, las caídas de protocolo desconocido pueden incrementarse si se reciben mensajes CDP en un puerto donde CDP está inhabilitado. Puede habilitar CDP mediante el comando cdp run en el modo de configuración global.

```
<#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
```

Identificador de VLAN con todos ceros en el encabezado 802.1Q

Los switches Catalyst de la serie 9000 también descartan tramas 802.1Q con ID de VLAN 0 cuando se reciben en los puertos de acceso. Sin embargo, estos paquetes no incrementan el contador de caídas de protocolo desconocido. En este ejemplo, investiguemos por qué el switch Catalyst 9500 no puede obtener una entrada ARP para el 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
```

Paso 1. Inicie una captura de paquetes en la interfaz que se conecta al dispositivo final.

<#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
```

Paso 2. Intente hacer ping al dispositivo final para generar algo de tráfico ARP.

<#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)
```

Paso 3. Detenga la captura de paquetes.

<#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
```

Paso 4. Observe que el dispositivo final está enviando una respuesta ARP, que en este caso es la trama 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.
   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
```

Paso 5. Observe que la respuesta ARP se encapsula en un encabezado 802.1Q usando el ID de VLAN 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
```

Paso 6. Exportar contenido de captura de paquetes.

<#root>

```
C9500-1#
```

monitor capture TAC export location flash:ARP.pcap

```
Export Started Successfully
```

Paso 7. Determine qué hace el switch con el paquete 17 mediante la herramienta packet tracer.

<#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
```

Paso 8. Mostrar resultados del rastreador de paquetes.

<#root>

```
C9500-1#
```

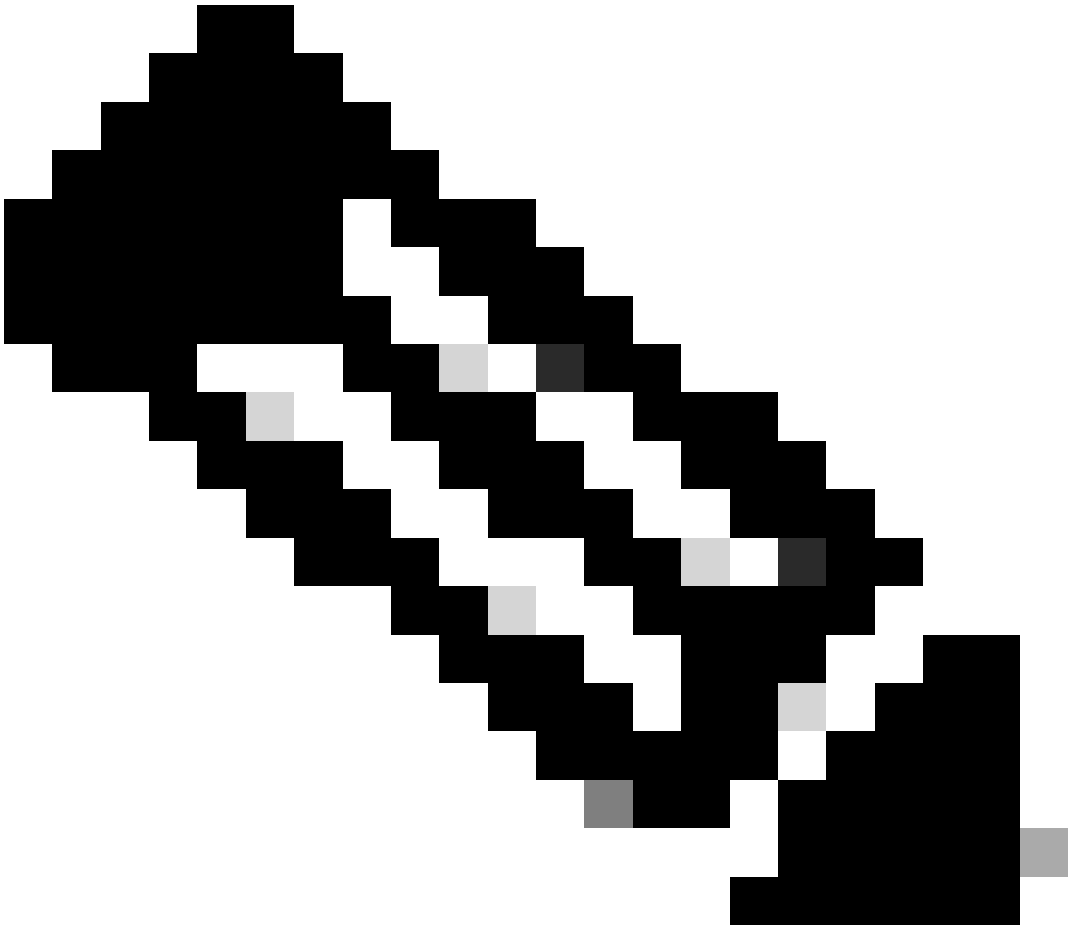
show platform hardware fed active forward last summary

```
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.
```



Nota: El paquete se descarta porque incluye el ID de VLAN 0.

Existen dos opciones para evitar este tipo de caídas.

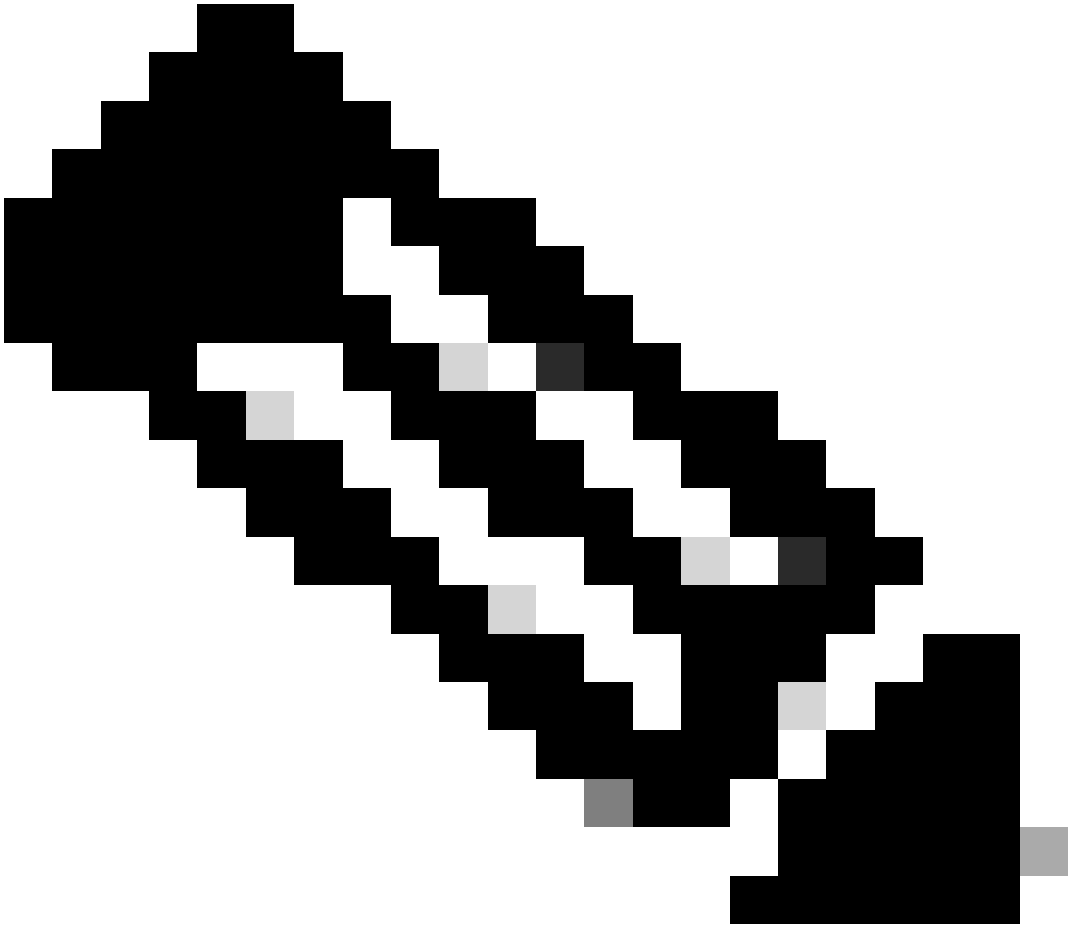
Opción 1: utilice el comando switchport voice vlan dot1p. De esta manera, las tramas recibidas con vlan 0 se asignan a la vlan de acceso.

```
interface TwentyFiveGigE1/0/5
 switchport access vlan 4
 switchport mode access
 switchport voice vlan dot1p
```

```
 load-interval 30
```

Opción 2: configure la interfaz como un puerto trunk. De esta manera, las tramas recibidas con vlan 0 se asignan a la vlan nativa.

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



Nota: Esto se ha visto comúnmente con los dispositivos Profinet.

Defectos relacionados

- Consulte Cisco bug ID CSCwe8812 para obtener más información.

Información relacionada

- Soporte de Etiquetado de Prioridad VLAN 0

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).