Operar e solucionar problemas de rastreamento de DHCP em switches Catalyst 9000

Contents

Introdução

Este documento descreve como operar e solucionar problemas de DHCP Snooping em Catalyst 9000 Series Switches

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Arquitetura dos switches Catalyst 9000 Series
- Arquitetura do software Cisco IOS® XE

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- C9200
- C9300
- C9400
- C9500
- C9600

Cisco IOS® XE 16.12.X

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

> **Observação**: consulte o guia de configuração apropriado para obter os comandos que são usados para ativar esses recursos em outras plataformas Cisco.

Informações de Apoio

Rastreamento de DHCP

O rastreamento de DHCP é um recurso de segurança usado para verificar o tráfego DHCP e bloquear qualquer pacote DHCP mal-intencionado. Ele atua como um firewall entre portas de usuário não confiáveis e portas de servidor DHCP na rede para evitar servidores DHCP mal-intencionados na rede, pois isso pode causar uma negação de serviço.

Operação de rastreamento de DHCP

O DHCP Snooping funciona com o conceito de interfaces confiáveis e não confiáveis. Através do caminho do tráfego DHCP, o switch verifica os pacotes DHCP recebidos nas interfaces e mantém um controle dos pacotes esperados do servidor DHCP (OFFER & ACK) sobre interfaces confiáveis. Em outras palavras, as interfaces não confiáveis bloqueiam os pacotes do servidor DHCP.

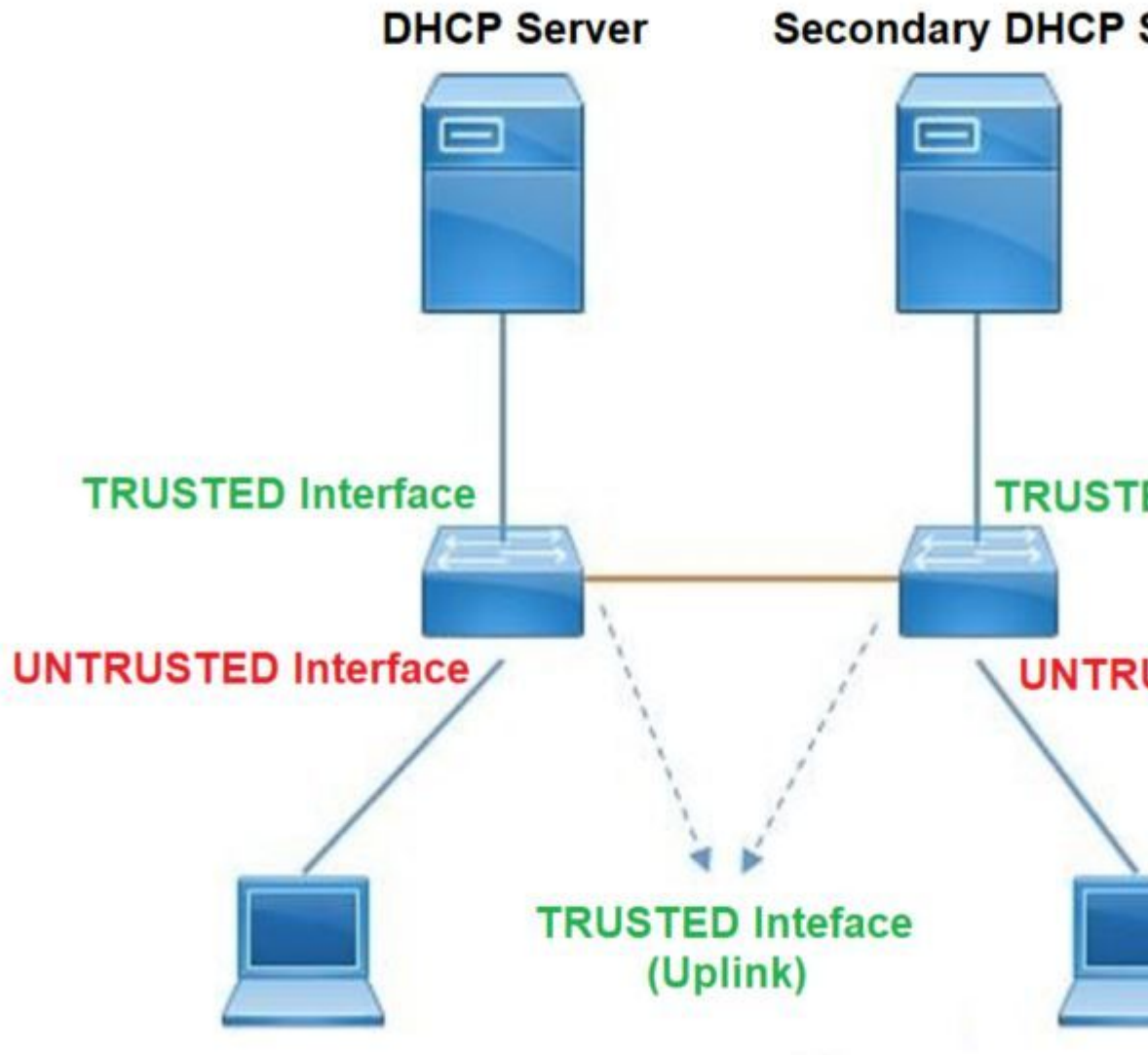
Os pacotes DHCP são bloqueados em interfaces não confiáveis.

- Um pacote de um servidor DHCP, como um pacote DHCPOFFER, DHCPACK, DHCPNAK ou DHCPLEASEQUERY, é recebido de fora da rede ou do firewall. Isso evita que um servidor DHCP invasor ataque a rede em portas não confiáveis.
- Um pacote recebido em uma interface não confiável, e o endereço MAC origem e o endereço de hardware do cliente DHCP não correspondem. Isso evita a falsificação de pacotes DHCP de um cliente invasor que pode criar um ataque de negação de serviço em um servidor DHCP.
- Uma mensagem de broadcast DHCPRELEASE ou DHCPDECLINE que tem um endereço MAC no banco de dados de associação de rastreamento de DHCP, mas as informações de interface no banco de dados de associação não correspondem à interface na qual a mensagem foi recebida. Isso evita ataques de negação de serviço aos clientes.
- Um pacote DHCP encaminhado por um agente de retransmissão DHCP que inclui um endereço IP de agente de retransmissão diferente de 0.0.0.0 ou o agente de retransmissão encaminha um pacote que inclui informações de opção 82 para uma porta não confiável. Isso evita falsificações de informações do agente de retransmissão na rede.

O switch no qual você configura o DHCP Snooping cria uma tabela de DHCP Snooping ou um banco de dados de associação de DHCP. Esta tabela é usada para manter um controle dos endereços IP atribuídos de um servidor DHCP legítimo. O banco de dados de vinculação também é usado por outros recursos de segurança do IOS, como Dynamic ARP Inspection e IP Source Guard.

> **Observação**: para permitir que o DHCP Snooping funcione corretamente, certifique-se de confiar em todas as portas de uplink para acessar o servidor DHCP e não confiar nas portas do usuário final.

Topologia



Configurar

Configuração global

<#root>

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

ip dhcp snooping

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

ip dhcp snooping trust

(Additional verification)

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

> **Observação:** para permitir pacotes option-82, você deve habilitar **ip dhcp snooping information option allow-untrusted.**

Verificar

Confirme se o DHCP Snooping está habilitado na VLAN desejada e verifique se as interfaces confiáveis e não confiáveis estão bem listadas. Se houver uma taxa configurada, verifique se ela também está listada.

<#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:
```

Quando os usuários recebem um IP por DHCP, eles são listados nesta saída.

- O DHCP Snooping remove a entrada no banco de dados quando o aluguel do endereço IP expira ou o switch recebe uma mensagem DHCPRELEASE do host.
- Verifique se as informações listadas para o endereço MAC do usuário final estão corretas.

<#root>

```
c9500#show ip dhcp snooping binding


MacAddress         IpAddress       Lease(sec) Type          VLAN Interface
------------------ --------------- ---------- ------------- ---- --------------------
00:A3:D1:44:20:46  10.0.0.3

85556

 dhcp-snooping 10   FortyGigabitEthernet1/0/2
Total number of bindings: 1
```

Esta tabela lista os vários comandos que podem ser usados para monitorar informações de DHCP Snooping.

Comando	Propósito
show ip dhcp snooping binding **show ip dhcp snooping binding** [endereço-IP] [endereço-MAC] [slot/porta ethernet da interface] [id-vlan]	Exibe apenas as associações configuradas dinamicamente no banco de dados de associações de rastreamento DHCP, também conhecido como tabela de associações. - Endereço IP de entrada de ligação - Endereço Mac de entrada de ligação - Interface de entrada de entrada de vinculação - VLAN de entrada de vinculação
show ip dhcp snooping database	Exibe o status e as estatísticas do banco de dados de bind de rastreamento DHCP.
show ip dhcp snooping statistics	Exibe as estatísticas de rastreamento de DHCP em forma resumida ou detalhada.
show ip source binding	Exibir as associações configuradas de forma dinâmica e estática.
show interface vlan xyz **show buffer input-interface Vlan xyz dump**	O pacote DHCP é enviado ao agente de retransmissão configurado na vlan do cliente através da vlan SVI do cliente. Se a fila de entrada mostrar o limite máximo de queda ou de alcance, é provável que o pacote dhcp do cliente tenha sido descartado e não tenha conseguido acessar o agente de retransmissão configurado. **Observação**: certifique-se de que os descartes não sejam vistos na fila de entrada. switch#**show int vlan 670** Carga por cinco segundos: 13%/0%; um minuto: 10%; cinco minutos: 10%

	A fonte de horário é NTP, 18:39:52.476 UTC até 10 de setembro de 2020 Vlan670 está ativa, o protocolo de linha está ativo , Autostate Habilitado O hardware é Ethernet SVI, o endereço é 00fd.227a.5920 (bia 00fd.227a.5920) Descrição: ion_media_client O endereço de Internet é 10.27.49.254/23 MTU 1500 bytes, BW 1000000 Kbit/seg, DLY 10 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulamento ARPA, loopback não definido Keepalive não suportado Tipo ARP: ARPA, Tempo limite ARP 04:00:00 Última entrada 03:01:29, saída 00:00:02, saída nunca travar A última limpeza dos contadores "show interface" nunca **Fila de entrada: 375/375/4020251/0** (tamanho/máx/**quedas**/liberações); Total de quedas de saída: 0 **<â€" 375 pacotes na entrada da fila /** 4020251 foram descartados

Troubleshooting

Solução de problemas de software

Verifique o que o switch recebe. Esses pacotes são processados no plano de controle da CPU, portanto, certifique-se de ver todos os pacotes na direção de inserção e punt e confirme se as informações estão corretas.

> **Cuidado**: use os comandos debug com cuidado. Esteja ciente de que muitos comandos de depuração têm impacto sobre a rede ativa e somente são recomendados para uso em um ambiente de laboratório quando o problema for reproduzido.

O recurso Depuração condicional permite habilitar seletivamente depurações e logs para recursos específicos com base em um conjunto de condições definidas por você. Isso é útil para conter informações de depuração somente para hosts ou tráfego específicos.

Uma condição se refere a um recurso ou identidade, em que a identidade pode ser uma interface, um endereço IP ou um endereço MAC e assim por diante..

Como habilitar a depuração condicional para depurações de pacotes e eventos para solucionar problemas do DHCP Snooping.

Comando	Propósito
debug condition mac <mac-address> Exemplo: switch#**debug condition mac**	Configura a depuração condicional para o endereço MAC especificado.

bc16.6509.3314	
debug condition vlan <VLAN Id> Exemplo: switch#**debug condition vlan 10**	Configura a depuração condicional para a VLAN especificada.
debug condition interface <interface> Exemplo: switch#**debug condition interface vinteCincoGigE 1/0/8**	Configura a depuração condicional para a interface especificada.

Para depurar o DHCP Snooping, use os comandos mostrados na tabela.

Comando	Propósito
debug dhcp [detail | oper | redundância]	**detalhar o** conteúdo do pacote DHCP **oper** DHCP internal OPER **redundância** Suporte a redundância de cliente DHCP
debug ip dhcp server packet detail	Decodificar as recepções e transmissões de mensagens em detalhes
debug ip dhcp server events	Relate atribuições de endereço, vencimento do leasing etc.
debug ip dhcp snooping agent	Debug dhcp snooping database read and write
debug ip dhcp snooping event	Evento de depuração entre cada componente
debug ip dhcp snooping packet	Depurar pacote DHCP no módulo de rastreamento de DHCP

Esta é uma saída de exemplo parcial do comando **debug ip dhcp snooping**.

<#root>

```
Apr 14 16:16:46.835: DHCP_SNOOPING: process new DHCP packet,
message type: DHCPDISCOVER, input interface: Fo1/0/2
, MAC da: ffff.ffff.ffff, MAC
```

sa: 00a3.d144.2046,

IP da: 255.255.255.255, IP sa: 0.0.0.0, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.0.
Apr 14 16:16:46.835: DHCP_SNOOPING: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is 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.

Para depurar eventos de rastreamento de DHCP, siga estas etapas:

> **Cuidado**: use os comandos debug com cuidado. Esteja ciente de que muitos **comandos de depuração** têm impacto na rede ativa e são recomendados para uso somente em um ambiente de laboratório quando o problema for reproduzido.

Etapas de resumo

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

Etapas detalhadas

	Comando ou Ação	**Propósito**
Passo 1	**enable** Exemplo: switch#**enable**	Ativa o modo EXEC privilegiado. • Digite sua senha, se solicitado.
Passo 2	**debug platform condition mac** {mac-address} Exemplo: switch#**debug platform condition mac 0001.6509.3314**	Configura a depuração condicional para o endereço MAC especificado.
Etapa 3	**debug platform condition start** Exemplo: switch#**debug platform condition start**	Inicia a depuração condicional (isso pode iniciar o rastreamento radioativo se houver uma correspondência em uma das condições).
Passo 4	**show platform condition** OR **show debug** Exemplo: switch#**show platform condition** switch#**show debug**	Exibe o conjunto de condições atual.
Etapa 5	**debug platform condition stop**	Interrompe a depuração condicional (isso pode interromper o

	Comando ou Ação	Propósito
	Exemplo: switch#**debug platform condition stop**	rastreamento radioativo).
Etapa 6	**show platform software trace message ios R0 reverse | incluir DHCP** Exemplo: switch#**show platform software trace message ios R0 reverse | incluir DHCP**	Exibe logs da HP mesclados do arquivo de rastreamento mais recente.
Etapa 7	**clear platform condition all** Exemplo: switch#**clear platform condition all**	Limpa todas as condições.

Este é um exemplo de saída parcial do **dplataforma de depuração** comando **dhcp-snoop all**.

<#root>

debug platform dhcp-snoop all

DHCP Server UDP port

(67)

DHCP Client UDP port

(68)

RELEASE

```
Apr 14 16:44:18.629: pak->vlan_id = 10
Apr 14 16:44:18.629: dhcp packet src_ip(10.0.0.6) dest_ip(10.0.0.1) src_udp(68) dest_udp(67) src_mac(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
```

Esta tabela lista os vários comandos que podem ser usados para depurar o DHCP Snooping na plataforma.

> **Cuidado**: use os comandos debug com cuidado. Esteja ciente de que muitos comandos de depuração têm um impacto na rede ativa e somente são recomendados para uso em um ambiente de laboratório quando o problema for reproduzido.

Comando	Propósito
switch#**debug platform dhcp-snoop [todos pacote | | pd-shim]**	**all** NGWC DHCP Snooping **packet** NGWC DHCP Snooping Informações de depuração de pacotes **pd-shim** NGWC DHCP Snooping IOS Shim Debug Info
switch#**debug platform software infrastructure punt dhcp-snoop**	Pacotes recebidos no FP que são apontados para o plano de controle)
switch#**debug platform software infrastructure inject**	Pacotes injetados no FP a partir do plano de controle

Solucionar problemas de tráfego de punt/caminho (CPU)

Verifique, da perspectiva do FED, qual tráfego é recebido em cada fila de CPU (o DHCP Snooping é um tipo de tráfego processado pelo plano de controle).

- Quando o tráfego chega ao switch, ele é enviado para a CPU na direção PUNT e é enviado para a fila

dhcp snoop.

- Depois que o tráfego é processado pelo switch, ele sai pela direção INJECT. Os pacotes DHCP OFFER e ACK caem na fila de controle/legado de L2.

<#root>

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


Statistics for all causes

Cause   Cause Info                  Rcvd         Dropped
--------------------------------------------------------------------------------
21      RP<->QFP keepalive          8533         0

79      dhcp snoop                  71           0      <<---- If drop counter increases, there can be a


96      Layer2 control protocols    45662        0
109     snoop packets               100          0
--------------------------------------------------------------------------------


c9500#show platform software fed sw active inject cause summary


Statistics for all causes

Cause Cause Info                  Rcvd           Dropped
--------------------------------------------------------------------------------

1     L2 control/legacy


         128354         0     <<---- dropped counter must NOT increase


2     QFP destination lookup      18             0
5     QFP <->RP keepalive         8585           0
12    ARP request or response     68             0
25    Layer2 frame to BD          81             0
--------------------------------------------------------------------------------
```

Você pode usar esse comando para confirmar o tráfego que é enviado para a CPU e verificar se o DHCP Snooping descarta o tráfego.

<#root>

```
c9500#

show platform software fed switch active punt cpuq rates

Punt Rate CPU Q Statistics

Packets per second averaged over 10 seconds, 1 min and 5 mins
================================================================================
Q  |              Queue              |  Rx  |  Rx   |  Rx   |  Drop  |  Drop  |  Drop
no |              Name               | 10s  |  1min |  5min |  10s   |  1min  |  5min
================================================================================
```

```
0 CPU_Q_DOT1X_AUTH                    0        0      0        0        0        0
1 CPU_Q_L2_CONTROL                    0        0      0        0        0        0
2 CPU_Q_FORUS_TRAFFIC                 0        0      0        0        0        0
3 CPU_Q_ICMP_GEN                      0        0      0        0        0        0
4 CPU_Q_ROUTING_CONTROL               0        0      0        0        0        0
5 CPU_Q_FORUS_ADDR_RESOLUTION         0        0      0        0        0        0
6 CPU_Q_ICMP_REDIRECT                 0        0      0        0        0        0
7 CPU_Q_INTER_FED_TRAFFIC             0        0      0        0        0        0
8 CPU_Q_L2LVX_CONTROL_PKT             0        0      0        0        0        0
9 CPU_Q_EWLC_CONTROL                  0        0      0        0        0        0
10 CPU_Q_EWLC_DATA                    0        0      0        0        0        0
11 CPU_Q_L2LVX_DATA_PKT               0        0      0        0        0        0
12 CPU_Q_BROADCAST                    0        0      0        0        0        0
13 CPU_Q_LEARNING_CACHE_OVFL          0        0      0        0        0        0
14 CPU_Q_SW_FORWARDING                0        0      0        0        0        0
15 CPU_Q_TOPOLOGY_CONTROL             2        2      2        0        0        0
16 CPU_Q_PROTO_SNOOPING               0        0      0        0        0        0
```

17 CPU_Q_DHCP_SNOOPING

```
0        0      0        0        0
```

0   <<---- drop counter must NOT increase

```
18 CPU_Q_TRANSIT_TRAFFIC              0        0      0        0        0        0
19 CPU_Q_RPF_FAILED                   0        0      0        0        0        0
20 CPU_Q_MCAST_END_STATION_SERVICE    0        0      0        0        0        0
21 CPU_Q_LOGGING                      0        0      0        0        0        0
22 CPU_Q_PUNT_WEBAUTH                 0        0      0        0        0        0
23 CPU_Q_HIGH_RATE_APP                0        0      0        0        0        0
24 CPU_Q_EXCEPTION                    0        0      0        0        0        0
25 CPU_Q_SYSTEM_CRITICAL              8        8      8        0        0        0
26 CPU_Q_NFL_SAMPLED_DATA             0        0      0        0        0        0
27 CPU_Q_LOW_LATENCY                  0        0      0        0        0        0
28 CPU_Q_EGR_EXCEPTION                0        0      0        0        0        0
29 CPU_Q_FSS                          0        0      0        0        0        0
30 CPU_Q_MCAST_DATA                   0        0      0        0        0        0
31 CPU_Q_GOLD_PKT                     0        0      0        0        0        0

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

Solucionar problemas de hardware

Driver do Mecanismo de Encaminhamento (FED)

O FED é o driver que programa o ASIC. Os comandos do FED são usados para verificar se os estados do hardware e do software são correspondentes.

Obter o valor DI_Handle

- O identificador de ID refere-se ao índice de destino de uma porta específica.

<#root>

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

```
Platform Security DHCP Snooping Vlan Information

Value of Snooping DI handle
 is::
0x7F7FAC23E438   <<---- If DHCP Snooping is not enabled the hardware handle can not be present




                                                                Port             Trust Mode
--------------------------------------------------------------------------------
                                                 FortyGigabitEthernet1/0/10
 trust <<---- Ensure TRUSTED ports are listed
```

Verifique o mapeamento ifm para determinar o Asic e o núcleo das portas.

- O IFM é um índice de interface interna mapeado para uma porta/núcleo/asic específica.

```
<#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
```

Use DI_Handle para obter o índice de hardware.

```
<#root>
c9500#show platform hardware fed switch active fwd-asic abstraction print-resource-handle 0x7F7FAC23E438
 0
Handle:0x7f7fac23e438 Res-Type:ASIC_RSC_DI Res-Switch-Num:255 Asic-Num:255 Feature-ID:AL_FID_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
```

Converta do hexadecimal o valor de índice 0x5f03 em decimal.

0x5f03 = 24323

Use esse valor de índice em decimal e os valores ASIC e Core nesse comando para ver quais sinalizadores estão definidos para a porta.

<#root>

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

asic

1

core

1

For asic 1 core 1

Module 0 - SifDestinationIndexTable[0][

24323

]

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

copySegment0 :

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

CSCvi39202)copySegment1 : 0x1
dpuSegment0 : 0x0
dpuSegment1 : 0x0
ecUnicast : 0x0
etherChannel0 : 0x0
etherChannel1 : 0x0
hashPtr1 : 0x0
stripSegment : 0x0

Certifique-se de que o rastreamento de DHCP esteja habilitado para a VLAN específica.

<#root>

c9500#show platform software fed switch 1 vlan 10

VLAN Fed Information

Vlan Id IF Id LE Handle STP Handle L3 IF Handle SVI IF
---
10 0x0000000000420011

0x00007f7fac235fa8

0x00007f7fac236798 0x0000000000000000 0x0000000000000000 15

c9500#

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

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

Handle:0x7f7fac235fa8 Res-Type:ASIC_RSC_VLAN_LE Res-Switch-Num:255 Asic-Num:255 Feature-ID:AL_FID_L2 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 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>
```

Esta tabela lista os vários comandos Punject show/debug comuns que podem ser usados para rastrear o caminho do pacote DHCP em uma rede ativa.

Comandos Punt/Inject show & debug comuns
debug plat soft fed switch acti inject 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|ative|standby>] inject verbose **â€" > use filter cpmand mostrado para definir o escopo dos rastreamentos para este host específico**
set platform software trace fed [switch<num|ative|standby>] inject debug boot **â€" > for reload**
set platform software trace fed [switch<num|ative|standby>] punt noise
show platform software fed [switch<num|ative|standby>] insere resumo da causa
show platform software fed [switch<num|ative|standby>] punt cause summary
show platform software fed [switch<num|ative|standby>] inject cpuq 0
show platform software fed [switch<num|ative|standby>] punt cpuq 17 (dhcp queue)
show platform software fed [switch<num|ative|standby>] ative inject packet-capture det
show platform software infrastructure inject
show platform software infrastructure punt
show platform software infrastructure lsmpi driver
debug platform software infra punt dhcp
debug platform software infra inject

Esses comandos são úteis para verificar se algum pacote DHCP foi recebido para um cliente específico.

- Este recurso permite capturar toda a comunicação de rastreamento de DHCP associada a um determinado endereço MAC do cliente que é processado pela CPU através do software IOS-DHCP.
- Essa funcionalidade é suportada para tráfego IPv4 e IPv6.

- Este recurso é habilitado automaticamente.

Importante: esses comandos estão disponíveis no Cisco IOS XE Gibraltar 16.12.X.

---

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

<#root>

```
C9300#
```

```
show platform dhcpsnooping client stats 0000.1AC2.C148
```

```
DHCPSN: DHCP snooping server
DHCPD:  DHCP protocol daemen
L2FWD:  Transmit Packet to driver in L2 format
FWD:    Transmit Packet to driver
Packet Trace for client MAC 0000.1AC2.C148:
Timestamp            Destination MAC  Destination Ip  VLAN  Message      Handler:Action
-------------------- ---------------- --------------- ----  ------------ --------------
06-27-2019 20:48:28  FFFF.FFFF.FFFF   255.255.255.255 88   DHCPDISCOVER PUNT:RECEIVED
06-27-2019 20:48:28  FFFF.FFFF.FFFF   255.255.255.255 88   DHCPDISCOVER PUNT:TO_DHCPSN
06-27-2019 20:48:28  FFFF.FFFF.FFFF   255.255.255.255 88   DHCPDISCOVER BRIDGE:RECEIVED
06-27-2019 20:48:28  FFFF.FFFF.FFFF   255.255.255.255 88   DHCPDISCOVER BRIDGE:TO_DHCPD
06-27-2019 20:48:28  FFFF.FFFF.FFFF   255.255.255.255 88   DHCPDISCOVER BRIDGE:TO_INJECT
06-27-2019 20:48:28  FFFF.FFFF.FFFF   255.255.255.255 88   DHCPDISCOVER L2INJECT:TO_FWD
06-27-2019 20:48:28  0000.0000.0000   192.168.1.1     0    DHCPDISCOVER INJECT:RECEIVED
06-27-2019 20:48:28  0000.0000.0000   192.168.1.1     0    DHCPDISCOVER INJECT:TO_L2FWD
06-27-2019 20:48:30  0000.0000.0000   10.1.1.3        0    DHCPOFFER    INJECT:RECEIVED
06-27-2019 20:48:30  0000.1AC2.C148   10.1.1.3        0    DHCPOFFER    INTERCEPT:RECEIVED
06-27-2019 20:48:30  0000.1AC2.C148   10.1.1.3        88   DHCPOFFER    INTERCEPT:TO_DHCPSN
06-27-2019 20:48:30  0000.1AC2.C148   10.1.1.3        88   DHCPOFFER    INJECT:CONSUMED
06-27-2019 20:48:30  FFFF.FFFF.FFFF   255.255.255.255 88   DHCPREQUEST  PUNT:RECEIVED
06-27-2019 20:48:30  FFFF.FFFF.FFFF   255.255.255.255 88   DHCPREQUEST  PUNT:TO_DHCPSN
06-27-2019 20:48:30  FFFF.FFFF.FFFF   255.255.255.255 88   DHCPREQUEST  BRIDGE:RECEIVED
06-27-2019 20:48:30  FFFF.FFFF.FFFF   255.255.255.255 88   DHCPREQUEST  BRIDGE:TO_DHCPD
06-27-2019 20:48:30  FFFF.FFFF.FFFF   255.255.255.255 88   DHCPREQUEST  BRIDGE:TO_INJECT
06-27-2019 20:48:30  FFFF.FFFF.FFFF   255.255.255.255 88   DHCPREQUEST  L2INJECT:TO_FWD
06-27-2019 20:48:30  0000.0000.0000   192.168.1.1     0    DHCPREQUEST  INJECT:RECEIVED
06-27-2019 20:48:30  0000.0000.0000   192.168.1.1     0    DHCPREQUEST  INJECT:TO_L2FWD
06-27-2019 20:48:30  0000.0000.0000   10.1.1.3        0    DHCPACK      INJECT:RECEIVED
06-27-2019 20:48:30  0000.1AC2.C148   10.1.1.3        0    DHCPACK      INTERCEPT:RECEIVED
06-27-2019 20:48:30  0000.1AC2.C148   10.1.1.3        88   DHCPACK      INTERCEPT:TO_DHCPSN
```

Use estes comandos para limpar o rastreamento.

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

Captura de pacote de caminho de CPU

Confirme se os pacotes DHCP Snooping chegam e deixam o plano de controle corretamente.

> **Observação**: para obter referências adicionais sobre como usar a ferramenta de captura de CPU do driver do mecanismo de encaminhamento, consulte a seção Leitura adicional.

<#root>

debug platform software fed

 [switch<num|active|standby>]

punt/inject

 packet-capture start

debug platform software fed

 [switch<num|active|standby>]

punt/inject

 packet-capture stop

show platform software fed

  [switch<num|active|standby>]

punt/inject

 packet-capture brief

PUNT

DISCOVER

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

physical: FortyGigabitEthernet1/0/2

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

[dhcp snoop],

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

src mac: 00a3.d144.2046

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

67

, src port:

68

OFFER

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

physical: FortyGigabitEthernet1/0/10

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

[dhcp snoop]

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

src mac: 701f.539a.fe46

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

src ip: 10.0.0.1

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

68

, src port:

67

REQUEST

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

physical: FortyGigabitEthernet1/0/2

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

[dhcp snoop]

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

src mac: 00a3.d144.2046

ether hdr : ethertype: 0x0800 (IPv4)

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

67

, src port:

68

ACK

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

physical: FortyGigabitEthernet1/0/10

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

[dhcp snoop]

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

src mac: 701f.539a.fe46

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

src ip: 10.0.0.1

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

68

, src port:

67

INJECT

DISCOVER

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

FortyGigabitEthernet1/0/2

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

src mac: 00a3.d144.2046

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

67

, src port:

68

OFFER

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

FortyGigabitEthernet1/0/2

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

src mac: 701f.539a.fe46

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

src ip: 10.0.0.1

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

68,

src port:

67

REQUEST

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

FortyGigabitEthernet1/0/2

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

src mac: 00a3.d144.2046

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

```
udp hdr : dest port:
 67
, src port:
68



ACK


------ Inject Packet Number: 53, Timestamp: 2021/04/14 19:53:03.278 ------
interface : pal:
FortyGigabitEthernet1/0/2
 [if-id: 0x0000000a]
metadata : cause: 1 [L2 control/legacy], sub-cause: 0, q-no: 0, linktype: MCP_LINK_TYPE_LAYER2 [10]
ether hdr : dest mac: ffff.ffff.ffff,
src mac: 701f.539a.fe46


ether hdr : ethertype: 0x0800 (IPv4)
ipv4 hdr : dest ip: 255.255.255.255,
src ip: 10.0.0.1


ipv4 hdr : packet len: 330, ttl: 255, protocol: 17 (UDP)
udp hdr : dest port:
68
, src port:
67
```

Rastreamentos úteis

Esses são rastreamentos binários que exibem eventos por processo ou componente. Neste exemplo, os rastreamentos mostram informações sobre o componente dhcpsn.

- Os rastreamentos podem ser girados manualmente, o que significa que você pode criar um novo arquivo antes de começar a solucionar problemas para que ele contenha informações mais precisas.

```
<#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 e explicações

Violações dos limites de taxa do DHCP.

Explicação: o rastreamento de DHCP detectou uma violação de limite de taxa de pacote DHCP na interface especificada.

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

Falsificação do servidor DHCP em uma porta não confiável.

Explicação:O recurso de rastreamento de DHCP descobriu determinados tipos de mensagens DHCP não permitidas na interface não confiável, o que indica que algum host está tentando atuar como um servidor DHCP.

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

O endereço MAC da Camada 2 não corresponde ao endereço MAC dentro da solicitação DHCP.

Explicação: O recurso de rastreamento de DHCP tentou a validação do endereço MAC e a verificação falhou. O endereço MAC origem no cabeçalho Ethernet não corresponde ao endereço no campo chaddr da mensagem de solicitação DHCP. Pode haver um host mal-intencionado que tente realizar um ataque de negação de serviço no servidor DHCP.

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

Opção 82 - Problema de inserção.

Explicação: o recurso de rastreamento de DHCP descobriu um pacote DHCP com valores de opção não permitidos na porta não confiável, o que indica que algum host está tentando atuar como um servidor ou retransmissão de DHCP.

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

O endereço MAC da Camada 2 foi recebido na porta errada.

Explicação: o recurso de rastreamento de DHCP detectou um host tentando realizar um ataque de negação de serviço em outro host na rede.

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

Mensagens DHCP recebidas na interface não confiável.

Explicação:O recurso de rastreamento de DHCP descobriu determinados tipos de mensagens DHCP não permitidas na interface não confiável, o que indica que algum host está tentando atuar como um servidor DHCP.

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

Falha na transferência de rastreamento de DHCP. Não é possível acessar a URL.

Explicação: falha na transferência da associação de rastreamento de DHCP.

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

Avisos de rastreamento de DHCP

Número de identificação do bug da Cisco	Descrição
CSCvi39202	O DHCP falha quando a confiança de rastreamento de DHCP está habilitada no uplink etherchannel.
CSCvp49518	O banco de dados de rastreamento de DHCP não é atualizado após o recarregamento.
CSCvk16813	O tráfego do cliente DHCP foi descartado com rastreamento de DHCP e uplinks de canal de porta ou de pilha cruzada.
CSCvd51480	Desligando o rastreamento de dhcp de ip e o rastreamento de dispositivo.
CSCvm55401	O rastreamento de DHCP pode descartar pacotes da opção 82 de dhcp com a opção allow-untrusted de informações de rastreamento de dhcp de ip.
CSCvx25841	O estado de confiança de rastreamento de DHCP é interrompido quando há uma alteração no segmento REP.
CSCvs15759	O servidor DHCP envia um pacote NAK durante o processo de renovação do DHCP.
CSCvk34927	A tabela de rastreamento de DHCP não foi atualizada do arquivo de banco de dados de rastreamento de DHCP durante o recarregamento.

SDA Border DHCP Snooping

CLI de estatísticas de rastreamento de DHCP.

Uma nova CLI disponível para o SDA verificar as estatísticas de rastreamento de DHCP.

> **Observação**: para obter referências adicionais sobre o processo DHCP/fluxo de pacote e decodificação da borda da estrutura de acesso SD da Cisco, consulte o guia na seção Informações relacionadas.

---

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  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
```

Informações Relacionadas

Guia de configuração de serviços de endereçamento IP, Cisco IOS XE Amsterdam 17.3.x (Switches Catalyst 9200)

Guia de configuração de serviços de endereçamento IP, Cisco IOS XE Amsterdam 17.3.x (Switches Catalyst 9300)

Guia de configuração de serviços de endereçamento IP, Cisco IOS XE Amsterdam 17.3.x (Switches Catalyst 9400)

Guia de configuração de serviços de endereçamento IP, Cisco IOS XE Amsterdam 17.3.x (Switches Catalyst 9500)

Guia de configuração de serviços de endereçamento IP, Cisco IOS XE Amsterdam 17.3.x (Switches Catalyst 9600)

Processo/fluxo de pacote e decodificação de DHCP de borda de malha de acesso SD da Cisco

Configurar a captura de pacotes de CPU FED nos Switches Catalyst 9000

Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.