DHCP-controle en probleemoplossing op Catalyst 9000 Switches

Inhoud

Inleiding

Dit document beschrijft hoe DHCP-signalering op Catalyst 9000 Series switches moet worden uitgevoerd en problemen moeten worden opgelost

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Catalyst 9000 Series Switches-architectuur
- Cisco IOS® XE-softwarearchitectuur

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- C9200
- C9300
- C9400
- C9500
- C9600

Cisco IOS® XE 16.12.X

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

> **Opmerking**: raadpleeg de juiste configuratiehandleiding voor de opdrachten die worden gebruikt om deze functies op andere Cisco-platforms in te schakelen.

Achtergrondinformatie

DHCP-controle

Dynamic Host Configuration Protocol (DHCP) Snooping is een beveiligingsfunctie die wordt gebruikt om DHCP-verkeer te controleren en zo een kwaadaardig DHCP-pakket te blokkeren. Het fungeert als een firewall tussen onvertrouwde gebruikershavens en DHCP-serverpoorten op het netwerk om schadelijke DHCP-servers in het netwerk te voorkomen, aangezien dit een denial of service kan veroorzaken.

DHCP-scanhandeling

DHCP Snooping werkt met het concept vertrouwde en onvertrouwde interfaces. Door het pad van het DHCP-verkeer controleert de switch de DHCP-pakketten die op de interfaces worden ontvangen en houdt hij een spoor bij van de verwachte DHCP-serverpakketten (OFFER & ACK) via vertrouwde interfaces. Met andere woorden, onbetrouwbare interfaces blokkeren DHCP Server-pakketten.

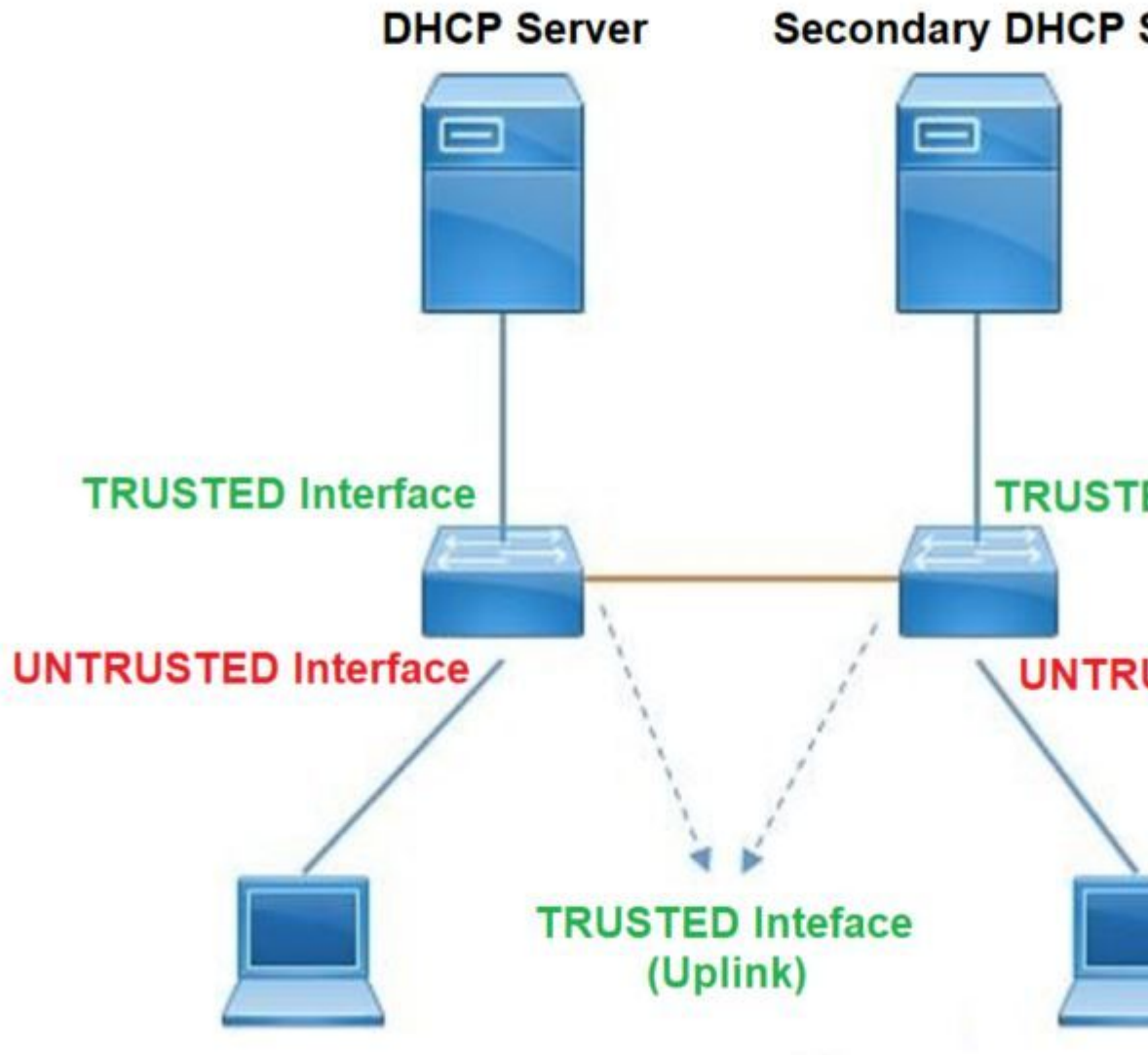
DHCP-pakketten worden geblokkeerd op onbetrouwbare interfaces.

- Een pakket van een server van DHCP, zoals een pakket DHCPOFFER, DHCPACK, DHCPNAK, of DHCPLEEQUERY, wordt ontvangen van buiten het netwerk of de firewall. Dit voorkomt een bedrieglijke DHCP-server van een aanval op het netwerk op onbetrouwbare poorten.
- Een pakket dat op een onbetrouwbare interface wordt ontvangen, en het adres van bron-MAC en het adres van de DHCP-client-hardware komen niet overeen. Dit voorkomt een parodie van DHCP-pakketten van een schurkenclient die een denial of service-aanval op een DHCP-server kan veroorzaken.
- Een DHCPRELEASE of DHCPDECLINE uitzendingsbericht dat een adres van MAC in het het snooping van DHCP bindende gegevensbestand heeft, maar de interfaceinformatie in het bindende gegevensbestand past niet de interface aan waarop het bericht werd ontvangen. Dit voorkomt denial of service-aanvallen op klanten.
- Een DHCP-pakket dat wordt doorgestuurd door een DHCP-relay-agent met een IP-adres dat niet 0.0.0.0 is, of de relay-agent sturen een pakket met optie-82-informatie door naar een niet-vertrouwde poort. Dit voorkomt parodie van relay-agentinformatie op het netwerk.

De switch waar u DHCP Snooping vormt bouwt een DHCP Snooping tabel of DHCP binding database. Deze tabel wordt gebruikt om de IP-adressen bij te houden die zijn toegewezen vanaf een legitieme DHCP-server. De bindende database wordt ook gebruikt door andere IOS-beveiligingsfuncties zoals Dynamic ARP Inspection en IP Source Guard.

> **Opmerking**: om DHCP-controle correct te laten werken, zorg ervoor dat u alle uplinkpoorten naar de DHCP-server vertrouwt en de poorten van de eindgebruiker afbreekt.

Topologie



Configureren

Wereldwijde configuratie

<#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 ar

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
```

> **Opmerking:** om optie-82-pakketten toe te staan, moet u **ip DHCP-snooping informatie optie toestaan-onbetrouwbaar.**

Verifiëren

Bevestig of DHCP-controle op het gewenste VLAN is ingeschakeld en zorg ervoor dat vertrouwde en onbetrouwbare interfaces goed worden vermeld. Als er een tarief wordt geconfigureerd, zorg er dan voor dat het ook wordt vermeld.

<#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:
```

Zodra gebruikers een IP via DHCP ontvangen, worden ze in deze uitvoer vermeld.

- DHCP Snooping verwijdert de ingang in het gegevensbestand wanneer de IP adreshuur verloopt of de switch een DHCPRELEASE bericht van de gastheer ontvangt.
- Zorg ervoor dat de informatie die vermeld staat voor het MAC-adres van de eindgebruiker juist is.

<#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
```

Deze tabel geeft een lijst van de verschillende opdrachten die kunnen worden gebruikt om DHCP-scaninformatie te bewaken.

Opdracht	Doel
Snooping van ip DHCP tonen **IP-hcp snooping-binding tonen** [IP-adres] [MAC-adres] [interface-Ethernet-sleuf/poort] [VLAN-id]	Toont slechts de dynamisch gevormde banden in het het snooping van DHCP bindende gegevensbestand, dat ook als bindende lijst wordt bedoeld. - Bindend IP-adres - Binding vermelding Mac-adres - Invoerinterface voor binding - Bindende ingang VLAN
IP DHCP-snooping database tonen	Toont de het snooping van DHCP bindende gegevensbestandstatus en statistieken.
snuffelstatistieken van ip DHCP tonen	Toont de DHCP-snuffelstatistieken in een samengevatte of gedetailleerde vorm.
IP-bronbinding tonen	Geef de dynamisch en statisch ingestelde bindingen weer.
toon interface VLAN xyz **Toon buffer input-interface VLAN xyz dump**	DHCP-pakket wordt verzonden naar relay agent die in de client-VLAN is geconfigureerd via client-VLAN SVI. Als de invoerwachtrij een daling of een maximale limiet toont, is het waarschijnlijk dat het DHCP-pakket van de client is gevallen en de Relay Agent niet kan bereiken zoals geconfigureerd. **Opmerking**: zorg ervoor dat er geen druppels worden gezien in de invoerwachtrij. switch#**show int VLAN 670**

	Belading gedurende vijf seconden: 13%/0%; één minuut: 10%; vijf minuten: 10% Tijdbron is NTP, 18:39:52.476 UTC Thu Sep 10 2020 VLAN670 is omhoog, het lijnprotocol is omhoog, Toegelaten Autostate Hardware is Ethernet SVI, adres is 00fd.227a.5920 (bia 00fd.227a.5920) Beschrijving: ion_media_client Het internetadres is 10.27.49.254/23 MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec, betrouwbaarheid 255/255, belasting 1/255, rxload 1/255 Insluiting ARPA, loopback niet ingesteld Keepalive niet ondersteund ARP type: ARPA, ARP Time-out 04:00:00 Laatste invoer 03:01:29, uitvoer 00:00:02, uitvoer hang nooit Laatste opheldering van "show interface" tellers nooit **Wachtrij voor invoeren: 375/375/4020251/0** (grootte/max/**dalingen**/spoelingen); Totale output dalingen: 0 **<â€” 375 pakketten in invoer in wachtrij / 4020251 zijn verwijderd**

Problemen oplossen

Software voor probleemoplossing

Controleer wat de switch ontvangt. Deze pakketten worden verwerkt in de CPU-besturingsplane, zodat u alle pakketten ziet in de richting Injecteren en Knippen en bevestigt of de informatie correct is.

> **Waarschuwing**: gebruik de debug commando's met de benodigde voorzichtigheid. Houd er rekening mee dat veel debug commando's invloed hebben op het live netwerk en dat ze alleen aangeraden worden om te gebruiken in een lab omgeving wanneer het probleem gereproduceerd wordt.

Met de functie Voorwaardelijk debuggen kunt u debuggen en logbestanden selectief inschakelen voor specifieke functies op basis van een reeks voorwaarden die u definieert. Dit is nuttig om te bevatten debug informatie aan slechts specifieke hosts of verkeer.

Een voorwaarde verwijst naar een eigenschap of identiteit, waar de identiteit een interface, IP-adres, of een MAC-adres kan zijn enzovoort..

Hoe om voorwaardelijke debug voor pakket en gebeurtenis toe te laten zuivert aan het oplossen van problemen DHCP Snooping.

Opdracht	Doel
debug voorwaarde mac <mac-adres> Voorbeeld: switch#**debug voorwaarde mac bc16.6509.3314**	Configureert voorwaardelijke debugging voor het MAC-adres dat is opgegeven.

debug voorwaarde VLAN <VLAN ID> Voorbeeld: switch#**debug voorwaarde VLAN 10**	Vormt voorwaardelijke debugging voor het gespecificeerde VLAN.
debug voorwaarde interface <interface> Voorbeeld: switch#**debug conditieinterface twinFiveGigE 1/0/8**	Vormt voorwaardelijke debugging voor de gespecificeerde interface.

Als u DHCP-controle wilt debuggen, gebruikt u de opdrachten in de tabel.

Opdracht	Doel
debug dhcp [detail | oper | redundantie]	**gedetailleerde** DHCP-pakketinhoud **Operationele** DHCP interne OPER ondersteuning van DHCP-clientredundantie voor redundantie
debug ip DHCP-server-pakketdetail	Ontvanging en verzending van berichten in detail decoderen
debug ip dhcp server gebeurtenissen	Rapporteer adrestoewijzingen, verloopdatums, enzovoort.
debug ip DHCP-snooping agent	Debug dhcp snooping database lezen en schrijven
debug ip dhcp snooping event	Debug gebeurtenis tussen elke componenten
debug ip DHCP-snoopingpakket	Debug DHCP-pakket in DHCP-snoopingmodule

Dit is een gedeeltelijke steekproefoutput van **het debug ip dhcp snooping** bevel.

<#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 flooc

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 (FortyGigabitEthernet1
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 flooc
Apr 14 16:16:48.839: DHCP_SNOOPING: received new DHCP packet from input interface (FortyGigabitEthernet1

Apr 14 16:16:48.840: DHCP_SNOOPING: process new DHCP packet,

message type: DHCPACK, input interface: Fo1/0/10,

 MAC da: ffff.ffff.ffff, MAC

sa: 701f.539a.fe46,

 IP da: 255.255.255.255, IP

sa: 10.0.0.1,

 DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 10.0.0.5, DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP chaddr: 0
Apr 14 16:16:48.840: DHCP_SNOOPING: add binding on port FortyGigabitEthernet1/0/2 ckt_id 0 FortyGigabitE
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.
```

Gebruik de volgende stappen om DHCP-scangebeurtenissen te debuggen:

Waarschuwing: gebruik de debug commando's met de benodigde voorzichtigheid. Houd er rekening mee dat veel **debug commando's van** invloed zijn op het live netwerk en dat ze alleen aangeraden worden om te gebruiken in een lab omgeving wanneer de kwestie gereproduceerd wordt.

Samenvatting van stappen

1. toelaten
2. debug platform voorwaarde mac {mac-adres}
3. debug platform voorwaarde start
4. toon platformvoorwaarde OF toon debug
5. debug platform voorwaarde stop
6. toon platform software spoor bericht ios R0 omgekeerd | met DHCP
7. perronconditie wissen alle

Gedetailleerde stappen

	Opdracht of handeling	**Doel**
Stap 1	**toelaten** Voorbeeld: switch#**activeren**	Schakelt geprivilegieerde EXEC-modus in. • Voer uw wachtwoord in indien dit wordt gevraagd.
Stap 2	**debug platform voorwaarde mac** {mac-adres} Voorbeeld: switch#**debug platformvoorwaarde mac 0001.6509.3314**	Configureert voorwaardelijke debugging voor het MAC-adres dat is opgegeven.
Stap 3	**debug platform voorwaarde start** Voorbeeld: switch#**debug platform voorwaarde start**	Start voorwaardelijke debugging (dit kan radioactief traceren starten als er een match is op een van de voorwaarden).
Stap 4	**toon platformvoorwaarde** OF **toon debug** Voorbeeld: switch#**show platform voorwaarde** switch#**show debug**	Toont de huidige omstandigheden die zijn ingesteld.
Stap 5	**debug platform voorwaarde stop** Voorbeeld: switch#**debug platform voorwaarde stop**	Stopt het voorwaardelijke zuiveren (dit kan het radioactieve traceren tegenhouden).

	Opdracht of handeling	Doel
Stap 6	**toon platform software spoor bericht ios R0 omgekeerd | met DHCP** Voorbeeld: switch#**show platform software trace bericht ios R0 omgekeerd | met DHCP**	Toont HP logs samengevoegd van het laatste overtrek bestand.
Stap 7	**perronconditie wissen alle** Voorbeeld: switch# **duidelijke platformvoorwaarde allen**	Ontruimt alle voorwaarden.

Dit is een voorbeeld van een deelsteekproef van de **debug-platform DHCP-snoop all**-opdracht.

<#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(00a
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 S
```

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_m
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 S
Apr 14 16:44:24.637: sending dhcp packet out after processing with SMAC = 00a3.d144.2046{mac} and SRC_AD
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) sr
Apr 14 16:44:24.640: ngwc_dhcpsn_process_pak(284): Packet handedover to SISF on vlan 10dhcp pkt processi
```

Deze tabel geeft een overzicht van de verschillende opdrachten die kunnen worden gebruikt om DHCP Snooping in platform te debuggen.

> **Waarschuwing**: gebruik de debug commando's met de benodigde voorzichtigheid. Houd er rekening mee dat veel debug commando's een impact hebben op het live netwerk en dat ze alleen aangeraden worden om te gebruiken in een lab omgeving wanneer de kwestie gereproduceerd wordt.

Opdracht	Doel
switch#**debug platform dhcp-snoop [all | pakje | PD-shim]**	**alle** NGWC DHCP-controle DHCP-**pakketdebuginformatie voor** scannen van pakketten **pd-shim** NGWC DHCP-ondersteuning voor IOS Shim Debug Info
switch#**debug platform software infrastructuur punt dhcp-snoop**	Pakketten die worden ontvangen op de FP (die worden gekopieerd naar het besturingsplane)
switch#**debug platform software infrastructuur injectie**	Pakketten die vanuit het besturingsplane in het FP worden geïnjecteerd

Probleemoplossing bij punt/pad verkeer (CPU)

Controleer vanuit het perspectief van de FED welk verkeer in elke CPU-wachtrij wordt ontvangen (DHCP Snooping is een type verkeer dat door de control-plane wordt verwerkt).

- Wanneer het verkeer in de switch komt, wordt het verzonden naar CPU in de richting VAN HET PUNT en naar de **dhcp snoop** rij verzonden.
- Zodra het verkeer is verwerkt door de switch, vertrekt het verkeer via de INJECT-richting. DHCP OFFER en ACK pakketten vallen in de L2 controle/legacy wachtrij.

<#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	

U kunt deze opdracht gebruiken om het verkeer te bevestigen dat naar de CPU is gestraft en te verifiëren of DHCP-controle het verkeer verlaagt.

<#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

--------------------------------------------------------------------------------
```

Hardware voor probleemoplossing

Forwarding Engine Driver (FED)

De FED is de chauffeur die de ASIC programmeert. FED-opdrachten worden gebruikt om te controleren of de hardware- en softwarestatus overeenkomen.

Verkrijg de waarde van DI_Handle

- De DI-handgreep verwijst naar de doelindex voor een specifieke poort.

<#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

Controleer de ifm-mapping om de essentie en kern van de poorten te bepalen.

- IFM is een interne interface-index die is toegewezen aan een specifieke poort/kern/asic.

<#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
```

Gebruik de DI_Handle om de hardware index.

<#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_DHCPSNOOPIN
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_in
<SNIP>
```

<-- Index is 0x5f03

Converteer van hexadecimaal de indexwaarde 0x5f03 naar decimaal.

0x5f03 = 24323

Gebruik deze indexwaarde in decimaal, en de waarden van ASIC en van de Kern in dit bevel om te zien welke vlaggen voor de haven worden geplaatst.

<#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

Zorg ervoor dat DHCP-controle is ingeschakeld voor het specifieke VLAN.

<#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 Lkp
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 00

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>
```

Deze tabel toont de verschillende Punject-opdrachten die kunnen worden gebruikt om het pad van het DHCP-pakket op een actief netwerk te overtrekken.

Gemeenschappelijke Punt / Injecteer show & debug opdrachten
debug plat soft fed swit acti injecteren add-filter oorzaak 255 sub_cause 0 src_mac 0 0 0 dst_mac 0 0 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>] inspuit breedsprakig **â€" > gebruik filter commando getoond om bereik de sporen naar deze specifieke host** set platform software trace fed [switch<num|active|standby>] inspuit debug-boot **â€" > voor opnieuw laden** set-platform softwarerelease [switch<num|active|standby>] puntruis show platform software fed [switch<num|active|standby>] samenvatting van de oorzaak van de injectie show platform software fed [switch<num|active|standby>] Punt cause overview toon platform software gevoed [switch<num|active|standby>] injecteer cpuq 0 show platform software fed [switch<num|active|standby>] punt cpuq 17 (dhcp wachtrij) show platform software fed [switch<num|active|standby>] actieve injecteer pakketopnamedatum toon platform software infrastructuur injecteren Toon platform software infrastructuur punt toon platform software infrastructuur lsmpi driver debug platform software infra punt dhcp debug platform software infra

Deze opdrachten zijn handig om te controleren of er een DHCP-pakket voor een bepaalde client is ontvangen.

- Deze eigenschap staat u toe om alle het snooping mededeling van DHCP te vangen verbonden aan een bepaald cliëntmac adres dat door cpu via de software IOS-DHCP wordt verwerkt.
- Deze functionaliteit wordt ondersteund voor zowel IPv4- als IPv6-verkeer.
- Deze optie wordt automatisch ingeschakeld.

Belangrijk: deze opdrachten zijn beschikbaar bij Cisco IOS XE Gibraltar 16.12.X.

---

switch#**show platform dhcpsnooping client stats** {mac-adres}
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
```

Gebruik deze opdrachten om het overtrekken te verwijderen.

switch#**clear platform dhcpsnooping pkt-trace ipv4**
switch#**clear platform dhcpsnooping pkt-trace ipv6**

CPU pakketvastlegging

Bevestig als DHCP-synchronisatiepakketten aankomen en het besturingsplane goed verlaten.

Opmerking: raadpleeg de sectie Verder lezen voor meer informatie over het gebruik van het opnamegereedschap van de Forwarding Engine Driver CPU.

<#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

Handige sporen

Dit zijn binaire sporen die gebeurtenissen per proces of component tonen. In dit voorbeeld tonen de sporen informatie over de component dhcpsn.

- De sporen kunnen handmatig worden gedraaid, wat betekent dat u een nieuw bestand kunt maken voordat u begint met probleemoplossing, zodat het schonere informatie bevat.

<#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
```

Syslogs en toelichtingen

Overtredingen van DHCP-snelheidslimieten.

Uitleg: DHCP-snuffelen detecteerde een overschrijding van de DHCP-pakketsnelheid op de gespecificeerde interface.

```
%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
```

DHCP-serverspoofing op een onvertrouwde poort.

Uitleg:De DHCP-snuffelfunctie ontdekte bepaalde typen DHCP-berichten die niet zijn toegestaan op de onbetrouwbare interface, wat aangeeft dat een host probeert te handelen als een DHCP-server.

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

Layer 2 MAC-adres komt niet overeen met het MAC-adres binnen het DHCP-verzoek.

Uitleg: De DHCP-snuffelfunctie heeft geprobeerd het MAC-adres te valideren en de controle is mislukt. Het MAC-adres van de bron in de Ethernet-header komt niet overeen met het adres in het veld Hoofdstuk van het DHCP-verzoekbericht. Er kan een kwaadwillige gastheer zijn die probeert om een ontkenning van de dienstaanval op de server van DHCP uit te voeren.

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

Optie 82 Invoegprobleem.

Uitleg: De DHCP-snuffelfunctie ontdekte een DHCP-pakket met optiewaarden die niet zijn toegestaan op de onvertrouwde poort, wat aangeeft dat een host probeert te handelen als een DHCP-relay of server.

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

Layer 2 MAC-adres ontvangen op verkeerde poort.

Uitleg: De DHCP-snuffelfunctie heeft een host gedetecteerd die probeert een denial of service-aanval uit te voeren op een andere host in het netwerk.

```
%DHCP_SNOOPING-5-DHCP_SNOOPING_FAKE_INTERFACE: DHCP_SNNOPING drop message with mismatched source interfa
```

DHCP-berichten ontvangen op de onbetrouwbare interface.

Uitleg:De DHCP-snuffelfunctie ontdekte bepaalde typen DHCP-berichten die niet zijn toegestaan op de onbetrouwbare interface, wat aangeeft dat een host probeert te handelen als een DHCP-server.

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

DHCP-snuffeloverdracht is mislukt. Kan URL niet openen.

Uitleg: De DHCP snooping binding transfer is mislukt.

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

DHCP-synchronisatievoorbehouden

Cisco Bug-id nummer	Beschrijving
CSCvi39202	DHCP mislukt wanneer DHCP-snuffelvertrouwen is ingeschakeld op uplink-etherchannel.
CSCvp49518	DHCP-snooping database wordt niet vernieuwd na opnieuw laden.
CSCvk16813	DHCP-clientverkeer is verbroken met DHCP-snooping en poortkanaal of cross-stack uplinks.
CSCvd51480	Het losmaken van IP DHCP snooping en apparaat-volgen.
CSCvm55401	DHCP-snuffelen kan de optie DHCP-optie 82-pakketten met de optie IP DHCP-snuffelinformatie laten vallen, maar niet vertrouwd.
CSCv25841	DHCP-snuffelstatus breekt wanneer er verandering is in REP-segment.
CSCv15759	DHCP-server verstuurt een NAK-pakket tijdens het DHCP-vernieuwingsproces.
CSCvk34927	DHCP-snoopingstabel niet bijgewerkt vanuit DHCP-snooping DB-bestand bij opnieuw laden.

SDA border-DHCP-controle

DHCP Snooping Statistics CLI.

Een nieuwe CLI beschikbaar voor SDA om DHCP-snuffelstatistieken te verifiëren.

> **Opmerking**: voor extra verwijzingen naar Cisco SD-Access Fabric Edge DHCP-proces/pakketstroom en decodering raadpleegt u de handleiding in het gedeelte Verwante informatie.

---

switch#**show platform fabric border dhcp snooping ipv4 statistieken**
switch#**show platform fabric border dhcp snooping ipv6 statistieken**

<#root>

```
SDA-9300-BORDER#
```

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

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

```
SDA-9300-BORDER#
```

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

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

Gerelateerde informatie

Configuratiehandleiding voor IP-adresseringsservices, Cisco IOS XE Amsterdam 17.3.x (Catalyst 9200 Switches)

Configuratiehandleiding voor IP-adresseringsservices, Cisco IOS XE Amsterdam 17.3.x (Catalyst 9300 Switches)

Configuratiehandleiding voor IP-adresseringsservices, Cisco IOS XE Amsterdam 17.3.x (Catalyst 9400 Switches)

Configuratiehandleiding voor IP-adresseringsservices, Cisco IOS XE Amsterdam 17.3.x (Catalyst 9500 Switches)

Configuratiehandleiding voor IP-adresseringsservices, Cisco IOS XE Amsterdam 17.3.x (Catalyst 9600 Switches)

Cisco SD-Access Fabric Edge DHCP-proces/pakketstroom en decodering

Configureer FED CPU-pakketvastlegging op Catalyst 9000 Switches

Technische ondersteuning en documentatie â€“ Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.