

Fonctionnement et dépannage de la surveillance DHCP sur les commutateurs Catalyst 9000

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Surveillance DHCP](#)

[Fonctionnement de la surveillance DHCP](#)

[Topologie](#)

[Configurer](#)

[Vérifier](#)

[Dépannage](#)

[Dépannage des logiciels](#)

[Dépannage du trafic point/chemin \(CPU\)](#)

[Dépannage du matériel](#)

[Capture des paquets du chemin du processeur](#)

[Traces utiles](#)

[Syslogs et explications](#)

[Avertissements de surveillance DHCP](#)

[Surveillance DHCP en limite SDA](#)

[Informations connexes](#)

Introduction

Ce document décrit comment utiliser et dépanner la surveillance DHCP sur les commutateurs de la gamme Catalyst 9000

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Architecture des commutateurs Catalyst 9000
- Architecture du logiciel Cisco IOS® XE


Composants utilisés

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

- C9200
- C9300
- C9400
- C9500
- C9600

Cisco IOS® XE 16.12.X

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

 Remarque : consultez le guide de configuration approprié pour connaître les commandes utilisées pour activer ces fonctions sur d'autres plates-formes Cisco.

Informations générales

Surveillance DHCP

La surveillance DHCP (Dynamic Host Configuration Protocol) est une fonctionnalité de sécurité utilisée pour vérifier le trafic DHCP afin de bloquer tout paquet DHCP malveillant. Il agit comme un pare-feu entre les ports utilisateur non approuvés et les ports du serveur DHCP sur le réseau pour empêcher les serveurs DHCP malveillants sur le réseau, car cela peut entraîner un déni de service.

Fonctionnement de la surveillance DHCP

La surveillance DHCP fonctionne avec le concept d'interfaces sécurisées et non sécurisées. Par le chemin du trafic DHCP, le commutateur vérifie les paquets DHCP reçus sur les interfaces et garde une trace des paquets de serveur DHCP attendus (OFFER & ACK) sur les interfaces approuvées. En d'autres termes, les interfaces non approuvées bloquent les paquets du serveur DHCP.


Les paquets DHCP sont bloqués sur les interfaces non approuvées.

- Un paquet provenant d'un serveur DHCP, comme un paquet DHCP OFFER, DHCP ACK, DHCP NAK ou DHCP RELEASE QUERY, provient de l'extérieur du réseau ou du pare-feu. Cela empêche un serveur DHCP non autorisé d'attaquer le réseau sur des ports non approuvés.
- Un paquet reçu sur une interface non approuvée, et l'adresse MAC source et l'adresse matérielle du client DHCP ne correspondent pas. Cela empêche l'usurpation de paquets DHCP d'un client non autorisé qui pourrait créer une attaque par déni de service sur un serveur DHCP.
- Message de diffusion DHCP RELEASE ou DHCP DECLINE dont l'adresse MAC figure dans la base de données de liaison de surveillance DHCP, mais dont les informations d'interface

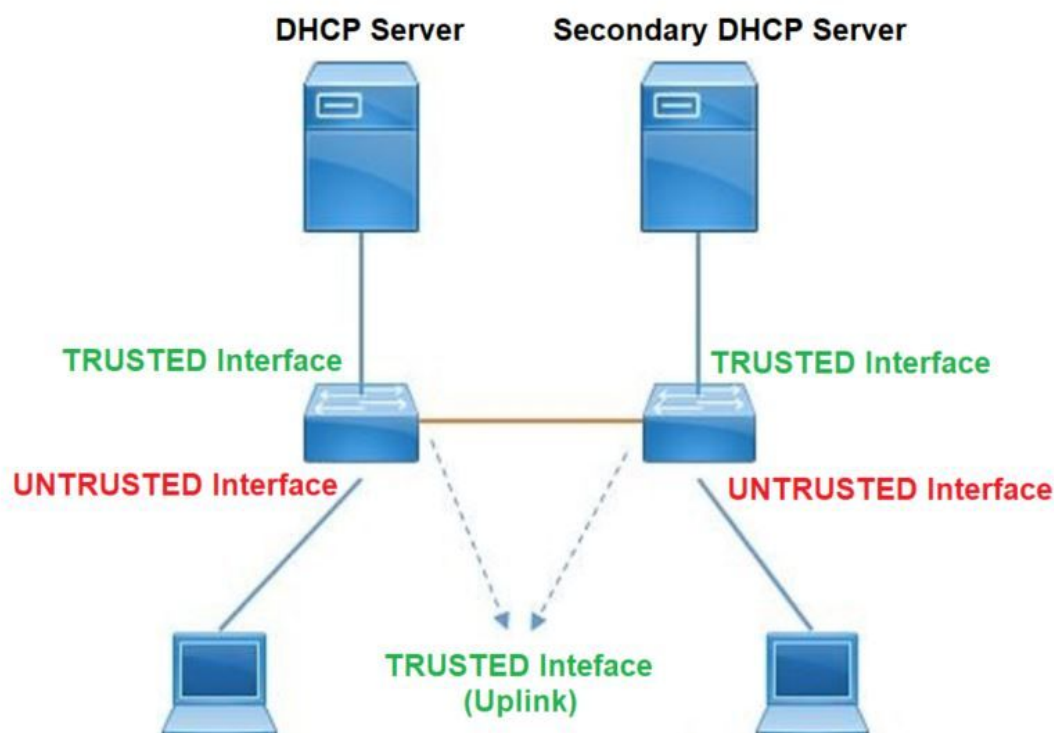
ne correspondent pas à l'interface sur laquelle le message a été reçu. Cela empêche les attaques par déni de service sur les clients.

- Paquet DHCP transféré par un agent de relais DHCP qui inclut une adresse IP d'agent de relais qui n'est pas 0.0.0.0, ou l'agent de relais transfère un paquet qui inclut des informations d'option 82 à un port non approuvé. Cela empêche l'usurpation des informations de l'agent de relais sur le réseau.

Le commutateur sur lequel vous configurez la surveillance DHCP crée une table de surveillance DHCP ou une base de données de liaison DHCP. Cette table permet de conserver une trace des adresses IP attribuées à partir d'un serveur DHCP légitime. La base de données de liaison est également utilisée par d'autres fonctions de sécurité IOS telles que l'inspection ARP dynamique et la protection de source IP.

 Remarque : pour permettre à la surveillance DHCP de fonctionner correctement, assurez-vous que tous les ports de liaison ascendante sont fiables pour atteindre le serveur DHCP et que les ports d'utilisateur final ne sont pas fiables.

Topologie



Configurer

Configuration globale

<#root>

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

```
ip dhcp snooping
```

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

```
ip dhcp snooping trust
```

(Additional verification)

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

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

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

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

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

```
ip dhcp snooping vlan 10
```

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

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

```
ip dhcp snooping information option
```

```
<-- Enable insertion of option 82
```

```
switch(config)#
```

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

```
<-- Disable insertion of option 82
```

```
### Example ###
```

Legitimate DHCP Server Interface and Secondary DHCP Server, if available

Server Interface

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

```
ip dhcp snooping trust
```

```
end
```

Uplink interface

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

```
ip dhcp snooping trust
```

```
end
```

User Interface

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

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

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

```
<< ----- Optional
```

```
end
```



Remarque : pour autoriser les paquets de l'option 82, vous devez activer l'option d'information de surveillance ip dhcp allow-untrusted.

Vérifier

Vérifiez si la surveillance DHCP est activée sur le VLAN souhaité et assurez-vous que les interfaces approuvées et non approuvées sont bien répertoriées. Si un débit est configuré, assurez-vous qu'il figure également dans la liste.

<#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:

Une fois que les utilisateurs reçoivent une adresse IP par DHCP, ils sont répertoriés dans ce résultat.

- La surveillance DHCP supprime l'entrée dans la base de données lorsque le bail de l'adresse IP expire ou lorsque le commutateur reçoit un message DHCPRELEASE de l'hôte.
- Assurez-vous que les informations répertoriées pour l'adresse MAC de l'utilisateur final sont correctes.


<#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
```

Ce tableau répertorie les différentes commandes qui peuvent être utilisées pour surveiller les informations de surveillance DHCP.


Commande	Objectif
<pre>show ip dhcp snooping binding show ip dhcp snooping binding [adresse IP] [adresse MAC] [interface port/emplacement Ethernet] [id_vlan]</pre>	<p>Affiche uniquement les liaisons configurées dynamiquement dans la base de données de liaison de surveillance DHCP, également appelée table de liaison.</p> <ul style="list-style-type: none">- Adresse IP de l'entrée de liaison- Adresse MAC de l'entrée de liaison- Interface d'entrée de liaison- VLAN d'entrée de liaison
<pre>show ip dhcp snooping database</pre>	<p>Affiche l'état et les statistiques de la base de données de liaison de surveillance DHCP.</p>
<pre>show ip dhcp snooping statistics</pre>	<p>Affiche les statistiques de surveillance DHCP sous forme</p>

	récapitulative ou détaillée.
show ip source binding	Affichez les liaisons configurées de manière dynamique et statique.
show interface vlan xyz show buffer input-interface Vlan xyz dump	<p>Le paquet DHCP est envoyé à l'agent de relais configuré dans le vlan client via l'interface SVI du vlan client. Si la file d'attente d'entrée indique une limite d'abandon ou d'atteinte maximale, il est probable que le paquet DHCP du client a été abandonné et n'a pas pu atteindre l'agent de relais configuré.</p> <hr/> <p> Remarque : assurez-vous que les abandons ne sont pas visibles dans la file d'attente d'entrée.</p> <hr/> <pre>switch#show int vlan 670 Charge pendant cinq secondes : 13 %/0 % ; une minute : 10 % ; cinq minutes : 10 % La source horaire est NTP, 18:39:52.476 UTC Thu Sep 10 2020 Vlan670 est actif, le protocole de ligne est actif , état automatique activé Le matériel est l'interface SVI Ethernet, l'adresse est 00fd.227a.5920 (bia 00fd.227a.5920) Description : ion_media_client L'adresse Internet est 10.27.49.254/23 MTU 1500 octets, BW 1000000 Kbit/s, DLY 10 usec, fiabilité 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA, bouclage non défini Keepalive non pris en charge Type ARP : ARPA, ARP Timeout 04:00:00 Dernière entrée 03:01:29, sortie 00:00:02, sortie ne se bloque jamais Dernière suppression des compteurs « show interface » jamais File d'attente d'entrée : 375/375/4020251/0 (size/max/drops/flushes) ; Total des pertes en sortie : 0 <— 375 paquets en entrée dans la file d'attente / 4020251 ont été abandonnés</pre>

Dépannage

Dépannage des logiciels

Vérifiez ce que le commutateur reçoit. Ces paquets sont traités au niveau du plan de contrôle du processeur, donc assurez-vous de voir tous les paquets dans la direction d'injection et de pointage, et vérifiez si les informations sont correctes.

 Attention : utilisez les commandes debug avec précaution. Sachez que de nombreuses commandes debug ont un impact sur le réseau actif et que leur utilisation est recommandée dans un environnement de travaux pratiques uniquement lorsque le problème est reproduit.

La fonctionnalité Débogage conditionnel vous permet d'activer de manière sélective des débogages et des journaux pour des fonctionnalités spécifiques en fonction d'un ensemble de conditions que vous définissez. Cela est utile pour contenir des informations de débogage uniquement pour des hôtes ou un trafic spécifiques.

Une condition fait référence à une fonctionnalité ou une identité, où l'identité peut être une interface, une adresse IP ou une adresse MAC, etc..

Comment activer le débogage conditionnel pour les débogages de paquets et d'événements afin de dépanner la surveillance DHCP.

Commande	Objectif
debug condition mac <adresse-mac> Exemple : switch#debug condition mac bc16.6509.3314	Configure le débogage conditionnel pour l'adresse MAC spécifiée.
debug condition vlan <ID VLAN> Exemple : switch#debug condition vlan 10	Configure le débogage conditionnel pour le VLAN spécifié.
debug condition interface <interface> Exemple : switch#debug condition interface vingtFiveGigE 1/0/8	Configure le débogage conditionnel pour l'interface spécifiée.

Pour déboguer la surveillance DHCP, utilisez les commandes indiquées dans le tableau.

Commande	Objectif
debug dhcp [detail opératrice redondance]	Détail du contenu des paquets DHCP Opérateur DHCP interne OPER Redondance Prise en charge de la redondance client DHCP
debug ip dhcp server packet detail	Décoder en détail les réceptions et les transmissions de messages
debug ip dhcp server events	Signaler les affectations d'adresses, l'expiration du bail, etc.
debug ip dhcp snooping agent	Debug dhcp snooping database read and write
debug ip dhcp snooping event	Événement de débogage entre chaque composant
debug ip dhcp snooping packet	Déboguer le paquet DHCP dans le module de surveillance DHCP

Ceci est un exemple de sortie partiel de la commande debug ip dhcp snooping.

<#root>

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

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

, MAC da: ffff.ffff.ffff, MAC

sa: 00a3.d144.2046,

IP da: 255.255.255.255, IP sa: 0.0.0.0, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.0.0
Apr 14 16:16:46.835: DHCP_SNOOPING: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is floor

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: 0.0.0.0
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 (FortyGigabitEthernet1/0/2)
Apr 14 16:16:48.838: Performing rate limit check


Apr 14 16:16:48.838: DHCP_SNOOPING: process new DHCP packet,
message type: DHCPREQUEST, input interface: Fo1/0/2,
MAC da: ffff.ffff.ffff, MAC
sa: 00a3.d144.2046,
IP da: 255.255.255.255, IP sa: 0.0.0.0, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.0.0
Apr 14 16:16:48.838: DHCP_SNOOPING: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is flooded
Apr 14 16:16:48.839: DHCP_SNOOPING: received new DHCP packet from input interface (FortyGigabitEthernet1/0/2)

Apr 14 16:16:48.840: DHCP_SNOOPING: process new DHCP packet,
message type: DHCPACK, input interface: Fo1/0/10,
MAC da: ffff.ffff.ffff, MAC
sa: 701f.539a.fe46,
IP da: 255.255.255.255, IP
sa: 10.0.0.1,
DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 10.0.0.5, DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP chaddr: 0.0.0.0
Apr 14 16:16:48.840: DHCP_SNOOPING: add binding on port FortyGigabitEthernet1/0/2 ckt_id 0 FortyGigabitEthernet1/0/2
Apr 14 16:16:48.840: DHCP_SNOOPING: added entry to table (index 331)

Apr 14 16:16:48.840:
DHCP_SNOOPING: dump binding entry: Mac=00:A3:D1:44:20:46 Ip=10.0.0.5
Lease=86400 Type=dhcp-snooping
Vlan=10 If=FortyGigabitEthernet1/0/2

Apr 14 16:16:48.840: No entry found for mac(00a3.d144.2046) vlan(10) FortyGigabitEthernet1/0/2
Apr 14 16:16:48.840: host tracking not found for update add dynamic (10.0.0.5, 0.0.0.0, 00a3.d144.2046)
Apr 14 16:16:48.840: platform lookup dest vlan for input_if: FortyGigabitEthernet1/0/10, is NOT tunnel,
Apr 14 16:16:48.840: DHCP_SNOOPING: direct forward dhcp reply to output port: FortyGigabitEthernet1/0/2.
```

Pour déboguer les événements de surveillance DHCP, procédez comme suit :

 Attention : utilisez les commandes debug avec précaution. Notez que de nombreuses commandes de débogage ont un impact sur le réseau actif et qu'il est recommandé de les utiliser dans un environnement de travaux pratiques uniquement lorsque le problème est reproduit.

Étapes récapitulatives

1. activer
2. debug platform condition mac {mac-address }
3. debug platform condition start
4. show platform condition OU show debug

5. debug platform condition stop
6. show platform software trace message ios R0 reverse | inclure DHCP
7. clear platform condition all

Étapes détaillées

	Commande ou action	Objectif
Étape 1	activer Exemple : switch#enable	Active le mode privilégié. • Saisissez votre mot de passe si vous y êtes invité.
Étape 2	debug platform condition mac {mac-address} Exemple : switch#debug platform condition mac 0001.6509.3314	Configure le débogage conditionnel pour l'adresse MAC spécifiée.
Étape 3	debug platform condition start Exemple : switch#debug platform condition start	Démarre le débogage conditionnel (cela peut démarrer le traçage radioactif s'il y a une correspondance sur l'une des conditions).
Étape 4	show platform condition OU show debug Exemple : switch#show platform condition switch#show debug	Affiche les conditions actuelles définies.
Étape 5	debug platform condition stop Exemple : switch#debug platform condition stop	Arrête le débogage conditionnel (cela peut arrêter le traçage radioactif).
Étape 6	show platform software trace message ios R0 reverse inclure DHCP	Affiche les journaux HP fusionnés à partir du dernier fichier de trace.

	Commande ou action	Objectif
	Exemple : switch#show platform software trace message ios R0 reverse inclure DHCP	
Étape 7	clear platform condition all Exemple : switch# clear platform condition all	Efface toutes les conditions.

Ceci est un exemple de sortie d'exemple partiel de la commande dplateforme de débogage dhcp-snoop all, commande.

<#root>

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

DHCP Server UDP port

(67)

DHCP Client UDP port

(68)

RELEASE

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

DISCOVER

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

OFFER

```
Apr 14 16:44:24.638: dhcp packet src_ip(10.0.0.1) dest_ip(255.255.255.255) src_udp(67) dest_udp(68) src_mac(00a3.d144.2046)
```

Apr 14 16:44:24.638: ngwc_dhcpsn_process_pak(305): Packet handedover to SISF on vlan 10
 Apr 14 16:44:24.638: dhcp pkt processing routine is called for pak with SMAC = 701f.539a.fe46{mac} and


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

Ce tableau répertorie les différentes commandes qui peuvent être utilisées pour déboguer la surveillance DHCP dans la plate-forme.

 Attention : utilisez les commandes debug avec précaution. Sachez que de nombreuses commandes debug ont un impact sur le réseau actif et que leur utilisation est recommandée dans un environnement de travaux pratiques uniquement lorsque le problème est reproduit.

Commande	Objectif
switch#debug platform dhcp-snoop [all paquet pd-shim]	Toutes les fonctions de surveillance DHCP NGWC Informations de débogage de paquet de surveillance DHCP NGWC pd-shim NGWC DHCP Snooping IOS Shim Debug Info
switch#debug platform infrastructure logicielle punt dhcp-snoop	Paquets reçus sur le FP et dirigés vers le plan de contrôle)
switch#debug platform software infrastructure injection	Paquets injectés dans le FP à partir du plan de contrôle

Dépannage du trafic point/chemin (CPU)

Vérifiez du point de vue FED quel trafic est reçu dans chaque file d'attente CPU (la surveillance DHCP est un type de trafic qui est traité par le plan de contrôle).

- Lorsque le trafic arrive dans le commutateur, il est envoyé au CPU dans la direction PUNT et est envoyé à la file d'attente de surveillance dhcp.
- Une fois que le trafic est traité par le commutateur, il part par la direction INJECT. Les paquets DHCP OFFER et ACK entrent dans la file d'attente de contrôle L2/héritée.

<#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

Vous pouvez utiliser cette commande pour confirmer le trafic envoyé au processeur et vérifier si la surveillance DHCP abandonne le trafic.

<#root>

```
c9500#
```

```
show platform software fed switch active punt cpuq rates
```

Punt Rate CPU Q Statistics

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

```
=====
```

Q no	Queue Name	Rx 10s	Rx 1min	Rx 5min	Drop 10s	Drop 1min	Drop 5min
0	CPU_Q_DOT1X_AUTH	0	0	0	0	0	0
1	CPU_Q_L2_CONTROL	0	0	0	0	0	0
2	CPU_Q_FORUS_TRAFFIC	0	0	0	0	0	0
3	CPU_Q_ICMP_GEN	0	0	0	0	0	0
4	CPU_Q_ROUTING_CONTROL	0	0	0	0	0	0
5	CPU_Q_FORUS_ADDR_RESOLUTION	0	0	0	0	0	0
6	CPU_Q_ICMP_REDIRECT	0	0	0	0	0	0
7	CPU_Q_INTER_FED_TRAFFIC	0	0	0	0	0	0
8	CPU_Q_L2LVX_CONTROL_PKT	0	0	0	0	0	0
9	CPU_Q_EWLC_CONTROL	0	0	0	0	0	0
10	CPU_Q_EWLC_DATA	0	0	0	0	0	0
11	CPU_Q_L2LVX_DATA_PKT	0	0	0	0	0	0
12	CPU_Q_BROADCAST	0	0	0	0	0	0
13	CPU_Q_LEARNING_CACHE_OVFL	0	0	0	0	0	0
14	CPU_Q_SW_FORWARDING	0	0	0	0	0	0
15	CPU_Q_TOPOLOGY_CONTROL	2	2	2	0	0	0
16	CPU_Q_PROTO_SNOOPING	0	0	0	0	0	0
17	CPU_Q_DHCP_SNOOPING	0	0	0	0	0	0
0	0	0	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

Dépannage du matériel

Pilote de moteur de transfert (FED)

FED est le pilote qui programme l'ASIC. Les commandes FED sont utilisées pour vérifier que les états du matériel et du logiciel correspondent.

Obtenir la valeur DI_Handle

- L'identificateur d'ID fait référence à l'index de destination d'un port spécifique.

<#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
```

Vérifiez le mappage ifm pour déterminer les ports Asic et Core.

- IFM est un index d'interface interne mappé à un port/coeur/base spécifique.

<#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
```

Utilisez DI_Handle pour obtenir l'index matériel.

<#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_DHCPSPNOOPI  
priv_ri/priv_si Handle: (nil)Hardware Indices/Handles:
```

```
index0:0x5f03
```

```
mtu_index/13u_ri_index0:0x0 index1:0x5f03 mtu_index/13u_ri_index1:0x0 index2:0x5f03 mtu_index/13u_ri_i  
<SNIP>
```

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

Convertissez la valeur d'index 0x5f03 hexadécimale en valeur décimale.

0x5f03 = 24323

Utilisez cette valeur d'index en notation décimale et les valeurs ASIC et Core de cette commande pour voir quels indicateurs sont définis pour le port.

<#root>

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

```
asic
```

```
1
```

```
core
```

```
1
```

For asic 1 core 1

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

```
24323
```

```
]
```

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

```
copySegment0 :
```

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

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

```
dpuSegment0 : 0x0
```

```
dpuSegment1 : 0x0
```

```
ecUnicast : 0x0
```

```
etherChannel0 : 0x0
```

```
etherChannel1 : 0x0
```

```
hashPtr1 : 0x0
```

```
stripSegment : 0x0
```

Assurez-vous que la surveillance DHCP est activée pour le VLAN spécifique.

<#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
---------	-------	-----------	------------	--------------	--------

```

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>

```

Ce tableau répertorie les différentes commandes Punject show/debug courantes qui peuvent être utilisées pour suivre le chemin d'un paquet DHCP sur un réseau actif.

Commandes communes Punt / Inject show & debug

```

debug plat soft fed switch acti injection add-filter cause 255 sub_cause 0 src_mac 0 0 0 dst_mac
0 0 src_ipv4 192.168.12.1 dst_ipv4 0.0.0.0 if_id 0xf

```

```

set platform software trace fed [switch<num|active|standby>] inject verbose — > use filter
cpmand illustré pour étendre les traces à cet hôte spécifique

```

```

set platform software trace fed [switch<num|active|standby>] inject debug boot — > pour
rechargement

```

```

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

```

```

show platform software fed [switch<num|active|standby>] injecter le résumé des causes

```

```

show platform software fed [switch<num|active|standby>] résumé des causes du problème

```

```

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

```

```

show platform software fed [switch<num|active|standby>] punt cpuq 17 (file dhcp)

```

```

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

```

```

show platform software infrastructure injection

```

```

show platform software infrastructure punt

```

```

show platform software infrastructure pilote lsmpi

```

```
debug platform software infra punt dhcp
```

```
debug platform software infra inject
```

Ces commandes sont utiles pour vérifier si un paquet DHCP est reçu pour un client particulier.

- Cette fonctionnalité vous permet de capturer toutes les communications de surveillance DHCP associées à une adresse MAC client donnée qui sont traitées par le processeur via le logiciel IOS-DHCP.
- Cette fonctionnalité est prise en charge pour le trafic IPv4 et IPv6.
- Cette fonction est activée automatiquement.

 Important : ces commandes sont disponibles sur 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
```

```
DHCPSPN: 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_DHCPSPN
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_DHCPSPN
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_DHCPSPN
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_DHCPDN
```


Utilisez ces commandes pour effacer la trace.

```
switch#clear platform dhcpsnooping pkt-trace ipv4
```

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

Capture des paquets du chemin du processeur

Vérifiez si les paquets de surveillance DHCP arrivent et quittent correctement le plan de contrôle.

 Remarque : pour obtenir des références supplémentaires sur l'utilisation de l'outil de capture CPU du pilote du moteur de transfert, reportez-vous à la section Lectures supplémentaires.

```
<#root>
```

```
debug platform software fed
```

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

```
punt/inject
```

```
packet-capture start
```

```
debug platform software fed
```

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

```
punt/inject
```

```
packet-capture stop
```

```
show platform software fed
```

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

```
punt/inject
```

```
packet-capture brief
```

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

```
DISCOVER
```

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

physical: FortyGigabitEthernet1/0/2

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

[dhcp snoop],

sub-cause: 11, q-no: 17, linktype: MCP_LINK_TYPE_IP [1]
ether hdr : dest mac: ffff.ffff.ffff,
src mac: 00a3.d144.2046

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

67

, src port:

68

OFFER

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

physical: FortyGigabitEthernet1/0/10

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

[dhcp snoop]

, sub-cause: 11, q-no: 17, linktype: MCP_LINK_TYPE_IP [1]
ether hdr : dest mac: ffff.ffff.ffff,
src mac: 701f.539a.fe46

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

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

68

, src port:

67

REQUEST

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

physical: FortyGigabitEthernet1/0/2

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

[dhcp snoop]

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

src mac: 00a3.d144.2046

ether hdr : ethertype: 0x0800 (IPv4)

ipv4 hdr : dest ip: 255.255.255.255, src ip: 0.0.0.0

ipv4 hdr : packet len: 365, ttl: 255, protocol: 17 (UDP)

udp hdr : dest port:

67

, src port:

68

ACK

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

physical: FortyGigabitEthernet1/0/10

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

[dhcp snoop]

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

src mac: 701f.539a.fe46

ether hdr : vlan: 10, ethertype: 0x8100

ipv4 hdr : dest ip: 255.255.255.255,

src ip: 10.0.0.1

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

udp hdr : dest port:

68

, src port:

67

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

Traces utiles

Il s'agit de suivis binaires qui affichent les événements par processus ou composant. Dans cet exemple, les suivis affichent des informations sur le composant dhcpsn.

- Les traces peuvent être pivotées manuellement, ce qui signifie que vous pouvez créer un nouveau fichier avant de commencer le dépannage afin qu'il contienne des informations plus propres.

```
<#root>
```

```
9500#
```

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

```
9500#
```

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

```
] dhcpcn verbose
```

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

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

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

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

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

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

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

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

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

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

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

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

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

```
0x7f7fac23e438
```

```
by dhcp snooping
```

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

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

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

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

0x7f7fac23e438

by dhcp snooping

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

c9500#set platform software trace fed [switch

] ASIC_app verbose

c9500#show logging proc fed internal | inc dhcp

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

VLAN event on vlan 10

, enabled 0

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

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

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

Program trust ports for this vlan

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

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

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

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

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

Suggested Traces

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

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

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

INJECT

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

set platform software trace fed [switch<num|active|standby>] ASIC_app verbose

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

PUNT

```
set platform software trace fed [switch<num|active|standby>] dhcpcn 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 et explications

Violations des limites de débit DHCP.

Explication : La surveillance DHCP a détecté une violation de limite de débit de paquets DHCP sur l'interface spécifiée.

```
%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 thre
```

Usurpation du serveur DHCP sur un port non approuvé.

Explication : La fonctionnalité de surveillance DHCP a détecté certains types de messages DHCP non autorisés sur l'interface non approuvée, ce qui indique que certains hôtes tentent d'agir en tant que serveur DHCP.

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

L'adresse MAC de couche 2 ne correspond pas à l'adresse MAC dans la requête DHCP.

Explication : la fonctionnalité de surveillance DHCP a tenté de valider l'adresse MAC et la vérification a échoué. L'adresse MAC source dans l'en-tête Ethernet ne correspond pas à l'adresse dans le champ chaddr du message de requête DHCP. Il peut y avoir un hôte malveillant qui tente d'effectuer une attaque par déni de service sur le serveur DHCP.

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

Problème d'insertion de l'option 82.

Explication : La fonctionnalité de surveillance DHCP a détecté un paquet DHCP avec des valeurs d'option non autorisées sur le port non approuvé, ce qui indique que certains hôtes tentent d'agir

en tant que relais ou serveur DHCP.

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

Adresse MAC de couche 2 reçue sur un port incorrect.

Explication : La fonctionnalité de surveillance DHCP a détecté un hôte tentant d'effectuer une attaque par déni de service sur un autre hôte du réseau.

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

Messages DHCP reçus sur l'interface non approuvée.

Explication : La fonctionnalité de surveillance DHCP a détecté certains types de messages DHCP non autorisés sur l'interface non approuvée, ce qui indique que certains hôtes tentent d'agir en tant que serveur DHCP.

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

Échec du transfert de surveillance DHCP. Impossible d'accéder à l'URL.

Explication : le transfert de liaison de surveillance DHCP a échoué.

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

Avertissements de surveillance DHCP


ID de bogue Cisco	Description
CSCvi39202	DHCP échoue lorsque la confiance de surveillance DHCP est activée sur l'etherchannel de liaison ascendante.
CSCvp49518	La base de données de surveillance DHCP n'est pas actualisée après le

	rechargement.
CSCvk16813	Le trafic client DHCP a été abandonné avec la surveillance DHCP et les liaisons ascendantes port-channel ou inter-pile.
CSCvd51480	Désassociation de la surveillance ip dhcp et du suivi de périphérique.
CSCvm55401	La surveillance DHCP peut abandonner l'option dhcp 82 paquets avec l'option ip dhcp snooping information option allow-untrusted.
CSCvx25841	L'état d'approbation de la surveillance DHCP est rompu en cas de modification du segment REP.
CSCvs15759	Le serveur DHCP envoie un paquet NAK pendant le processus de renouvellement DHCP.
CSCvk34927	Table de surveillance DHCP non mise à jour à partir du fichier de base de données de surveillance DHCP lors du rechargement.

Surveillance DHCP en limite SDA

CLI des statistiques de surveillance DHCP.

Une nouvelle interface de ligne de commande est disponible pour SDA afin de vérifier les statistiques de surveillance DHCP.

 Remarque : pour obtenir des références supplémentaires sur le processus DHCP/flux de paquets et le décodage de la périphérie du fabric Cisco SD-Access, reportez-vous au guide de la section Informations connexes.

```
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 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

Informations connexes

[Guide de configuration des services d'adressage IP, Cisco IOS XE Amsterdam 17.3.x \(commutateurs Catalyst 9200\)](#)

[Guide de configuration des services d'adressage IP, Cisco IOS XE Amsterdam 17.3.x \(commutateurs Catalyst 9300\)](#)

[Guide de configuration des services d'adressage IP, Cisco IOS XE Amsterdam 17.3.x \(commutateurs Catalyst 9400\)](#)

[Guide de configuration des services d'adressage IP, Cisco IOS XE Amsterdam 17.3.x \(commutateurs Catalyst 9500\)](#)

[Guide de configuration des services d'adressage IP, Cisco IOS XE Amsterdam 17.3.x \(commutateurs Catalyst 9600\)](#)

[Processus/flux de paquets DHCP de périphérie de fabric Cisco SD-Access et décodage](#)

[Configuration de la capture de paquets CPU FED sur les commutateurs Catalyst 9000](#)

[Assistance et documentation techniques - Cisco Systems](#)

À propos de cette traduction

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

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