Fehlerbehebung bei der Integrität der DHCP-Snooping-Datenbank aufgrund von NTP

Inhalt

Einleitung

In diesem Dokument wird die Beziehung zwischen NTP und der DHCP-Snooping-Datenbank beschrieben. Dabei wird die Zeitsynchronisierung bei der Aufzeichnung und Wiederherstellung der DHCP-Bindungen hervorgehoben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

Grundlegendes Verständnis von:

- Architektur von Switches der Catalyst 9000-Serie
- Cisco IOS® XE Software und Kommandozeile
- DHCP (Dynamic Host Configuration Protocol), DHCP-Snooping und verwandte Funktionen
- NTP (Network Time Protocol)

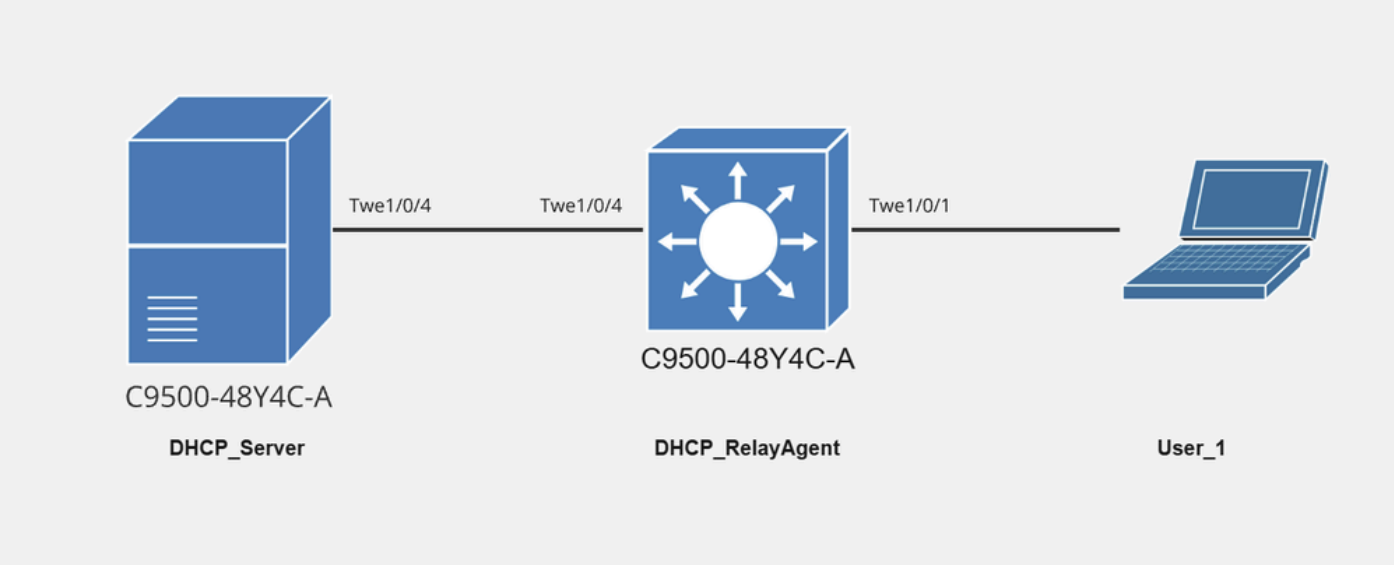
Verwendete Komponenten

Die Informationen in diesem Dokument beziehen sich auf den Cisco Catalyst Switch C950 mit der

Cisco IOS® Software, Version 17.12.4.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Topologie



Netzwerkdiagramm mit Benutzer_1

Rolle von NTP- und NTP-Erreichbarkeit bei der Auffüllung der DHCP-Snooping-Datenbank

Bei einem Switch oder Netzwerkgerät mit aktiviertem DHCP-Snooping enthält die Bindungstabelle dynamische Echtzeitinformationen zu IP-Adressen, MAC-Adressen, VLANs und Lease-Ablaufzeiten. Diese Informationen sind für die Überprüfung von DHCP-Clients und für den Schutz des Netzwerks vor nicht autorisierten DHCP-Servern unerlässlich.

Die Snooping-Datenbank ist jedoch in der Regel dazu gedacht, diese Informationen dauerhaft bereitzustellen, sodass sie nach einem Neustart wiederhergestellt werden kann. Die Datenbank kann regelmäßig gesichert werden, und die Informationen werden in einer dauerhaften Datei gespeichert (z. B. flash:backup.text). Damit diese Sicherungsmaßnahme ordnungsgemäß funktioniert, ist eine genaue Systemzeit erforderlich, insbesondere für Zeitstempel für den Leasinablauf und andere zeitkritische Daten.

NTP ist für eine genaue Synchronisierung der Systemuhr unerlässlich. Das System benötigt die genaue Zeit, um:

- Berechnen Sie den Lease-Ablauf für DHCP-Bindungen.
- Stellen Sie sicher, dass die richtigen Zeitstempel in die Snooping-Datenbank geschrieben werden, wenn die Bindungstabelle gespeichert wird.

Wenn der NTP-Server nicht erreichbar ist oder das System seine Uhr nicht synchronisieren kann, kann das System keine exakte Zeitreferenz zur korrekten Verarbeitung der Ablaufzeitstempel für DHCP-Leases verwenden. Dies führt zu den folgenden Problemen:

1. Problem mit Leasingablaufzeit

Ein falscher Zeitstempel kann u. a. folgende Probleme verursachen:

- Fehlerhafter Ablauf oder Verlängerung von Leasingverträgen.
- Veraltete oder veraltete DHCP-Bindungsinformationen in der Snooping-Datenbank.

2. Auswirkungen auf Binding Table Backup

Wenn der NTP-Server erreichbar ist, kann das System genaue Zeitstempel für jede DHCP-Lease generieren und die Bindungstabelle korrekt in der Snooping-Datenbank sichern.

Wenn der NTP-Server nicht erreichbar ist, kann das Gerät die korrekte aktuelle Zeit nicht ermitteln. Dies führt zu 0 Versuchen, gültige Bindungsinformationen in die Datenbank zu schreiben.

3. Unzuverlässige Datenbanksicherung

In der Snooping-Datenbank werden Bindungsinformationen dauerhaft gespeichert, einschließlich der Ablaufzeit für jede Lease.

Ohne genaue Systemzeit vom NTP kann das Gerät beim Speichern in der Datenbank keine genauen Zeitstempel für Lease-Ablaufdaten schreiben.

Wenn der NTP-Server zeitweilig erreichbar ist, führt dies zu einem Integritätsproblem zwischen der DHCP-Bindungstabelle und der DHCP-Snooping-Datenbanktabelle. Die Snooping-Datenbankdaten werden daher als unvollständig oder falsch angesehen.

Basiskonfiguration

Schritt 1: Aktivieren Sie DHCP-Snooping global und unter den VLANs auf dem Relay-Agent. In diesem Fall sind der Relay-Agent und der Access Switch identisch.

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

Schritt 2: Konfigurieren Sie die DHCP-Snooping-Vertrauensstellung auf allen Schnittstellen des Switches, die DHCP-Angebote von echten DHCP-Servern erhalten. Die Anzahl dieser Schnittstellen hängt vom Netzwerkdesign und der Anordnung der DHCP-Server ab. Dies sind die Schnittstellen, die zum echten DHCP-Server führen.

<#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
```

Schritt 3: Konfigurieren Sie die DHCP-Snooping-Datenbank an einem Speicherort, um die Tabelle mit den DHCP-Snooping-Bindungen zu überwachen, den Zustand der Datenbankvorgänge zu verfolgen und zu überprüfen, ob die Datenbank ordnungsgemäß aktualisiert und übertragen wird.

<#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
```

Szenario 1 - NTP-Server nicht erreichbar

<#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)

Nun wird angezeigt, dass User_1 die IP 10.10.10.1 in VLAN 10 erhalten hat.

Dies ist die Bindungstabelle für DHCP-Snooping mit der IP-Adresse, MAC-Adresse und Schnittstelle von User_1 für 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
```

Im Allgemeinen wird, wenn der Benutzer eine IP-Adresse erhält, die Snooping-Bindungstabelle dynamisch erstellt und die entsprechenden Informationen anschließend der Snooping-Datenbank hinzugefügt. Da der NTP-Server jedoch nicht erreichbar ist, wurden insgesamt 0 Versuche unternommen, die Bindungsinformationen zu aktualisieren oder an die Datenbank zu übertragen.

<#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)
```

Szenario 2 - Erreichbarkeit des NTP-Servers

<#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
```

Sobald der Benutzer eine IP-Adresse erhält, wird die Snooping-Bindungstabelle dynamisch erstellt, und die entsprechenden Informationen werden anschließend der Snooping-Datenbank hinzugefügt. Es wurde also insgesamt 1 Versuch unternommen, die Datenbank zu aktualisieren oder zu übertragen, wobei alle erfolgreich waren. Fehlgeschlagene Schreibvorgänge, Lesevorgänge und Übertragungen sind nicht aufgetreten.

<#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>

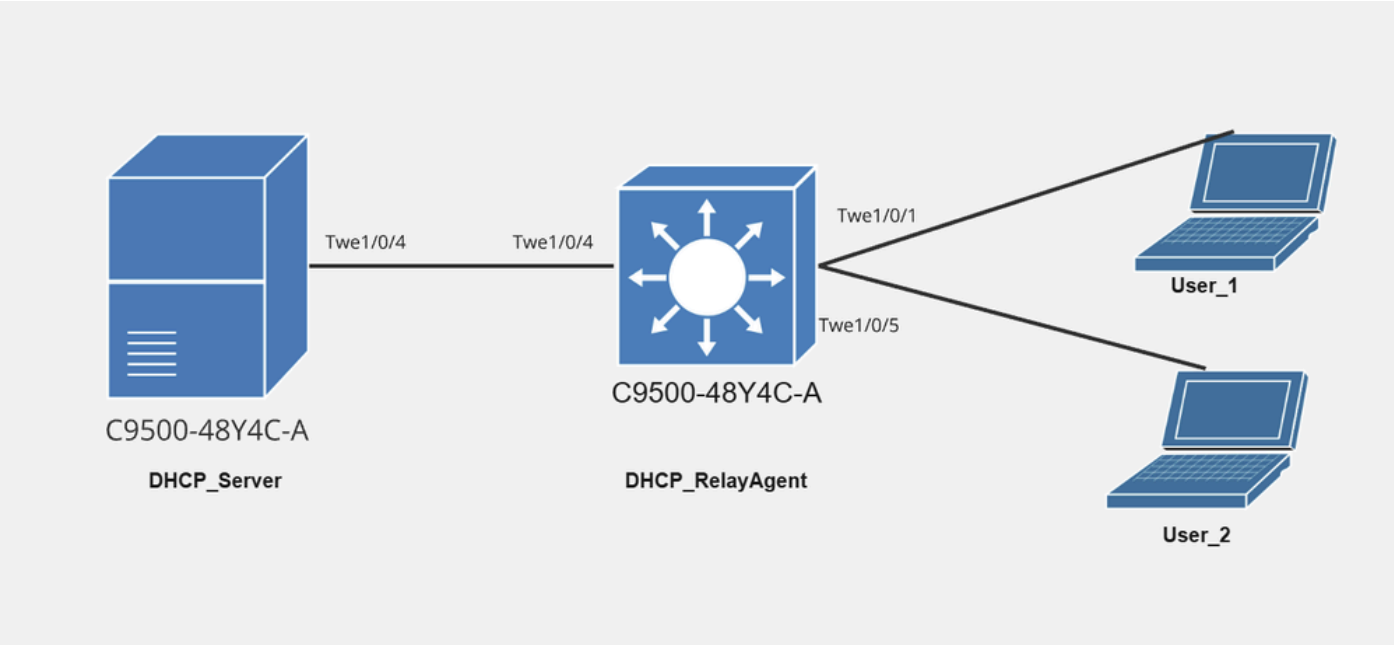
DHCP_RelayAgent#more flash:dhcpsnoopingdatabase.txt

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

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

```
END
```

Szenario 3 - NTP-Server mit zeitweiliger Erreichbarkeit



Netzwerkdiagramm mit Benutzer_1 und Benutzer_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

Nun wird angezeigt, dass User_1 die IP 10.10.10.1 in VLAN 10 erhalten hat.

Dies ist die Bindungstabelle für DHCP-Snooping mit der IP-Adresse, MAC-Adresse und Schnittstelle von User_1 für 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
```

Nach einer Weile war das NTP nicht erreichbar, aber User_2 erhielt seine IP-Adresse 10.10.10.2 in VLAN 10 und wurde in der Bindungstabelle aktualisiert, jedoch nicht in die Snooping-

Datenbanktabelle verschoben.

<#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)

Dies ist die Tabelle mit der DHCP-Snooping-Bindung, in der die IP-Adresse, die MAC-Adresse und die Schnittstelle für User_2 auf TwentyFiveGigE1/0/5 angezeigt werden.

<#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
```

Der Eintrag in der Snooping-Datenbank wird nicht inkrementiert, und die Gesamtzahl der erfolgreichen Schreibvorgänge bleibt bei 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
```

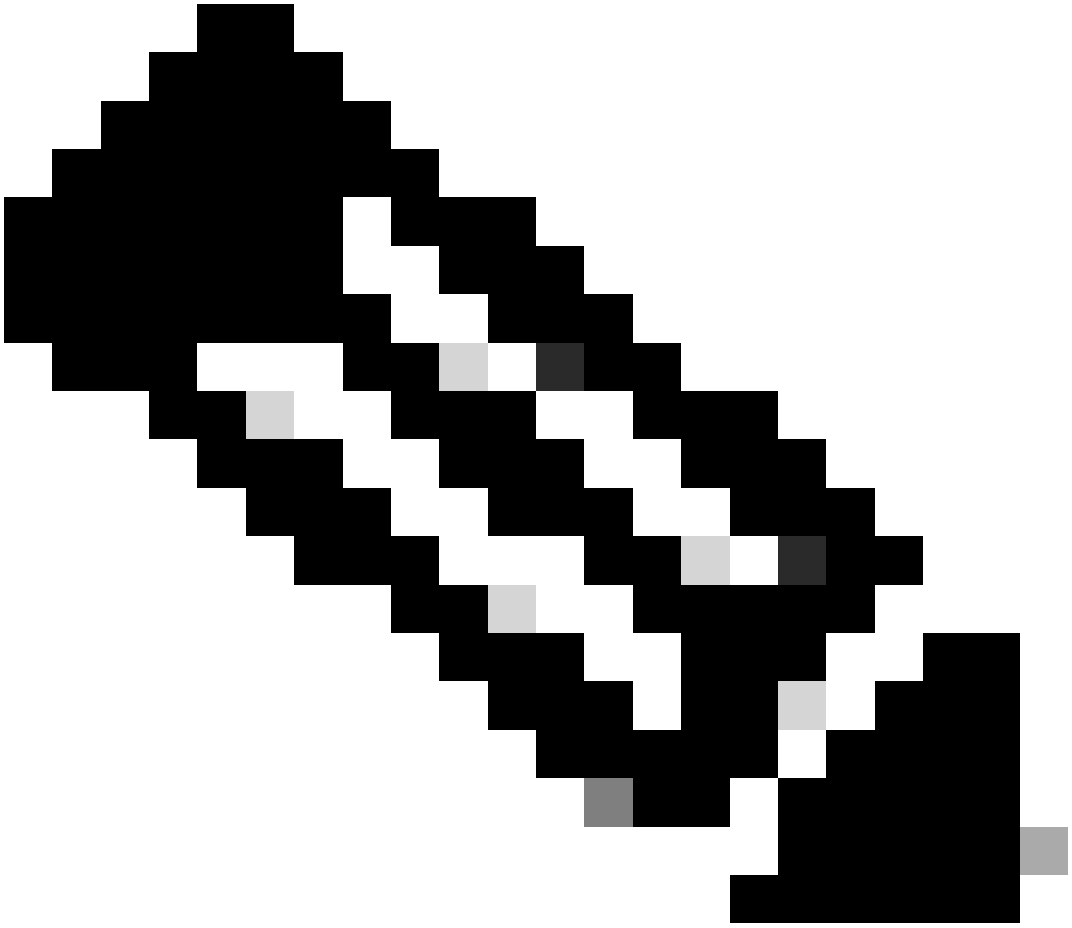
Sobald der Zugriff auf den NTP-Server möglich ist, synchronisiert das System die Bindungstabelle für DHCP-Snooping und die DHCP-Snooping-Datenbank. Dieses Szenario ist hier nicht dargestellt. Ein ähnliches Ergebnis lässt sich jedoch erzielen, wenn die NTP-Serverkonfiguration entfernt wird.

Nach Entfernen der NTP-Konfiguration wird der Eintrag für User_2 zur Snooping-Datenbanktabelle hinzugefügt.
In diesem Fall verwendet der Switch die Uhrzeit des Systems.

<#root>

```
DHCP_RelayAgent#configure terminal

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



Anmerkung: Zu Demonstrationszwecken haben wir die NTP-Serverkonfiguration entfernt. Technisch gesehen ist das Ergebnis von erreichbarem NTP-Server und nicht konfiguriertem NTP-Server ähnlich.

```
*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.**

Schlussfolgerung

- Wenn die IP-Adresse des NTP-Servers vorhanden und erreichbar ist, werden sowohl die DHCP-Snooping-Bindungstabelle als auch die Snooping-Datenbank ausgefüllt. Die Einträge müssen über die vom NTP-Server synchronisierte Uhrzeit mit einem exakten Zeitstempel versehen werden.
- Wenn die IP-Adresse des NTP-Servers vorhanden, aber nicht erreichbar ist, wird die Bindungstabelle für DHCP-Snooping weiterhin ausgefüllt, aber die Einträge können nicht in die Snooping-Datenbank eingefügt werden, da das System die Zeit für eine genaue Lease-Verwaltung nicht synchronisieren kann.
- Wenn die NTP-Server-IP nicht konfiguriert ist oder nicht vorhanden ist, enthalten sowohl die DHCP-Snooping-Bindungstabelle als auch die Snooping-Datenbank noch Einträge, aber die Zeitstempel in der Snooping-Datenbank sind nicht zuverlässig, da sie auf der lokalen Systemzeit basieren können.
- Zusammenfassend ist festzuhalten, dass für eine genaue und zuverlässige Verwaltung der DHCP-Snooping-Datenbank NTP von entscheidender Bedeutung ist.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.