Risoluzione dei problemi di integrità del database con snooping DHCP a causa di NTP

Sommario

Introduzione

In questo documento viene descritta la relazione tra NTP e il database dello snooping DHCP, evidenziando la sincronizzazione dell'ora nella registrazione e nel ripristino dei binding DHCP.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

Conoscenze di base di:

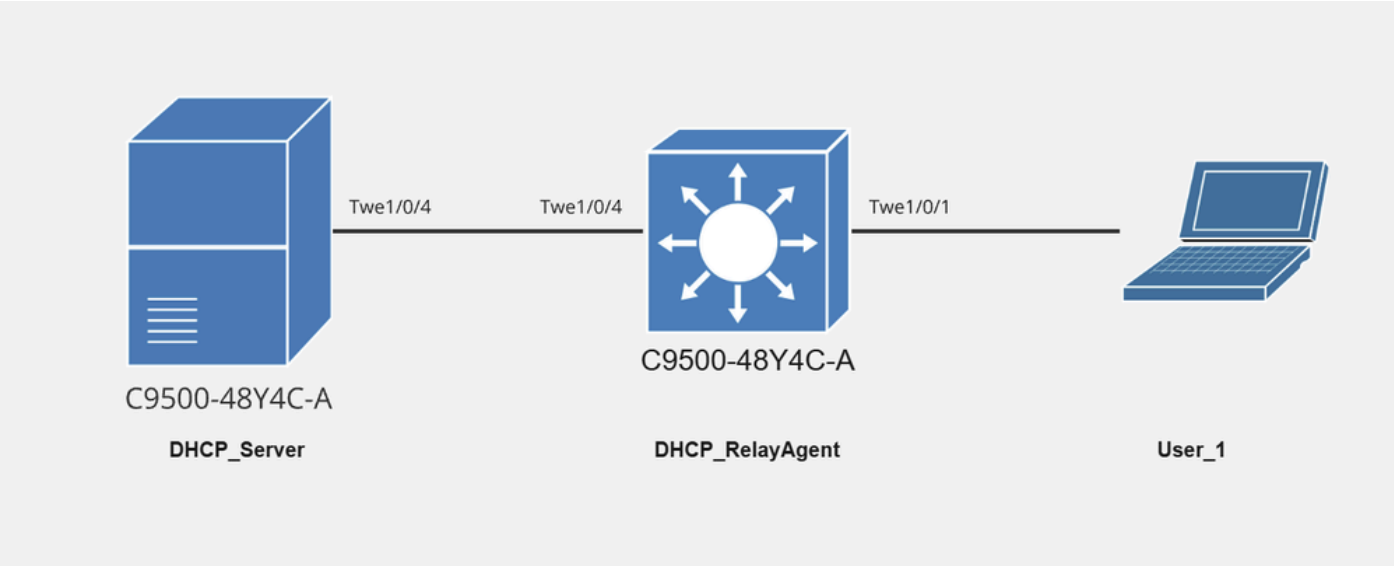
- Catalyst serie 9000 Switch Architettura
- Software Cisco IOS® XE e riga di comando
- DHCP (Dynamic Host Configuration Protocol), snooping DHCP e funzionalità correlate
- NTP (Network Time Protocol)

Componenti usati

Per la stesura del documento, è stato usato Cisco Catalyst C9500 con software Cisco IOS® versione 17.12.4.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Topologia



Network_Diagram con User_1

Ruolo della raggiungibilità NTP e NTP nel popolamento del database di snooping DHCP

In uno switch o dispositivo di rete con snooping DHCP abilitato, la tabella di binding contiene informazioni dinamiche in tempo reale su indirizzi IP, indirizzi MAC, VLAN e tempi di scadenza del lease. Queste informazioni sono fondamentali per verificare i client DHCP e proteggere la rete dai server DHCP non autorizzati.

Tuttavia, il database di snooping è in genere destinato a fornire persistenza per queste informazioni, in modo che possano essere ripristinate dopo un riavvio. È possibile eseguire periodicamente il backup del database e le informazioni vengono memorizzate in un file persistente, ad esempio flash:backup.text.Per il corretto funzionamento di questa procedura di backup, è necessario conoscere l'ora esatta del sistema, in particolare l'ora di scadenza del lease e altri dati sensibili al tempo.

L'NTP è essenziale per assicurare che l'orologio di sistema sia sincronizzato in modo accurato. Il sistema si basa sull'ora esatta per:

- Calcola la scadenza del lease per i binding DHCP.
- Assicurarsi che i timestamp corretti vengano scritti nel database di snooping quando la tabella di associazione viene salvata.

Se il server NTP non è raggiungibile o se il sistema non è in grado di sincronizzare il proprio

orologio, il sistema non può disporre di un riferimento orario accurato per gestire correttamente i timestamp di scadenza per i lease DHCP. Ciò comporta i problemi riportati di seguito.

1. Scadenza del lease

Un timestamp errato potrebbe causare problemi quali:

- Scadenza o rinnovo errati dei leasing.
- Informazioni sul binding DHCP non aggiornate o obsolete nel database dello snooping.

2. Impatto sul backup della tabella di binding

Quando il server NTP è raggiungibile, il sistema può generare timestamp accurati per ciascun lease DHCP ed eseguire correttamente il backup della tabella di binding nel database di snooping.

Se il server NTP non è raggiungibile, il dispositivo non è in grado di determinare l'ora corrente corretta e ciò comporta 0 tentativi di scrittura di informazioni di binding valide nel database.

3. Backup inaffidabile del database

Il database di snooping memorizza le informazioni di binding in modo persistente, inclusa la scadenza di ogni lease.

Senza un tempo di sistema accurato dall'NTP, il dispositivo non è in grado di scrivere un timestamp accurato per le scadenze del lease durante il salvataggio nel database.

Se il server NTP è raggiungibile in modo intermittente, si verifica un problema di integrità tra la tabella di binding DHCP e la tabella del database dello snooping DHCP. Di conseguenza, i dati del database dello snooping vengono considerati incompleti o errati.

Configurazione di base

Passaggio 1. Abilitare lo snooping DHCP a livello globale e nelle VLAN, sull'agente di inoltro. In questo caso, l'agente di inoltro e lo switch di accesso sono gli stessi.

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

Passaggio 2. Configurare il trust dello snooping DHCP su tutte le interfacce dello switch che ricevono offerte DHCP da server DHCP autentici. Il numero di interfacce dipende dalla progettazione della rete e dal posizionamento dei server DHCP. Queste sono le interfacce che vanno verso il server DHCP autentico.

```
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
```

Passaggio 3. Configurare il database dello snooping DHCP in una posizione per monitorare la tabella di binding dello snooping DHCP, tenere traccia dello stato delle operazioni del database e verificare che il database venga aggiornato e trasferito correttamente.

<#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 - Server NTP non raggiungibile

<#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)
```

Ora possiamo vedere che l'utente User_1 ha ricevuto l'IP 10.10.10.1 nella vlan 10.

Di seguito è riportata la tabella di binding Snooping DHCP, che mostra l'indirizzo IP, l'indirizzo MAC e l'interfaccia di User_1 su 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 generale, quando l'utente riceve un indirizzo IP, la tabella di associazione dello snooping viene creata in modo dinamico e le informazioni corrispondenti vengono aggiunte al database dello snooping. Tuttavia, in questo caso, poiché il server NTP non è raggiungibile, sono stati eseguiti 0 tentativi totali di aggiornare o trasferire le informazioni di binding nel 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 - Server NTP raggiungibile

<#root>

DHCP_RelayAgent# ping vrf Mgmt-vrf 10.81.254.131

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

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

<#root>

DHCP_RelayAgent#show ip dhcp snooping binding

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

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

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

Una volta che l'utente riceve un indirizzo IP, la tabella di associazione dello snooping viene creata in modo dinamico e le informazioni corrispondenti vengono successivamente aggiunte al database dello snooping. Di conseguenza, è stato eseguito un tentativo totale di aggiornamento o trasferimento del database, con tutte le operazioni completate. Non sono stati eseguiti scritture, letture o trasferimenti non riusciti.

<#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>

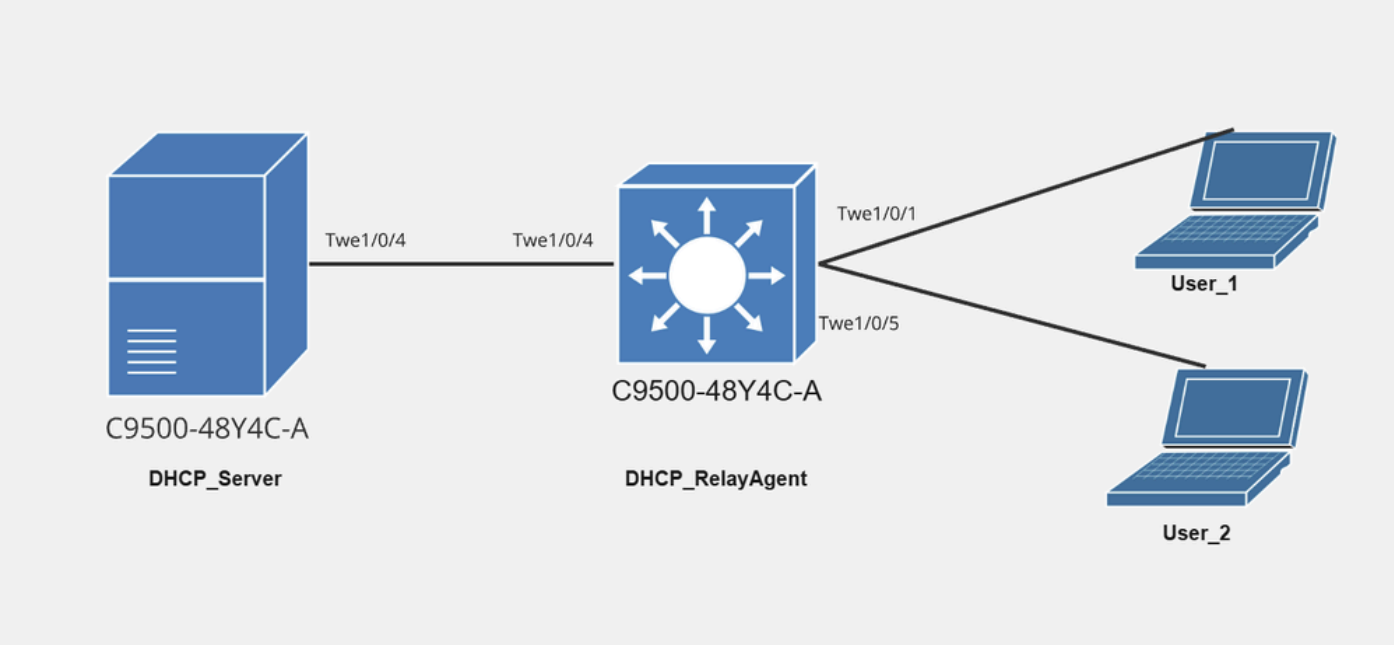
DHCP_RelayAgent#more flash:dhcpsnoopingdatabase.txt

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

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

```
END
```

Scenario 3 - Server NTP raggiungibile in modo intermittente



Esempio di rete con 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

Ora possiamo vedere che l'utente User_1 ha ricevuto l'IP 10.10.10.1 nella vlan 10.

Di seguito è riportata la tabella di binding Snooping DHCP, che mostra l'indirizzo IP, l'indirizzo MAC e l'interfaccia di User_1 su 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
```

Dopo un po', il NTP non è più raggiungibile, ma l'utente 2 ha ottenuto l'indirizzo IP 10.10.10.2 nella vlan 10 e l'indirizzo è stato aggiornato nella tabella di binding, ma non è stato inserito nella tabella del database di snooping.

<#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)
```

Questa è la tabella di binding dello snooping DHCP, che mostra l'indirizzo IP, l'indirizzo MAC e l'interfaccia per User_2 su TwentyFiveGigE1/0/5

<#root>

```
DHCP_RelayAgent#show ip dhcp snooping binding

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

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

La voce nel database di snooping non viene incrementata e il totale delle operazioni di scrittura riuscite rimane 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
```

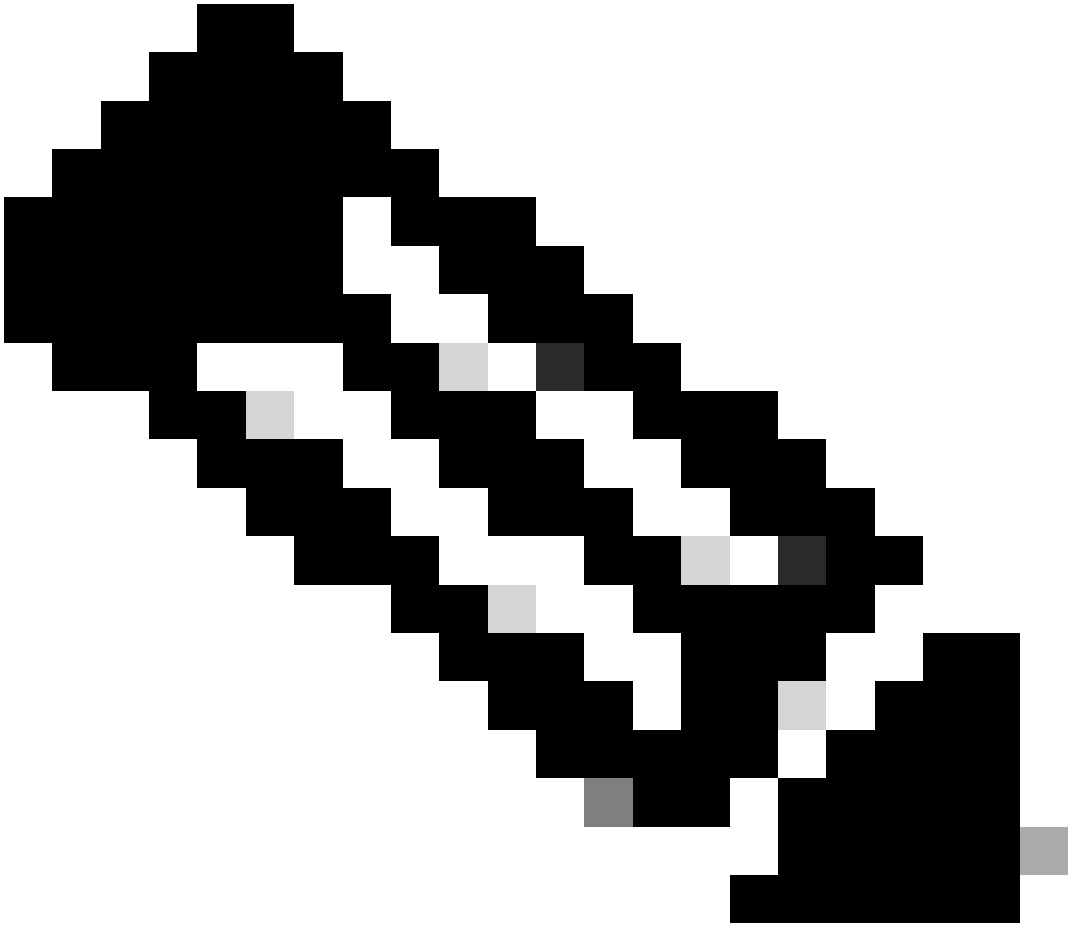
Quando il server NTP diventa accessibile, il sistema sincronizza la tabella di binding dello snooping DHCP e il database dello snooping DHCP. Questo scenario non viene mostrato qui. Tuttavia, risultati simili possono essere raggiunti rimuovendo la configurazione del server NTP.

Dopo aver rimosso la configurazione NTP, la voce per User_2 viene aggiunta alla tabella del database snooping.
In questo caso, lo switch usa l'ora di clock del sistema.

<#root>

```
DHCP_RelayAgent#configure terminal
```

DHCP_RelayAgent(config)# no ntp server 10.81.254.131



Nota: A scopo dimostrativo è stata rimossa la configurazione del server NTP. Tecnicamente, il risultato di Server NTP raggiungibile e Server NTP non configurato è simile.

```
*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.**

Conclusioni

- Se l'indirizzo IP del server NTP è presente e raggiungibile, vengono popolati sia la tabella di binding dello snooping DHCP che il database dello snooping. Le voci devono essere contrassegnate con un timestamp accurato utilizzando l'ora sincronizzata del server NTP.
- Se l'IP del server NTP è presente ma non raggiungibile, la tabella di binding dello snooping DHCP è ancora popolata, ma le voci non possono essere popolate nel database dello snooping, poiché il sistema non è in grado di sincronizzare il tempo per una gestione accurata del lease.
- Se l'indirizzo IP del server NTP non è configurato o non esiste, sia la tabella di binding dello snooping DHCP che il database dello snooping contengono ancora delle voci, ma i timestamp nel database dello snooping non sono affidabili, in quanto possono essere basati sull'ora del sistema locale.
- Per una gestione accurata e affidabile del database dello snooping DHCP, il protocollo NTP è fondamentale.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).