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

Contenido

Introducción

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

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

Cisco IOS® XE 16.12.X

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.

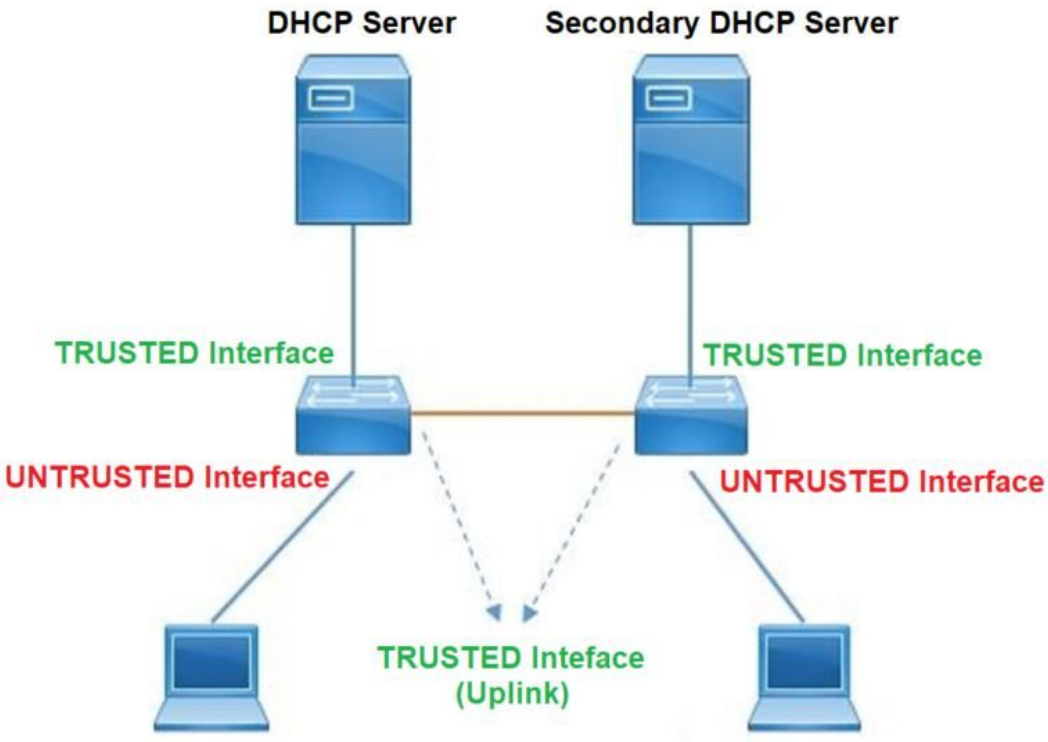
- Se recibe un paquete de un servidor DHCP, como un paquete DHCPOFFER, DHCPACK, DHCPNAK o DHCPLEASEQUERY, desde fuera de la red o firewall. Esto evita que un servidor DHCP no autorizado ataque a la red en puertos no fiables.
- Un paquete recibido en una interfaz no confiable y la dirección MAC de origen 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 usuario final.

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 a

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
show ip dhcp snooping binding show ip dhcp snooping binding [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 entrada de enlace - VLAN de entrada de enlace
show ip dhcp snooping database	Muestra el estado y las estadísticas de la base de datos de

	enlace de snooping DHCP.
show ip dhcp snooping statistics	Muestra las estadísticas de snooping de DHCP en forma resumida o detallada.
show ip source binding	Muestra los enlaces configurados dinámica y estáticamente.
show interface vlan xyz show buffer input-interface Vlan xyz dump	El paquete DHCP se envía al agente de retransmisión configurado en la VLAN del cliente a través de la VLAN SVI del cliente. Si la cola de entrada muestra el límite máximo de descarte o alcance, es probable que el paquete DHCP del cliente se descartó y no pudo alcanzar el agente de retransmisión configurado. Nota: Asegúrese de que no se vean caídas en la cola de entrada. switch#show int vlan 670 Carga durante cinco segundos: 13%/0%; un minuto: 10%; cinco minutos: 10% La fuente horaria es NTP, 18:39:52.476 UTC Jue Sep 10 2020 VLAN670 está activa, el protocolo de línea está activo, Autostate habilitado El hardware es Ethernet SVI, la dirección es 00fd.227a.5920 (bia 00fd.227a.5920) Descripción: ion_media_client La dirección de Internet es 10.27.49.254/23 MTU 1500 bytes, BW 1000000 Kbits/seg, DLY 10 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulación ARPA, loopback no configurado Keepalive no compatible Tipo ARP: ARPA, tiempo de espera ARP 04:00:00 Última entrada 03:01:29, salida 00:00:02, salida bloqueada nunca Último borrado de contadores "show interface" nunca Cola de entrada: 375/375/4020251/0 (tamaño/máx/caídas/vaciados); caídas de salida totales: 0 <— 375 paquetes en la entrada de la cola / 4020251 se han descartado

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 solamente 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 función de depuración condicional para depurar paquetes y eventos al solucionar problemas de detección DHCP.

Comando	Propósito
debug condition mac <mac-address> Ejemplo: switch#debug condition mac bc16.6509.3314	Configura la depuración condicional para la dirección MAC especificada.
debug condition vlan <VLAN Id> Ejemplo: switch#debug condition vlan 10	Configura la depuración condicional para la VLAN especificada.
debug condition interface <interface> Ejemplo: switch#debug condition interface TwentyFiveGigE 1/0/8	Configura la depuración condicional para la interfaz especificada.

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

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

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

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: DHCPOFFER, 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
```

```
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 replyto output port: FortyGigabitEthernet1/0/2.
Apr 14 16:16:48.838: DHCP_SNOOPING: received new DHCP packet from input interface (FortyGigabitEthernet
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
Apr 14 16:16:48.838: DHCP_SNOOPING: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is floo
Apr 14 16:16:48.839: DHCP_SNOOPING: received new DHCP packet from input interface (FortyGigabitEthernet

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:
Apr 14 16:16:48.840: DHCP_SNOOPING: add binding on port FortyGigabitEthernet1/0/2 ckt_id 0 FortyGigabit
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 replyto 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 | incluir DHCP
7. clear platform condition all

PASOS DETALLADOS

	Comando o acción	Propósito
Paso 1	enable Ejemplo: switch#enable	Habilita el modo EXEC privilegiado. • Ingrese su contraseña si se le pide que lo haga.
Paso 2	debug platform condition mac {mac-address} Ejemplo: switch#debug platform condition mac 0001.6509.3314	Configura la depuración condicional para la dirección MAC especificada.
Paso 3	debug platform condition start Ejemplo: switch#debug platform condition start	Inicia la depuración condicional (esto puede iniciar el seguimiento radioactivo si hay una coincidencia en una de las condiciones).
Paso 4	show platform condition OR show debug Ejemplo: switch#show platform condition switch#show debug	Muestra el conjunto de condiciones actuales.
Paso 5	debug platform condition stop Ejemplo: switch#debug platform condition stop	Detiene la depuración condicional (esto puede detener el seguimiento radiactivo).
Paso 6	show platform software trace message ios R0 reverse | incluir DHCP Ejemplo:	Muestra los registros de HP combinados a partir del archivo de seguimiento más reciente.

	Comando o acción	Propósito
	switch#show platform software trace message ios R0 reverse | incluir DHCP	
Paso 7	clear platform condition all Ejemplo: switch# clear platform condition all	Borra todas las condiciones.

Este es un ejemplo parcial de salida del ejemplo del comando debug platform 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(00
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
```

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_
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
Apr 14 16:44:24.637: sending dhcp packet out after processing with SMAC = 00a3.d144.2046{mac} and SRC_A
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 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 vlan 10dhcp pkt process
```

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#debug platform dhcp-snoop [all | paquete | pd-shim]	all NGWC DHCP Snooping packet NGWC DHCP Snooping Packet Debug Info pd-shim NGWC DHCP Snooping IOS Shim Debug Info
switch#debug platform software infrastructure punt dhcp-snoop	Paquetes que se reciben en el FP y que se envían al plano de control).
switch#debug platform software infrastructure inject	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.

```
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  |              Queue              |  Rx  |  Rx   |  Rx   |  Drop  |  Drop  |  Drop
no |              Name               | 10s  |  1min |  5min |  10s   |  1min  |  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 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_DHCPSNOOPI
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_i
<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-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
```

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      0x0000000000420011

0x00007f7fac235fa8

 0x00007f7fac236798  0x0000000000000000  0x0000000000000000  15
```

c9500#

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

0x00007f7fac235fa8 1 <<---- Last number might be 1 or 0, 1 means detailed, 0 means brief output

Handle:0x7f7fac235fa8 Res-Type:ASIC_RSC_VLAN_LE Res-Switch-Num:255 Asic-Num:255 Feature-ID:AL_FID_L2 Lk
priv_ri/priv_si Handle: (nil)Hardware Indices/Handles: index0:0xf mtu_index/l3u_ri_index0:0x0 sm handle
Cookie length: 56
00 00 00 00 00 00 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0

Detailed Resource Information (ASIC_INSTANCE# 0)

LEAD_VLAN_IGMP_MLD_SNOOPING_ENABLED_IPV4 value 1 Pass   <<---- Verify the highlighted values, if any are

LEAD_VLAN_IGMP_MLD_SNOOPING_ENABLED_IPV6 value 0 Pass

LEAD_VLAN_ARP_OR_ND_SNOOPING_ENABLED_IPV4 value 1 Pass

LEAD_VLAN_ARP_OR_ND_SNOOPING_ENABLED_IPV6 value 1 Pass
LEAD_VLAN_BLOCK_L2_LEARN value 0 Pass
LEAD_VLAN_CONTENT_MATCHING_ENABLED value 0 Pass
LEAD_VLAN_DEST_MOD_INDEX_TVLAN_LE value 0 Pass

LEAD_VLAN_DHCP_SNOOPING_ENABLED_IPV4 value 1 Pass

LEAD_VLAN_DHCP_SNOOPING_ENABLED_IPV6 value 1 Pass
LEAD_VLAN_ENABLE_SECURE_VLAN_LEARNING_IPV4 value 0 Pass
LEAD_VLAN_ENABLE_SECURE_VLAN_LEARNING_IPV6 value 0 Pass
LEAD_VLAN_EPOCH value 0 Pass
LEAD_VLAN_L2_PROCESSING_STP_TCN value 0 Pass
LEAD_VLAN_L2FORWARD_IPV4_MULTICAST_PKT value 0 Pass
LEAD_VLAN_L2FORWARD_IPV6_MULTICAST_PKT value 0 Pass
LEAD_VLAN_L3_IF_LE_INDEX_PRIO value 0 Pass
LEAD_VLAN_L3IF_LE_INDEX value 0 Pass
LEAD_VLAN_LOOKUP_VLAN value 15 Pass
LEAD_VLAN_MCAST_LOOKUP_VLAN value 15 Pass
LEAD_VLAN_RIET_OFFSET value 4095 Pass
LEAD_VLAN_SNOOPING_FLOODING_ENABLED_IGMP_OR_MLD_IPV4 value 1 Pass
LEAD_VLAN_SNOOPING_FLOODING_ENABLED_IGMP_OR_MLD_IPV6 value 1 Pass
LEAD_VLAN_SNOOPING_PROCESSING_STP_TCN_IGMP_OR_MLD_IPV4 value 0 Pass
LEAD_VLAN_SNOOPING_PROCESSING_STP_TCN_IGMP_OR_MLD_IPV6 value 0 Pass
LEAD_VLAN_VLAN_CLIENT_LABEL value 0 Pass
LEAD_VLAN_VLAN_CONFIG value 0 Pass
LEAD_VLAN_VLAN_FLOOD_ENABLED value 0 Pass
LEAD_VLAN_VLAN_ID_VALID value 1 Pass
LEAD_VLAN_VLAN_LOAD_BALANCE_GROUP value 15 Pass
LEAD_VLAN_VLAN_ROLE value 2 Pass
LEAD_VLAN_VLAN_FLOOD_MODE_BITS value 3 Pass
LEAD_VLAN_LVX_VLAN value 0 Pass
LEAD_VLAN_EGRESS_DEJAVU_CANON value 0 Pass
LEAD_VLAN_EGRESS_INGRESS_VLAN_MODE value 0 Pass
LEAD_VLAN_EGRESS_LOOKUP_VLAN value 0 Pass
LEAD_VLAN_EGRESS_LVX_VLAN value 0 Pass
LEAD_VLAN_EGRESS_SGACL_DISABLED value 3 Pass
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 Punject show/debug que se pueden utilizar para rastrear la trayectoria del paquete DHCP en una red activa.

Comandos comunes Punt / 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 command 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>] punt noise
show platform software fed [switch<num|active|standby>] inject cause summary
show platform software fed [switch<num|active|standby>] punt cause summary
show platform software fed [switch<num|active|standby>] inject cpuq 0
show platform software fed [switch<num|active|standby>] punt 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 punt
show platform software infrastructure lsmpi driver
debug platform software infra punt 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.

Nota: Estos comandos están disponibles en Cisco IOS XE Gibraltar 16.12.X.

---

switch#show platform dhcpsnooping client stats {mac-address}
switch#show platform dhcpv6snooping ipv6 client stats {mac-address}

<#root>

C9300#

show platform dhcpsnooping client stats 0000.1AC2.C148

```
DHCPSN: 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_DHCPSN
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_DHCPSN
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_DHCPSN
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_DHCPSN
```

Utilice estos comandos para borrar el seguimiento.

switch#clear platform dhcpsnooping pkt-trace ipv4
switch#clear platform dhcpsnooping 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 DHCPSN.

- 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<num|active|standby>] 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 0x7f7fac

0x7f7fac23e438

by dhcp snooping
2021/04/14 19:24:27.507394 {fed_F0-0}{1}: [inject] [23451]: (debug): TX: getting REP RI from dhcpsn fai
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 0x7f7fac

0x7f7fac23e438

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

c9500#set platform software trace fed [switch<num|active|standby>] 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 thres
```

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 ty
```

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 ma
```

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 optio
```

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_SNNOPING drop message with mismatched source interf
```

Mensajes DHCP recibidos en la interfaz no fiable.

Explicación: La función de snooping DHCP detectó ciertos tipos de mensajes DHCP no permitidos en la interfaz no confiable, 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
CSCvi39202	El DHCP falla cuando la confianza de indagación DHCP está habilitada en el EtherChannel de link ascendente.
CSCvp49518	La base de datos de detección DHCP no se actualiza después de la recarga.
CSCvk16813	El tráfico del cliente DHCP se interrumpe con el snooping DHCP y los enlaces ascendentes de canal de puerto o entre pilas.
CSCvd51480	Desvinculación de la indagación DHCP IP y el seguimiento de dispositivos.
CSCvm55401	El snooping DHCP puede descartar la opción DHCP 82 paquetes con la opción ip DHCP snooping information option allow-untrusted.
CSCvx25841	El estado de confianza de snooping DHCP se interrumpe cuando hay un cambio en el segmento REP.
CSCvs15759	El servidor DHCP envía un paquete NAK durante el proceso de renovación de DHCP.
CSCvk34927	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  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 Instanc
-------------------  ---------------------- ----------------------  ---------------------  ------------
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
```

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).