# Dépannage des abandons de protocole inconnus dans les commutateurs Catalyst 9000

## Table des matières



## Introduction

Ce document décrit les causes courantes des abandons de protocole inconnus dans les commutateurs de la gamme Catalyst 9000.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Commutateurs de la gamme Catalyst 9000
- Cisco IOS® XE

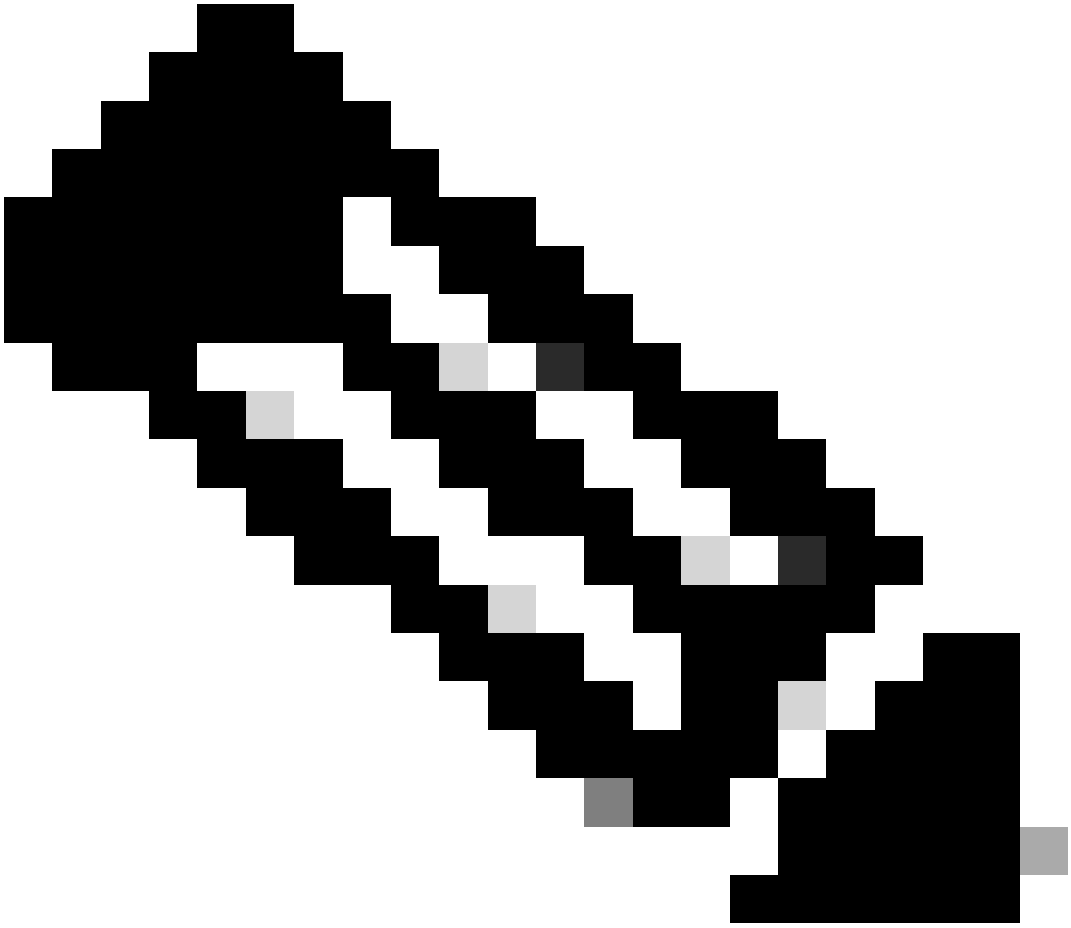
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

# Informations générales

Des abandons de protocole inconnu se produisent lorsque l'ethertype d'une trame n'est pas reconnu, ce qui signifie que le protocole encapsulé n'est pas pris en charge ou n'est pas configuré au niveau de l'interface du commutateur. En outre, l'adresse MAC de destination de la trame doit être une adresse de plan de contrôle de multidiffusion, répertoriées dans cette commande.

<#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
```



Remarque : les abandons de protocole inconnus n'incrémentent pas lorsque l'adresse MAC de destination est diffusée.

## Dépannage

Étape 1. Assurez-vous que les abandons de protocole inconnus augmentent.

<#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
```

Étape 2 : configuration d'une capture de paquets dans l'interface concernée et correspondance des adresses MAC de destination commençant par 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
```

Étape 3. Démarrez la capture de paquets et vérifiez le compteur 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
```

Étape 4. Arrêtez la capture de paquets après quelques abandons de protocole inconnus.

```
<#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
```

Étape 5 : exportation du contenu de la capture de paquets

<#root>

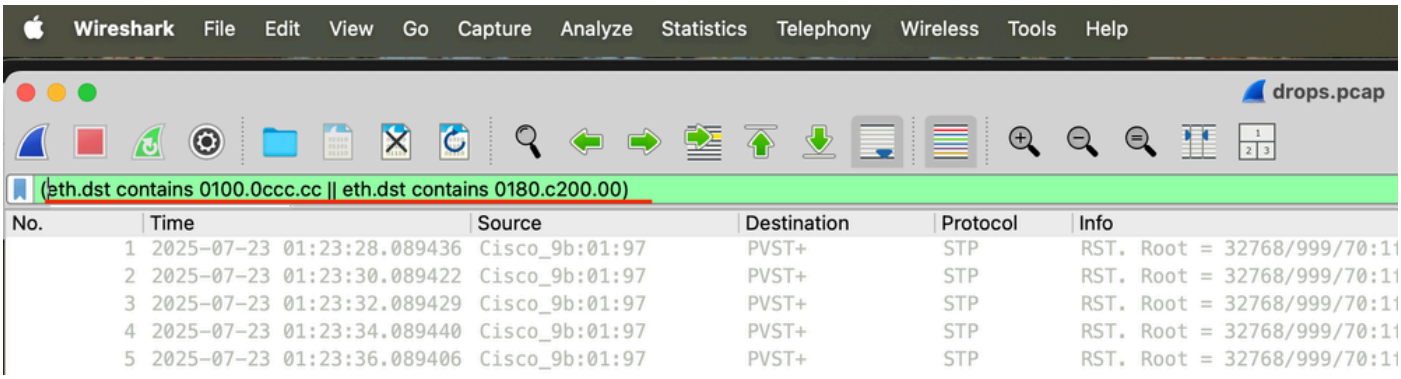
```
Switch#

monitor capture port5 export location flash:drops.pcap

Export Started Successfully

Switch#
Export completed for capture point port5
```

Étape 6. Transférez la capture de paquets sur votre ordinateur.

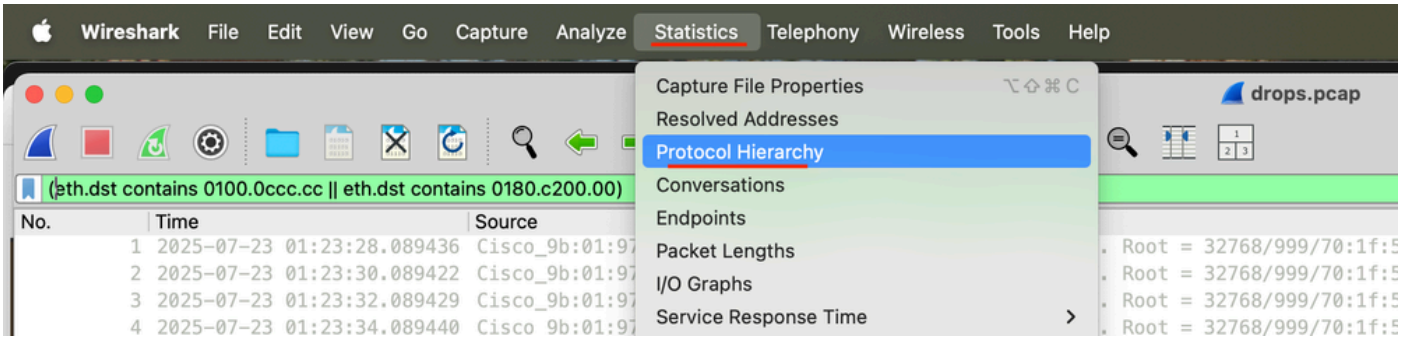
<#root>

```
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)
```

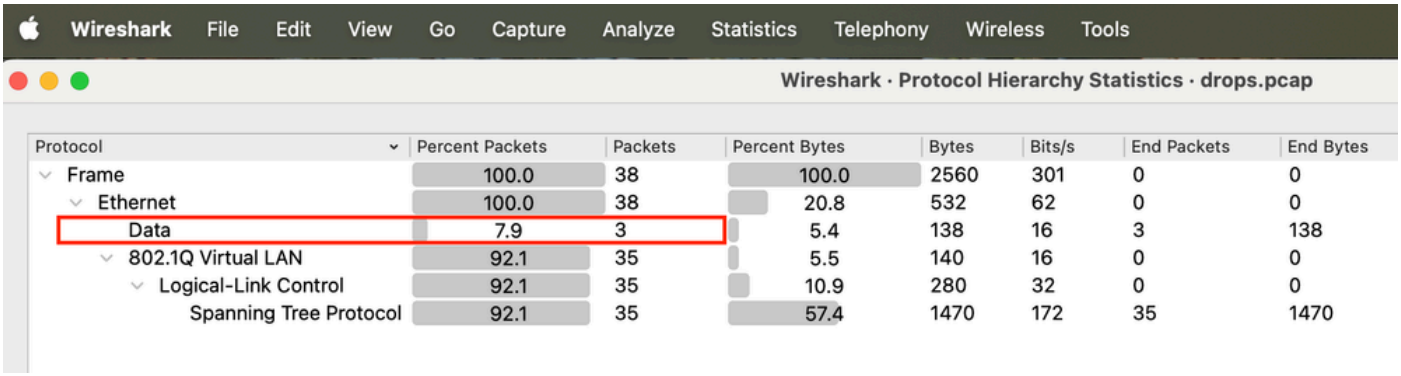
Étape 7. Ouvrez la capture de paquets dans Wireshark et utilisez ce filtre (eth.dst contient 0100.0ccc.cc || eth.dst contient 0180.c200.00) pour se concentrer sur les adresses de multidiffusion du processeur.



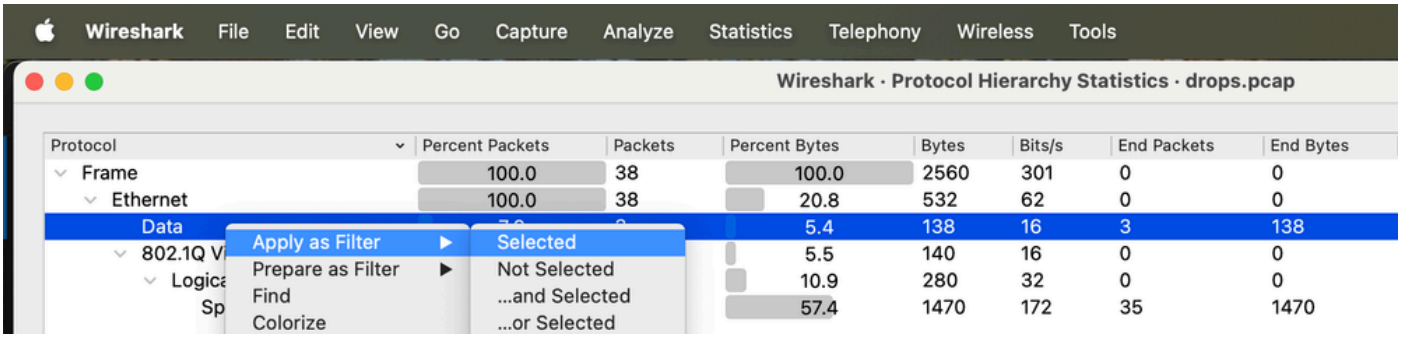

Étape 8. Accédez à Statistics, puis cliquez sur Protocol Hierarchy.




Étape 9. Développez l'arborescence des protocoles et vérifiez que l'interface du commutateur est configurée pour ces protocoles. Tout élément étiqueté comme Data entraîne des abandons de protocole inconnus, car l'ethertype est inconnu.

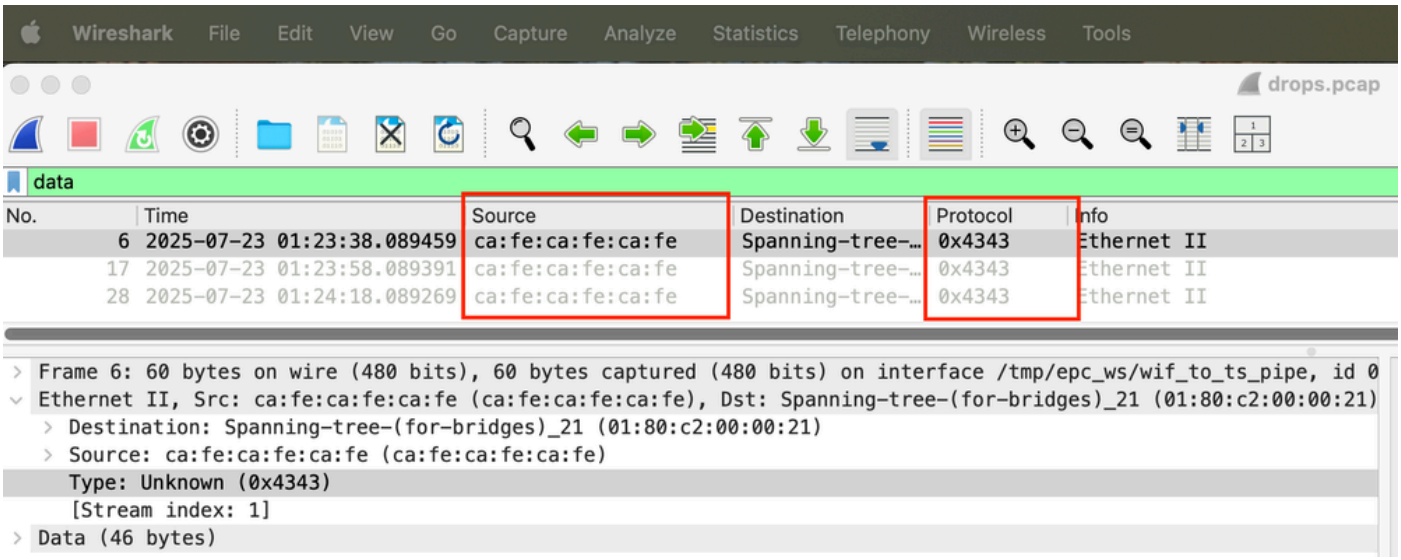



Étape 10. Cliquez avec le bouton droit sur Data, accédez à Apply as Filter et cliquez sur Selected pour filtrer les trames de protocole inconnues.




Étape 11. Revenez à la fenêtre principale de Wireshark pour déterminer l'adresse MAC source et

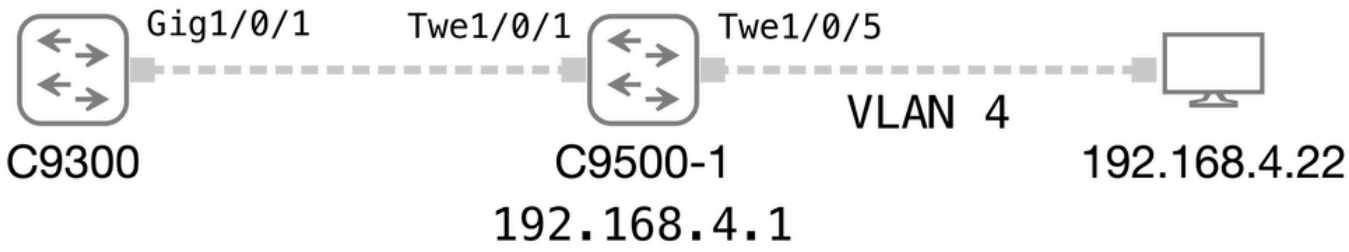
l’ethertype des protocoles inconnus.




Dans ce cas, l'adresse MAC source CAFE.CAFE.CAFE provoque des abandons de protocole inconnus, car l'ethertype 0x4343 n'est pas pris en charge.

## Problèmes courants

Les exemples de cette section sont basés sur ce schéma de topologie de réseau.




### Dynamic Trunking Protocol (DTP)

Les messages DTP peuvent potentiellement provoquer des abandons de protocole inconnus s’ils sont reçus sur un port où le protocole DTP est désactivé. Vous pouvez activer DTP en utilisant la commande no switchport nonegotiate en mode de configuration d'interface.

<#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
```

## Protocole LLDP (Link Layer Discovery Protocol)

Les messages LLDP peuvent également provoquer des abandons de protocole inconnus s'ils sont reçus sur le port où LLDP est désactivé. Vous pouvez activer LLDP en utilisant la commande lldp run en mode de configuration 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
```

## Cisco Discovery Protocol (CDP)

De même, les abandons de protocole inconnus peuvent s'incrémenter si des messages CDP sont reçus sur un port où le protocole CDP est désactivé. Vous pouvez activer le CDP en utilisant la commande cdp run en mode de configuration 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
```

## Identificateur de VLAN à 0 dans l'en-tête 802.1Q

Les commutateurs de la gamme Catalyst 9000 abandonnent également les trames 802.1Q avec l'ID de VLAN 0 lorsqu'ils sont reçus sur les ports d'accès. Cependant, ces paquets n'incrémentent pas le compteur de abandons de protocole inconnu. Dans cet exemple, examinons pourquoi le commutateur Catalyst 9500 ne peut pas obtenir une entrée ARP pour l'hôte 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
```

Étape 1. Démarrez une capture de paquets dans l’interface de connexion au périphérique 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
```

Étape 2 : envoi d’une requête ping au périphérique final pour générer du trafic 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)
```

Étape 3. Arrêtez la capture de paquets.

<#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
```

Étape 4. Notez que le périphérique final envoie une réponse ARP, dans ce cas la trame 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
```

Étape 5. Notez que la réponse ARP est encapsulée dans un en-tête 802.1Q à l'aide de l'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
```

Étape 6 : exportation du contenu de la capture de paquets

<#root>

```
C9500-1#
```

**monitor capture TAC export location flash:ARP.pcap**

```
Export Started Successfully
```

Étape 7. Déterminez ce que le commutateur fait du paquet 17 à l'aide de l'outil 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
```

Étape 8 : affichage des résultats du traceur de paquets

<#root>

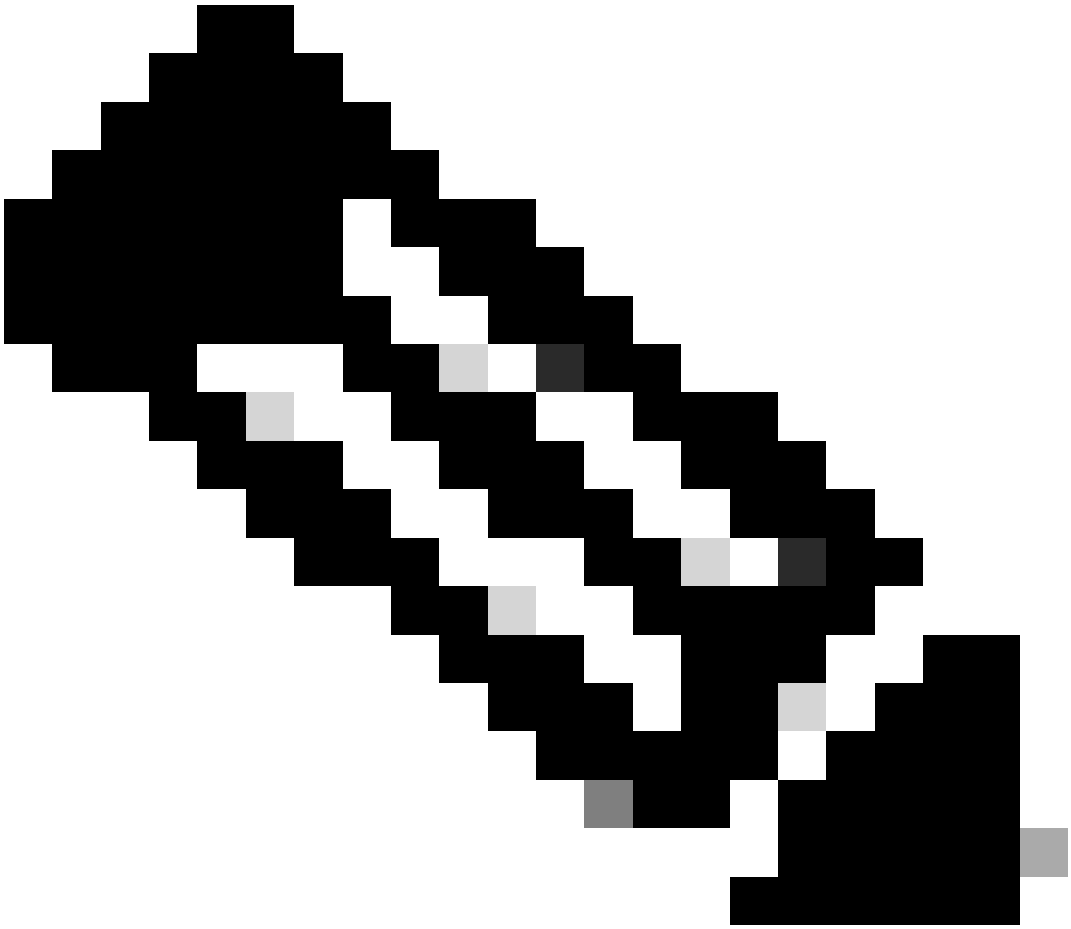
```
C9500-1#
```

**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.
```

---



Remarque : Le paquet est abandonné car il inclut l'ID de VLAN 0.

---

Il existe deux options pour empêcher ce type de chutes.

Option 1 : utilisez la commande switchport voice vlan dot1p. De cette manière, les trames reçues avec le VLAN 0 sont affectées au VLAN d’accès.

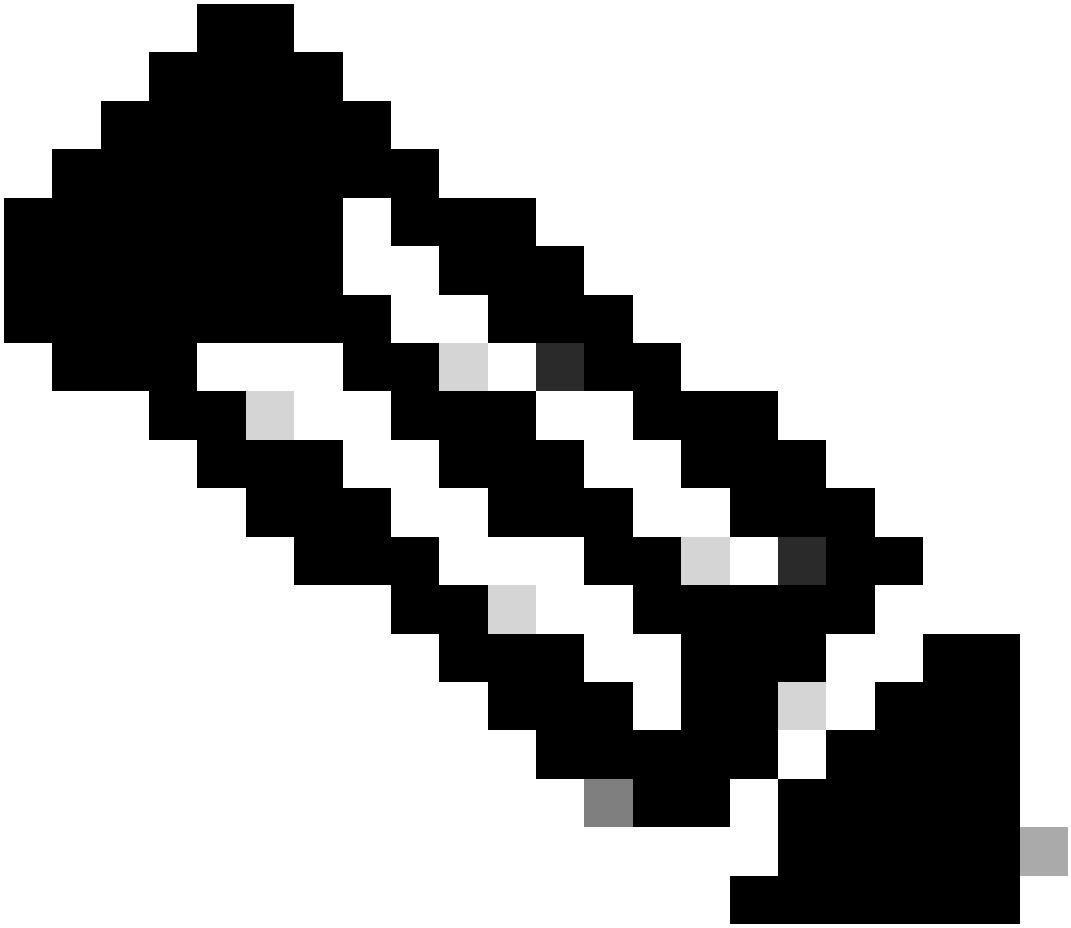
```
interface TwentyFiveGigE1/0/5
 switchport access vlan 4
 switchport mode access
 switchport voice vlan dot1p
```

```
 load-interval 30
```

Option 2 : configurez l'interface en tant que port agrégé. De cette manière, les trames reçues avec le VLAN 0 sont attribuées au VLAN natif.

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

---



Remarque : Cela est souvent le cas avec les périphériques Profinet.

---

## Défauts associés

- Consultez l'ID de bogue Cisco CSCwe8812 pour plus d'informations.

## Informations connexes

- Prise en charge du marquage prioritaire VLAN 0

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.