

# Funcionamiento y solución de problemas de detección DHCP en switches Catalyst 9000

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Snooping DHCP](#)

[Operación DHCP Snooping](#)

[Topología](#)

[Configurar](#)

[Verificación](#)

[Troubleshoot](#)

[Solucionar problemas de software](#)

[Solución de problemas de tráfico de ruta/punto \(CPU\)](#)

[Solucionar problemas de hardware](#)

[Captura de paquetes de ruta de CPU](#)

[Seguimientos útiles](#)

[Registros del sistema y explicaciones](#)

[Advertencias de indagación DHCP](#)

[Detección DHCP de frontera SDA](#)

[Información Relacionada](#)

## Introducción

Este documento describe cómo operar y resolver problemas de DHCP Snooping en los switches Catalyst 9000 Series

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Arquitectura de switches Catalyst serie 9000
- Arquitectura de software Cisco IOS® XE

### Componentes Utilizados

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

- C9200
- C9300
- C9400
- C9500
- C9600

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.

---

**Nota:** Consulte la guía de configuración correspondiente para conocer los comandos que se utilizan para habilitar estas funciones en otras plataformas de Cisco.

---

## Antecedentes

### Snooping DHCP

El snooping del protocolo de configuración dinámica de host (DHCP) es una función de seguridad que se utiliza para comprobar el tráfico DHCP y bloquear cualquier paquete DHCP malintencionado. Actúa como un firewall entre los puertos de usuario no fiables y los puertos del servidor DHCP de la red para evitar servidores DHCP malintencionados en la red, ya que puede provocar una denegación de servicio.

### Operación DHCP Snooping

El snooping de DHCP funciona con el concepto de interfaces fiables y no fiables. A través de la trayectoria del tráfico DHCP, el switch verifica los paquetes DHCP recibidos en las interfaces y realiza un seguimiento de los paquetes de servidor DHCP esperados (OFFER & ACK) sobre interfaces confiables. En otras palabras, las interfaces no confiables bloquean los paquetes del servidor DHCP.

Los paquetes DHCP se bloquean en interfaces no fiables.

- Se recibe un paquete de un servidor DHCP, como un paquete DHCPOFFER, DHCPACK, DHCPNAK o DHCPLEASEQUERY, desde fuera de la red o firewall. Esto evita que un servidor DHCP no autorizado ataque a la red en puertos no fiables.
- Un paquete recibido en una interfaz no confiable y la dirección MAC de origen y la dirección de hardware del cliente DHCP no coinciden. Esto evita la suplantación de paquetes DHCP de un cliente no autorizado que podría crear un ataque de denegación de servicio en un servidor DHCP.
- Mensaje de difusión DHCPRELEASE o DHCPDECLINE que tiene una dirección MAC en la base de datos de enlace de snooping DHCP, pero la información de interfaz de la base de datos de enlace no coincide con la interfaz en la que se recibió el mensaje. Esto evita ataques de denegación de servicio en los clientes.
- Un paquete DHCP reenviado por un agente de retransmisión DHCP que incluye una dirección IP de agente de retransmisión que no es 0.0.0.0, o el agente de retransmisión reenvía un paquete que incluye información de la opción 82 a un puerto no confiable. Esto evita la suplantación de la información del agente relay en la red.

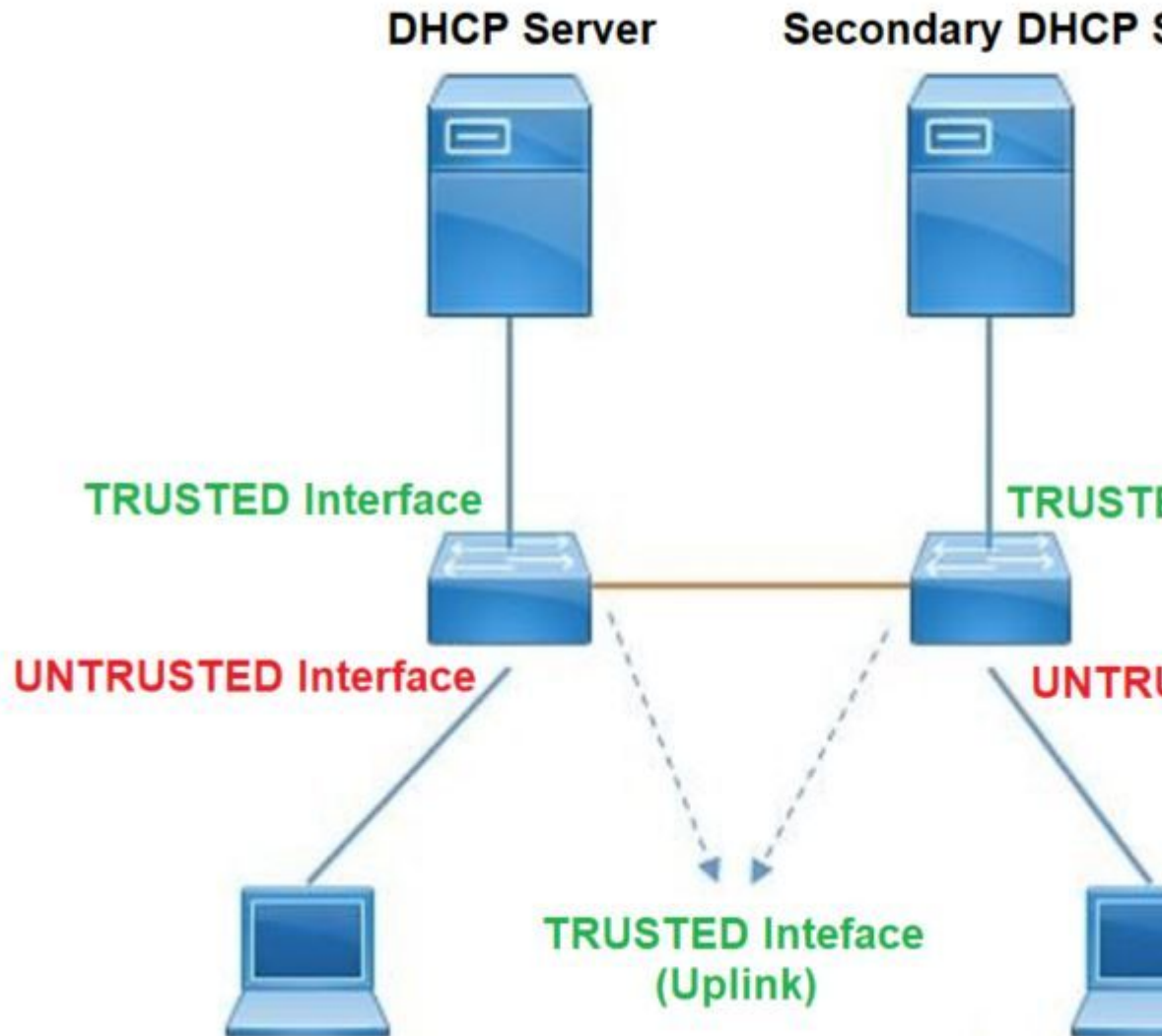
El switch en el que se configura la indagación DHCP crea una tabla de indagación DHCP o una base de datos de enlace DHCP. Esta tabla se utiliza para realizar un seguimiento de las direcciones IP asignadas desde un servidor DHCP legítimo. La base de datos de enlace también la utilizan otras funciones de seguridad del IOS, como Dynamic ARP Inspection e IP Source Guard.

---

**Nota:** Para permitir que la detección DHCP funcione correctamente, asegúrese de que confía en todos los puertos de enlace ascendente para alcanzar el servidor DHCP y desconfíe de los puertos del

---

## Topología



## Configurar

Configuración global

```
<#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:** Para permitir los paquetes de la opción 82, debe habilitar la **opción ip dhcp snooping information option allow-untrusted**.

---

## Verificación

Confirme si DHCP Snooping está habilitado en la VLAN deseada y asegúrese de que las interfaces fiables y no fiables estén bien enumeradas. Si hay una velocidad configurada, asegúrese de que también se muestra.

```
<#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:

Una vez que los usuarios reciben una dirección IP por DHCP, aparecen en esta salida.

- El snooping de DHCP elimina la entrada de la base de datos cuando caduca la concesión de la dirección IP o cuando el switch recibe un mensaje DHCPRELEASE del host.
- Asegúrese de que la información indicada para la dirección MAC del usuario final es correcta.

<#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
```

Esta tabla enumera los diversos comandos que se pueden utilizar para monitorear la información de DHCP Snooping.

Comando	Propósito
<b>show ip dhcp snooping binding</b> <b>show ip dhcp snooping binding</b> [IP-address] [MAC-address] [interface ethernet slot/port] [vlan-id]	Muestra sólo los enlaces configurados dinámicamente en la base de datos de enlace de snooping DHCP, también denominada tabla de enlace.  - Dirección IP de entrada de enlace - Entrada de enlace Dirección Mac - Interfaz de entrada de enlace - VLAN de entrada de enlace
<b>show ip dhcp snooping database</b>	Muestra el estado y las estadísticas de la base de datos de enlace de snooping DHCP.
<b>show ip dhcp snooping statistics</b>	Muestra las estadísticas de snooping de DHCP en forma resumida o detallada.
<b>show ip source binding</b>	Mostrar los enlaces configurados dinámica y estáticamente.
<b>show interface vlan xyz</b> <b>show buffer input-interface Vlan xyz dump</b>	El paquete DHCP se envía al agente de retransmisión configurado en la vlan del cliente a través de la SVI de la vlan del cliente. Si la cola de entrada muestra el límite máximo de descarte o alcance, es probable que el paquete dhcp del cliente se haya descartado y no haya podido alcanzar el agente de retransmisión configurado.  <b>Nota:</b> Asegúrese de que no se vean caídas en la cola de entrada.  switch# <b>show int vlan 670</b>

	<p>Carga durante cinco segundos: 13%/0%; un minuto: 10%; cinco minutos: 10%</p> <p>La fuente horaria es NTP, 18:39:52.476 UTC Jue Sep 10 2020</p> <p>Vlan670 está activo, el protocolo de línea está activo, Autostate habilitado</p> <p>El hardware es Ethernet SVI, la dirección es 00fd.227a.5920 (bia 00fd.227a.5920)</p> <p>Descripción: ion_media_client</p> <p>La dirección de Internet es 10.27.49.254/23</p> <p>MTU 1500 bytes, BW 1000000 Kbits/seg, DLY 10 usec, reliability 255/255, txload 1/255, rxload 1/255</p> <p>Encapsulación ARPA, loopback no configurado</p> <p>Keepalive no compatible</p> <p>Tipo ARP: ARPA, tiempo de espera ARP 04:00:00</p> <p>Última entrada 03:01:29, salida 00:00:02, salida bloqueada nunca</p> <p>Último borrado de contadores "show interface" nunca</p> <p><b>Cola de entrada: 375/375/4020251/0</b> (tamaño/máximo/caídas/vaciados); caídas de salida totales: 0</p> <p><b>Se han descartado 375 paquetes en la entrada de la cola / 4020251</b></p>
--	---

## Troubleshoot

### Solucionar problemas de software

Verifique lo que recibe el switch. Estos paquetes se procesan en el plano de control de la CPU, así que asegúrese de ver todos los paquetes en la dirección de inyección y punteo, y confirme si la información es correcta.

---

**Precaución:** utilice los comandos debug con precaución. Tenga en cuenta que muchos comandos debug tienen impacto en la red activa y solo se recomiendan para su uso en un entorno de laboratorio cuando se reproduce el problema.

---

La característica Depuración condicional permite habilitar selectivamente depuraciones y registros para características específicas basadas en un conjunto de condiciones definidas. Esto es útil para contener información de depuración sólo para hosts o tráfico específicos.

Una condición se refiere a una función o identidad, donde la identidad podría ser una interfaz, una dirección IP o una dirección MAC, etc..

Cómo habilitar la depuración condicional para depuraciones de paquetes y eventos para solucionar problemas de detección DHCP.

Comando	Propósito
<p><b>debug condition mac</b> &lt;mac-address&gt;</p> <p>Ejemplo:</p>	<p>Configura la depuración condicional para la dirección MAC especificada.</p>



switch# <b>debug condition mac bc16.6509.3314</b>	
<b>debug condition vlan &lt;VLAN Id&gt;</b> Ejemplo: switch# <b>debug condition vlan 10</b>	Configura la depuración condicional para la VLAN especificada.
<b>debug condition interface &lt;interface&gt;</b> Ejemplo: switch# <b>debug condition interface TwentyFiveGigE 1/0/8</b>	Configura la depuración condicional para la interfaz especificada.

Para depurar DHCP Snooping, utilice los comandos que se muestran en la tabla.

Comando	Propósito
<b>debug dhcp</b> [detail   oper   redundancia]	<b>detail</b> DHCP packet content <b>oper</b> DHCP internal OPER <b>redundancy</b> DHCP client redundancy support
<b>debug ip dhcp server packet detail</b>	Decodificar las recepciones de mensajes y la transmisión en detalle
<b>debug ip dhcp server events</b>	Informar sobre asignaciones de direcciones, vencimiento de concesiones, etc.
<b>debug ip dhcp snooping agent</b>	Debug dhcp snooping database read and write
<b>debug ip dhcp snooping event</b>	Evento de depuración entre cada componente
<b>debug ip dhcp snooping packet</b>	Debug DHCP packet in dhcp snooping module

Este es un ejemplo parcial del resultado 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 flooded

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: DHCP REQUEST, 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 (FortyGigabitEthernet1/0/10)

Apr 14 16:16:48.840: DHCP\_SNOOPING: process new DHCP packet,

message type: DHCP ACK, 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.

Para depurar eventos de detección DHCP, siga estos pasos:

**Precaución:** utilice los comandos debug con precaución. Tenga en cuenta que muchos **comandos debug** tienen impacto en la red activa y solo se recomiendan para su uso en un entorno de laboratorio cuando se reproduce el problema.

#### Pasos de resumen

1. enable
2. debug platform condition mac { mac-address }
3. debug platform condition start
4. show platform condition OR show debug
5. debug platform condition stop
6. show platform software trace message ios R0 reverse | include DHCP
7. clear platform condition all

#### PASOS DETALLADOS

	Comando o acción	Propósito
Paso 1	<b>enable</b> Ejemplo: switch# <b>enable</b>	Habilita el modo EXEC privilegiado. <ul style="list-style-type: none"><li>• Ingrese su contraseña si se le pide que lo haga.</li></ul>
Paso 2	<b>debug platform condition mac</b> { mac-address } Ejemplo: switch# <b>debug platform condition mac 0001.6509.3314</b>	Configura la depuración condicional para la dirección MAC especificada.
Paso 3	<b>debug platform condition start</b> Ejemplo: switch# <b>debug platform condition start</b>	Inicia la depuración condicional (esto puede iniciar el seguimiento radioactivo si hay una coincidencia en una de las condiciones).
Paso 4	<b>show platform condition</b> OR <b>show debug</b> Ejemplo: switch# <b>show platform condition</b> switch# <b>show debug</b>	Muestra el conjunto de condiciones actuales.
Paso 5	<b>debug platform condition stop</b> Ejemplo:	Detiene la depuración condicional (esto puede detener el seguimiento

	Comando o acción	Propósito
	switch# <b>debug platform condition stop</b>	radiactivo).
Paso 6	<b>show platform software trace message ios R0 reverse   include DHCP</b> Ejemplo: switch# <b>show platform software trace message ios R0 reverse   include DHCP</b>	Muestra los registros de HP combinados a partir del archivo de seguimiento más reciente.
Paso 7	<b>clear platform condition all</b> Ejemplo: switch# <b>clear platform condition all</b>	Borra todas las condiciones.

Este es un ejemplo parcial de salida de ejemplo de la **dplataforma de depuración comando 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{mac})
```

```
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{mac})
```

```
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\_...  
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

#### 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.

#### ACK

Apr 14 16:44:24.640: dhcp packet 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 vlan 10dhcp pkt processi

Esta tabla enumera los diversos comandos que se pueden utilizar para depurar DHCP Snooping en la plataforma.

**Precaución:** utilice los comandos debug con precaución. Tenga en cuenta que muchos comandos debug tienen un impacto en la red activa, y solo se recomiendan para su uso en un entorno de laboratorio cuando se reproduce el problema.

Comando	Propósito
switch# <b>debug platform dhcp-snoop [all   paquete   pd-shim]</b>	<b>all</b> NGWC DHCP Snooping <b>packet</b> NGWC DHCP Snooping Packet Debug Info <b>pd-shim</b> NGWC DHCP Snooping IOS Shim Debug Info
switch# <b>debug platform software infrastructure punt dhcp-snoop</b>	Paquetes recibidos en el FP que se envían al plano de control)
switch# <b>debug platform software infrastructure inject</b>	Paquetes inyectados en el FP desde el plano de control

## Solución de problemas de tráfico de ruta/punto (CPU)

Verifique desde la perspectiva de la FED qué tráfico se recibe en cada cola de la CPU (la detección DHCP es un tipo de tráfico que procesa el plano de control).

- Cuando el tráfico entra en el switch, se envía a la CPU en la dirección PUNT y se envía a la cola de

**snoop dhcp.**

- Una vez que el tráfico es procesado por el switch, el tráfico sale a través de la dirección INJECT. Los paquetes de OFERTA DHCP y ACK caen en la cola de control/heredada 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	<<---- If drop counter increases, there can be a
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		<<---- dropped counter must NOT increase
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	

Puede utilizar este comando para confirmar el tráfico que se dirige a la CPU y verificar si la detección de DHCP descarta tráfico.

<#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 <<---- 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

```

---

## Solucionar problemas de hardware

### Controlador de motor de reenvío (FED)

La FED es el controlador que programa el ASIC. Los comandos FED se utilizan para verificar que los estados de hardware y software coinciden.

Obtenga el valor DI\_Handle

- El identificador de ID hace referencia al índice de destino para un puerto específico.

<#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
```

Verifique la asignación de ifm para determinar el Asic y el Núcleo de los puertos.

- IFM es un índice de interfaz interna asignado a un puerto/núcleo/básico específico.

<#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
```

Utilice DI\_Handle para obtener el índice de 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/l3u_ri_index0:0x0 index1:0x5f03 mtu_index/l3u_ri_index1:0x0 index2:0x5f03 mtu_index/l3u_ri_index2:0x0
<SNIP>
```

```
<-- Index is 0x5f03
```

Convierta de hexadecimal el valor de índice 0x5f03 a decimal.



0x5f03 = 24323

Utilice este valor de índice en decimal y los valores ASIC y Core en este comando para ver qué indicadores se establecen para el puerto.

<#root>

```
c9500#show platform hardware fed switch 1 fwd-asic regi read register-name SifDestinationIndexTable-24323
```

```
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
```

Asegúrese de que DHCP Snooping esté habilitado para la VLAN específica.

<#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	0x00000000000420011				
----	---------------------	--	--	--	--

```
0x00007f7fac235fa8
```

0x00007f7fac236798	0x0000000000000000	0x0000000000000000	15
--------------------	--------------------	--------------------	----



```

LEAD_VLAN_EGRESS_VLAN_CLIENT_LABEL value 0 Pass
LEAD_VLAN_EGRESS_VLAN_ID_VALID value 1 Pass
LEAD_VLAN_EGRESS_VLAN_LOAD_BALANCE_GROUP value 15 Pass
LEAD_VLAN_EGRESS_INTRA_POD_BCAST value 0 Pass

LEAD_VLAN_EGRESS_DHCP_SNOOPING_ENABLED_IPV4 value 1 Pass

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>

```

Esta tabla enumera los diversos comandos comunes de Punct show/debug que se pueden utilizar para rastrear la trayectoria del paquete DHCP en una red activa.

### Comandos comunes Punct / Inject show & debug

```
debug plat soft fed swit acti 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 " " > use filter cpmand  
show to scope the traces to this specific host
```

```
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>] inject cause summary
```

```
show platform software fed [switch<num|active|standby>] punct cause summary
```

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

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

```
show platform software fed [switch<num|active|standby>] active inject packet-capture det
```

```
show platform software infrastructure inject
```

```
show platform software infrastructure punct
```

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

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

```
debug platform software infra inject
```

Estos comandos son útiles para verificar si se recibe algún paquete DHCP para un cliente en particular.

- Esta función le permite capturar toda la comunicación de snooping DHCP asociada con una dirección MAC de cliente dada que es procesada por la CPU a través del software IOS-DHCP.
- Esta funcionalidad es compatible con el tráfico IPv4 e IPv6.

- Esta función se activa automáticamente.

**Importante:** estos comandos están disponibles en Cisco IOS XE Gibraltar 16.12.X.

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

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

<#root>

C9300#

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

DHCP SN: DHCP snooping server

DHCPD: DHCP protocol daemen

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

Utilice estos comandos para borrar el seguimiento.

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

```
switch#clear platform dhcp snooping pkt-trace ipv6
```

# Captura de paquetes de ruta de CPU

Confirme si los paquetes de indagación DHCP llegan y salen del plano de control correctamente.

---

**Nota:** Para obtener referencias adicionales sobre cómo utilizar la herramienta de captura de CPU del controlador del motor de reenvío, consulte la sección Lectura adicional.

---

```
<#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], pal: 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], 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

**REQUEST**

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

**physical: FortyGigabitEthernet1/0/2**

[if-id: 0x0000000a], pal: 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
```

## Seguimientos útiles

Estos son seguimientos binarios que muestran eventos por proceso o componente. En este ejemplo, los seguimientos muestran información sobre el componente dhcpcn.

- Los seguimientos se pueden girar manualmente, lo que significa que puede crear un nuevo archivo antes de comenzar a solucionar problemas para que contenga información más limpia.

```
<#root>
```

```
9500#
```

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

```
9500#
```

```
set platform software trace fed [switch
```

```
] dhcpsn 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}: [dhcpsn] [17035]: (info):
```

```
VLAN event on vlan 10, enabled 1
```

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

```
2021/04/14 19:24:19.159978 {fed_F0-0}{1}: [dhcpsn] [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}: [dhcpsn] [17035]: (debug): trusted_if_q size=1 for vlan=10
```

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

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

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

```
2021/04/14 19:24:27.507365 {fed_F0-0}{1}: [dhcpsn] [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 0x7f7fac3
```

```
0x7f7fac23e438
```

```
by dhcp snooping
```

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

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

```
2021/04/14 19:24:29.511780 {fed_F0-0}{1}: [dhcpsn] [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 0x7f7fac3
```

```
0x7f7fac23e438
```

```
by dhcp snooping
```

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

```
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
```

## Registros del sistema y explicaciones

Infracciones de los límites de velocidad DHCP.

Explicación: El snooping de DHCP detectó una violación del límite de velocidad del paquete DHCP en la interfaz especificada.

%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

Suplantación del servidor DHCP en un puerto no fiable.

Explicación: La función de snooping de DHCP detectó ciertos tipos de mensajes DHCP no permitidos en la interfaz no fiable, lo que indica que algún host está intentando actuar como servidor DHCP.

%DHCP\_SNOOPING-5-DHCP\_SNOOPING\_UNTRUSTED\_PORT: DHCP\_SNOOPING drop message on untrusted port, message type

La dirección MAC de capa 2 no coincide con la dirección MAC de la solicitud DHCP.

Explicación: La función de snooping DHCP intentó la validación de la dirección MAC y la comprobación falló. La dirección MAC de origen del encabezado Ethernet no coincide con la dirección del campo chaddr del mensaje de solicitud DHCP. Puede haber un host malintencionado que intente llevar a cabo un ataque de denegación de servicio en el servidor DHCP.

%DHCP\_SNOOPING-5-DHCP\_SNOOPING\_MATCH\_MAC\_FAIL: DHCP\_SNOOPING drop message because the chaddr doesn't match

Opción 82 problema de inserción.

Explicación: La función de snooping DHCP detectó un paquete DHCP con valores de opción no permitidos en el puerto no confiable, lo que indica que algún host está intentando actuar como servidor o relé DHCP.

%DHCP\_SNOOPING-5-DHCP\_SNOOPING\_NONZERO\_GIADDR: DHCP\_SNOOPING drop message with non-zero giaddr or option

Dirección MAC de capa 2 recibida en puerto incorrecto.

Explicación: La función de snooping de DHCP ha detectado un host que intenta llevar a cabo un ataque de denegación de servicio en otro host de la red.

%DHCP\_SNOOPING-5-DHCP\_SNOOPING\_FAKE\_INTERFACE: DHCP\_SNOOPING drop message with mismatched source interface

Mensajes DHCP recibidos en la interfaz no fiable.

Explicación: La función de snooping de DHCP detectó ciertos tipos de mensajes DHCP no permitidos en la interfaz no fiable, lo que indica que algún host está intentando actuar como servidor DHCP.

%DHCP\_SNOOPING-5-DHCP\_SNOOPING\_UNTRUSTED\_PORT: DHCP\_SNOOPING drop message on untrusted port: GigabitEth

Error en la transferencia de indagación DHCP. No se puede acceder a la URL.

Explicación: La transferencia de enlace de snooping DHCP falló.

%DHCP\_SNOOPING-4-AGENT\_OPERATION\_FAILED: DHCP snooping binding transfer failed. Unable to access URL

## Advertencias de indagación DHCP

Número de ID de bug de Cisco	Descripción
<a href="#">CSCvi39202</a>	El DHCP falla cuando la confianza de indagación DHCP está habilitada en el EtherChannel de link ascendente.
<a href="#">CSCvp49518</a>	La base de datos de detección DHCP no se actualiza después de la recarga.
<a href="#">CSCvk16813</a>	El tráfico del cliente DHCP se interrumpe con el snooping DHCP y los enlaces ascendentes de canal de puerto o entre pilas.
<a href="#">CSCvd51480</a>	Desenlace de ip dhcp snooping y device-tracking.
<a href="#">CSCvm55401</a>	El snooping DHCP puede descartar la opción dhcp 82 paquetes con la opción ip dhcp snooping information option allow-untrusted.
<a href="#">CSCvx25841</a>	El estado de confianza de snooping DHCP se interrumpe cuando hay cambios en el segmento REP.
<a href="#">CSCvs15759</a>	El servidor DHCP envía un paquete NAK durante el proceso de renovación de DHCP.
<a href="#">CSCvk34927</a>	La tabla de snooping DHCP no se actualizó desde el archivo DB de snooping DHCP al volver a cargar.

## Detección DHCP de frontera SDA

CLI de estadísticas de snooping DHCP.

Una nueva CLI disponible para SDA para verificar las estadísticas de snooping de DHCP.

**Nota:** Para obtener referencias adicionales sobre el proceso DHCP/flujo de paquetes y decodificación de Cisco SD-Access Fabric Edge, consulte la guía en la sección Información Relacionada.

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

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

<#root>

SDA-9300-BORDER#

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

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

## Información Relacionada

[Guía de configuración de IP Addressing Services, Cisco IOS XE Amsterdam 17.3.x \(switches Catalyst 9200\)](#)

[Guía de configuración de IP Addressing Services, Cisco IOS XE Amsterdam 17.3.x \(switches Catalyst 9300\)](#)

[Guía de configuración de IP Addressing Services, Cisco IOS XE Amsterdam 17.3.x \(switches Catalyst 9400\)](#)

[Guía de configuración de IP Addressing Services, Cisco IOS XE Amsterdam 17.3.x \(switches Catalyst 9500\)](#)

[Guía de configuración de IP Addressing Services, Cisco IOS XE Amsterdam 17.3.x \(switches Catalyst 9600\)](#)

[Proceso DHCP/Flujo de paquetes y decodificación de Cisco SD-Access Fabric Edge](#)

[Configuración de la captura de paquetes de CPU FED en switches Catalyst 9000](#)

[Soporte Técnico y Documentación - Cisco Systems](#)



## 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).