Solucionar problemas de integridad de base de datos de detección DHCP debido a NTP

Contenido

Introducción

Este documento describe la relación entre NTP y la base de datos de snooping DHCP, destacando la sincronización de tiempo en la grabación y restaurando los enlaces DHCP.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

Conocimientos básicos sobre:

- Arquitectura de switches Catalyst serie 9000
- Software Cisco IOS® XE y línea de comandos
- DHCP (protocolo de configuración dinámica de host), snooping de DHCP y funciones relacionadas
- NTP (protocolo de tiempo de red)

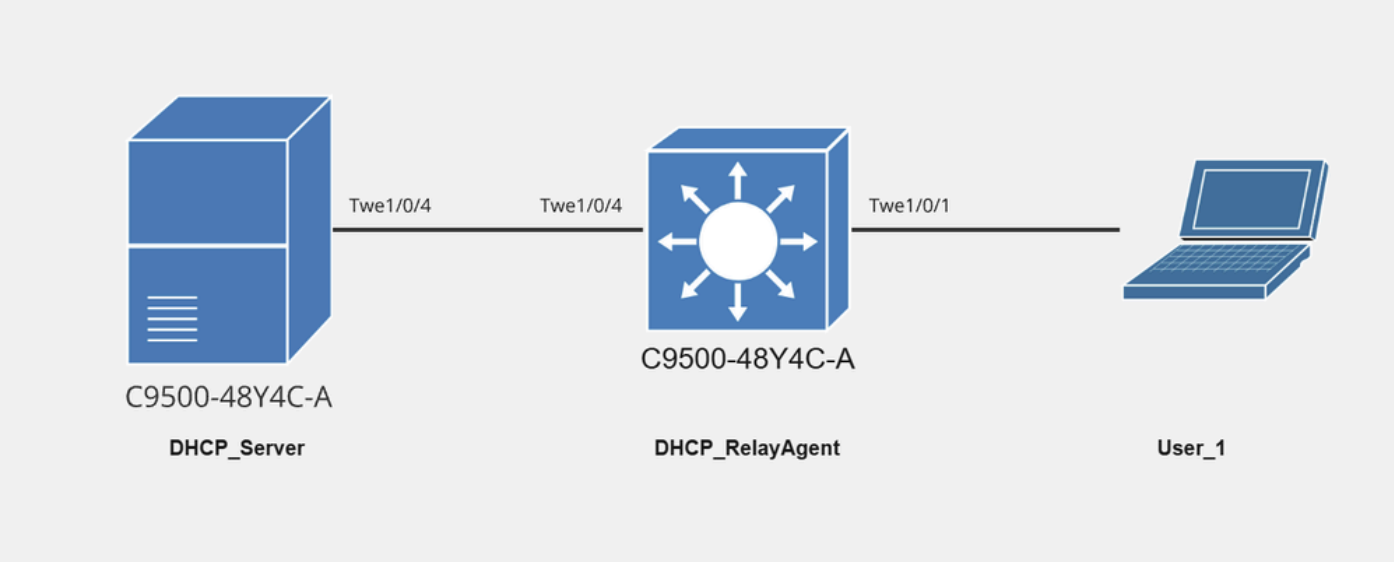
Componentes Utilizados

La información de este documento se basa en Cisco Catalyst C9500 en Cisco IOS® Software

Release 17.12.4.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Topología



Diagrama_de_red con User_1

Función de la accesibilidad NTP y NTP en la población de la base de datos de detección DHCP

En un switch o dispositivo de red con el snooping DHCP habilitado, la tabla de enlace contiene información dinámica en tiempo real acerca de las direcciones IP, las direcciones MAC, las VLAN y los tiempos de vencimiento de las concesiones. Esta información es vital para verificar los clientes DHCP y proteger la red de los servidores DHCP no autorizados.

Sin embargo, la base de datos de indagación suele estar diseñada para proporcionar persistencia para esta información, de modo que se pueda restaurar después de un reinicio. Se puede realizar una copia de seguridad periódica de la base de datos y la información se almacena en un archivo persistente (por ejemplo, flash:backup.text).Para que este procedimiento de copia de seguridad funcione correctamente, es necesario que el sistema tenga una hora exacta, especialmente para las marcas de tiempo de caducidad de los arrendamientos y otros datos sensibles al tiempo.

NTP es esencial para garantizar que el reloj del sistema se sincronice con precisión. El sistema depende de la hora exacta para:

- Calcule el vencimiento de la concesión para las vinculaciones DHCP.
- Asegúrese de que se escriben las marcas de tiempo correctas en la base de datos de indagación cuando se guarda la tabla de enlace.

Si el servidor NTP es inalcanzable o si el sistema no puede sincronizar su reloj, el sistema no puede tener una referencia horaria precisa para manejar correctamente las marcas de tiempo de vencimiento para las concesiones DHCP. Esto lleva a los siguientes problemas:

1. Problema de tiempo de vencimiento del arrendamiento

Una marca de tiempo incorrecta podría ocasionar problemas como:

- Expiración o renovación de arrendamientos incorrecta.
- Información de enlace DHCP obsoleta o desactualizada en la base de datos de detección.

2. Impacto en el backup de la tabla vinculante

Cuando el servidor NTP es accesible, el sistema puede generar marcas de tiempo precisas para cada concesión DHCP y realizar una copia de seguridad correcta de la tabla de enlace en la base de datos de indagación.

Si el servidor NTP no es accesible, el dispositivo no podrá determinar la hora actual correcta, lo que provocará 0 intentos de escribir información de enlace válida en la base de datos.

3. Copia de seguridad de base de datos no fiable

La base de datos de indagación almacena información de enlace de forma persistente, incluido el tiempo de caducidad de cada concesión.

Sin una hora exacta del sistema de NTP , el dispositivo no puede escribir marcas de tiempo precisas para los vencimientos de arrendamiento al guardar en la base de datos.

Si el servidor NTP se puede alcanzar de forma intermitente, se produce un problema de integridad entre la tabla de enlace DHCP y la tabla de base de datos de snooping DHCP. Como resultado, los datos de la base de datos de snooping se consideran incompletos o incorrectos.

Configuración base

Paso 1. Habilite la indagación DHCP globalmente y bajo las VLAN, en el agente relay. En este caso, el agente relay y el switch de acceso son iguales.

```
DHCP_RelayAgent#configure terminal
DHCP_RelayAgent(config)#ip dhcp snooping
DHCP_RelayAgent(config)#ip dhcp snooping vlan 10
```

Paso 2. Configure la confianza de indagación DHCP en todas las interfaces del switch que reciben ofertas DHCP de servidores DHCP genuinos. El número de estas interfaces depende del diseño de la red y de la ubicación de los servidores DHCP. Estas son las interfaces que van hacia el servidor DHCP genuino.

<#root>

```
DHCP_RelayAgent# show running-configuration interface TwentyFiveGigE1/0/4

Building configuration...
Current configuration : 84 bytes
!
interface TwentyFiveGigE1/0/4
 switchport mode trunk
 ip dhcp snooping trust
end
```

Paso 3. Configure la base de datos de snooping DHCP en una ubicación para supervisar la tabla de enlace de snooping DHCP, realizar un seguimiento del estado de las operaciones de la base de datos y comprobar que la base de datos se actualiza y transfiere correctamente.

<#root>

```
DHCP_RelayAgent#configure terminal
DHCP_RelayAgent(config)#ip dhcp snooping database bootflash:dhcpsnoopingdatabase.txt
DHCP_RelayAgent(config)#ip dhcp snooping database timeout 300
DHCP_RelayAgent(config)#ip dhcp snooping database write-delay 15
```

```
DHCP_RelayAgent#show running-configuration | include database

ip dhcp snooping database bootflash:dhcpsnoopingdatabase.txt
ip dhcp snooping database write-delay 15
```

Situación 1: servidor NTP inalcanzable

<#root>

```
DHCP_RelayAgent# ping vrf Mgmt-vrf 10.81.254.131

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.81.254.131, timeout is 2 seconds:
……
Success rate is 0 percent (0/0)
```

Ahora podemos ver que User_1 ha recibido la IP 10.10.10.1 en vlan 10.

Esta es la tabla de enlace de DHCP Snooping, que muestra la dirección IP, la dirección MAC y la interfaz del usuario User_1 en TwentyFiveGigE1/0/1

<#root>

DHCP_RelayAgent#show ip dhcp snooping binding

```
MacAddress          IpAddress        Lease(sec)    Type           VLAN   Interface
------------------  ---------------  ----------   --------------  ----   --------------------
78:BC:1A:0B:D5:1F   10.10.10.1       86372        dhcp-snooping   10     TwentyFiveGigE1/0/1

Total number of bindings: 1
```

En general, una vez que el usuario recibe una dirección IP, la tabla de enlace de snooping se crea dinámicamente y la información correspondiente se agrega posteriormente a la base de datos de snooping. Pero, en este caso, como el servidor NTP es inalcanzable, ha habido 0 intentos totales de actualizar o transferir la información de enlace a la base de datos.

<#root>

DHCP_RelayAgent#show ip dhcp snooping database

```
Agent URL : bootflash:dhcpsnoopingdatabase.txt
Write delay Timer : 15 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running

Last Succeded Time : 18:37:38 UTC Mon Mar 17 2025
Last Failed Time : None
Last Failed Reason : No failure recorded.
```

Total Attempts : 0

```
         Startup Failures : 0
```

Successful Transfers : 0

```
   Failed Transfers : 0
Successful Reads : 0       Failed Reads : 0
```

Successful Writes : 0

```
      Failed Writes : 0
Media Failures : 0
```

<#root>

DHCP_RelayAgent#more flash:dhcpsnoopingdatabase.txt

%Error opening bootflash:dhcpsnoopingdatabase.txt (No such file or directory)

<#root>

```
*Mar 18 11:12:21.264: DHCP_SNOOPING: process new DHCP packet, message type: DHCPACK, input interface: Vl
*Mar 18 11:12:21.264: DHCP_SNOOPING: binary dump of option 82, length: 20 data:
0x52 0x12 0x1 0x6 0x0 0x4 0x0 0xA 0x1 0x1 0x2 0x8 0x0 0x6 0x78 0xBC 0x1A 0xB 0xC2 0x60
*Mar 18 11:12:21.264: DHCP_SNOOPING: binary dump of extracted circuit id, length: 8 data:
0x1 0x6 0x0 0x4 0x0 0xA 0x1 0x1
*Mar 18 11:12:21.264: DHCP_SNOOPING: binary dump of extracted remote id, length: 10 data:
0x2 0x8 0x0 0x6 0x78 0xBC 0x1A 0xB 0xC2 0x60
*Mar 18 11:12:21.264: actual_fmt_cid OPT82_FMT_CID_VLAN_MOD_PORT_INTF global_opt82_fmt_rid OPT82_FMT_RID
*Mar 18 11:12:21.264: DHCP_SNOOPING: opt82 data indicates local packet
*Mar 18 11:12:21.264: DHCP_SNOOPING: opt82 data indicates local packet
*Mar 18 11:12:21.264: DHCP_SNOOPING opt82_fmt_cid_intf OPT82_FMT_CID_VLAN_MOD_PORT_INTF opt82_fmt_cid_gl
*Mar 18 11:12:21.264: DHCP_SNOOPING: vlan_id 10 VNI 0 mod 1 port 1
*Mar 18 11:12:21.264: DHCP_SNOOPING: mod 1 port 1 idb Twe1/0/1 found for 78bc.1a0b.d51f
*Mar 18 11:12:21.264: DHCP_SNOOPING: add binding on port TwentyFiveGigE1/0/1 ckt_id 0 TwentyFiveGigE1/0/
*Mar 18 11:12:21.264: DHCP_SNOOPING: dhcp binding entry already exists, update binding lease time to (86

*Mar 18 11:12:21.264: ipaddr: 10.10.10.1, hwidb: TwentyFiveGigE1/0/1, type: 1, phyidb: TwentyFiveGigE1/0

*Mar 18 11:12:21.264: DHCP_SNOOPING: Reroute dhcp pak, message type: DHCPACK
*Mar 18 11:12:21.264: DHCP_SNOOPING: remove relay information option.
*Mar 18 11:12:21.264: DHCP_SNOOPING opt82_fmt_cid_intf OPT82_FMT_CID_VLAN_MOD_PORT_INTF opt82_fmt_cid_gl
*Mar 18 11:12:21.264: DHCP_SNOOPING: vlan_id 10 VNI 0 mod 1 port 1
*Mar 18 11:12:21.264: DHCP_SNOOPING: mod 1 port 1 idb Twe1/0/1 found for 78bc.1a0b.d51f
*Mar 18 11:12:21.264: DHCP_SNOOPING: calling forward_dhcp_reply
*Mar 18 11:12:21.264: platform lookup dest vlan for input_if: Vlan10, is NOT tunnel, if_output: Vlan10,
*Mar 18 11:12:21.264: DHCP_SNOOPING opt82_fmt_cid_intf OPT82_FMT_CID_VLAN_MOD_PORT_INTF opt82_fmt_cid_gl
*Mar 18 11:12:21.264: DHCP_SNOOPING: vlan_id 10 VNI 0 mod 1 port 1
*Mar 18 11:12:21.264: DHCP_SNOOPING: mod 1 port 1 idb Twe1/0/1 found for 78bc.1a0b.d51f
*Mar 18 11:12:21.264: DHCP_SNOOPING: vlan 10 after pvlan check
*Mar 18 11:12:21.264: DHCP Memory dump is printed for direct forward reply

765DFA772750: FFFF FFFFFFFF 78BC1A0B C2FF0800
765DFA772760: 4500015E 00230000 FF11A64E 0A0A0A14
765DFA772770: FFFFFFFF 00430044 014A36A8 02010600
765DFA772780: BAF1E48A 00008000 00000000 0A0A0A01
765DFA772790: 00000000 0A0A0A14 78BC1A0B D51F0000
765DFA7727A0: 00000000 00000000 00000000 00000000
765DFA7727B0: 00000000 00000000 00000000 00000000
765DFA7727C0: 00000000 00000000 00000000 00000000
765DFA7727D0: 00000000 00000000 00000000 00000000
765DFA7727E0: 00000000 00000000 00000000 00000000
765DFA7727F0: 00000000 00000000 00000000 00000000
765DFA772800: 00000000 00000000 00000000 00000000
765DFA772810: 00000000 00000000 00000000 00000000
765DFA772820: 00000000 00000000 00000000 00000000
765DFA772830: 00000000 00000000 00000000 00000000
765DFA772840: 00000000 00000000 00000000 00000000
765DFA772850: 00000000 00000000 00000000 00000000
```

```
765DFA772860: 00000000 00000000 63825363 3501053D
765DFA772870: 1A006369 73636F2D 37386263 2E316130
765DFA772880: 622E6435 31662D56 6C313036 040A0A0A
765DFA772890: 0A330400 0151803A 040000A8 C03B0400
765DFA7728A0: 01275001 04FFFFFF 00FF0000 00000000
765DFA7728B0: 00000000 00000000 00000000 00FF
*Mar 18 11:12:21.273: DHCP_SNOOPING: direct forward dhcp replyto output port: TwentyFiveGigE1/0/1.
```

***Mar 18 11:12:38.546: Write delay timer expired**

***Mar 18 11:12:38.546: Restarting write delay timer.**

***Mar 18 11:13:38.546: Write delay timer expired**

***Mar 18 11:13:38.546: Restarting write delay timer.**

***Mar 18 11:14:08.547: Write delay timer expired**

***Mar 18 11:14:08.547: Restarting write delay timer.**

```
*Mar 18 11:14:14.266: %SYS-5-CONFIG_I: Configured from console by admin on vty0 (10.110.129.206)
```

Situación 2: se puede acceder al servidor NTP

<#root>

DHCP_RelayAgent# ping vrf Mgmt-vrf 10.81.254.131

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.81.254.131, timeout is 2 seconds:
!!!!!
```

Success rate is 100 percent (5/5), round-trip min/avg/max = 175/175/176 ms

<#root>

DHCP_RelayAgent#show ip dhcp snooping binding

```
MacAddress          IpAddress        Lease(sec)    Type          VLAN   Interface
------------------  ---------------  ----------   -------------  ----   --------------------
```

78:BC:1A:0B:D5:1F   10.10.10.1   86372   dhcp-snooping 10   TwentyFiveGigE1/0/1

```
Total number of bindings: 1
```

Una vez que el usuario recibe una dirección IP, se crea dinámicamente la tabla de enlace de snooping y, posteriormente, se agrega la información correspondiente a la base de datos de snooping.Como resultado, se ha producido un intento total de actualizar o transferir la base de datos, y todos ellos se han realizado correctamente. No ha habido escrituras, lecturas o transferencias fallidas.

<#root>

DHCP_RelayAgent#show ip dhcp snooping database

```
Agent URL : bootflash:dhcpsnoopingdatabase.txt
Write delay Timer : 15 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : 29 (00:00:29)
Abort Timer Expiry : Not Running

Last Succeded Time : 18:39:27 UTC Mon Mar 17 2025
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts : 1
         Startup Failures : 0

Successful Transfers : 1
   Failed Transfers : 0
Successful Reads : 0       Failed Reads : 0

Successful Writes : 1
      Failed Writes : 0
Media Failures : 0
```

<#root>

DHCP_RelayAgent#more flash:dhcpsnoopingdatabase.txt

```
67d86a58
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
```

10.10.10.1   10   78bc.1a0b.d51f   67D9BBCA   Twe1/0/1   8b21f6ef

```
END
```

Escenario 3: servidor NTP de acceso intermitente

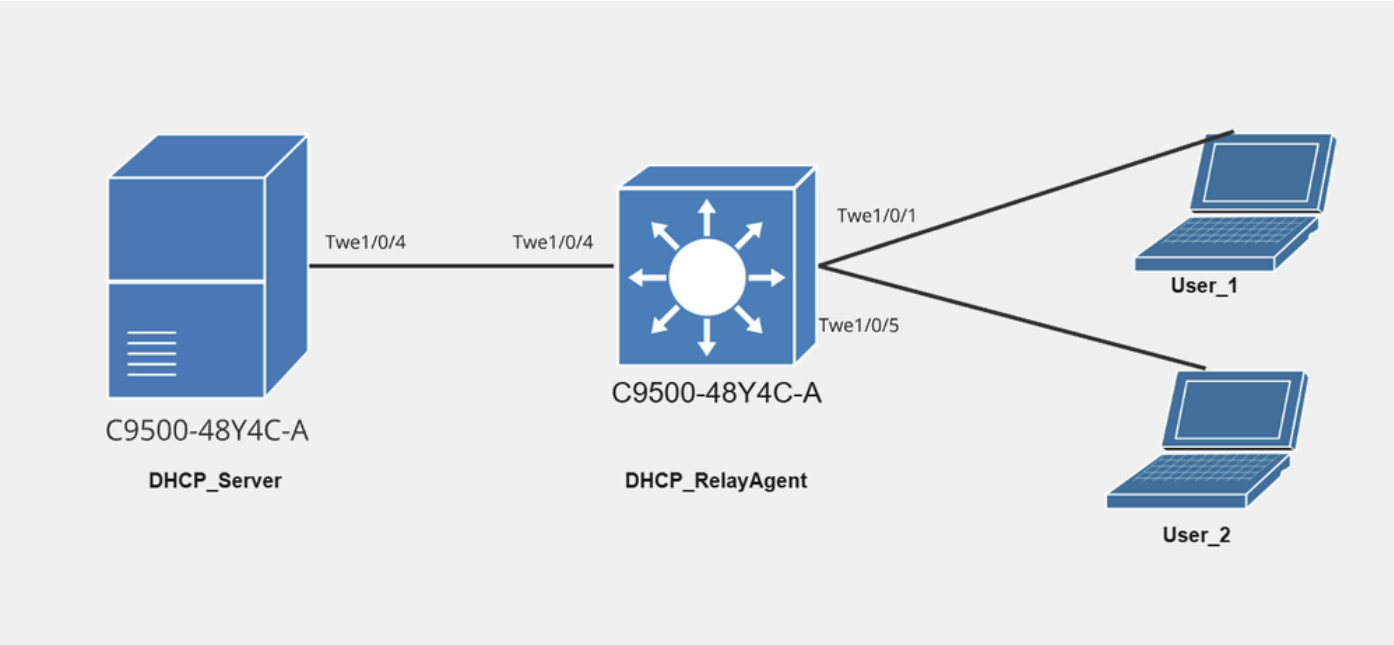


Diagrama de red con User_1 y User_2

<#root>

```
DHCP_RelayAgent# ping vrf Mgmt-vrf 10.81.254.131


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.81.254.131, timeout is 2 seconds:
!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 175/175/176 ms
```

Ahora podemos ver que User_1 ha recibido la IP 10.10.10.1 en vlan 10.

Esta es la tabla de enlace de DHCP Snooping, que muestra la dirección IP, la dirección MAC y la interfaz del usuario User_1 en TwentyFiveGigE1/0/1

<#root>

```
DHCP_RelayAgent#show ip dhcp snooping binding


MacAddress IpAddress Lease(sec) Type VLAN Interface
------------------ --------------- ---------- ------------ ---- --------------------

78:BC:1A:0B:D5:1F 10.10.10.1 86372 dhcp-snooping 10 TwentyFiveGigE1/0/1
```

```
Total number of bindings: 1
```

<#root>

DHCP_RelayAgent#show ip dhcp snooping database

```
Agent URL : bootflash:dhcpsnoopingdatabase.txt
Write delay Timer : 15 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : 29 (00:00:29)
Abort Timer Expiry : Not Running

Last Succeded Time : 18:40:20 UTC Mon Mar 17 2025
Last Failed Time : None
Last Failed Reason : No failure recorded.
```

Total Attempts : 1

```
         Startup Failures : 0
```

Successful Transfers : 1

```
   Failed Transfers : 0
Successful Reads : 0       Failed Reads : 0
```

Successful Writes : 1

```
      Failed Writes : 0
Media Failures : 0
```

<#root>

DHCP_RelayAgent#more flash:dhcpsnoopingdatabase.txt

```
67d86a58
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
```

10.10.10.1 10 78bc.1a0b.d51f 67D9BBCA Twe1/0/1 8b21f6ef

```
END
```

Después de un tiempo, el NTP pasó a ser inalcanzable, pero User_2 obtuvo su dirección IP 10.10.10.2 en vlan 10 y se actualizó en la tabla de enlace pero no se insertó en la tabla de la base

de datos de indagación.

<#root>

```
DHCP_RelayAgent# ping vrf Mgmt-vrf 10.81.254.131

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.81.254.131, timeout is 2 seconds:
.....
Success rate is 0 percent (0/0)
```

Esta es la tabla de enlace de DHCP Snooping, que muestra la dirección IP, la dirección MAC y la interfaz para User_2 en TwentyFiveGigE1/0/5

<#root>

```
DHCP_RelayAgent#show ip dhcp snooping binding

MacAddress          IpAddress        Lease(sec)   Type           VLAN   Interface
------------------  ---------------  ----------   -------------  ----   --------------------
78:BC:1A:0B:D5:1F   10.10.10.1       86217        dhcp-snooping  10     TwentyFiveGigE1/0/1

F8:E5:7E:75:04:46   10.10.10.2       85336        dhcp-snooping  10     TwentyFiveGigE1/0/5
Total number of bindings: 2
```

La entrada en la base de datos de indagación no aumenta y el total de escrituras correctas sigue siendo 1.

<#root>

```
DHCP_RelayAgent#show ip dhcp snooping database

Agent URL : bootflash:dhcpsnoopingdatabase.txt
Write delay Timer : 15 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : 29 (00:00:29)
Abort Timer Expiry : Not Running

Last Succeded Time : 18:41:38 UTC Mon Mar 17 2025
Last Failed Time : None
```

```
Last Failed Reason : No failure recorded.


Total Attempts : 1

         Startup Failures : 0


Successful Transfers : 1

   Failed Transfers : 0
Successful Reads : 0       Failed Reads : 0


Successful Writes : 1

      Failed Writes : 0
Media Failures : 0
```

<#root>

```
DHCP_RelayAgent#more flash:dhcpsnoopingdatabase.txt


67d86a58
TYPE DHCP-SNOOPING
VERSION 1
BEGIN

10.10.10.1  10  78bc.1a0b.d51f  67D9BBCA  Twe1/0/1  8b21f6ef


END
```

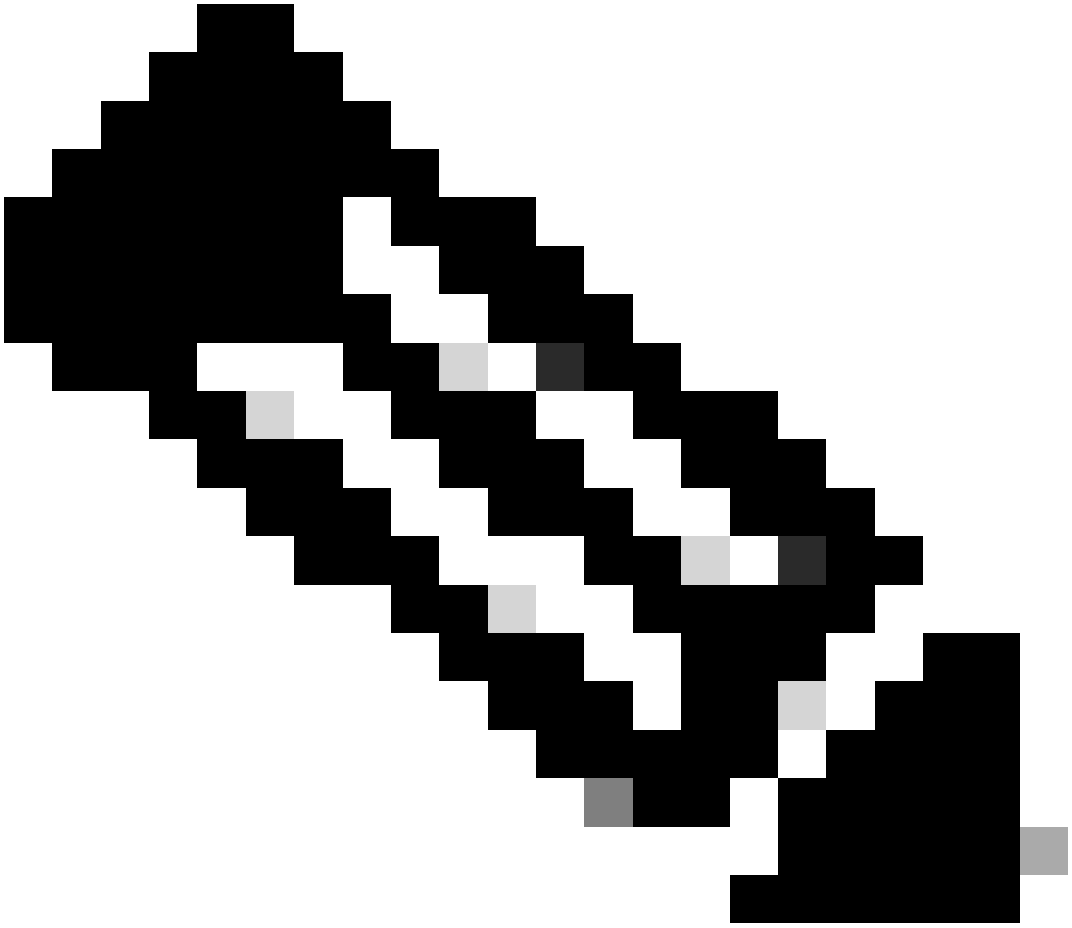
Cuando se puede acceder al servidor NTP, el sistema sincroniza la tabla de enlace de snooping DHCP y la base de datos de snooping DHCP. Este escenario no se muestra aquí. Sin embargo, se pueden lograr resultados similares si se elimina la configuración del servidor NTP.

Una vez eliminada la configuración NTP, la entrada correspondiente a User_2 se agrega a la tabla de base de datos de snooping.
En este caso, el switch utiliza la hora del reloj del sistema.

<#root>

```
DHCP_RelayAgent#configure terminal

DHCP_RelayAgent(config)# no ntp server 10.81.254.131
```



Nota: A modo de demostración, hemos eliminado la configuración del servidor NTP. Técnicamente, el resultado de un servidor NTP accesible y un servidor NTP no configurado es similar.

```
*Mar 17 17:26:26.475: %DHCP_SNOOPING-4-NTP_NOT_RUNNING: NTP is not running; reloaded binding lease expir
*Mar 17 17:26:26.486: %DHCP_SNOOPING-6-AGENT_OPERATION_SUCCEEDED: DHCP snooping database Write succeeded
```

<#root>

DHCP_RelayAgent#show ip dhcp snooping binding

```
MacAddress          IpAddress       Lease(sec)   Type            VLAN   Interface
------------------  --------------  ----------   -------------   ----   --------------------
78:BC:1A:0B:D5:1F   10.10.10.1      86217        dhcp-snooping   10     TwentyFiveGigE1/0/1
```

F8:E5:7E:75:04:46 10.10.10.2 85336 dhcp-snooping 10 TwentyFiveGigE1/0/5

Total number of bindings: 2

<#root>

DHCP_RelayAgent#show ip dhcp snooping database

Agent URL : bootflash:dhcpsnoopingdatabase.txt
Write delay Timer : 15 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : 29 (00:00:29)
Abort Timer Expiry : Not Running

Last Succeded Time : 18:42:16 UTC Mon Mar 17 2025
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts : 2

Startup Failures : 0

Successful Transfers : 2

Failed Transfers : 0
Successful Reads : 0 Failed Reads : 0

Successful Writes : 2

Failed Writes : 0
Media Failures : 0

<#root>

DHCP_RelayAgent#more flash:dhcpsnoopingdatabase.txt

67d86a58
TYPE DHCP-SNOOPING
VERSION 1
BEGIN

10.10.10.1 10 78bc.1a0b.d51f 67D9BBCA Twe1/0/1 8b21f6ef

10.10.10.2 10 f8e5.7e75.0446 67D9B6DC Twe1/0/5 bef43442

END

<#root>

```
*Mar 18 11:36:38.283: DHCP_SNOOPING: Reroute dhcp pak, message type: DHCPACK
*Mar 18 11:36:38.283: DHCP_SNOOPING: remove relay information option.
*Mar 18 11:36:38.283: DHCP_SNOOPING opt82_fmt_cid_intf OPT82_FMT_CID_VLAN_MOD_PORT_INTF opt82_fmt_cid_gl
*Mar 18 11:36:38.283: DHCP_SNOOPING: vlan_id 10 VNI 0 mod 1 port 1
*Mar 18 11:36:38.283: DHCP_SNOOPING: mod 1 port 1 idb Twe1/0/5 found for f8e5.7e75.0446
*Mar 18 11:36:38.283: DHCP_SNOOPING: calling forward_dhcp_reply
*Mar 18 11:36:38.283: platform lookup dest vlan for input_if: Vlan10, is NOT tunnel, if_output: Vlan10,
*Mar 18 11:36:38.283: DHCP_SNOOPING opt82_fmt_cid_intf OPT82_FMT_CID_VLAN_MOD_PORT_INTF opt82_fmt_cid_gl
*Mar 18 11:36:38.283: DHCP_SNOOPING: vlan_id 10 VNI 0 mod 1 port 1
*Mar 18 11:36:38.283: DHCP_SNOOPING: mod 1 port 1 idb Twe1/0/5 found for f8e5.7e75.0446
*Mar 18 11:36:38.283: DHCP_SNOOPING: vlan 10 after pvlan check
*Mar 18 11:36:38.283: DHCP Memory dump is printed for direct forward reply
765DFA80B990: FFFF FFFFFFFF 78BC1A0B C2FF0800
765DFA80B9A0: 4500015E 002B0000 FF11A646 0A0A0A14
765DFA80B9B0: FFFFFFFF 00430044 014A51AD 02010600
765DFA80B9C0: ED9296E4 00008000 00000000 0A0A0A01
765DFA80B9D0: 00000000 0A0A0A14 78BC1A0B D51F0000
765DFA80B9E0: 00000000 00000000 00000000 00000000
765DFA80B9F0: 00000000 00000000 00000000 00000000
765DFA80BA00: 00000000 00000000 00000000 00000000
765DFA80BA10: 00000000 00000000 00000000 00000000
765DFA80BA20: 00000000 00000000 00000000 00000000
765DFA80BA30: 00000000 00000000 00000000 00000000
765DFA80BA40: 00000000 00000000 00000000 00000000
765DFA80BA50: 00000000 00000000 00000000 00000000
765DFA80BA60: 00000000 00000000 00000000 00000000
765DFA80BA70: 00000000 00000000 00000000 00000000
765DFA80BA80: 00000000 00000000 00000000 00000000
765DFA80BA90: 00000000 00000000 00000000 00000000
765DFA80BAA0: 00000000 00000000 63825363 3501053D
765DFA80BAB0: 1A006369 73636F2D 37386263 2E316130
765DFA80BAC0: 622E6435 31662D56 6C313036 040A0A0A
765DFA80BAD0: 0A330400 0151803A 040000A8 C03B0400
765DFA80BAE0: 01275001 04FFFFFF 00FF0000 00000000
765DFA80BAF0: 00000000 00000000 00000000 00FF
*Mar 18 11:36:38.291: DHCP_SNOOPING: direct forward dhcp replyto output port: TwentyFiveGigE1/0/5.
*Mar 18 11:37:25.795: DHCP_SNOOPING: checking expired snoop binding entries
*Mar 18 11:37:36.694: %SYS-5-CONFIG_I: Configured from console by admin on vty0 (10.110.129.206)
*Mar 18 11:37:38.956: DHCPD: Reload workspace interface GigabitEthernet0/0 tableid 1.
*Mar 18 11:37:38.956: DHCPD: Sending notification of DISCOVER:
*Mar 18 11:37:38.956: DHCPD: htype 1 chaddr 7c21.0e1e.59b6
*Mar 18 11:37:38.956: DHCPD: table id 1 = vrf Mgmt-vrf
*Mar 18 11:37:38.956: DHCPD: interface = GigabitEthernet0/0
*Mar 18 11:37:38.956: DHCPD: class id 436973636f204e394b2d433933333243
*Mar 18 11:37:38.956: DHCPD: FSM state change INVALID
*Mar 18 11:37:38.956: DHCPD: Workspace state changed from INIT to INVALID
*Mar 18 11:37:39.957: DHCPD: Reload workspace interface GigabitEthernet0/0 tableid 1.
*Mar 18 11:37:39.957: DHCPD: Sending notification of DISCOVER:
*Mar 18 11:37:39.957: DHCPD: htype 1 chaddr 7c21.0e1e.59b6
*Mar 18 11:37:39.957: DHCPD: table id 1 = vrf Mgmt-vrf
*Mar 18 11:37:39.957: DHCPD: interface = GigabitEthernet0/0
*Mar 18 11:37:39.957: DHCPD: class id 436973636f204e394b2d433933333243
```

```
*Mar 18 11:37:39.957: DHCPD: FSM state change INVALID
*Mar 18 11:37:39.957: DHCPD: Workspace state changed from INIT to INVALID
*Mar 18 11:37:50.819: Write delay timer expired
*Mar 18 11:37:50.819: Restarting write delay timer.
*Mar 18 11:37:50.819: %DHCP_SNOOPING-4-NTP_NOT_RUNNING: NTP is not running; reloaded binding lease expir
*Mar 18 11:37:50.827: to string : 10.10.10.1 10 78bc.1a0b.d51f 67DAAC45 Twe1/0/1
*Mar 18 11:37:50.827: to string : 10.10.10.2 10 f8e5.7e75.0446 67D9B6DC Twe1/0/5
*Mar 18 11:37:50.832: %DHCP_SNOOPING-6-AGENT_OPERATION_SUCCEEDED: DHCP snooping database Write succeeded
*Mar 18 11:37:50.832: Resetting fail log parameters.
```

Conclusión

- Si la IP del servidor NTP está presente y es accesible, se rellenan tanto la tabla de enlace de snooping DHCP como la base de datos de snooping. Las entradas deben tener una marca de tiempo precisa usando la hora sincronizada del servidor NTP.
- Si la IP del servidor NTP está presente pero no es accesible, la tabla de enlace de snooping de DHCP se sigue rellenando, pero las entradas no se pueden rellenar en la base de datos de snooping, ya que el sistema no puede sincronizar la hora para una administración de concesiones precisa.
- Si la IP del servidor NTP no está configurada o no existe, tanto la tabla de enlace de snooping DHCP como la base de datos de snooping siguen conteniendo entradas, pero las marcas de tiempo de la base de datos de snooping no son fiables, ya que pueden basarse en la hora del sistema local.
- En resumen, para una administración precisa y confiable de la base de datos de snooping de DHCP, el NTP es crucial.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).