Troubleshoot DHCP Snooping Database Integrity Due to NTP

Contents

Introduction

This document describes the relationship between NTP and the DHCP snooping database, highlighting time synch in recording and restoring DHCP bindings.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics :

Basic understanding of :

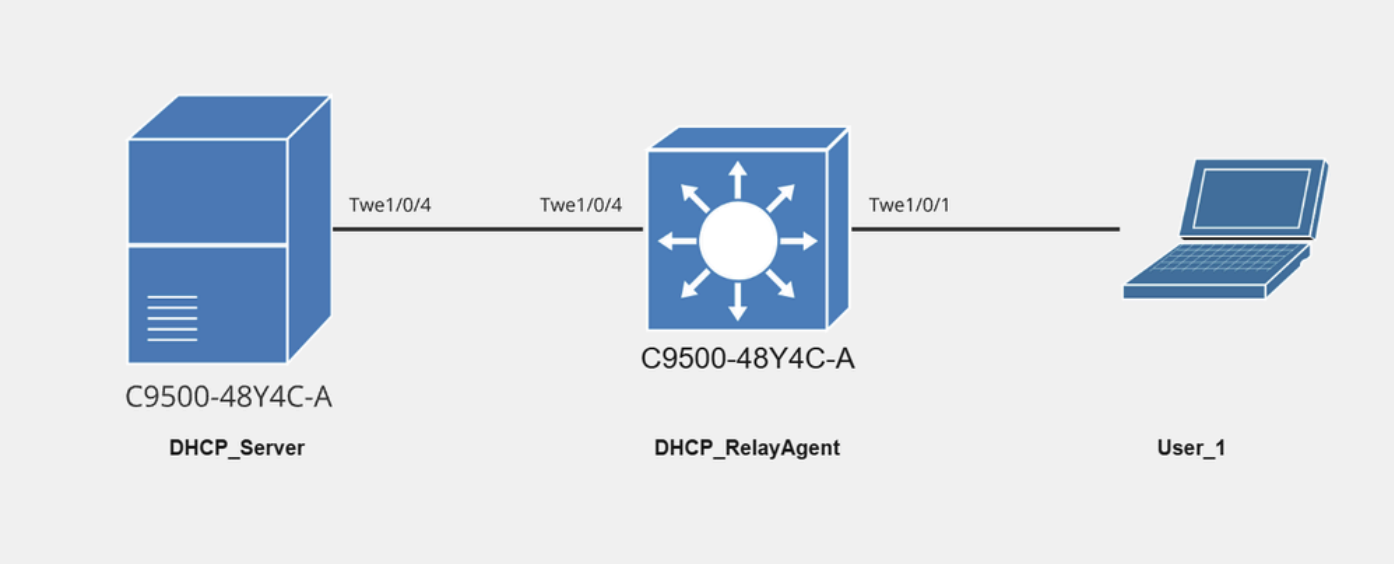
- Catalyst 9000 Series Switches Architecture
- Cisco IOS® XE Software and command line
- DHCP (Dynamic Host Configuration Protocol), DHCP Snooping and Related Features
- NTP (Network Time Protocol)

Components Used

The information in this document is based on the Cisco Catalyst C9500 on Cisco IOS® Software Release 17.12.4.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Topology



Network_Diagram with User_1

Role of NTP & NTP reachability in DHCP Snooping Database Population

In a switch or network device with DHCP snooping enabled, the binding table holds real-time dynamic information about IP addresses, MAC addresses, VLANs, and lease expiration times. This information is vital for verifying DHCP clients and protecting the network from rogue DHCP servers.

However, the snooping database is typically intended to provide persistence for this information, so it can be restored after a reboot. The database can be backed up periodically, and the information is stored in a persistent file (for example, flash:backup.text).In order for this backup procedure to function properly, exact system time is necessary, particularly for lease expiration timestamps and other time-sensitive data.

NTP is essential in ensuring that the system clock is synchronized accurately. The system relies on the accurate time to:

- Calculate the lease expiration for DHCP bindings.
- Ensure that the correct timestamps are written to the snooping database when the binding table is saved.

If the NTP server is unreachable or if the system cannot synchronize its clock, the system cannot have an accurate time reference to correctly handle the expiration timestamps for DHCP leases. This leads to the below problems:

1. Lease Expiration Time Issue

An incorrect timestamp could lead to issues like:

- Incorrect expiration or renewal of leases.
- Stale or outdated DHCP binding information in the snooping database.

2. Impact on Binding Table Backup

When the NTP server is reachable, the system can generate accurate timestamps for each DHCP lease and correctly back up the binding table into the snooping database.

If the NTP server is not reachable, the device fail to be able to determine the correct current time, leading to 0 attempts to write valid binding information into the database.

3. Unreliable Database Backup

The snooping database stores binding information persistently, including the expiration time for each lease.

Without accurate system time from NTP , the device fails to write accurate timestamps for lease expirations when saving to the database.

If NTP server is intermittently reachable, it results into the integrity issue between the DHCP binding table and the DHCP snooping database table.As a result, the snooping database data is considered to be incomplete or incorrect.

Base Configuration

Step 1. Enable DHCP snooping globally and under the VLANs, on the relay agent. In this case,the relay agent and the access switch are same.

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

Step 2. Configure DHCP snooping trust on all interface/s of the switch that receive DHCP offers from genuine DHCP server/s. The number of such interfaces depends on the Network design and placement of DHCP servers. These are the interfaces which are going towards the genuine DHCP Server.


```
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
```

Step 3. Configure the DHCP snooping database into a location to monitor the the DHCP snooping binding table, track the health of the database operations and verify that the database is being correctly updated and transferred.

```
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
```

Scenario 1 - NTP Server Unreachable

<#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)

Now we can see the User_1 has received the IP 10.10.10.1 in vlan 10.

Here is the DHCP Snooping binding table, showing the IP Address, MAC Address and interface of the User_1 on 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
```

In general, once the user receives an IP address, the snooping binding table is dynamically created, and the corresponding information is subsequently added to the snooping database. But, in this case, as the NTP server is unreachable, there have been 0 total attempts to update or transfer the binding information to the database.

<#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)
```

Scenario 2 - NTP Server Reachable

<#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
```

Once the user receives an IP address, the snooping binding table is dynamically created, and the corresponding information is subsequently added to the snooping database.As a result, there have been 1 total attempt to update or transfer the database, with all of them being successful. There have been no failed writes, reads, or transfers.

<#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>

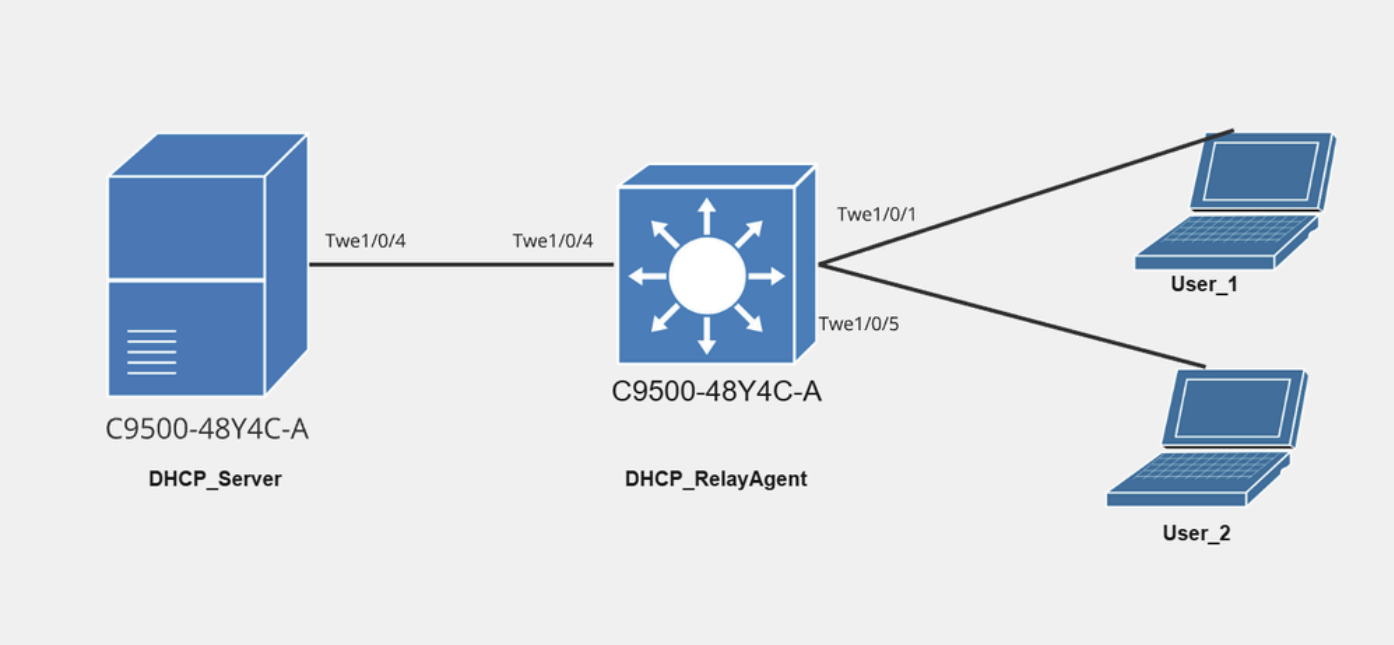
```
DHCP_RelayAgent#more flash:dhcpsnoopingdatabase.txt


67d86a58
TYPE DHCP-SNOOPING
VERSION 1
BEGIN

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


END
```

Scenario 3 - NTP Server Intermittently Reachable



Network Diagram with User_1 and 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

Now we can see the User_1 has received the IP 10.10.10.1 in vlan 10.

Here is the DHCP Snooping binding table, showing the IP Address, MAC Address and interface of the User_1 on 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
```

After a while, the NTP went unreachable, but User_2 got its IP address 10.10.10.2 in vlan 10 and it was updated in binding table but not pushed into the snooping database table.

<#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)

Here is the DHCP Snooping binding table, showing the IP Address, MAC Address and interface for User_2 on 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
```

The entry on the snooping database is not incremented and the total successful writes remains 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
```

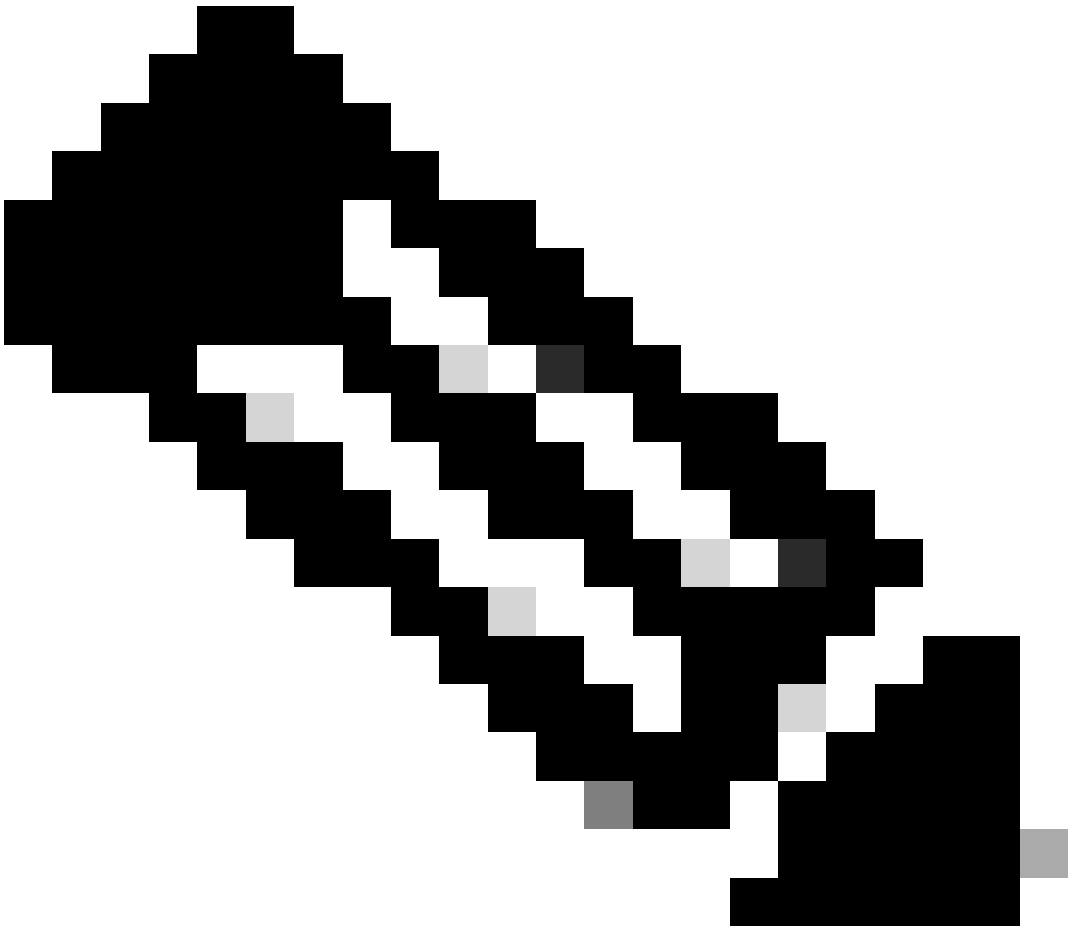
When the NTP server becomes accessible, the system synchronizes the DHCP snooping binding table and the DHCP snooping database. This scenario is not shown here. But, similar results can be achieved by removing the NTP server configuration.

Once the NTP configuration is removed, the entry for User_2 is added to the snooping database table. In this case, the switch uses the clock time of the system.

<#root>

```
DHCP_RelayAgent#configure terminal
```

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



Note: For demonstration purposes we have removed the NTP server configuration.Technically the result of NTP server reachable & NTP server not configured is 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.**

Conclusion

- If the NTP server IP is present and reachable, both the DHCP snooping binding table and the snooping database is populated. The entries must be accurately timestamped using the synchronized time from the NTP server.
- If the NTP server IP is present but not reachable, the DHCP snooping binding table is still populated, but the entries cannot be populated in the snooping database, as the system is not be able to synchronize the time for accurate lease management.
- If the NTP server IP is not configured or does not exist, both the DHCP snooping binding table and the snooping database still contain entries, but the timestamps in the snooping database falls unreliable, as they can be based on the local system time.
- In summary, for accurate and reliable management of the DHCP snooping database, NTP is crucial.