

Probleemoplossing voor DHCP-signalering van database-integriteit vanwege NTP

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Topologie](#)

[Rol van NTP & NTP bereikbaarheid in DHCP-scanning database populatie](#)

[1. Uitgifte van verlooptijden van leaseovereenkomsten](#)

[2. Effect op bindende tabelback-up](#)

[3. Onbetrouwbare back-up van database](#)

[Basisconfiguratie](#)

[Scenario 1 - NTP-server onbereikbaar](#)

[Scenario 2 - NTP-server bereikbaar](#)

[Scenario 3 - NTP-server met tussenpozen bereikbaar](#)

[Conclusie](#)

Inleiding

Dit document beschrijft het verband tussen NTP en de DHCP-snooping database, waarbij tijdsynch wordt gemarkeerd bij het opnemen en herstellen van DHCP-banden.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

Basiskennis van :

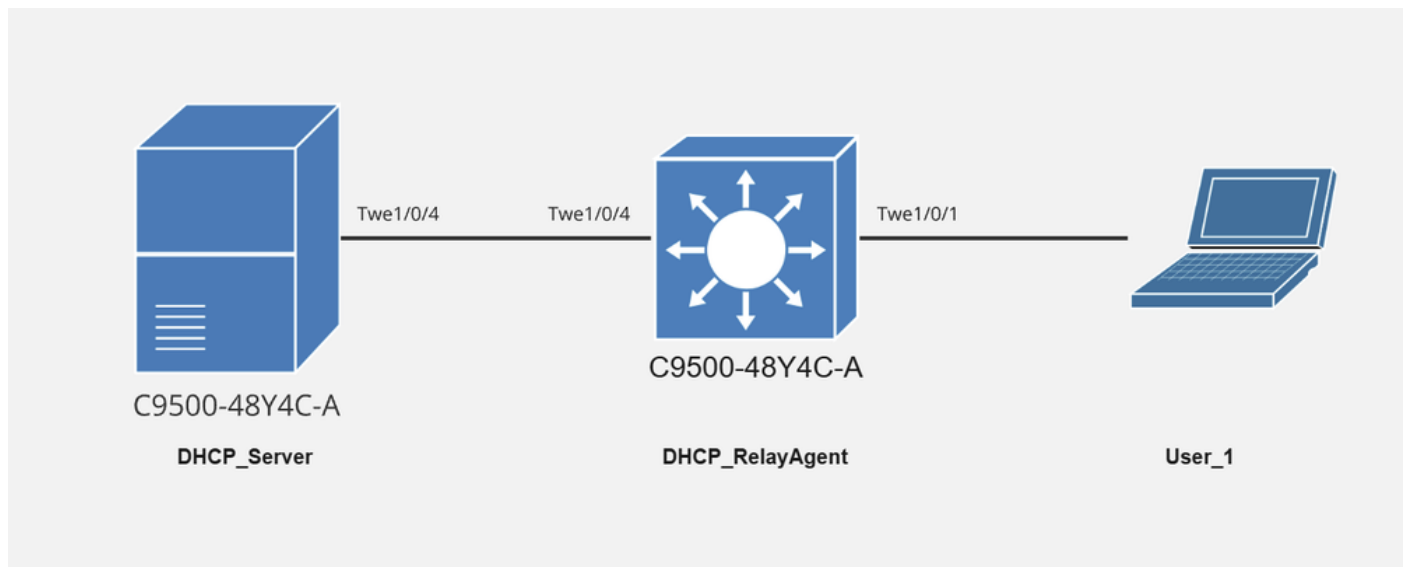
- Catalyst 9000 Series Switches-architectuur
- Cisco IOS® XE-software en opdrachtregel
- DHCP (Dynamic Host Configuration Protocol), DHCP-controle en verwante functies
- NTP (Network Time Protocol)

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Catalyst C9500 op Cisco IOS®-softwarerelease 17.12.4.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Topologie



Network_Diagram met gebruiker_1

Rol van NTP & NTP bereikbaarheid in DHCP-scanning database populatie

In een switch of netwerkkapparaat met DHCP-snooping ingeschakeld, bevat de bindende tabel real-time dynamische informatie over IP-adressen, MAC-adressen, VLAN's en verlooptijden voor leasen. Deze informatie is van vitaal belang voor het verifiëren van DHCP-clients en het beschermen van het netwerk tegen schurkenDHCP-servers.

De spionagedatabase is echter meestal bedoeld om deze informatie te laten voortduren, zodat deze na een herstart kan worden hersteld. Van de database kan periodiek een back-up worden gemaakt en de informatie wordt opgeslagen in een persistent bestand (bijvoorbeeld flitser:back-up.text). Om deze back-upprocedure goed te laten functioneren, is de exacte systeemtijd nodig, met name voor verlooptijdstempels van leaseverlooptijdstempels en andere tijdgevoelige gegevens.

NTP is essentieel om ervoor te zorgen dat de systeemklok nauwkeurig wordt gesynchroniseerd. Het systeem is afhankelijk van de juiste tijd om:

- Bereken de verlooptijdstempel van de lease voor DHCP-banden.
- Zorg ervoor dat de juiste tijdstempels worden geschreven naar de snooping database wanneer de bindende tabel wordt opgeslagen.

Als de NTP-server onbereikbaar is of als het systeem de klok niet kan synchroniseren, kan het systeem geen nauwkeurige tijdsverwijzing hebben om de verlooptijdstempels voor DHCP-leases

correct te verwerken. Dit leidt tot de volgende problemen:

1. Uitgifte van verlooptijden van leaseovereenkomsten

Een onjuist tijdstempel kan leiden tot problemen zoals:

- Onjuiste afloop of vernieuwing van leases.
- Verouderde of verouderde DHCP-bindingsinformatie in de snuffeldatabase.

2. Effect op bindende tabelback-up

Wanneer de NTP-server bereikbaar is, kan het systeem nauwkeurige tijdstempels genereren voor elke DHCP-lease en een correcte back-up maken van de bindende tabel in de snuffeldatabase.

Als de NTP-server niet bereikbaar is, kan het apparaat niet de juiste huidige tijd bepalen, wat leidt tot 0 pogingen om geldige bindende informatie in de database te schrijven.

3. Onbetrouwbare back-up van database

De snuffeldatabase slaat continu bindende informatie op, inclusief de verlooptijd voor elke lease.

Zonder nauwkeurige systeemtijd van NTP, slaagt het apparaat er niet in om nauwkeurige timestamps voor leaseverloopdatums te schrijven wanneer het opslaan aan het gegevensbestand.

Als NTP-server af en toe bereikbaar is, resulteert dit in het integriteitsprobleem tussen de DHCP-bindende tabel en de DHCP-snooping database tabel. Als gevolg daarvan worden de snooping database gegevens als onvolledig of onjuist beschouwd.

Basisconfiguratie

Stap 1. Schakel DHCP-spionage wereldwijd en onder de VLAN's in op de relay-agent. In dit geval zijn de relay agent en de access switch hetzelfde.

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

Stap 2. Configureer het DHCP-snuffelvertrouwen op alle interfaces van de switch die DHCP-aanbiedingen ontvangen van echte DHCP-server(s). Het aantal dergelijke interfaces hangt af van het netwerkontwerp en de plaatsing van DHCP-servers. Dit zijn de interfaces die naar de echte DHCP-server gaan.

<#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
```

Stap 3. Configureer de DHCP-snooping database in een locatie om de DHCP snooping binding tabel te bewaken, volg de status van de database-bewerkingen en controleer of de database correct wordt bijgewerkt en overgebracht.

<#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
```

Scenario 1 - NTP-server onbereikbaar

<#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)
```

Nu kunnen we zien dat Gebruiker_1 IP 10.10.10.1 in VLAN 10 heeft ontvangen.

Hier is de DHCP Snooping bindende tabel, die het IP-adres, het MAC-adres en de interface van User_1 op TwentyFiveGigE1/0/1 toont

<#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 het algemeen wordt, zodra de gebruiker een IP-adres ontvangt, de snuffelbindingstabel dynamisch gemaakt en wordt de bijbehorende informatie vervolgens toegevoegd aan de snuffeldatabase. Maar, in dit geval, aangezien de server NTP onbereikbaar is, zijn er 0 totale pogingen geweest om de bindende informatie bij te werken of over te brengen naar de 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 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_opt82_fmt_rid
*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_opt82_fmt_rid
*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_opt82_fmt_rid
*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 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 bereikbaar

<#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

Zodra de gebruiker een IP-adres ontvangt, wordt de snuffelbindende tabel dynamisch aangemaakt en wordt de bijbehorende informatie vervolgens toegevoegd aan de snuffeldatabase. Als gevolg daarvan is er 1 totale poging geweest om de database bij te werken of over te dragen, waarbij ze allemaal succesvol zijn. Er zijn geen mislukte schrijfsels, lezers of overdrachtsbetalingen geweest.

<#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>

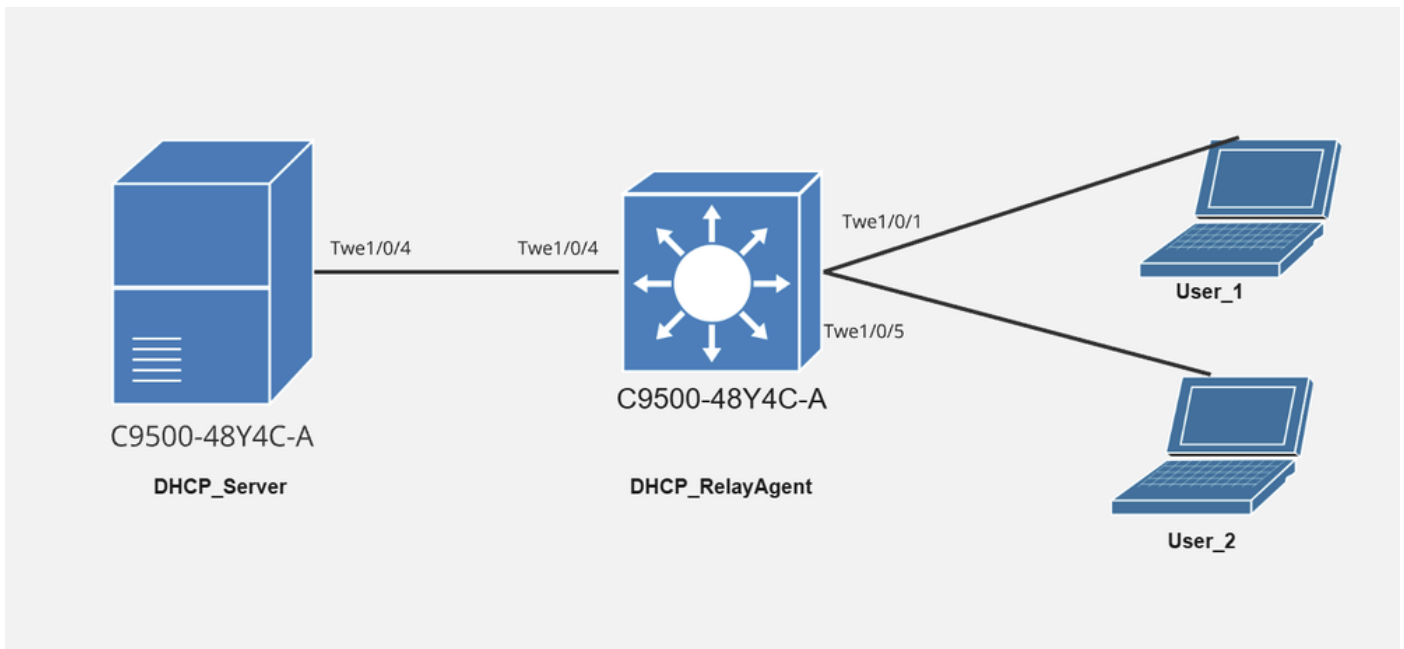
DHCP_RelayAgent#more flash:dhcpsnoopingdatabase.txt

67d86a58
TYPE DHCP-SNOOPING
VERSION 1
BEGIN

10.10.10.1 10 78bc.1a0b.d51f 67D9BBCA Tve1/0/1 8b21f6ef

END

Scenario 3 - NTP-server met tussenpozen bereikbaar



Netwerkdigram met Gebruiker_1 en Gebruiker_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

Nu kunnen we zien dat Gebruiker_1 IP 10.10.10.1 in VLAN 10 heeft ontvangen.

Hier is de DHCP Snooping bindende tabel, die het IP-adres, het MAC-adres en de interface van User_1 op TwentyFiveGigE1/0/1 toont

<#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 Tve1/0/1 8b21f6ef

END

Na een tijdje, het NTP werd onbereikbaar, maar Gebruiker_2 kreeg zijn IP-adres 10.10.10.2 in VLAN 10 en het werd bijgewerkt in bindende tabel maar niet geduwd in de spionagedatabase tabel.

<#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)

Hier is de DHCP Snooping bindende tabel, die het IP-adres, het MAC-adres en de interface voor User_2 op TwentyFiveGigE1/0/5 toont

<#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

De vermelding in de snooping database wordt niet verhoogd en het totaal succesvolle schrijfwerk blijft 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 Tve1/0/1 8b21f6ef

END

Wanneer de NTP-server toegankelijk wordt, synchroniseert het systeem de DHCP-snoopingbindende tabel en de DHCP-snooping database. Dit scenario wordt hier niet getoond. Maar, kunnen de gelijkaardige resultaten worden bereikt door de NTP serverconfiguratie te verwijderen.

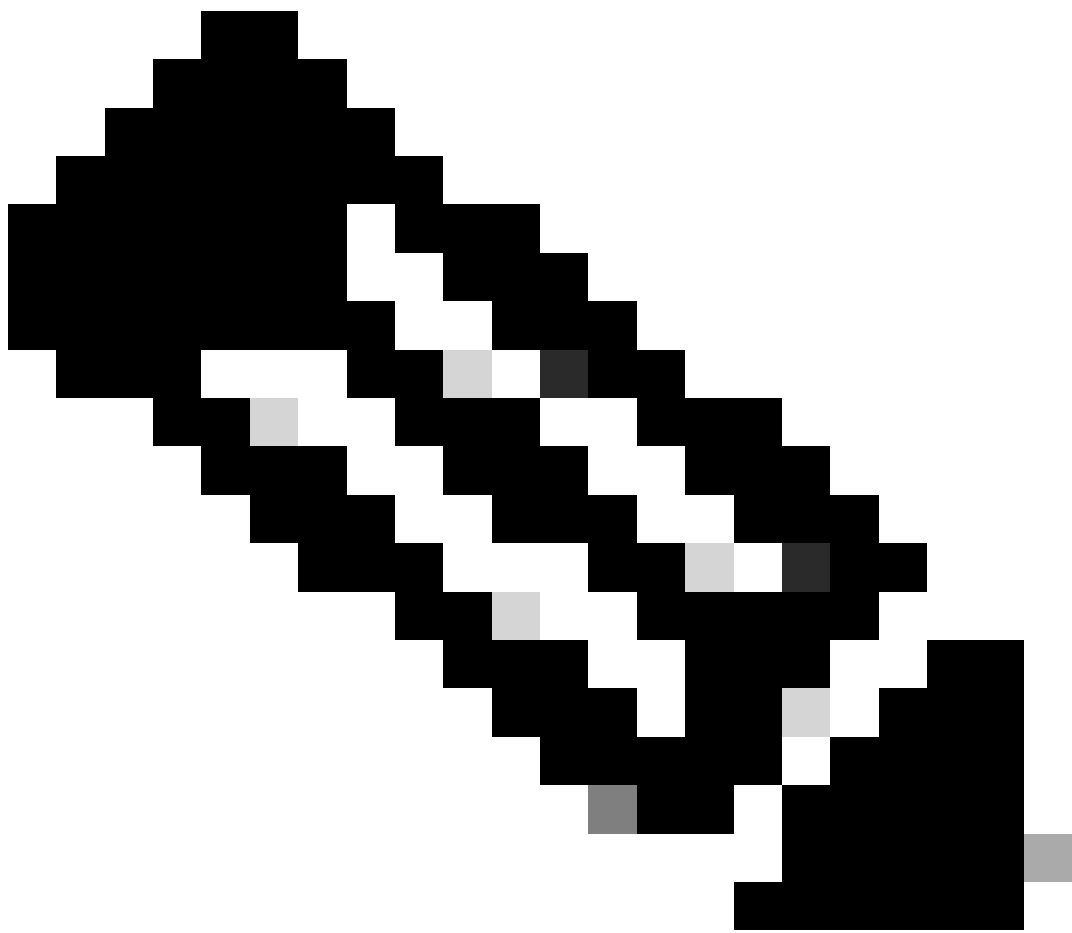
Zodra de NTP configuratie is verwijderd, wordt de vermelding voor User_2 toegevoegd aan de snuffeldatabase tabel.

In dit geval gebruikt de switch de kloktijd van het systeem.

<#root>

DHCP_RelayAgent#configure terminal

DHCP_RelayAgent(config)# no ntp server 10.81.254.131



Opmerking: Voor demonstratiedoeleinden hebben we de NTP-serverconfiguratie verwijderd. Technisch gezien is het resultaat van NTP-server bereikbaar en NTP-server niet geconfigureerd vergelijkbaar.

*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 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.
```

Conclusie

- Als de NTP server IP aanwezig en bereikbaar is, zijn zowel de DHCP-snooping bindende tabel als de snooping database ingevuld. De vermeldingen moeten nauwkeurig worden getimd met behulp van de gesynchroniseerde tijd van de NTP-server.
- Als de NTP server IP aanwezig maar niet bereikbaar is, is de DHCP snooping bindende tabel nog steeds ingevuld, maar de vermeldingen kunnen niet worden ingevuld in de snooping database, aangezien het systeem niet in staat is om de tijd te synchroniseren voor nauwkeurig leasebeheer.
- Als de NTP server IP niet is geconfigureerd of niet bestaat, bevatten zowel de DHCP-snuffelbindende tabel als de snuffeldatabase nog steeds vermeldingen, maar de tijdstempels in de snuffeldatabase vallen onbetrouwbaar, omdat ze kunnen worden gebaseerd op de lokale systeemtijd.
- Samenvattend, voor nauwkeurig en betrouwbaar beheer van de DHCP snooping database, NTP is cruciaal.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.