# Risoluzione dei problemi relativi alle perdite di protocollo sconosciute negli switch Catalyst 9000

## Sommario



## Introduzione

Questo documento descrive le cause più comuni delle perdite di protocollo sconosciute negli switch Catalyst serie 9000.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Switch Catalyst serie 9000
- Cisco IOS® XE

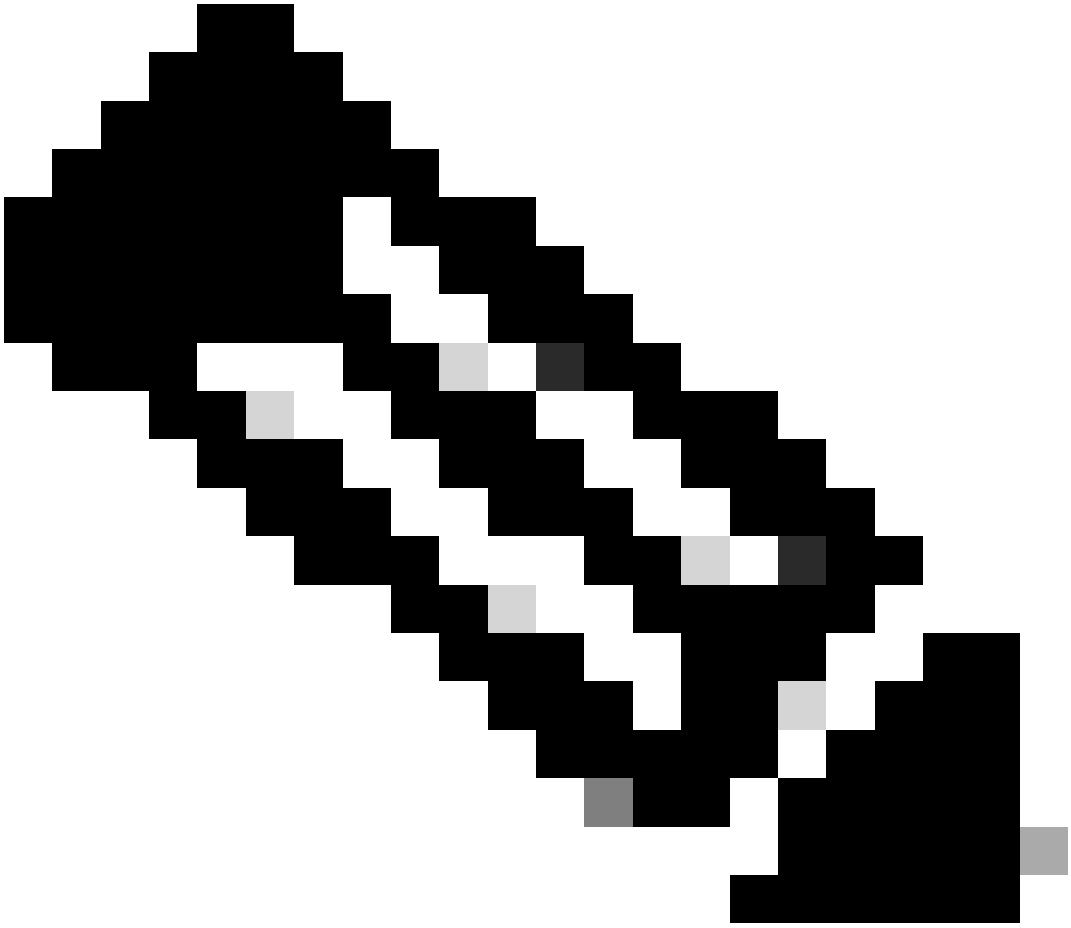
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

# Premesse

Le interruzioni del protocollo sconosciute si verificano quando l'ethertype di un frame non viene riconosciuto, il che significa che il protocollo incapsulato non è supportato o non è configurato sull'interfaccia dello switch. Inoltre, l'indirizzo MAC di destinazione del frame deve essere un indirizzo del control plane multicast, elencato in questo 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: le interruzioni di protocollo sconosciute non vengono incrementate quando viene trasmesso l'indirizzo MAC di destinazione.

## Risoluzione dei problemi

Passaggio 1. Verificare che le interruzioni di protocollo sconosciute siano in aumento.

<#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
```

Passaggio 2. Configurare l'acquisizione di un pacchetto nell'interfaccia interessata e abbinare gli indirizzi MAC di destinazione a partire da 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
```

Passaggio 3. Avviare l'acquisizione dei pacchetti e controllare il contatore delle perdite di protocollo sconosciute.

```
<#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
```

Passaggio 4. Arrestare l'acquisizione dei pacchetti dopo alcune interruzioni sconosciute del protocollo.

```
<#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
```

Passaggio 5. Esportare il contenuto dell'acquisizione del pacchetto.

<#root>

```
Switch#
```

**monitor capture port5 export location flash:drops.pcap**

```
Export Started Successfully

Switch#
Export completed for capture point port5
```

Passaggio 6. Trasferire l'acquisizione dei pacchetti al computer.

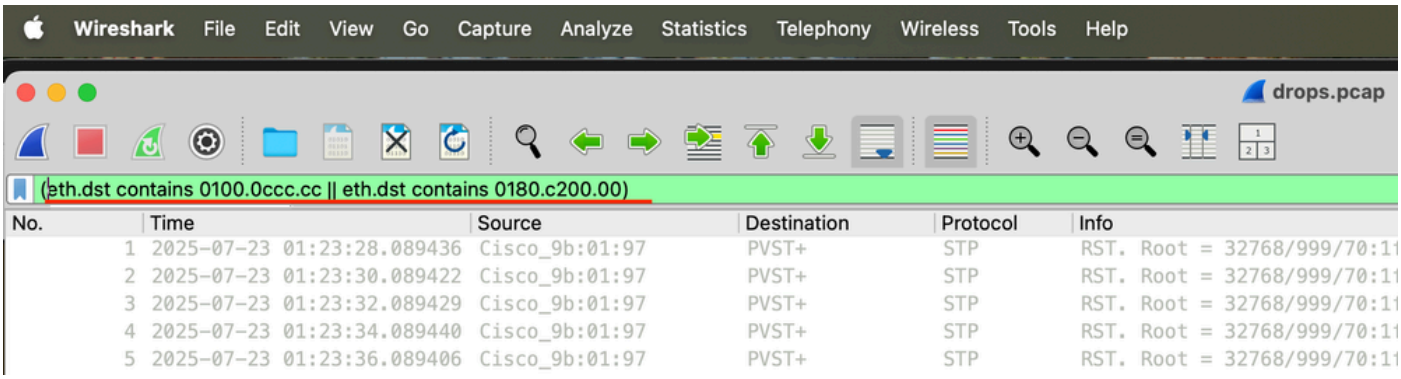
<#root>

```
Switch#
```

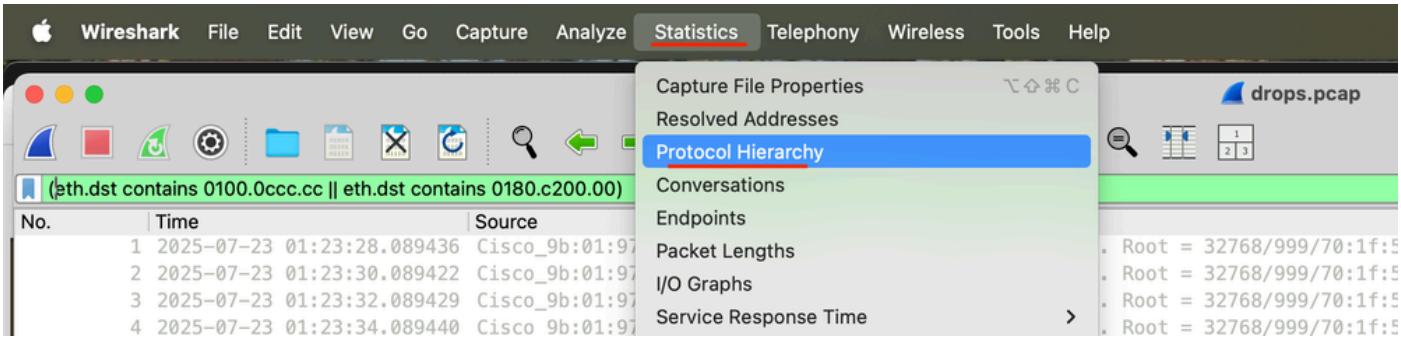
**copy flash: ftp: vrf Mgmt-vrf**

```
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)
```

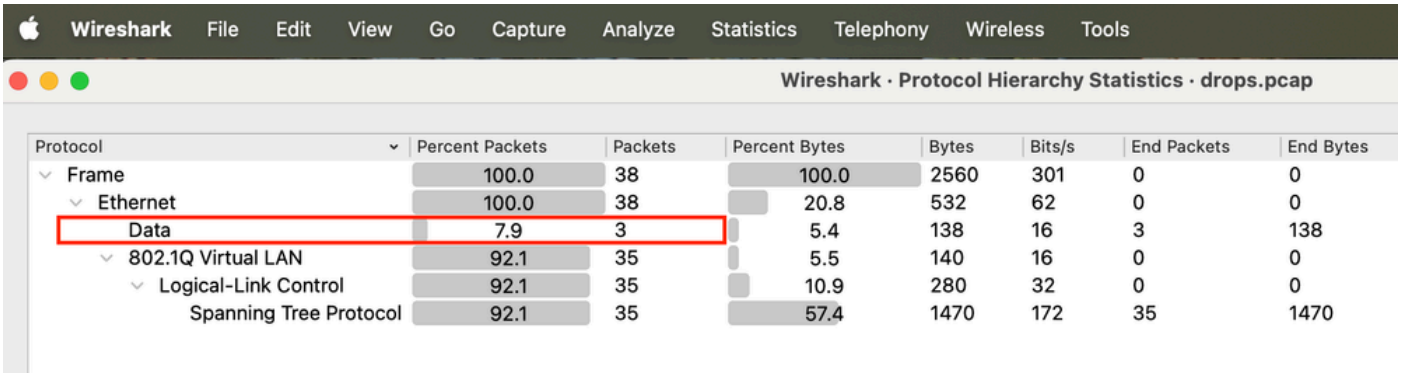
Passaggio 7. Aprire l'acquisizione del pacchetto in Wireshark e utilizzare questo filtro (eth.dst contiene 0100.0ccc.cc || eth.dst contiene 0180.c200.00) per concentrarsi sugli indirizzi multicast della CPU.



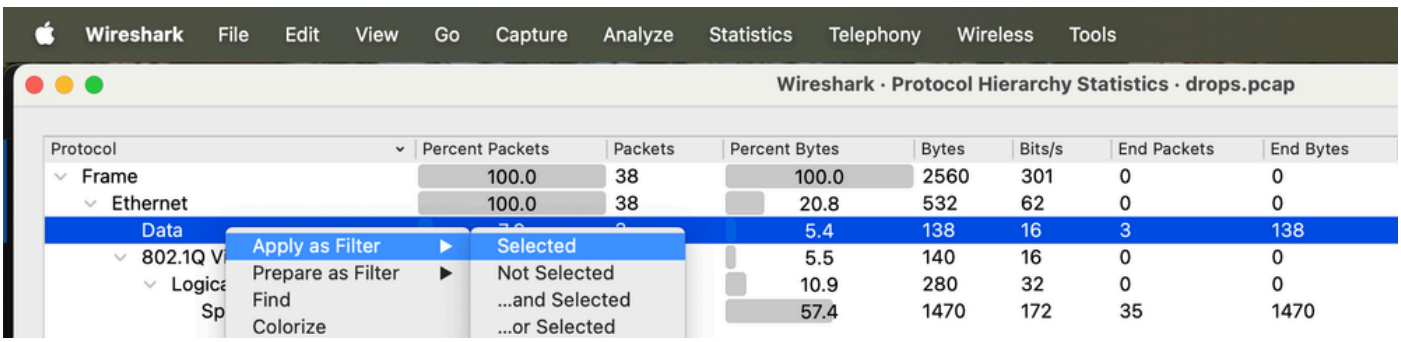

Passaggio 8. Andare a Statistiche e fare clic su Gerarchia protocollo.



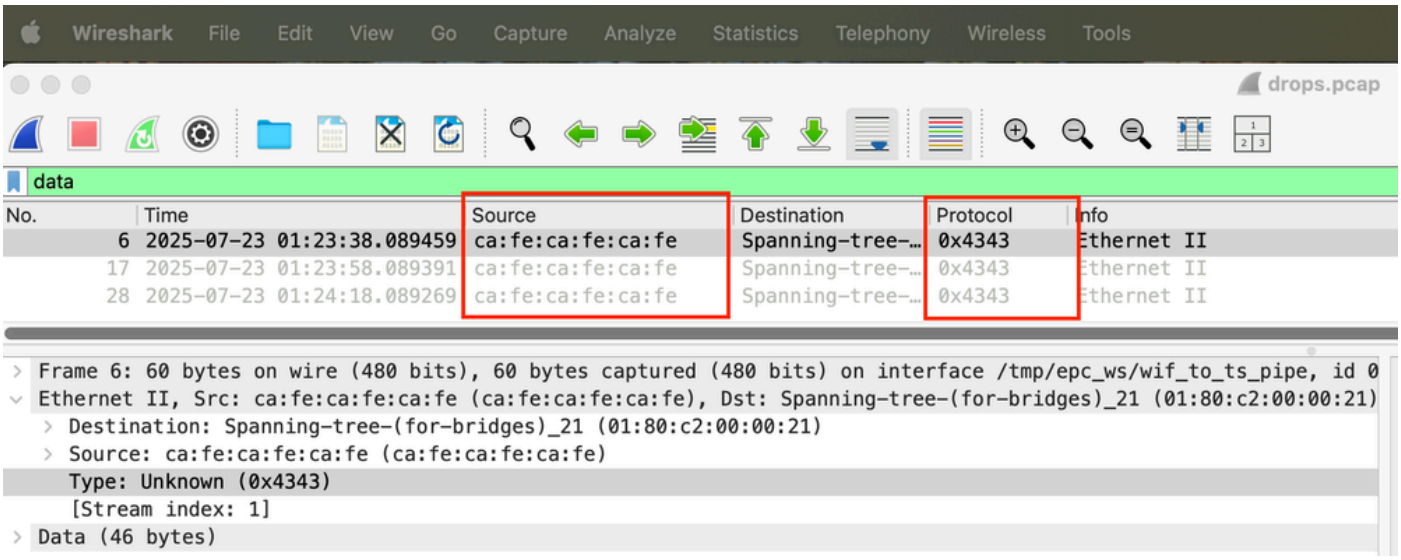

Passaggio 9. Espandere la struttura del protocollo e verificare che l'interfaccia dello switch sia configurata per questi protocolli. Qualsiasi elemento etichettato come Data causa la perdita di protocollo sconosciuta perché l'ethertype è sconosciuto.




Passaggio 10. Fare clic con il pulsante destro del mouse su Data, selezionare Apply as Filter (Applica come filtro), quindi fare clic su Selected (Selezionati) per filtrare i frame di protocollo sconosciuti.



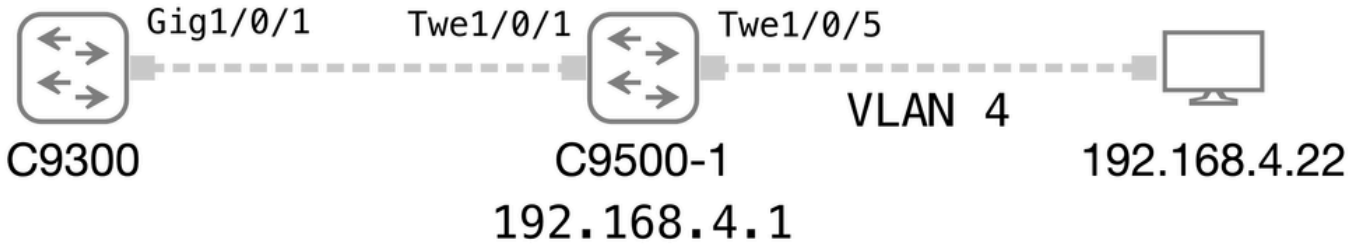
Passaggio 11. Tornare alla finestra principale di Wireshark per determinare l'indirizzo MAC di origine e l'ethertype per i protocolli sconosciuti.




In questo caso, l'indirizzo MAC di origine CAFE.CAFE.CAFE sta causando perdite di protocollo sconosciute perché ethertype 0x4343 non è supportato.

## Problemi comuni

Gli esempi in questa sezione si basano sul diagramma della topologia di rete.




### Protocollo DTP (Dynamic Trunking Protocol)

I messaggi DTP potrebbero causare potenziali perdite di protocollo sconosciute se ricevuti su una porta dove DTP è disabilitato. È possibile abilitare il DTP utilizzando il comando no switchport nonegotiate in modalità di configurazione interfaccia.

```
<#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)

I messaggi LLDP possono inoltre causare perdite di protocollo sconosciute se ricevuti su una porta in cui LLDP è disabilitato. È possibile abilitare LLDP utilizzando il comando lldp run in modalità di configurazione globale.

```
<#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
```

## Protocollo CDP (Cisco Discovery Protocol)

Analogamente, le eliminazioni di protocolli sconosciuti possono aumentare se i messaggi CDP vengono ricevuti su una porta dove CDP è disabilitato. È possibile abilitare CDP utilizzando il comando cdp run in modalità di configurazione globale.

<#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
```

## Identificatore VLAN all-zeros nell'intestazione 802.1Q

Anche gli switch Catalyst serie 9000 rilasciano i frame 802.1Q con ID VLAN 0 quando vengono ricevuti sulle porte di accesso. Tuttavia, questi pacchetti non incrementano il contatore delle perdite di protocollo sconosciute. Nell'esempio, esamineremo perché lo switch Catalyst 9500 non riesce a ottenere una voce ARP per l'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
```

Passaggio 1. Avviare l'acquisizione di un pacchetto nell'interfaccia di connessione al dispositivo terminale.

<#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
```

Passaggio 2. Provare a eseguire il ping del dispositivo terminale per generare del traffico 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)
```

Passaggio 3. Arrestare l'acquisizione del pacchetto.

<#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
```

Passaggio 4. Si noti che il dispositivo terminale sta inviando una risposta ARP, che in questo caso è il 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.
   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
```

Passaggio 5. Si noti che la risposta ARP è incapsulata in un'intestazione 802.1Q con ID 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: 00000000000000000000000000000000
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
```

Passaggio 6. Esportare il contenuto dell'acquisizione del pacchetto.

```
<#root>

C9500-1#

monitor capture TAC export location flash:ARP.pcap

Export Started Successfully
```

Passaggio 7. Determinare l'azione dello switch sul pacchetto 17 utilizzando lo strumento 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
```

Passaggio 8. Visualizzare i risultati del rilevamento pacchetti.

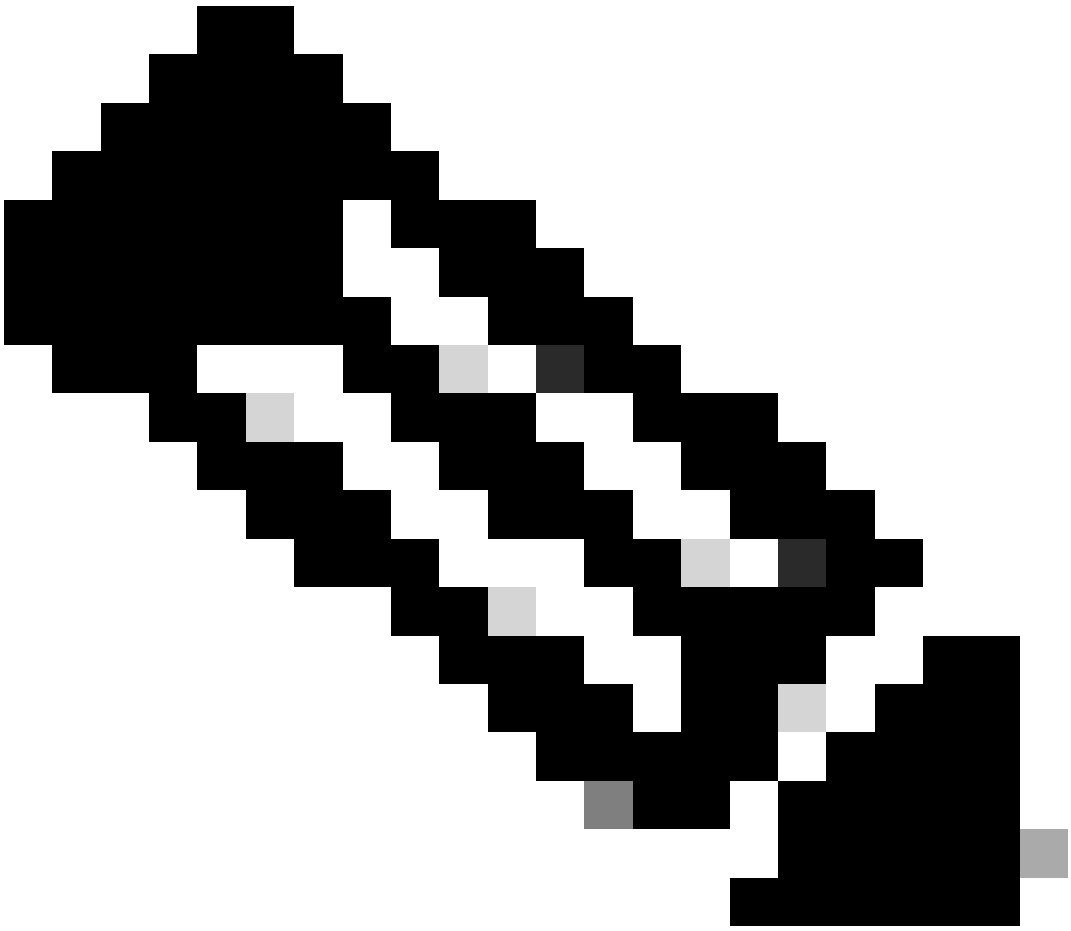
```
<#root>

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: Il pacchetto viene scartato perché include l'ID VLAN 0.

---

Ci sono due opzioni per prevenire questo tipo di cadute.

Opzione 1: usare il comando switchport voice vlan dot1p. In questo modo, i frame ricevuti con la vlan 0 vengono assegnati alla vlan di accesso.

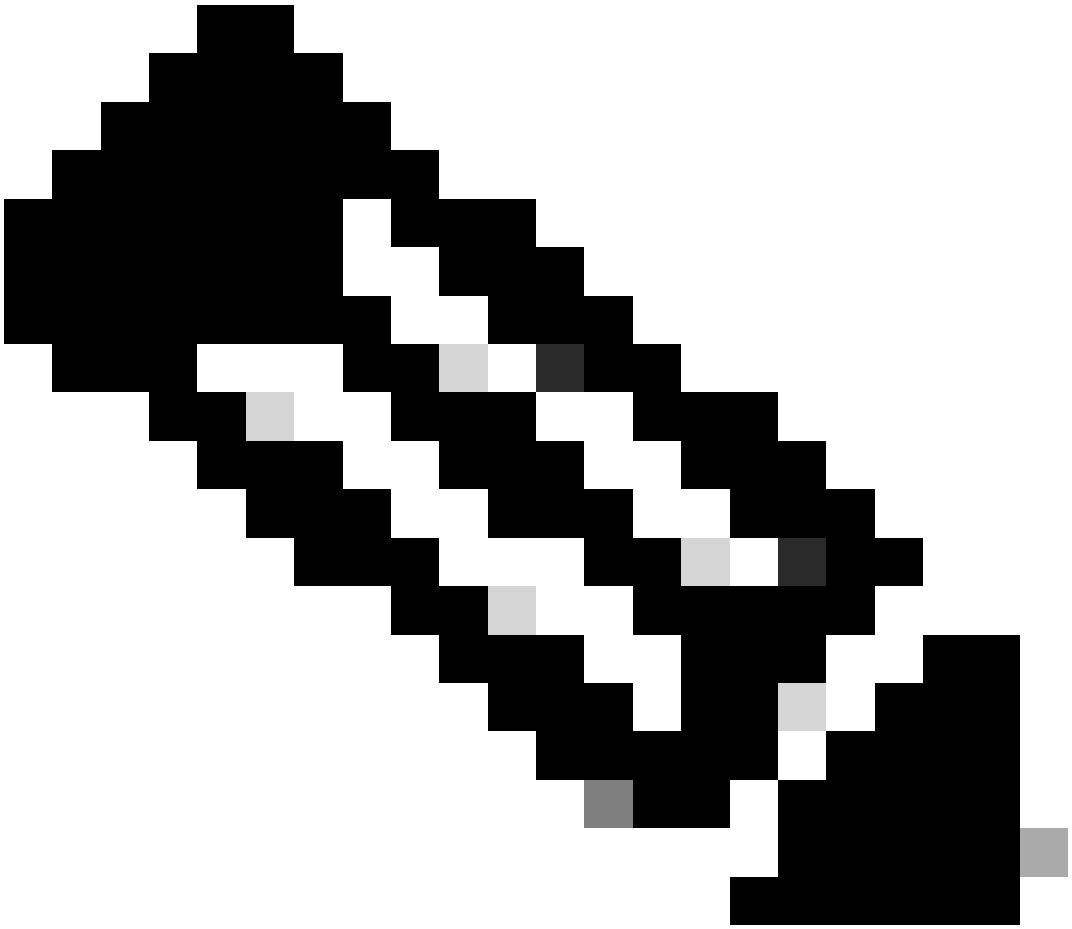
```
interface TwentyFiveGigE1/0/5
 switchport access vlan 4
 switchport mode access
```

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

Opzione 2: configurare l'interfaccia come porta trunk. In questo modo, i frame ricevuti con la vlan 0 vengono assegnati alla vlan nativa.

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

---



Nota: Questa condizione è stata comunemente riscontrata nei dispositivi Profinet.

---

## Difetti correlati

- Per ulteriori informazioni, vedere l'ID bug Cisco CSCwe8812.

## Informazioni correlate

- Supporto VLAN 0 Priority Tagging

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).