

Funzionamento e risoluzione dei problemi di snooping DHCP sugli switch Catalyst 9000

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Snooping DHCP](#)

[Operazione di snooping DHCP](#)

[Topologia](#)

[Configurazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Risoluzione dei problemi software](#)

[Risoluzione dei problemi relativi al traffico di punti e percorsi \(CPU\)](#)

[Risoluzione dei problemi hardware](#)

[Acquisizione pacchetti percorso CPU](#)

[Tracce utili](#)

[Syslog e spiegazioni](#)

[Avvisi sullo snooping DHCP](#)

[Snooping DHCP bordo SDA](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come usare gli switch Catalyst serie 9000 e come risolvere i problemi relativi allo snooping DHCP

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Catalyst serie 9000 Switch Architettura
- Architettura software Cisco IOS® XE

Componenti usati

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

- C9200
- C9300
- C9400
- C9500
- C9600

Cisco IOS® XE 16.12.X

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.



Nota: per i comandi che vengono utilizzati per abilitare queste funzionalità su altre piattaforme Cisco, consultare la guida alla configurazione appropriata.

Premesse

Snooping DHCP

Lo snooping DHCP (Dynamic Host Configuration Protocol) è una funzionalità di sicurezza utilizzata per controllare il traffico DHCP e bloccare eventuali pacchetti DHCP dannosi. Funziona come un firewall tra le porte utente non attendibili e le porte server DHCP sulla rete per impedire la presenza di server DHCP dannosi nella rete, in quanto può causare un rifiuto del servizio.

Operazione di snooping DHCP

Lo snooping DHCP si basa sul concetto di interfacce attendibili e non attendibili. Tramite il percorso del traffico DHCP, lo switch verifica i pacchetti DHCP ricevuti sulle interfacce e tiene traccia dei pacchetti del server DHCP previsti (offer & ACK) sulle interfacce attendibili. In altre parole, le interfacce non attendibili bloccano i pacchetti del server DHCP.


Pacchetti DHCP bloccati su interfacce non attendibili.

- Un pacchetto proveniente da un server DHCP, ad esempio un pacchetto DHCP, DHCPcproffer, DHCPcprofferACK, DHCPcprofferNAK o DHCPcprofferLEASEQUERY, viene ricevuto dall'esterno della rete o del firewall. In questo modo si evita che un server DHCP non autorizzato attacchi la rete su porte non attendibili.
- Un pacchetto ricevuto su un'interfaccia non attendibile e l'indirizzo MAC di origine e l'indirizzo hardware del client DHCP non corrispondono. In questo modo si evita lo spoof dei pacchetti DHCP da parte di un client non autorizzato che potrebbe creare un attacco Denial of Service su un server DHCP.
- Messaggio broadcast DHCPRELEASE o DHCPDECLINE con indirizzo MAC nel database di

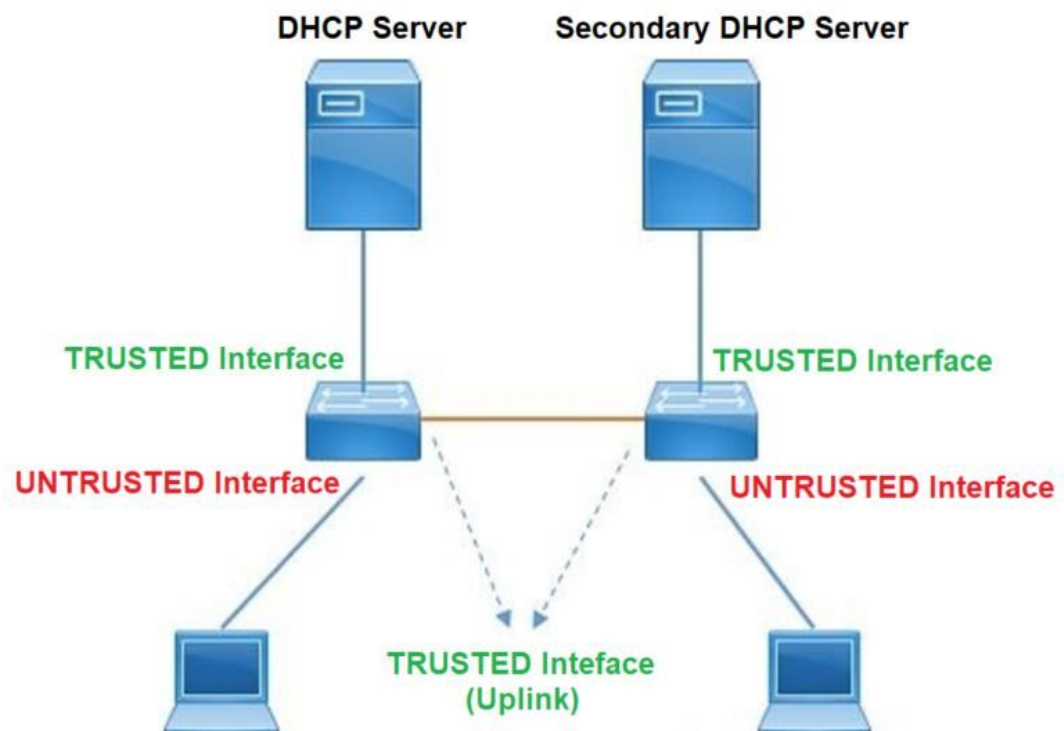
binding dello snooping DHCP, ma le informazioni di interfaccia nel database di binding non corrispondono all'interfaccia su cui è stato ricevuto il messaggio. In questo modo si evitano attacchi Denial of Service sui client.

- Un pacchetto DHCP inoltrato da un agente di inoltro DHCP che include un indirizzo IP dell'agente di inoltro diverso da 0.0.0.0 oppure l'agente di inoltro inoltra un pacchetto che include informazioni sull'opzione 82 a una porta non attendibile. In questo modo si evitano le informazioni dell'agente di inoltro spoof sulla rete.

Lo switch su cui si configura lo snooping DHCP crea una tabella di snooping DHCP o un database di binding DHCP. Questa tabella viene utilizzata per tenere traccia degli indirizzi IP assegnati da un server DHCP legittimo. Il database di binding viene inoltre utilizzato da altre funzionalità di sicurezza di IOS, ad esempio Ispezione ARP dinamica e Protezione origine IP.

 Nota: per consentire il corretto funzionamento dello snooping DHCP, verificare che tutte le porte uplink siano attendibili per il server DHCP e le porte dell'utente finale non siano attendibili.

Topologia



Configurazione

Configurazione globale

<#root>

1. Enable DHCP snooping globally on the switch
switch(config)#

```
ip dhcp snooping
```

2. Designate ports that forward traffic toward the DHCP server as trusted
switch(config-if)#

```
ip dhcp snooping trust
```

(Additional verification)

- List uplink ports according to the topology, ensure all the uplink ports toward the DHCP server are
trusted

- List the port where the Legitimate DHCP Server is connected (include any Secondary DHCP Server)
- Ensure that no other port is configured as trusted

3. Configure DHCP rate limiting on each untrusted port (Optional)
switch(config-if)#

```
ip dhcp snooping limit rate 10 << ----- 10 packets per second (pps)
```

4. Enable DHCP snooping in specific VLAN
switch(config)#

```
ip dhcp snooping vlan 10
```

<< ----- Allow the switch to snoop the traffic for that specific VLAN

5. Enable the insertion and removal of option-82 information DHCP packets
switch(config)#

```
ip dhcp snooping information option
```

<-- Enable insertion of option 82

```
switch(config)#
```

```
no ip dhcp snooping information option
```

<-- Disable insertion of option 82

Example

Legitimate DHCP Server Interface and Secondary DHCP Server, if available

Server Interface

```
interface FortyGigabitEthernet1/0/5
switchport mode access
switchport mode access vlan 11

ip dhcp snooping trust
```

end

Uplink interface

```
interface FortyGigabitEthernet1/0/10
switchport mode trunk

ip dhcp snooping trust
```

end

User Interface

<< ----- All interfaces are UNTRUSTED by default

```
interface FortyGigabitEthernet1/0/2
switchport access vlan 10
switchport mode access
```

```
ip dhcp snooping limit rate 10
```

<< ----- Optional

end



Nota: per consentire i pacchetti dell'opzione 82, è necessario abilitare l'opzione allow-untrusted delle informazioni sullo snooping dhcp ip.

Verifica

Verificare che lo snooping DHCP sia abilitato sulla VLAN desiderata e che le interfacce attendibili e non attendibili siano correttamente elencate. Se è stata configurata una tariffa, verificare che sia elencata.

<#root>

switch#show ip dhcp snooping

Switch DHCP snooping is

enabled

Switch DHCP gleaning is disabled

DHCP snooping is configured on following VLANs:

10-11

DHCP

snooping is operational on following VLANs

:

<<---- Configured and operational on Vlan 10 & 11

10-11

DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is disabled

<<---- Option 82 can not be added to DHCP packet

circuit-id default format: vlan-mod-port

remote-id: 00a3.d144.1a80 (MAC)

Option 82 on untrusted port is not allowed

Verification of hwaddr field is enabled

Verification of giaddr field is enabled

DHCP snooping trust/rate is configured on the following Interfaces:

Interface

Trusted

| Allow option | Rate limit (pps) |
|--------------|------------------|
|--------------|------------------|

| | |
|---------------------------|--|
| FortyGigabitEthernet1/0/2 | |
|---------------------------|--|

no

| | |
|----|----|
| no | 10 |
|----|----|

<<--- Trust is NOT set on this interface

Custom circuit-ids:

FortyGigabitEthernet1/0/10

yes

| | |
|-----|-----------|
| yes | unlimited |
|-----|-----------|

<<--- Trust is set on this interface

Custom circuit-ids:

Gli utenti che ricevono un IP tramite DHCP vengono elencati in questo output.

- Lo snooping DHCP rimuove la voce nel database quando scade il lease dell'indirizzo IP o lo switch riceve un messaggio DHCPRELEASE dall'host.
- Verificare che le informazioni elencate per l'indirizzo MAC dell'utente finale siano corrette.


<#root>

```
c9500#show ip dhcp snooping binding
```

```
MacAddress      IPAddress      Lease(sec) Type          VLAN Interface
-----
00:A3:D1:44:20:46  10.0.0.3
85556
  dhcp-snooping 10   FortyGigabitEthernet1/0/2
Total number of bindings: 1
```

In questa tabella vengono elencati i vari comandi che è possibile utilizzare per monitorare le informazioni dello snooping DHCP.

| Comando | Scopo |
|--|---|
| <pre>show ip dhcp snooping binding show ip dhcp snooping binding [IP-address] [MAC-address] [interface ethernet slot/port] [vlan-id]</pre> | Visualizza solo i binding configurati in modo dinamico nel database di binding dello snooping DHCP, definito anche tabella di binding. - Indirizzo IP voce di binding - Indirizzo Mac della voce di binding - Interfaccia di input voce di binding - VLAN voce di binding |
| <pre>show ip dhcp snooping database</pre> | Visualizza lo stato e le statistiche del database di binding dello snooping DHCP. |
| <pre>mostra statistiche snooping ip dhcp</pre> | Visualizza le statistiche dello snooping DHCP in forma di riepilogo o di dettaglio. |


| | |
|---|--|
| show ip source binding | Visualizza le associazioni configurate in modo dinamico e statico. |
| <p>show interface vlan xyz</p> <p>show buffer input-interface Vlan xyz dump</p> | <p>Il pacchetto DHCP viene inviato all'agente di inoltro configurato nella vlan client tramite la SVI della vlan client. Se la coda di input mostra una perdita o raggiunge il limite massimo, è probabile che il pacchetto dhcp del client sia stato scartato e non sia stato in grado di raggiungere l'agente di inoltro configurato.</p> <hr/> <p> Nota: assicurarsi che i rilasci non vengano visualizzati nella coda di input.</p> <hr/> <p>switch#show int vlan 670 Carico per cinque secondi: 13%/0%; un minuto: 10%; cinque minuti: 10% La fonte del tempo è NTP, 18:39:52.476 UTC Thu Sep 10 2020</p> <p>Vlan670 è attivo, il protocollo di linea è attivo, la funzione di autostazione è abilitata L'hardware è Ethernet SVI, l'indirizzo è 00fd.227a.5920 (bia 00fd.227a.5920) Descrizione: ion_media_client L'indirizzo Internet è 10.27.49.254/23 MTU 1500 byte, BW 1000000 Kbit/sec, DLY 10 usec, affidabilità 255/255, txload 1/255, rxload 1/255 ARPA di incapsulamento, loopback non impostato Keepalive non supportato Tipo ARP: ARPA, timeout ARP 04:00:00 Ultimo ingresso 03:01:29, uscita 00:00:02, uscita mai bloccata Ultima cancellazione dei contatori "show interface" mai Coda di input: 375/375/4020251/0 (dimensioni/max/drop/flush); Totale perdite di output: 0 ← 375 pacchetti in input nella coda / 4020251 sono stati eliminati</p> |

Risoluzione dei problemi

Risoluzione dei problemi software

Verificare cosa riceve lo switch. Questi pacchetti vengono elaborati al control-plane della CPU, in

modo da verificare che tutti i pacchetti vengano inseriti nelle direzioni punt e punt e che le informazioni siano corrette.

 **Attenzione:** usare con cautela i comandi di debug. Tenere presente che molti comandi di debug influiscono sulla rete in tempo reale e si consiglia di utilizzarli in un ambiente lab quando il problema viene riprodotto.

La funzione Debug condizionale consente di abilitare in modo selettivo i debug e i log per funzionalità specifiche in base a un insieme di condizioni definite dall'utente. Questa opzione risulta utile per contenere le informazioni di debug solo su host o traffico specifici.

Una condizione si riferisce a una funzionalità o a un'identità, dove l'identità può essere un'interfaccia, un indirizzo IP o un indirizzo MAC e così via..

Come abilitare il debug condizionale per i debug di pacchetti ed eventi per risolvere i problemi relativi allo snooping DHCP.

| Comando | Scopo |
|---|--|
| <code>debug condition mac <indirizzo-mac></code> Esempio: <code>condizione switch#debug mac bc16.6509.3314</code> | Configura il debug condizionale per l'indirizzo MAC specificato. |
| <code>debug condition vlan <ID VLAN></code> Esempio: <code>switch#debug condizione vlan 10</code> | Configura il debug condizionale per la VLAN specificata. |
| <code>debug condition interface <interfaccia></code> Esempio: <code>switch#debug condition interface - 250GigE 1/0/8</code> | Configura il debug condizionale per l'interfaccia specificata. |

Per eseguire il debug dello snooping DHCP, utilizzare i comandi illustrati nella tabella.

| Comando | Scopo |
|--|------------------------------------|
| <code>debug dhcp [detail oper </code> | dettaglio contenuto pacchetto DHCP |

| | |
|--|---|
| ridondanza] | OPER interno DHCP oper ridondanza Supporto ridondanza client DHCP |
| dettagli pacchetto server dhcp debug ip | Decodificare in dettaglio la ricezione e la trasmissione dei messaggi |
| debug ip dhcp server events | Segnala assegnazioni di indirizzi, scadenza del lease e così via. |
| debug ip dhcp snooping agent | Lettura e scrittura del database di snooping dhcp di debug |
| debug ip dhcp snooping event | Evento di debug tra ogni componente |
| debug ip dhcp snooping packet | Debug del pacchetto DHCP nel modulo di snooping dhcp |

questo è l'output di esempio parziale del comando debug ip dhcp snooping.

<#root>

Apr 14 16:16:46.835: DHCP_SNOOPING: process new DHCP packet,

message type: DHCPDISCOVER, input interface: Fo1/0/2

, MAC da: ffff.ffff.ffff, MAC

sa: 00a3.d144.2046,

IP da: 255.255.255.255, IP sa: 0.0.0.0, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.0.0

Apr 14 16:16:46.835: DHCP_SNOOPING: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is flood

Apr 14 16:16:48.837: DHCP_SNOOPING:

received new DHCP packet from input interface (FortyGigabitEthernet1/0/10)

Apr 14 16:16:48.837: DHCP_SNOOPING:

process new DHCP packet, message type: DHCP OFFER, input interface: Fo1/0/10,

MAC da: ffff.ffff.ffff, MAC

sa: 701f.539a.fe46,

IP da: 255.255.255.255, IP sa: 10.0.0.1, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 10.0.0.5, DHCP siaddr: 0.0.0.0

Apr 14 16:16:48.837: platform lookup dest vlan for input_if: FortyGigabitEthernet1/0/10, is NOT tunnel,

Apr 14 16:16:48.837: DHCP_SNOOPING: direct forward dhcp reply to output port: FortyGigabitEthernet1/0/2.


Apr 14 16:16:48.838: DHCP_SNOOPING: received new DHCP packet from input interface (FortyGigabitEthernet1/0/10)

Apr 14 16:16:48.838: Performing rate limit check

Apr 14 16:16:48.838: DHCP_SNOOPING: process new DHCP packet,

```
message type: DHCPREQUEST, input interface: Fo1/0/2,
MAC da: ffff.ffff.ffff, MAC
sa: 00a3.d144.2046,
IP da: 255.255.255.255, IP sa: 0.0.0.0, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.0.0
Apr 14 16:16:48.838: DHCP_SNOOPING: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is flooded
Apr 14 16:16:48.839: DHCP_SNOOPING: received new DHCP packet from input interface (FortyGigabitEthernet1/0/2)
Apr 14 16:16:48.840: DHCP_SNOOPING: process new DHCP packet,
message type: DHCPACK, input interface: Fo1/0/10,
MAC da: ffff.ffff.ffff, MAC
sa: 701f.539a.fe46,
IP da: 255.255.255.255, IP
sa: 10.0.0.1,
DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 10.0.0.5, DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP chaddr: 0.0.0.0
Apr 14 16:16:48.840: DHCP_SNOOPING: add binding on port FortyGigabitEthernet1/0/2 ckt_id 0 FortyGigabitEthernet1/0/2
Apr 14 16:16:48.840: DHCP_SNOOPING: added entry to table (index 331)
Apr 14 16:16:48.840:
DHCP_SNOOPING: dump binding entry: Mac=00:A3:D1:44:20:46 Ip=10.0.0.5
Lease=86400 Type=dhcp-snooping
Vlan=10 If=FortyGigabitEthernet1/0/2
Apr 14 16:16:48.840: No entry found for mac(00a3.d144.2046) vlan(10) FortyGigabitEthernet1/0/2
Apr 14 16:16:48.840: host tracking not found for update add dynamic (10.0.0.5, 0.0.0.0, 00a3.d144.2046)
Apr 14 16:16:48.840: platform lookup dest vlan for input_if: FortyGigabitEthernet1/0/10, is NOT tunnel
Apr 14 16:16:48.840: DHCP_SNOOPING: direct forward dhcp reply to output port: FortyGigabitEthernet1/0/2.
```

Per eseguire il debug degli eventi di snooping DHCP, attenersi alla seguente procedura:

 **Attenzione:** usare con cautela i comandi di debug. Tenere presente che molti comandi di debug hanno un impatto sulla rete in tempo reale e si consiglia di utilizzarli in un ambiente lab solo quando il problema viene riprodotto.

Passi di riepilogo

1. attivare
2. debug platform condition mac {mac-address }
3. avvio condizione piattaforma di debug
4. show platform condition OR show debug
5. arresto condizione piattaforma di debug
6. show platform software trace message ios R0 reverse | includere DHCP
7. cancella tutte le condizioni della piattaforma

Passi dettagliati

| | Comando o azione | Scopo |
|-------------|--|---|
| Passaggio 1 | <p>attivare</p> <p>Esempio:</p> <p>switch#enable</p> | <p>Abilita la modalità di esecuzione privilegiata.</p> <ul style="list-style-type: none"> • Se richiesto, immettere la password. |
| Passaggio 2 | <p>debug platform condition mac {indirizzo-mac}</p> <p>Esempio:</p> <p>switch#debug condizione piattaforma mac 0001.6509.3314</p> | <p>Configura il debug condizionale per l'indirizzo MAC specificato.</p> |
| Passaggio 3 | <p>avvio condizione piattaforma di debug</p> <p>Esempio:</p> <p>avvio condizione piattaforma switch#debug</p> | <p>Avvia il debug condizionale (ciò può avviare la traccia radioattiva se una delle condizioni soddisfa una delle condizioni).</p> |
| Passaggio 4 | <p>show platform condition OR show debug</p> <p>Esempio:</p> <p>switch#show platform condition</p> <p>switch#show debug</p> | <p>Visualizza il set di condizioni corrente.</p> |
| Passaggio 5 | <p>arresto condizione piattaforma di debug</p> <p>Esempio:</p> <p>switch#debug platform condition stop</p> | <p>Interrompe il debug condizionale (ciò può interrompere la traccia radioattiva).</p> |
| Passaggio 6 | <p>show platform software trace message ios R0 reverse includere DHCP</p> <p>Esempio:</p> <p>switch#show platform software trace message ios R0 reverse includere DHCP</p> | <p>Visualizza i registri HP uniti dall'ultimo file di traccia.</p> |
| Passaggio | <p>cancela tutte le condizioni della piattaforma</p> | <p>Cancela tutte le condizioni.</p> |

| | Comando o azione | Scopo |
|---|--|-------|
| 7 | Esempio: switch# cancella tutte le condizioni della piattaforma | |

Questo è un esempio di output di esempio parziale della piattaforma di debug dhcp-snoop all.

<#root>

```
debug platform dhcp-snoop all
```

DHCP Server UDP port

(67)

DHCP Client UDP port

(68)

RELEASE

```
Apr 14 16:44:18.629: pak->vlan_id = 10
Apr 14 16:44:18.629: dhcp packet src_ip(10.0.0.6) dest_ip(10.0.0.1) src_udp(68) dest_udp(67) src_mac(00a3.d144.2046)
Apr 14 16:44:18.629: ngwc_dhcpsn_process_pak(305): Packet handedover to SISF on vlan 10
Apr 14 16:44:18.629: dhcp pkt processing routine is called for pak with SMAC = 00a3.d144.2046{mac} and SRC_ADDR = 10.0.0.6
```

DISCOVER

```
Apr 14 16:44:24.637: dhcp packet src_ip(0.0.0.0) dest_ip(255.255.255.255) src_udp(68) dest_udp(67) src_mac(00a3.d144.2046)
Apr 14 16:44:24.637: ngwc_dhcpsn_process_pak(305): Packet handedover to SISF on vlan 10
Apr 14 16:44:24.637: dhcp pkt processing routine is called for pak with SMAC = 00a3.d144.2046{mac} and SRC_ADDR = 0.0.0.0
Apr 14 16:44:24.637: sending dhcp packet out after processing with SMAC = 00a3.d144.2046{mac} and SRC_ADDR = 0.0.0.0
Apr 14 16:44:24.638: pak->vlan_id = 10
```

OFFER

```
Apr 14 16:44:24.638: dhcp packet src_ip(10.0.0.1) dest_ip(255.255.255.255) src_udp(67) dest_udp(68) src_mac(00a3.d144.2046)
Apr 14 16:44:24.638: ngwc_dhcpsn_process_pak(305): Packet handedover to SISF on vlan 10
Apr 14 16:44:24.638: dhcp pkt processing routine is called for pak with SMAC = 701f.539a.fe46{mac} and SRC_ADDR = 10.0.0.1
```


REQUEST

```
Apr 14 16:44:24.638: ngwc_dhcpsn_process_pak(284): Packet handedover to SISF on vlan 10
c9500#dhcp pkt processing routine is called for pak with SMAC = 0a3.d144.2046{mac} and SRC_ADDR = 0.0.0.0
```

ACK

Apr 14 16:44:24.640: dhcp paket src_ip(10.10.10.1) dest_ip(255.255.255.255) src_udp(67) dest_udp(68) s
 Apr 14 16:44:24.640: ngwc_dhcpsn_process_pak(284): Packet handedover to SISF on v1an 10dhcp pkt process

In questa tabella vengono elencati i vari comandi che possono essere utilizzati per eseguire il debug dello snooping DHCP nella piattaforma.

 **Attenzione:** usare con cautela i comandi di debug. Tenere presente che molti comandi di debug hanno un impatto sulla rete in tempo reale e si consiglia di utilizzarli in un ambiente lab quando il problema viene riprodotto.

| Comando | Scopo |
|--|--|
| switch#debug platform dhcp-snoop [tutte pacchetto pd-shim] | tutti gli snooping DHCP NGWC pacchetto NGWC DHCP Snooping Packet Debug Info pd-shim NGWC DHCP Snooping IOS Shim Debug Info |
| switch#debug platform software infrastructure punt dhcp-snoop | Pacchetti ricevuti sull'FP e puntati sul control plane) |
| switch#debug inserimento infrastruttura software piattaforma | Pacchetti che vengono iniettati nell'FP dal control plane |

Risoluzione dei problemi relativi al traffico di punti e percorsi (CPU)

Verificare dal punto di vista del feed il traffico ricevuto in ciascuna coda della CPU (lo snooping DHCP è un tipo di traffico elaborato dal control-plane).

- Quando il traffico arriva allo switch, viene inviato alla CPU in direzione PUNT e alla coda dello snoop dhcp.
- Una volta elaborato dallo switch, il traffico parte attraverso la direzione INJECT. I pacchetti DHCP offer e ACK rientrano nella coda di controllo/legacy L2.

<#root>

```
c9500#show platform software fed switch active punt cause summary
```

Statistics for all causes

| Cause | Cause Info | Rcvd | Dropped |
|-------|--------------------------|-------|---------|
| 21 | RP<->QFP keepalive | 8533 | 0 |
| 79 | dhcp snoop | 71 | 0 |
| 96 | Layer2 control protocols | 45662 | 0 |
| 109 | snoop packets | 100 | 0 |

c9500#show platform software fed sw active inject cause summary

Statistics for all causes

| Cause | Cause Info | Rcvd | Dropped |
|-------|-------------------------|--------|---------|
| 1 | L2 control/legacy | 128354 | 0 |
| 2 | QFP destination lookup | 18 | 0 |
| 5 | QFP <->RP keepalive | 8585 | 0 |
| 12 | ARP request or response | 68 | 0 |
| 25 | Layer2 frame to BD | 81 | 0 |

È possibile utilizzare questo comando per confermare il traffico puntato alla CPU e verificare se lo snooping DHCP riduce il traffico.

<#root>

c9500#

show platform software fed switch active punt cpuq rates

Punt Rate CPU Q Statistics

Packets per second averaged over 10 seconds, 1 min and 5 mins

| Q no | Queue Name | Rx 10s | Rx 1min | Rx 5min | Drop 10s | Drop 1min | Drop 5min |
|------|-----------------------------|--------|---------|---------|----------|-----------|-----------|
| 0 | CPU_Q_DOT1X_AUTH | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | CPU_Q_L2_CONTROL | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | CPU_Q_FORUS_TRAFFIC | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | CPU_Q_ICMP_GEN | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | CPU_Q_ROUTING_CONTROL | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | CPU_Q_FORUS_ADDR_RESOLUTION | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | CPU_Q_ICMP_REDIRECT | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | CPU_Q_INTER_FED_TRAFFIC | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 | CPU_Q_L2LVX_CONTROL_PKT | 0 | 0 | 0 | 0 | 0 | 0 |
| 9 | CPU_Q_EWLC_CONTROL | 0 | 0 | 0 | 0 | 0 | 0 |
| 10 | CPU_Q_EWLC_DATA | 0 | 0 | 0 | 0 | 0 | 0 |

| | | | | | | | |
|------------------------|---------------------------------------|---|---|---|---|---|---|
| 11 | CPU_Q_L2LVX_DATA_PKT | 0 | 0 | 0 | 0 | 0 | 0 |
| 12 | CPU_Q_BROADCAST | 0 | 0 | 0 | 0 | 0 | 0 |
| 13 | CPU_Q_LEARNING_CACHE_OVFL | 0 | 0 | 0 | 0 | 0 | 0 |
| 14 | CPU_Q_SW_FORWARDING | 0 | 0 | 0 | 0 | 0 | 0 |
| 15 | CPU_Q_TOPOLOGY_CONTROL | 2 | 2 | 2 | 0 | 0 | 0 |
| 16 | CPU_Q_PROTO_SNOOPING | 0 | 0 | 0 | 0 | 0 | 0 |
| 17 CPU_Q_DHCP_SNOOPING | | | | | | | |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | <<---- drop counter must NOT increase | | | | | | |
| 18 | CPU_Q_TRANSIT_TRAFFIC | 0 | 0 | 0 | 0 | 0 | 0 |
| 19 | CPU_Q_RPF_FAILED | 0 | 0 | 0 | 0 | 0 | 0 |
| 20 | CPU_Q_MCAST_END_STATION_SERVICE | 0 | 0 | 0 | 0 | 0 | 0 |
| 21 | CPU_Q_LOGGING | 0 | 0 | 0 | 0 | 0 | 0 |
| 22 | CPU_Q_PUNT_WEBAUTH | 0 | 0 | 0 | 0 | 0 | 0 |
| 23 | CPU_Q_HIGH_RATE_APP | 0 | 0 | 0 | 0 | 0 | 0 |
| 24 | CPU_Q_EXCEPTION | 0 | 0 | 0 | 0 | 0 | 0 |
| 25 | CPU_Q_SYSTEM_CRITICAL | 8 | 8 | 8 | 0 | 0 | 0 |
| 26 | CPU_Q_NFL_SAMPLED_DATA | 0 | 0 | 0 | 0 | 0 | 0 |
| 27 | CPU_Q_LOW_LATENCY | 0 | 0 | 0 | 0 | 0 | 0 |
| 28 | CPU_Q_EGR_EXCEPTION | 0 | 0 | 0 | 0 | 0 | 0 |
| 29 | CPU_Q_FSS | 0 | 0 | 0 | 0 | 0 | 0 |
| 30 | CPU_Q_MCAST_DATA | 0 | 0 | 0 | 0 | 0 | 0 |
| 31 | CPU_Q_GOLD_PKT | 0 | 0 | 0 | 0 | 0 | 0 |

Risoluzione dei problemi hardware

Driver motore di inoltro (FED)

FED è il driver che programma l'ASIC. I comandi FED vengono utilizzati per verificare che gli stati dell'hardware e del software corrispondano.

Ottenete il valore DI DI_Handle

- L'handle DI fa riferimento all'indice di destinazione di una porta specifica.

<#root>

```
c9500#show platform software fed switch active security-fed dhcp-snoop vlan vlan-id 10
```

Platform Security DHCP Snooping Vlan Information

Value of Snooping DI handle

is::

```
0x7F7FAC23E438 <<---- If DHCP Snooping is not enabled the hardware handle can not be present
```



```

-----
Port                                     Trust Mode
-----
FortyGigabitEthernet1/0/10

trust <<---- Ensure TRUSTED ports are listed

```

Controllare il mapping di ifm per determinare l'elemento Asic e Core delle porte.

- IFM è un indice di interfaccia interno mappato a una porta/core/base specifica.

<#root>

```
c9500#show platform software fed switch active ifm mappings
```

```

Interface          IF_ID  Inst Asic Core Port SubPort Mac Cntx LPN GPN Type Active
FortyGigabitEthernet1/0/10

0xa
  3
1  1
  1  0    4  4  2  2  NIF Y

```

Utilizzate DI_Handle per ottenere l'indice hardware.

<#root>

```

c9500#show platform hardware fed switch active fwd-asic abstraction print-resource-handle 0x7F7FAC23E438
0
Handle:0x7f7fac23e438 Res-Type:ASIC_RSC_DI Res-Switch-Num:255 Asic-Num:255 Feature-ID:AL_FID_DHCP Snooping
priv_ri/priv_si Handle: (nil)Hardware Indices/Handles:
index0:0x5f03
  mtu_index/13u_ri_index0:0x0 index1:0x5f03 mtu_index/13u_ri_index1:0x0 index2:0x5f03 mtu_index/13u_ri_index2:0x0
<SNIP>
<-- Index is 0x5f03

```

Converte da esadecimale il valore di indice 0x5f03 a decimale.

0x5f03 = 24323

Utilizzare questo valore di indice in decimal e i valori ASIC e Core in questo comando per verificare i flag impostati per la porta.

```
<#root>
```

```
c9500#show platform hardware fed switch 1 fwd-asic regi read register-name SifDestinationIndexTable-2432
```

```
asic
```

```
1
```

```
core
```

```
1
```

```
For asic 1 core 1
```

```
Module 0 - SifDestinationIndexTable[0][
```

```
24323
```

```
]
```

```
<-- the decimal hardware index matches 0x5f03 = 24323
```

```
copySegment0 :
```

```
0x1 <----- If you find this as 0x0, means that the traffic is not forwarded out of this port. (refer to
```

```
CSCvi39202)copySegment1 : 0x1
```

```
dpuSegment0 : 0x0
```

```
dpuSegment1 : 0x0
```

```
ecUnicast : 0x0
```

```
etherChannel0 : 0x0
```

```
etherChannel1 : 0x0
```

```
hashPtr1 : 0x0
```

```
stripSegment : 0x0
```

Verificare che lo snooping DHCP sia abilitato per la VLAN specifica.

```
<#root>
```

```
c9500#show platform software fed switch 1 vlan 10
```

```
VLAN Fed Information
```

```
Vlan Id IF Id LE Handle STP Handle L3 IF Handle SVI IF
```

```
-----  
10 0x0000000000420011
```

```
0x00007f7fac235fa8
```

```
0x00007f7fac236798 0x0000000000000000 0x0000000000000000 15
```

```
c9500#
```

```
show platform hardware fed switch active fwd-asic abstraction print-resource-handle
```



```
LEAD_VLAN_EGRESS_DHCP_SNOOPING_ENABLED_IPV6 value 1 Pass
LEAD_VLAN_EGRESS_VXLAN_FLOOD_MODE value 0 Pass
LEAD_VLAN_MAX value 0 Pass
<SNIP>
```

In questa tabella vengono elencati i vari comandi show/debug di Punct comuni che possono essere usati per tracciare il percorso del pacchetto DHCP su una rete attiva.

Comandi Punct/Inject show & debug comuni

```
debug platform soft fed swit action inject add-filter cause 255 sub_cause 0 src_mac 0 0 dst_mac 0 0 src_ipv4 192.168.12.1 dst_ipv4 0.0.0.0 if_id 0xf
```

```
set platform software trace fed [switch<num|active|standby>] inject verbose — > usa il comando filter mostrato per definire l'ambito delle tracce su questo host specifico
```

```
set platform software trace fed [switch<num|active|standby>] inject debug boot — > for reload
```

```
set platform software trace fed [switch<num|active|standby>] punct noise
```

```
show platform software fed [switch<num|active|standby>] inserimento riepilogo causa
```

```
show platform software fed [switch<num|active|standby>] riepilogare le cause
```

```
show platform software fed [switch<num|active|standby>] inserire cpuq 0
```

```
show platform software fed [switch<num|active|standby>] punct cpuq 17 (coda dhcp)
```

```
show platform software fed [switch<num|active|standby>] active inserisce la det di acquisizione dei pacchetti
```

```
show platform software infrastructure inject
```

```
show platform software infrastructure punct
```

```
show platform software infrastructure driver lsmpi
```

```
debug platform software infra punct dhcp
```

```
debug platform software infra inject
```

Questi comandi sono utili per controllare se un pacchetto DHCP viene ricevuto per un particolare client.

- Questa funzione consente di acquisire tutte le comunicazioni di snooping DHCP associate a un determinato indirizzo MAC del client elaborate dalla CPU tramite il software IOS-DHCP.
- Questa funzionalità è supportata sia per il traffico IPv4 che per il traffico IPv6.

- Questa funzione viene attivata automaticamente.

 **Importante:** questi comandi sono disponibili da Cisco IOS XE Gibraltar 16.12.X.

```
switch#show platform dhcp snooping stato client {mac-address}
```

```
switch#show platform dhcpv6 stato client ipv6 snooping {mac-address}
```

<#root>

C9300#

```
show platform dhcp snooping client stats 0000.1AC2.C148
```

DHCP SN: DHCP snooping server

DHCPD: DHCP protocol daemon

L2FWD: Transmit Packet to driver in L2 format

FWD: Transmit Packet to driver

Packet Trace for client MAC 0000.1AC2.C148:

| Timestamp | Destination MAC | Destination Ip | VLAN | Message | Handler:Action |
|---------------------|-----------------|-----------------|------|--------------|----------------------|
| 06-27-2019 20:48:28 | FFFF.FFFF.FFFF | 255.255.255.255 | 88 | DHCPDISCOVER | PUNT:RECEIVED |
| 06-27-2019 20:48:28 | FFFF.FFFF.FFFF | 255.255.255.255 | 88 | DHCPDISCOVER | PUNT:TO_DHCP SN |
| 06-27-2019 20:48:28 | FFFF.FFFF.FFFF | 255.255.255.255 | 88 | DHCPDISCOVER | BRIDGE:RECEIVED |
| 06-27-2019 20:48:28 | FFFF.FFFF.FFFF | 255.255.255.255 | 88 | DHCPDISCOVER | BRIDGE:TO_DHCPD |
| 06-27-2019 20:48:28 | FFFF.FFFF.FFFF | 255.255.255.255 | 88 | DHCPDISCOVER | BRIDGE:TO_INJECT |
| 06-27-2019 20:48:28 | FFFF.FFFF.FFFF | 255.255.255.255 | 88 | DHCPDISCOVER | L2INJECT:TO_FWD |
| 06-27-2019 20:48:28 | 0000.0000.0000 | 192.168.1.1 | 0 | DHCPDISCOVER | INJECT:RECEIVED |
| 06-27-2019 20:48:28 | 0000.0000.0000 | 192.168.1.1 | 0 | DHCPDISCOVER | INJECT:TO_L2FWD |
| 06-27-2019 20:48:30 | 0000.0000.0000 | 10.1.1.3 | 0 | DHCPOFFER | INJECT:RECEIVED |
| 06-27-2019 20:48:30 | 0000.1AC2.C148 | 10.1.1.3 | 0 | DHCPOFFER | INTERCEPT:RECEIVED |
| 06-27-2019 20:48:30 | 0000.1AC2.C148 | 10.1.1.3 | 88 | DHCPOFFER | INTERCEPT:TO_DHCP SN |
| 06-27-2019 20:48:30 | 0000.1AC2.C148 | 10.1.1.3 | 88 | DHCPOFFER | INJECT:CONSUMED |
| 06-27-2019 20:48:30 | FFFF.FFFF.FFFF | 255.255.255.255 | 88 | DHCPREQUEST | PUNT:RECEIVED |
| 06-27-2019 20:48:30 | FFFF.FFFF.FFFF | 255.255.255.255 | 88 | DHCPREQUEST | PUNT:TO_DHCP SN |
| 06-27-2019 20:48:30 | FFFF.FFFF.FFFF | 255.255.255.255 | 88 | DHCPREQUEST | BRIDGE:RECEIVED |
| 06-27-2019 20:48:30 | FFFF.FFFF.FFFF | 255.255.255.255 | 88 | DHCPREQUEST | BRIDGE:TO_DHCPD |
| 06-27-2019 20:48:30 | FFFF.FFFF.FFFF | 255.255.255.255 | 88 | DHCPREQUEST | BRIDGE:TO_INJECT |
| 06-27-2019 20:48:30 | FFFF.FFFF.FFFF | 255.255.255.255 | 88 | DHCPREQUEST | L2INJECT:TO_FWD |
| 06-27-2019 20:48:30 | 0000.0000.0000 | 192.168.1.1 | 0 | DHCPREQUEST | INJECT:RECEIVED |
| 06-27-2019 20:48:30 | 0000.0000.0000 | 192.168.1.1 | 0 | DHCPREQUEST | INJECT:TO_L2FWD |
| 06-27-2019 20:48:30 | 0000.0000.0000 | 10.1.1.3 | 0 | DHCPACK | INJECT:RECEIVED |
| 06-27-2019 20:48:30 | 0000.1AC2.C148 | 10.1.1.3 | 0 | DHCPACK | INTERCEPT:RECEIVED |
| 06-27-2019 20:48:30 | 0000.1AC2.C148 | 10.1.1.3 | 88 | DHCPACK | INTERCEPT:TO_DHCP SN |


Utilizzare questi comandi per cancellare la traccia.

```
switch#clear platform dhcp snooping pkt-trace ipv4
```

```
switch#clear platform dhcpsnooping pkt-trace ipv6
```

Acquisizione pacchetti percorso CPU

Confermare l'arrivo dei pacchetti di snooping DHCP e lasciare correttamente il control plane.

 Nota: per ulteriori informazioni sull'utilizzo dello strumento di acquisizione CPU driver motore di inoltro, consultare la sezione Ulteriori informazioni.

```
<#root>
```

```
debug platform software fed
```

```
[switch<num|active|standby>]
```

```
punt/inject
```

```
packet-capture start
```

```
debug platform software fed
```

```
[switch<num|active|standby>]
```

```
punt/inject
```

```
packet-capture stop
```

```
show platform software fed
```

```
[switch<num|active|standby>]
```

```
punt/inject
```

```
packet-capture brief
```

```
### PUNT ###
```

```
DISCOVER
```

```
----- Punt Packet Number: 16, Timestamp: 2021/04/14 19:10:09.924 -----  
interface :
```

```
physical: FortyGigabitEthernet1/0/2
```

```
[if-id: 0x0000000a], pa1: FortyGigabitEthernet1/0/2 [if-id: 0x0000000a]  
metadata : cause: 79
```

```
[dhcp snoop],
```

```
sub-cause: 11, q-no: 17, linktype: MCP_LINK_TYPE_IP [1]  
ether hdr : dest mac: ffff.ffff.ffff,
```

```
src mac: 00a3.d144.2046
```

ether hdr : ethertype: 0x0800 (IPv4)
ipv4 hdr : dest ip: 255.255.255.255, src ip: 0.0.0.0
ipv4 hdr : packet len: 347, ttl: 255, protocol: 17 (UDP)
udp hdr : dest port:

67

, src port:

68

OFFER

----- Punt Packet Number: 23, Timestamp: 2021/04/14 19:10:11.926 -----
interface :

physical: FortyGigabitEthernet1/0/10

[if-id: 0x00000012], pa1: FortyGigabitEthernet1/0/10 [if-id: 0x00000012]
metadata : cause: 79

[dhcp snoop]

, sub-cause: 11, q-no: 17, linktype: MCP_LINK_TYPE_IP [1]
ether hdr : dest mac: ffff.ffff.ffff,

src mac: 701f.539a.fe46

ether hdr : vlan: 10, ethertype: 0x8100
ipv4 hdr : dest ip: 255.255.255.255,

src ip: 10.0.0.1

ipv4 hdr : packet len: 330, ttl: 255, protocol: 17 (UDP)
udp hdr : dest port:

68

, src port:

67

REQUEST

----- Punt Packet Number: 24, Timestamp: 2021/04/14 19:10:11.927 -----
interface :

physical: FortyGigabitEthernet1/0/2

[if-id: 0x0000000a], pa1: FortyGigabitEthernet1/0/2 [if-id: 0x0000000a]
metadata : cause: 79

[dhcp snoop]

, sub-cause: 11, q-no: 17, linktype: MCP_LINK_TYPE_IP [1]
ether hdr : dest mac: ffff.ffff.ffff,

src mac: 00a3.d144.2046

ether hdr : ethertype: 0x0800 (IPv4)
ipv4 hdr : dest ip: 255.255.255.255, src ip: 0.0.0.0
ipv4 hdr : packet len: 365, ttl: 255, protocol: 17 (UDP)
udp hdr : dest port:

67

, src port:

68

ACK

----- Punt Packet Number: 25, Timestamp: 2021/04/14 19:10:11.929 -----
interface :

physical: FortyGigabitEthernet1/0/10

[if-id: 0x00000012], pal: FortyGigabitEthernet1/0/10 [if-id: 0x00000012]
metadata : cause: 79

[dhcp snoop]

, sub-cause: 11, q-no: 17, linktype: MCP_LINK_TYPE_IP [1]
ether hdr : dest mac: ffff.ffff.ffff,

src mac: 701f.539a.fe46

ether hdr : vlan: 10, ethertype: 0x8100
ipv4 hdr : dest ip: 255.255.255.255,
src ip: 10.0.0.1

ipv4 hdr : packet len: 330, ttl: 255, protocol: 17 (UDP)
udp hdr : dest port:

68

, src port:

67

INJECT

DISCOVER

----- Inject Packet Number: 33, Timestamp: 2021/04/14 19:53:01.273 -----
interface : pal:

FortyGigabitEthernet1/0/2

[if-id: 0x0000000a]
metadata : cause: 25 [Layer2 frame to BD], sub-cause: 1, q-no: 0, linktype: MCP_LINK_TYPE_IP [1]
ether hdr : dest mac: ffff.ffff.ffff,

src mac: 00a3.d144.2046

ether hdr : ethertype: 0x0800 (IPv4)
ipv4 hdr : dest ip: 255.255.255.255, src ip: 0.0.0.0
ipv4 hdr : packet len: 347, ttl: 255, protocol: 17 (UDP)
udp hdr : dest port:

67

, src port:

68

OFFER

----- Inject Packet Number: 51, Timestamp: 2021/04/14 19:53:03.275 -----
interface : pal:

FortyGigabitEthernet1/0/2

[if-id: 0x0000000a]
metadata : cause: 1 [L2 control/legacy], sub-cause: 0, q-no: 0, linktype: MCP_LINK_TYPE_LAYER2 [10]
ether hdr : dest mac: ffff.ffff.ffff,

src mac: 701f.539a.fe46

ether hdr : ethertype: 0x0800 (IPv4)
ipv4 hdr : dest ip: 255.255.255.255,

src ip: 10.0.0.1

ipv4 hdr : packet len: 330, ttl: 255, protocol: 17 (UDP)
udp hdr : dest port:

68,

src port:

67

REQUEST

----- Inject Packet Number: 52, Timestamp: 2021/04/14 19:53:03.276 -----
interface : pal:

FortyGigabitEthernet1/0/2

[if-id: 0x0000000a]
metadata : cause: 25 [Layer2 frame to BD], sub-cause: 1, q-no: 0, linktype: MCP_LINK_TYPE_IP [1]
ether hdr : dest mac: ffff.ffff.ffff,

src mac: 00a3.d144.2046

```
ether hdr : ethertype: 0x0800 (IPv4)
ipv4 hdr : dest ip: 255.255.255.255, src ip: 0.0.0.0
ipv4 hdr : packet len: 365, ttl: 255, protocol: 17 (UDP)
udp hdr : dest port:
```

67

, src port:

68

ACK

```
----- Inject Packet Number: 53, Timestamp: 2021/04/14 19:53:03.278 -----
interface : pal:
```

FortyGigabitEthernet1/0/2

[if-id: 0x0000000a]

```
metadata : cause: 1 [L2 control/legacy], sub-cause: 0, q-no: 0, linktype: MCP_LINK_TYPE_LAYER2 [10]
ether hdr : dest mac: ffff.ffff.ffff,
```

src mac: 701f.539a.fe46

```
ether hdr : ethertype: 0x0800 (IPv4)
ipv4 hdr : dest ip: 255.255.255.255,
```

src ip: 10.0.0.1

```
ipv4 hdr : packet len: 330, ttl: 255, protocol: 17 (UDP)
udp hdr : dest port:
```

68

, src port:

67

Tracce utili

Tracce binarie che visualizzano eventi per processo o componente. In questo esempio, le tracce mostrano informazioni sul componente dhcpdn.

- Le tracce possono essere ruotate manualmente, il che significa che è possibile creare un nuovo file prima di iniziare a risolvere il problema in modo che contenga informazioni più nitide.

```
<#root>
```

```
9500#
```

```
request platform software trace rotate all
```

9500#

set platform software trace fed [switch

] dhcpcn verbose

c9500#show logging proc fed internal | inc dhcp

<<----- DI_Handle must match with the output which retrieves the DI handle

2021/04/14 19:24:19.159536 {fed_F0-0}{1}: [dhcpcn] [17035]: (info):

VLAN event on vlan 10, enabled 1

2021/04/14 19:24:19.159975 {fed_F0-0}{1}: [dhcpcn] [17035]: (debug): Program trust ports for this vlan

2021/04/14 19:24:19.159978 {fed_F0-0}{1}: [dhcpcn] [17035]: (debug):

GPN (10) if_id (0x0000000000000012) <<----- if_id must match with the TRUSTED port

2021/04/14 19:24:19.160029 {fed_F0-0}{1}: [dhcpcn] [17035]: (debug): trusted_if_q size=1 for vlan=10

2021/04/14 19:24:19.160041 {fed_F0-0}{1}: [dhcpcn] [17035]: (ERR): update ri has failed vlanid[10]

2021/04/14 19:24:19.160042 {fed_F0-0}{1}: [dhcpcn] [17035]: (debug): vlan mode changed to enable

2021/04/14 19:24:27.507358 {fed_F0-0}{1}: [dhcpcn] [23451]: (debug): get di for vlan_id 10

2021/04/14 19:24:27.507365 {fed_F0-0}{1}: [dhcpcn] [23451]: (debug): Allocated rep_ri for vlan_id 10

2021/04/14 19:24:27.507366 {fed_F0-0}{1}: [inject] [23451]: (verbose): Changing di_handle from 0x7f7fac

0x7f7fac23e438

by dhcp snooping

2021/04/14 19:24:27.507394 {fed_F0-0}{1}: [inject] [23451]: (debug): TX: getting REP RI from dhcpcn fai

2021/04/14 19:24:29.511774 {fed_F0-0}{1}: [dhcpcn] [23451]: (debug): get di for vlan_id 10

2021/04/14 19:24:29.511780 {fed_F0-0}{1}: [dhcpcn] [23451]: (debug): Allocated rep_ri for vlan_id 10

2021/04/14 19:24:29.511780 {fed_F0-0}{1}: [inject] [23451]: (verbose): Changing di_handle from 0x7f7fac

0x7f7fac23e438

by dhcp snooping

2021/04/14 19:24:29.511802 {fed_F0-0}{1}: [inject] [23451]: (debug): TX: getting REP RI from dhcpcn fai

c9500#set platform software trace fed [switch

```
] asic_app verbose
```

```
c9500#show logging proc fed internal | inc dhcp
```

```
2021/04/14 20:13:56.742637 {fed_F0-0}{1}: [dhcpsn] [17035]: (info):
```

```
VLAN event on vlan 10
```

```
, enabled 0
```

```
2021/04/14 20:13:56.742783 {fed_F0-0}{1}: [dhcpsn] [17035]: (debug): vlan mode changed to disable
```

```
2021/04/14 20:14:13.948214 {fed_F0-0}{1}: [dhcpsn] [17035]: (info): VLAN event on vlan 10, enabled 1
```

```
2021/04/14 20:14:13.948686 {fed_F0-0}{1}: [dhcpsn] [17035]: (debug):
```

```
Program trust ports for this vlan
```

```
2021/04/14 20:14:13.948688 {fed_F0-0}{1}: [dhcpsn] [17035]: (debug):
```

```
GPN (10) if_id (0x0000000000000012) <<---- if_id must match with the TRUSTED port
```

```
2021/04/14 20:14:13.948740 {fed_F0-0}{1}: [dhcpsn] [17035]: (debug): trusted_if_q size=1 for vlan=10
```

```
2021/04/14 20:14:13.948753 {fed_F0-0}{1}: [dhcpsn] [17035]: (ERR): update ri has failed vlanid[10]
```

```
2021/04/14 20:14:13.948754 {fed_F0-0}{1}: [dhcpsn] [17035]: (debug): vlan mode changed to enable
```

Suggested Traces

```
set platform software trace fed [switch<num|active|standby>] pm_tdl verbose
set platform software trace fed [switch<num|active|standby>] pm_vec verbose
set platform software trace fed [switch<num|active|standby>] pm_vlan verbose
```

INJECT

```
set platform software trace fed [switch<num|active|standby>] dhcpsn verbose
set platform software trace fed [switch<num|active|standby>] asic_app verbose
set platform software trace fed [switch<num|active|standby>] inject verbose
```

PUNT

```
set platform software trace fed [switch<num|active|standby>] dhcpsn verbose
set platform software trace fed [switch<num|active|standby>] asic_app verbse
set platform software trace fed [switch<num|active|standby>] punt ver
```

Syslog e spiegazioni

Violazioni dei limiti di velocità DHCP.

Spiegazione: lo snooping DHCP ha rilevato una violazione del limite di velocità del pacchetto DHCP sull'interfaccia specificata.

```
%DHCP_SNOOPING-4-DHCP_SNOOPING_ERRDISABLE_WARNING: DHCP Snooping received 300 DHCP packets on interface  
%DHCP_SNOOPING-4-DHCP_SNOOPING_RATE_LIMIT_EXCEEDED: The interface Fa0/2 is receiving more than the three
```

Spoofing del server DHCP su una porta non attendibile.

Spiegazione:La funzionalità di snooping DHCP ha individuato alcuni tipi di messaggi DHCP non consentiti sull'interfaccia non attendibile. Ciò indica che alcuni host stanno tentando di agire come server DHCP.

```
%DHCP_SNOOPING-5-DHCP_SNOOPING_UNTRUSTED_PORT: DHCP_SNOOPING drop message on untrusted port, message ty
```

L'indirizzo MAC di layer 2 non corrisponde all'indirizzo MAC nella richiesta DHCP.

Spiegazione: La funzionalità di snooping DHCP ha tentato la convalida dell'indirizzo MAC e il controllo non è riuscito. L'indirizzo MAC di origine nell'intestazione Ethernet non corrisponde all'indirizzo nel campo chaddr del messaggio di richiesta DHCP. È possibile che un host dannoso tenti di eseguire un attacco Denial of Service sul server DHCP.

```
%DHCP_SNOOPING-5-DHCP_SNOOPING_MATCH_MAC_FAIL: DHCP_SNOOPING drop message because the chaddr doesn't ma
```

Opzione 82 - Problema di inserimento.

Spiegazione: La funzionalità di snooping DHCP ha rilevato un pacchetto DHCP con valori di opzione non consentiti sulla porta non attendibile. Questo indica che alcuni host stanno tentando di fungere da relay o server DHCP.

```
%DHCP_SNOOPING-5-DHCP_SNOOPING_NONZERO_GIADDR: DHCP_SNOOPING drop message with non-zero giaddr or optio
```

Indirizzo MAC di layer 2 ricevuto su porta errata.

Spiegazione: La funzionalità di snooping DHCP ha rilevato un host che sta tentando di eseguire

un attacco Denial of Service su un altro host della rete.

%DHCP_SNOOPING-5-DHCP_SNOOPING_FAKE_INTERFACE: DHCP_SNOOPING drop message with mismatched source interf

Messaggi DHCP ricevuti sull'interfaccia non attendibile.

Spiegazione:La funzionalità di snooping DHCP ha individuato alcuni tipi di messaggi DHCP non consentiti sull'interfaccia non attendibile. Ciò indica che alcuni host stanno tentando di agire come server DHCP.

%DHCP_SNOOPING-5-DHCP_SNOOPING_UNTRUSTED_PORT: DHCP_SNOOPING drop message on untrusted port: GigabitEth

Trasferimento snooping DHCP non riuscito. Impossibile accedere all'URL.

Spiegazione: trasferimento binding snooping DHCP non riuscito.

%DHCP_SNOOPING-4-AGENT_OPERATION_FAILED: DHCP snooping binding transfer failed. Unable to access URL

Avvisi sullo snooping DHCP


| Numero ID bug Cisco | Descrizione |
|----------------------------|--|
| CSCvi3920 | DHCP non riesce quando il trust di snooping DHCP è abilitato su uplink etherchannel. |
| CSCvp49518 | Il database dello snooping DHCP non viene aggiornato dopo il ricaricamento. |
| CSCvk16813 | Traffico client DHCP interrotto con snooping DHCP e uplink port-channel o cross-stack. |
| CSCvd51480 | Rimozione del binding dallo snooping ip dhcp e dalla traccia dei dispositivi. |
| CSCvm5401 | Lo snooping DHCP può eliminare i pacchetti dell'opzione 82 dhcp con l'opzione |

| | |
|----------------------------|--|
| | ip dhcp snooping information allow-untrusted. |
| CSCvx25841 | Lo stato di attendibilità dello snooping DHCP si interrompe quando il segmento REP viene modificato. |
| CSCvs15759 | Il server DHCP invia un pacchetto NAK durante il processo di rinnovo DHCP. |
| CSCvk34927 | Tabella snooping DHCP non aggiornata dal file DB di snooping DHCP al momento del ricaricamento. |

Snooping DHCP bordo SDA

CLI statistiche snooping DHCP.

Nuova CLI disponibile per SDA per verificare le statistiche dello snooping DHCP.

 Nota: per ulteriori riferimenti su processo DHCP/flusso di pacchetti e decodifica Cisco SD-Access Fabric Edge, consultare la guida nella sezione Informazioni correlate.

```
switch#show platform fabric border dhcp snooping statistiche ipv4
```

```
switch#show platform fabric border dhcp snooping ipv6 statistiche
```

<#root>

SDA-9300-BORDER#

```
show platform fabric border dhcp snooping ipv4 statistics
```

| Timestamp | Source IP | Destination IP | Source Remote Locator | Lisp Instance ID | VLAN | PROCESS |
|---------------------|------------|----------------|-----------------------|------------------|------|---------|
| 08-05-2019 00:24:16 | 10.30.30.1 | 10.40.40.1 | 192.168.0.1 | 8189 | 88 | 10 |
| 08-05-2019 00:24:16 | 10.30.30.1 | 10.40.40.1 | 192.168.0.1 | 8189 | 88 | 11 |

SDA-9300-BORDER#

```
show platform fabric border dhcp snooping ipv6 statistics
```

| Timestamp | Source IP | Destination IP | Source Remote Locator | Lisp Instance |
|---------------------|------------------------|------------------------|-----------------------|---------------|
| 08-05-2019 00:41:46 | 11:11:11:11:11:11:11:1 | 22:22:22:22:22:22:22:1 | 192.168.0.3 | 8089 |
| 08-05-2019 00:41:47 | 11:11:11:11:11:11:11:1 | 22:22:22:22:22:22:22:1 | 192.168.0.3 | 8089 |

Informazioni correlate

[Guida alla configurazione dei servizi di indirizzamento IP, Cisco IOS XE Amsterdam 17.3.x \(switch Catalyst 9200\)](#)

[Guida alla configurazione dei servizi di indirizzamento IP, Cisco IOS XE Amsterdam 17.3.x \(switch Catalyst 9300\)](#)

[Guida alla configurazione dei servizi di indirizzamento IP, Cisco IOS XE Amsterdam 17.3.x \(switch Catalyst 9400\)](#)

[Guida alla configurazione dei servizi di indirizzamento IP, Cisco IOS XE Amsterdam 17.3.x \(switch Catalyst 9500\)](#)

[Guida alla configurazione dei servizi di indirizzamento IP, Cisco IOS XE Amsterdam 17.3.x \(switch Catalyst 9600\)](#)

[Cisco SD-Access Fabric Edge - Processo DHCP/flusso pacchetti e decodifica](#)

[Configurazione dell'acquisizione di pacchetti CPU FED sugli switch Catalyst 9000](#)

[Documentazione e supporto tecnico – Cisco Systems](#)

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).