

Identificar e Solucionar Problemas de Integridade do Banco de Dados de Rastreamento DHCP Devido a NTP

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Topologia](#)

[Função da acessibilidade de NTP e NTP na população do banco de dados de rastreamento de DHCP](#)

[1. Emissão do Tempo de Expiração do Leasing](#)

[2. Impacto no Backup da Tabela de Vinculação](#)

[3. Backup de Banco de Dados Não Confiável](#)

[Configuração de base](#)

[Cenário 1 - Servidor NTP inalcançável](#)

[Cenário 2 - Servidor NTP alcançável](#)

[Cenário 3 - Servidor NTP Intermitentemente Acessível](#)

[Conclusão](#)

Introdução

Este documento descreve a relação entre o NTP e o banco de dados de rastreamento de DHCP, destacando a sincronização de tempo na gravação e restauração de associações de DHCP.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

Entendimento básico de:

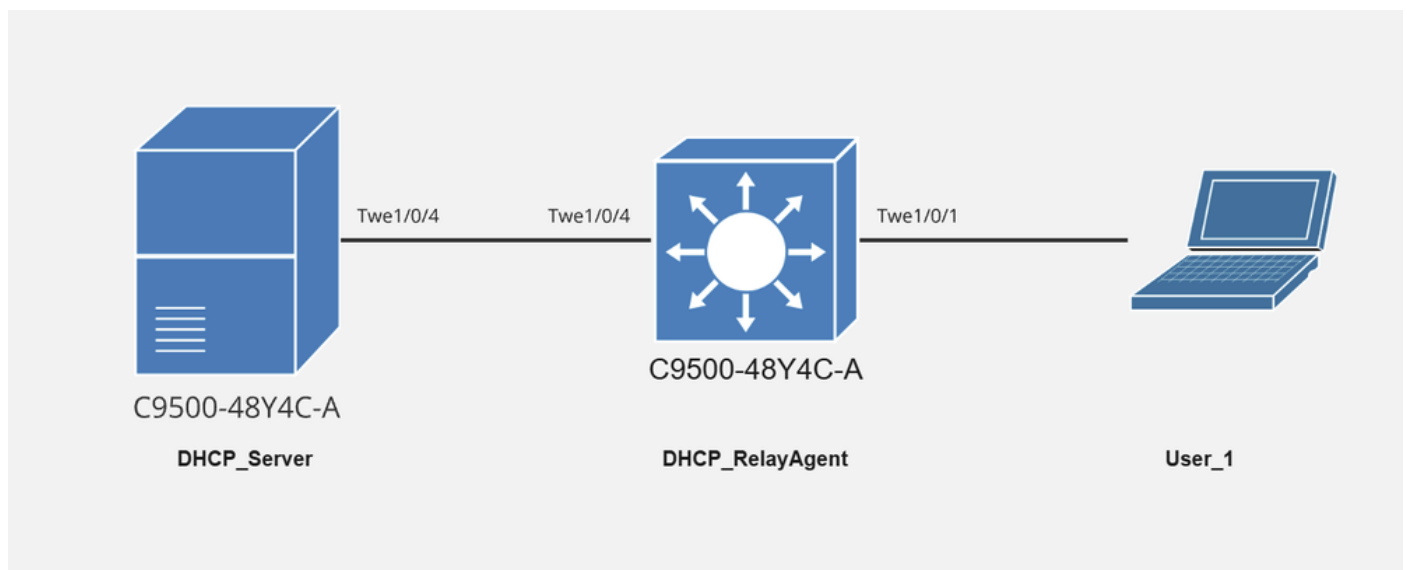
- Arquitetura dos switches Catalyst 9000 Series
- Software Cisco IOS® XE e linha de comando
- DHCP (Dynamic Host Configuration Protocol), rastreamento de DHCP e recursos relacionados
- NTP (Network Time Protocol, Protocolo de tempo de rede)

Componentes Utilizados

As informações neste documento são baseadas no Cisco Catalyst C9500 no Cisco IOS® Software Release 17.12.4.

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.

Topologia



Diagrama_de_Nete com Usuário_1

Função da acessibilidade de NTP e NTP na população do banco de dados de rastreamento de DHCP

Em um switch ou dispositivo de rede com rastreamento de DHCP habilitado, a tabela de ligação mantém informações dinâmicas em tempo real sobre endereços IP, endereços MAC, VLANs e tempos de expiração de concessão. Essas informações são vitais para verificar os clientes DHCP e proteger a rede contra servidores DHCP invasores.

No entanto, o banco de dados de rastreamento normalmente tem o objetivo de fornecer persistência para essas informações, de modo que elas possam ser restauradas após uma reinicialização. O backup do banco de dados pode ser feito periodicamente, e as informações são armazenadas em um arquivo persistente (por exemplo, `flash:backup.text`). Para que esse procedimento de backup funcione corretamente, é necessário o horário exato do sistema, particularmente para carimbos de data/hora de expiração de leasing e outros dados sensíveis ao tempo.

O NTP é essencial para garantir que o relógio do sistema esteja sincronizado com precisão. O sistema depende do tempo exato para:

- Calcule a expiração do aluguel para vinculações DHCP.
- Certifique-se de que os carimbos de data/hora corretos sejam gravados no banco de dados de rastreamento quando a tabela de associação for salva.

Se o servidor NTP estiver inacessível ou se o sistema não puder sincronizar seu relógio, o sistema não poderá ter uma referência de tempo precisa para tratar corretamente os carimbos de data/hora de expiração para concessões de DHCP. Isso leva aos seguintes problemas:

1. Emissão do Tempo de Expiração do Leasing

Um carimbo de data/hora incorreto pode causar problemas como:

- Expiração ou renovação incorreta de locações.
- Informações de associação DHCP obsoletas ou desatualizadas no banco de dados de rastreamento.

2. Impacto no Backup da Tabela de Vinculação

Quando o servidor NTP estiver acessível, o sistema poderá gerar carimbos de data/hora precisos para cada concessão de DHCP e fazer o backup correto da tabela de vinculação no banco de dados de rastreamento.

Se o servidor NTP não estiver acessível, o dispositivo não poderá determinar a hora atual correta, levando a 0 tentativas de gravar informações de vinculação válidas no banco de dados.

3. Backup de Banco de Dados Não Confiável

O banco de dados de rastreamento armazena informações de vinculação persistentemente, incluindo o tempo de expiração de cada leasing.

Sem o tempo preciso do sistema do NTP, o dispositivo não grava carimbos de data/hora precisos para expirações de leasing ao salvar no banco de dados.

Se o servidor NTP for alcançável intermitentemente, isso resultará no problema de integridade entre a tabela de ligação DHCP e a tabela de banco de dados de rastreamento DHCP. Como resultado, os dados do banco de dados de rastreamento são considerados incompletos ou incorretos.

Configuração de base

Etapa 1. Ative o rastreamento de DHCP globalmente e sob as VLANs, no agente de retransmissão. Nesse caso, o agente de retransmissão e o switch de acesso são iguais.

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

Etapa 2. Configurar a relação de confiança de rastreamento de DHCP em todas as interfaces do switch que recebe ofertas de DHCP dos servidores DHCP genuínos. O número dessas interfaces depende do projeto de rede e do posicionamento dos servidores DHCP. Essas são as interfaces que estão indo em direção ao Servidor DHCP genuíno.

<#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
```

Etapa 3. Configure o banco de dados de rastreamento de DHCP em um local para monitorar a tabela de associação de rastreamento de DHCP, rastrear a integridade das operações do banco de dados e verificar se o banco de dados está sendo corretamente atualizado e transferido.

<#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
```

Cenário 1 - Servidor NTP inalcançável

<#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)

Agora podemos ver que User_1 recebeu o IP 10.10.10.1 na vlan 10.

Esta é a tabela de ligação de rastreamento de DHCP, mostrando o endereço IP, o endereço MAC e a interface do User_1 em 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

Em geral, quando o usuário recebe um endereço IP, a tabela de ligação de rastreamento é criada dinamicamente e as informações correspondentes são adicionadas subsequentemente ao banco de dados de rastreamento. Mas, nesse caso, como o servidor NTP está inacessível, houve 0 tentativas no total para atualizar ou transferir as informações de ligação para o banco de dados.

<#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 Succeeded 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: Vlan10
*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_VLAN_MOD_PORT_INTF
*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_global
*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 Tve1/0/1 found for 78bc.1a0b.d51f
*Mar 18 11:12:21.264: DHCP_SNOOPING: add binding on port TwentyFiveGigE1/0/1 ckt_id 0 TwentyFiveGigE1/0/1
*Mar 18 11:12:21.264: DHCP_SNOOPING: dhcp binding entry already exists, update binding lease time to (86400)
*Mar 18 11:12:21.264: ipaddr: 10.10.10.1, hwidb: TwentyFiveGigE1/0/1, type: 1, phyidb: TwentyFiveGigE1/0/1
*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_global
*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 Tve1/0/1 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_global
*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 Tve1/0/1 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 reply to 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)

```

Cenário 2 - Servidor NTP alcançável

```
<#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

Quando o usuário recebe um endereço IP, a tabela de associação de rastreamento é criada dinamicamente e as informações correspondentes são adicionadas subsequentemente ao banco de dados de rastreamento. Como resultado, houve uma tentativa total de atualizar ou transferir o banco de dados, com todos eles sendo bem-sucedidos. Não houve falhas em gravações, leituras ou transferências.

<#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 Succeeded 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

```

Cenário 3 - Servidor NTP Intermitentemente Acessível

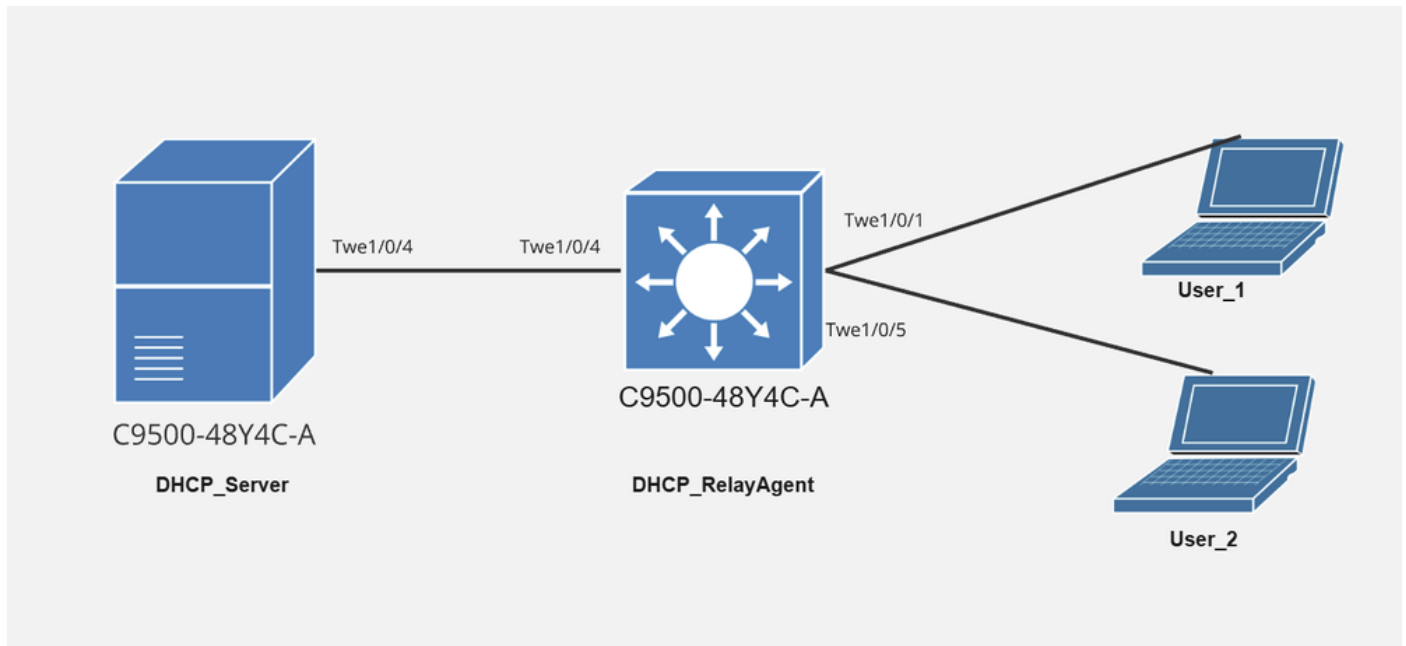


Diagrama de Rede com User_1 e User_2

<#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

Agora podemos ver que User_1 recebeu o IP 10.10.10.1 na vlan 10.

Esta é a tabela de ligação de rastreamento de DHCP, mostrando o endereço IP, o endereço MAC e a interface do User_1 em 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 Succeeded 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

Depois de um tempo, o NTP ficou inacessível, mas User_2 obteve seu endereço IP 10.10.10.2 na vlan 10 e foi atualizado na tabela de ligação, mas não foi enviado para a tabela de banco de dados de rastreamento.

<#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 é a tabela de ligação de rastreamento de DHCP, mostrando o endereço IP, o endereço MAC e a interface para User_2 em 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

A entrada no banco de dados de rastreamento não é incrementada e o total de gravações bem-sucedidas permanece 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 Succeeded 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

Quando o servidor NTP se torna acessível, o sistema sincroniza a tabela de associação de rastreamento de DHCP e o banco de dados de rastreamento de DHCP. Este cenário não é mostrado aqui. Porém, resultados semelhantes podem ser obtidos removendo-se a configuração do servidor NTP.

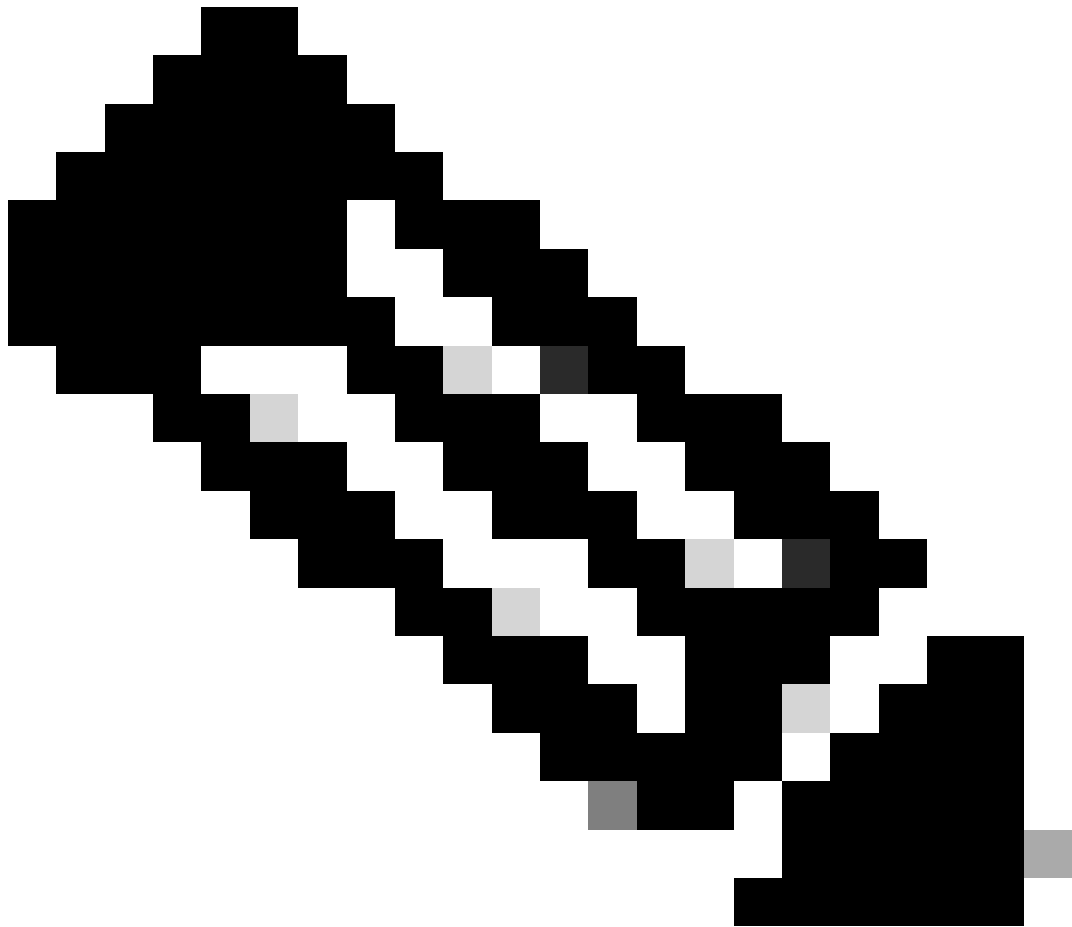
Quando a configuração do NTP for removida, a entrada para User_2 será adicionada à tabela do banco de dados de rastreamento.

Nesse caso, o switch usa a hora do relógio do sistema.

<#root>

DHCP_RelayAgent#configure terminal

DHCP_RelayAgent(config)# no ntp server 10.81.254.131



Note: Para fins de demonstração, removemos a configuração do servidor NTP.
Tecnicamente, o resultado do servidor NTP acessível e do servidor NTP não configurado é semelhante.

```
*Mar 17 17:26:26.475: %DHCP_SNOOPING-4-NTP_NOT_RUNNING: NTP is not running; reloaded binding lease expired
*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 Succeeded 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_gi
*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_gi
*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: DHCPDP: Reload workspace interface GigabitEthernet0/0 tableid 1.
*Mar 18 11:37:38.956: DHCPDP: Sending notification of DISCOVER:
*Mar 18 11:37:38.956: DHCPDP: htype 1 chaddr 7c21.0e1e.59b6
*Mar 18 11:37:38.956: DHCPDP: table id 1 = vrf Mgmt-vrf
*Mar 18 11:37:38.956: DHCPDP: interface = GigabitEthernet0/0
*Mar 18 11:37:38.956: DHCPDP: class id 436973636f204e394b2d433933333243
*Mar 18 11:37:38.956: DHCPDP: FSM state change INVALID
*Mar 18 11:37:38.956: DHCPDP: Workspace state changed from INIT to INVALID
*Mar 18 11:37:39.957: DHCPDP: Reload workspace interface GigabitEthernet0/0 tableid 1.
*Mar 18 11:37:39.957: DHCPDP: Sending notification of DISCOVER:
*Mar 18 11:37:39.957: DHCPDP: htype 1 chaddr 7c21.0e1e.59b6
*Mar 18 11:37:39.957: DHCPDP: table id 1 = vrf Mgmt-vrf
*Mar 18 11:37:39.957: DHCPDP: interface = GigabitEthernet0/0
*Mar 18 11:37:39.957: DHCPDP: 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 expired

*Mar 18 11:37:50.827: to string : 10.10.10.1 10 78bc.1a0b.d51f 67DAAC45 Tue1/0/1

*Mar 18 11:37:50.827: to string : 10.10.10.2 10 f8e5.7e75.0446 67D9B6DC Tue1/0/5

*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.
```

Conclusão

- Se o IP do servidor NTP estiver presente e acessível, a tabela de associação de rastreamento de DHCP e o banco de dados de rastreamento serão preenchidos. As entradas devem ser carimbadas com precisão usando a hora sincronizada do servidor NTP.
- Se o IP do servidor NTP estiver presente, mas não acessível, a tabela de associação de rastreamento de DHCP ainda será preenchida, mas as entradas não poderão ser preenchidas no banco de dados de rastreamento, pois o sistema não poderá sincronizar o horário para o gerenciamento preciso de leasing.
- Se o IP do servidor NTP não estiver configurado ou não existir, a tabela de associação de rastreamento DHCP e o banco de dados de rastreamento ainda conterão entradas, mas os carimbos de data/hora no banco de dados de rastreamento não serão confiáveis, pois podem ser baseados na hora do sistema local.
- Em resumo, para um gerenciamento preciso e confiável do banco de dados de rastreamento de DHCP, o NTP é crucial.

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.