Risoluzione dei problemi relativi a DHCP sugli switch Catalyst 9000

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi relativi a DHCP su switch Catalyst 9000.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Architettura degli switch Catalyst serie 9000.
- Protocollo DHCP (Dynamic Host Configuration Protocol).

Componente utilizzato

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e

hardware:

- C9200
- C9300
- C9500
- C9400
- C9600

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.

Prodotti correlati

Il presente documento può essere utilizzato anche per le seguenti versioni hardware e software:

- Switch Catalyst serie 3650/3850 con Cisco IOS® XE 16.x.

Risoluzione dei problemi

Quando si risolvono i problemi relativi a DHCP, alcune informazioni critiche devono essere confermate per poter isolare la causa del problema. È molto importante disegnare una topologia della rete dall'origine alla destinazione e identificare i dispositivi che si trovano tra di loro e i loro ruoli.

In base a questi ruoli, è possibile eseguire alcune azioni per avviare la risoluzione dei problemi.

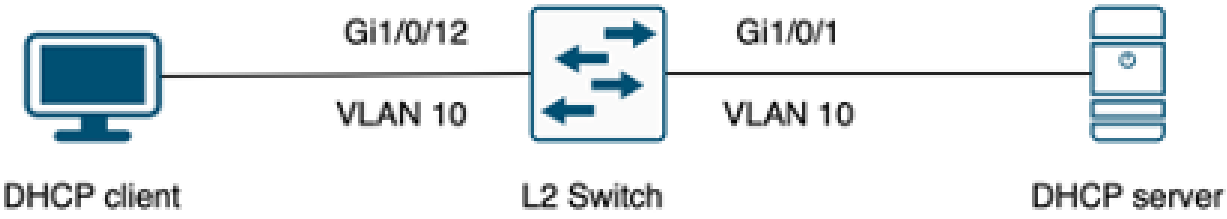
Switch configurato come bridge di livello 2

In questo scenario, lo switch deve ricevere e inoltrare il pacchetto DHCP senza alcuna modifica.

Passaggio 1. Confermare il percorso del pacchetto.

- Identificare le interfacce a cui sono connessi il client e il dispositivo dell'hop successivo verso il server DHCP.
- Identificare la VLAN o le VLAN interessate.

Esempio: si consideri la topologia seguente, in cui il client connesso all'interfaccia Gigabit Ethernet 1/0/12 nella VLAN 10 su uno switch C9300 non è in grado di accettare un indirizzo IP tramite DHCP. Il server DHCP è connesso all'interfaccia Gigabit Ethernet1/0/1 anche sulla VLAN 10.



Client connesso a uno switch di layer 2.

Suggerimento: se il problema riguarda più dispositivi e VLAN, scegliere un client per eseguire la risoluzione.

Passaggio 2. Controllate il tracciato del livello 2

- La VLAN deve essere creata e attiva sullo switch.

<#root>

```
c9300#show vlan brief

VLAN Name                             Status    Ports

---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/2, Gi1/0/3, Gi1/0/4, Gi1/0/5, Gi1/0/6, Gi1/0/7
                                                Gi1/0/8, Gi1/0/9, Gi1/0/10, Gi1/0/11, Gi1/0/13
                                                Gi1/0/14, Gi1/0/15, Gi1/0/16, Gi1/0/17, Gi1/0/18
                                                Gi1/0/19, Gi1/0/20, Gi1/0/21, Gi1/0/22, Gi1/0/23
                                                Gi1/0/24

10   users                            active    Gi1/0/12


1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

- La VLAN deve essere autorizzata sulle interfacce in entrata e in uscita.

<#root>

```
interface GigabitEthernet1/0/12
 description Client Port

 switchport access vlan 10


 switchport mode access

interface GigabitEthernet1/0/1
 description DHCP SERVER

 switchport mode trunk
```

<#root>

```
c9300#show interfaces trunk

Port          Mode             Encapsulation  Status        Native vlan
Gi1/0/1       on               802.1q         trunking      1

Port          Vlans allowed on trunk
Gi1/0/1       1-4094

Port          Vlans allowed and active in management domain
Gi1/0/1       1,
```

```
10


Port            Vlans in spanning tree forwarding state and not pruned


Gi1/0/1         1,10
```

- Lo switch deve conoscere l'indirizzo MAC del client nella VLAN corretta.

```
c9300-01#show mac address interface gi1/0/12
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  10    7018.a7e8.4f46    DYNAMIC     Gi1/0/12
```

- Se lo snooping DHCP è configurato, verificare che l'interfaccia di trust sia impostata correttamente.

Passaggio 3. Verificare che lo switch riceva i pacchetti di individuazione DHCP sulla porta del client.

- È possibile utilizzare lo strumento Embedded Packet Capture (EPC).
- Per filtrare solo i pacchetti DHCP, configurare un ACL.

```
c9300(config)#ip access-list extended DHCP
c9300(config-ext-nacl)#permit udp any any eq 68
c9300(config-ext-nacl)#permit udp any any eq 67
c9300(config-ext-nacl)#end

c9300#show access-lists DHCP
Extended IP access list DHCP
    10 permit udp any any eq bootpc
    20 permit udp any any eq bootps
```

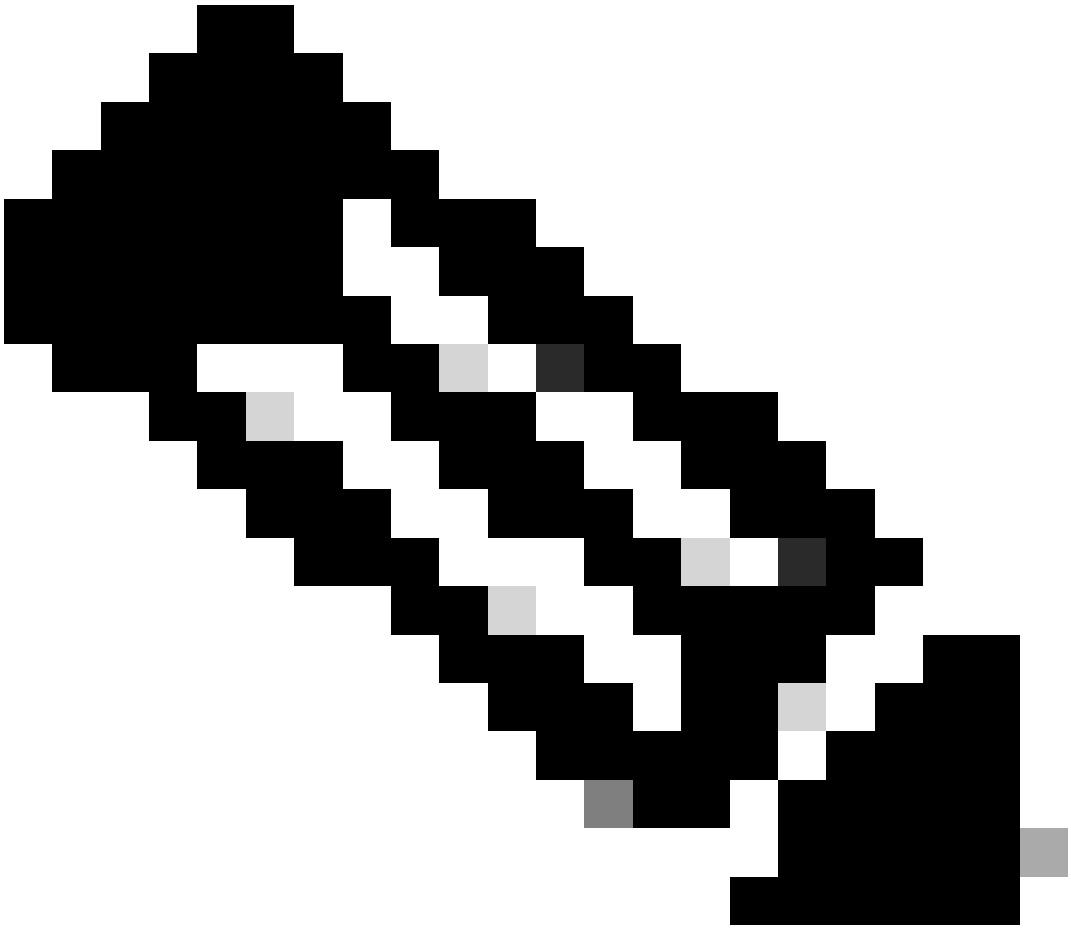
- Configurare e avviare l'acquisizione dei pacchetti in direzione in entrata sulla porta del client.

```
c9300#monitor capture cap interface GigabitEthernet1/0/12 in access-list DHCP
c9300#monitor capture cap start
Started capture point : cap

c9300#monitor capture cap stop
Capture statistics collected at software:
```

```
        Capture duration - 66 seconds
        Packets received - 5
        Packets dropped - 0
        Packets oversized - 0

Bytes dropped in asic - 0

Stopped capture point : cap
```

- Verificare il contenuto dell'acquisizione.

```
c9300#show monitor capture cap buffer brief
Starting the packet display ........ Press Ctrl + Shift + 6 to exit
1   0.000000      0.0.0.0 -> 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0x9358003
2   3.653608      0.0.0.0 -> 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0x935800
```

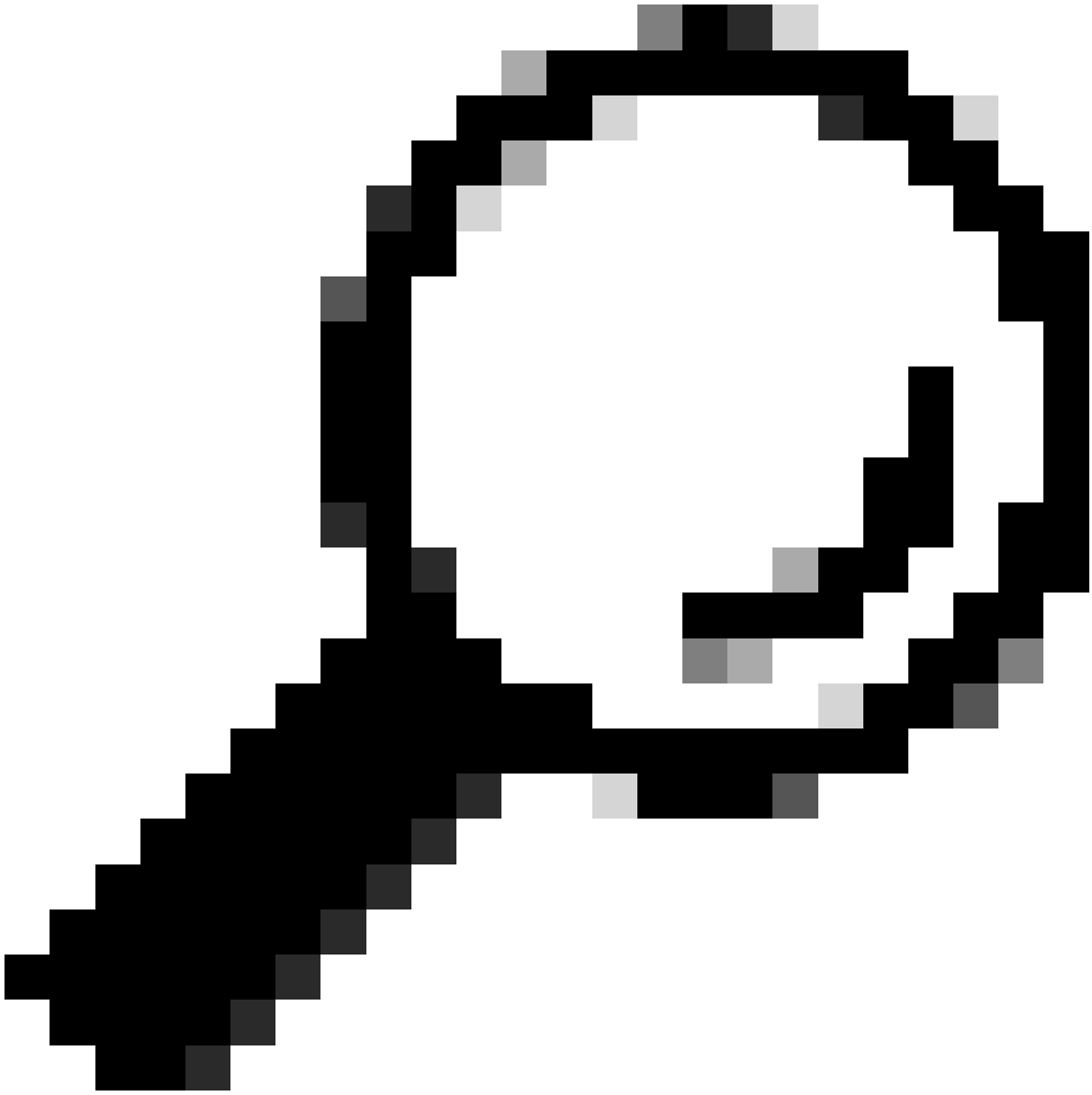


Nota: in circostanze normali, se si prende un EPC in ENTRAMBE le direzioni sulla porta del client, è possibile vedere il processo DORA completato.

Passaggio 4. Accertarsi che lo switch stia inoltrando il messaggio di rilevamento DHCP.

- È possibile eseguire un'acquisizione sulla porta di uscita in direzione uscita.

```
c9300#monitor capture cap interface GigabitEthernet1/0/1 out access-list DHCP
c9300#show monitor capture cap buffer brief
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

1   0.000000      0.0.0.0 -> 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0x4bf2a30e
2   0.020893      0.0.0.0 -> 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0xe4331741
```



Suggerimento: per verificare che l'individuazione DHCP raccolta nell'acquisizione appartenga al client in fase di risoluzione dei problemi, è possibile applicare il filtro dhcp.hw.mac_addr all'EPC utilizzando l'opzione display-filter.

A questo punto, è stato confermato che lo switch sta inoltrando i pacchetti DHCP e che la risoluzione dei problemi può essere spostata sul server DHCP.

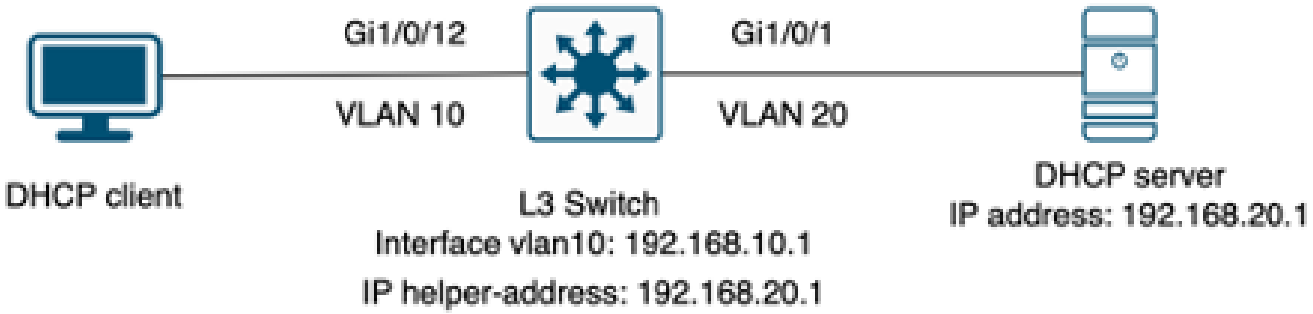
Switch configurato come agente di inoltro

L'agente di inoltro viene utilizzato quando i client e i server DHCP non appartengono allo stesso dominio di broadcast.

Quando lo switch è configurato come agente di inoltro, i pacchetti DHCP vengono modificati nello switch; per i pacchetti inviati dal client, lo switch aggiunge le proprie informazioni (indirizzo IP e

indirizzo MAC) al pacchetto e lo invia all'hop successivo verso il server DHCP. I pacchetti ricevuti dal server DHCP vengono indirizzati all'agente di inoltro, quindi lo switch li inoltra nuovamente al client.

Continuando con l'esempio dello scenario precedente, si supponga che un client sia connesso all'interfaccia Gigabit Ethernet 1/0/12 sulla VLAN 10 e non sia in grado di ottenere un indirizzo IP tramite DHCP. Ora lo switch C9000 è il gateway predefinito per la VLAN 10 ed è configurato come agente di inoltro. Il server DHCP è connesso all'interfaccia Gigabit Ethernet 1/0/1 sulla VLAN 20.



Il client si è connesso a uno switch di layer 3 configurato come agente di inoltro.

Passaggio 1. Confermare che lo switch sta ricevendo il comando DHCP discover.

- Eseguire un'acquisizione pacchetto sull'interfaccia rivolta verso il client. Fare riferimento al passaggio 3 dello scenario precedente.

Passaggio 2. Controllare la configurazione dell'helper IP.

- Il servizio DHCP deve essere abilitato.

```
show run all | in dhcp
service dhcp
```

- IP helper sotto la VLAN 10 SVI.

<#root>

```
interface vlan10
 ip address 192.168.10.1 255.255.255.0

ip helper-address 192.168.20.1
```

Passaggio 3. Verificare la connettività ai server DHCP.

- Lo switch deve avere connettività unicast con il server DHCP dalla VLAN client. È possibile eseguire il test con un ping.

```
c9300-01#ping 192.168.20.1 source vlan 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Passaggio 4. Verificare che lo switch stia inoltrando i pacchetti DHCP all'hop successivo.

- È possibile eseguire un pacchetto del server dhcp ip di debug.

<#root>

```
*Feb  2 23:14:20.435: DHCPD: tableid for 192.168.10.1 on Vlan10 is 0
*Feb  2 23:14:20.435: DHCPD: client's VPN is .
*Feb  2 23:14:20.435: DHCPD: No option 125
*Feb  2 23:14:20.435: DHCPD: No option 124
*Feb  2 23:14:20.435: DHCPD: Option 125 not present in the msg.
*Feb  2 23:14:20.435: DHCPD: using received relay info.
*Feb  2 23:14:20.435: DHCPD: Looking up binding using address 192.168.10.1
*Feb  2 23:14:20.435:
```

DHCPD: setting giaddr to 192.168.10.1.

```
*Feb  2 23:14:20.435:
```

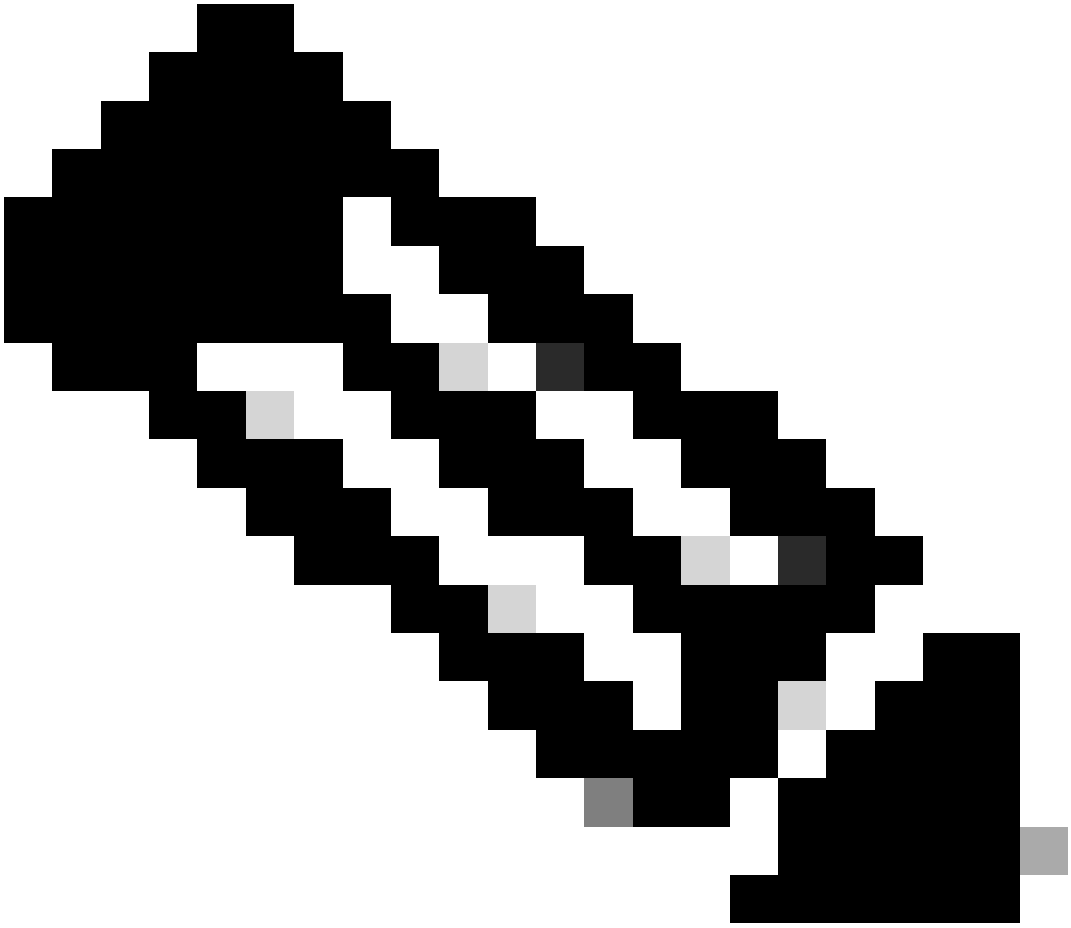
DHCPD: BOOTREQUEST from 0170.18a7.e84f.46 forwarded to 192.168.20.1.

- Acquisire i pacchetti. È possibile utilizzare EPC sul control plane.

```
monitor capture cap control-plane both access-list DHCP
monitor capture cap [start | stop]
```

- L'SPAN può essere usato anche sulla porta di uscita.

```
Monitor session 1 source interface Gi1/0/1 tx
Monitor session 1 destination interface [interface ID] encapsulation replicate
```



Nota: è necessario configurare un solo agente di inoltro sul percorso.

Switch configurato come server DHCP

In questo scenario, l'ambito DHCP dello switch è configurato localmente.

Passaggio 1. Controllare la configurazione di base.

- È necessario creare il pool e configurare la rete, la subnet mask e il router predefinito.

```
ip dhcp pool VLAN10
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
```

- I servizi DHCP devono essere abilitati.

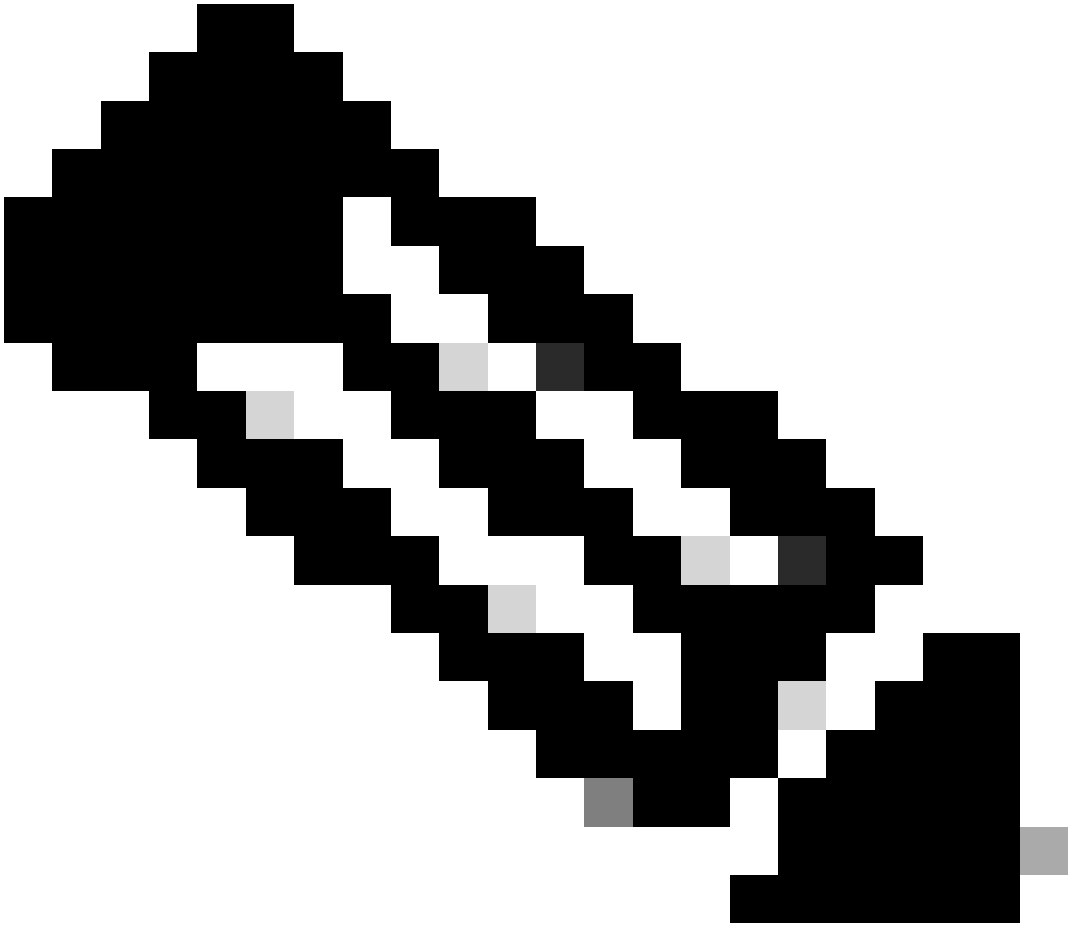
```
show run all | in dhcp
service dhcp
```

- Lo switch deve disporre di connettività unicast alle reti configurate nei pool.

```
ping 192.168.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

- Tutti gli indirizzi IP configurati staticamente devono essere esclusi dall'intervallo del pool.

```
ip dhcp excluded-address 192.168.10.1
```

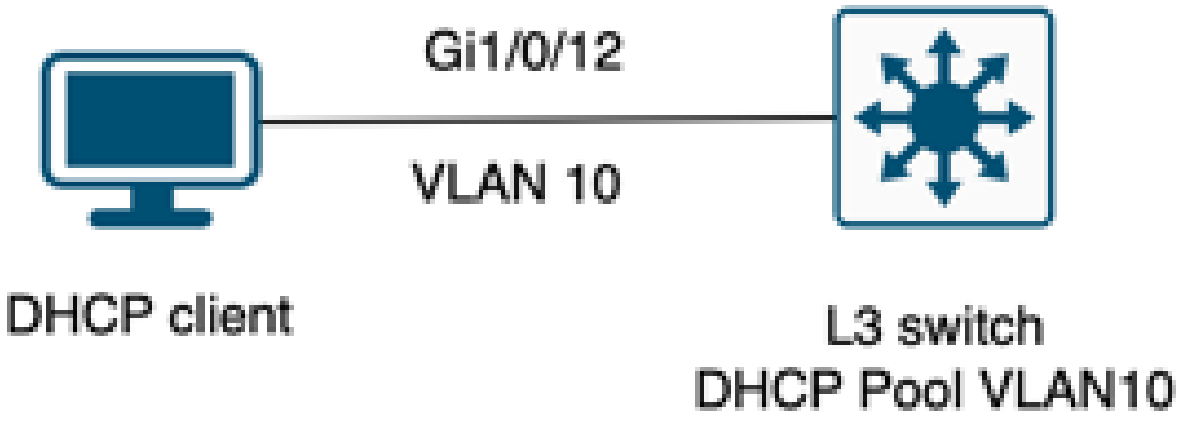


Nota: se lo switch è configurato come server DHCP o agente di inoltro, il DHCP del servizio deve essere abilitato.

Passaggio 2. Verificare che lo switch disponga di indirizzi IP in leasing.

- È possibile usare i dettagli del pacchetto del server dhcp debug ip.

Esempio 1: il client si connette direttamente allo switch Catalyst 9000 configurato come server DHCP sulla VLAN 10.



Il client è connesso a uno switch di livello 3 configurato come server DHCP.

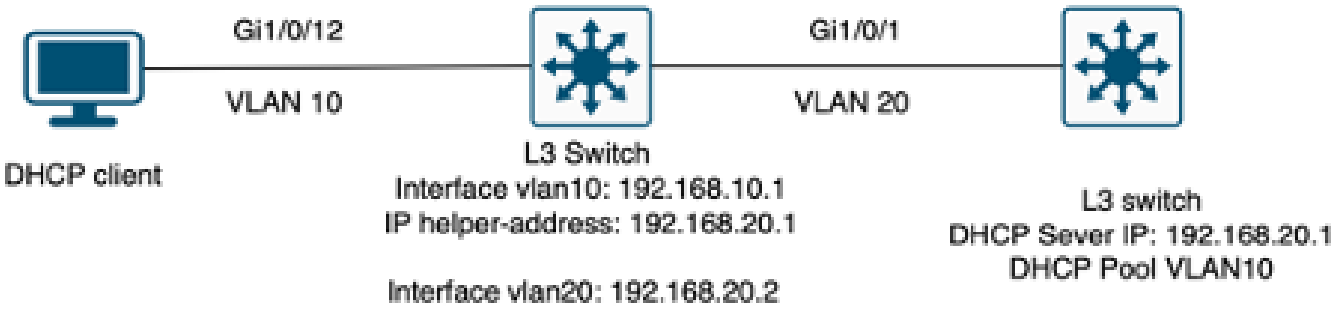
<#root>

```
Feb 16 19:03:33.828:

DHCPD: DHCPDISCOVER received from client

 0063.6973.636f.2d39.6335.342e.3136.6237.2e37.6436.342d.5477.6531.2f30.2f31

on interface Vlan10.DHCPD: Setting only requested parameters


*Feb 16 19:03:33.828: DHCPD: Option 125 not present in the msg.
*Feb 16 19:03:33.828:

DHCPD: egress Interfce Vlan10


*Feb 16 19:03:33.828:

DHCPD: broadcasting BOOTREPLY to client 9c54.16b7.7d64.


*Feb 16 19:03:33.828: Option 82 not present
*Feb 16 19:03:33.828: DHCPD: tableid for 192.168.10.1 on Vlan10 is 0
*Feb 16 19:03:33.828: DHCPD: client's VPN is .
*Feb 16 19:03:33.828: DHCPD: No option 125
*Feb 16 19:03:33.828: DHCPD: Option 124: Vendor Class Information
*Feb 16 19:03:33.828:   DHCPD: Enterprise ID: 9
*Feb 16 19:03:33.829:   DHCPD: Vendor-class-data-len: 10
*Feb 16 19:03:33.829:   DHCPD: Data: 4339333030582D313259
*Feb 16 19:03:33.829:

DHCPD: DHCPREQUEST received from client

 0063.6973.636f.2d39.6335.342e.3136.6237.2e37.6436.342d.5477.6531.2f30.2f31

on interface Vlan10
```

```
*Feb 16 19:03:33.829: DHCPD: Client is Selecting (

DHCP Request with Requested IP = 192.168.10.2

,

Server ID = 192.168.10.1

)
*Feb 16 19:03:33.829: DHCPD: Option 125 not present in the msg.
*Feb 16 19:03:33.829: DHCPD: No default domain to append - abort updateDHCPD: Setting only requested pa
*Feb 16 19:03:33.829: DHCPD: Option 125 not present in the msg.
*Feb 16 19:03:33.829: DHCPD: egress Interfce Vlan10
*Feb 16 19:03:33.829:

DHCPD: broadcasting BOOTREPLY to client 9c54.16b7.7d64
```

Esempio 2: il client non è connesso direttamente allo switch Catalyst 9000 configurato come server DHCP.

In questo scenario, il client è connesso a uno switch L3 impostato come gateway e agente di inoltro predefiniti e il server DHCP è ospitato su uno switch Catalyst 9000 adiacente sulla VLAN 20.



Client non connesso direttamente allo switch di layer 3 che funziona come server DHCP.

<#root>

```
*Feb 16 19:56:35.783: DHCPD:

DHCPDISCOVER received from client

 0063.6973.636f.2d39.6335.342e.3136.6237.2e37.6436.342d.5477.6531.2f30.2f31

through relay 192.168.10.1.


*Feb 16 19:56:35.783: DHCPD: Option 125 not present in the msg.
*Feb 16 19:56:35.783: Option 82 not present
*Feb 16 19:56:35.783: Option 82 not present
*Feb 16 19:56:35.783: DHCPD: Option 125 not present in the msg.DHCPD: Setting only requested parameters
*Feb 16 19:56:35.783: DHCPD: Option 125 not present in the msg.
*Feb 16 19:56:35.783: DHCPD:

egress Interfce Vlan20
```

```
*Feb 16 19:56:35.783: DHCPD:
```

unicasting BOOTREPLY for client 9c54.16b7.7d64 to relay 192.168.10.1.

```
*Feb 16 19:56:35.785: Option 82 not present
*Feb 16 19:56:35.785: DHCPD: tableid for 192.168.20.1 on Vlan20 is 0
*Feb 16 19:56:35.785: DHCPD: client's VPN is .
*Feb 16 19:56:35.785: DHCPD: No option 125
*Feb 16 19:56:35.785: DHCPD: Option 124: Vendor Class Information
*Feb 16 19:56:35.785:   DHCPD: Enterprise ID: 9
*Feb 16 19:56:35.785:   DHCPD: Vendor-class-data-len: 10
*Feb 16 19:56:35.785:   DHCPD: Data: 4339333030582D313259
*Feb 16 19:56:35.785: DHCPD:
```

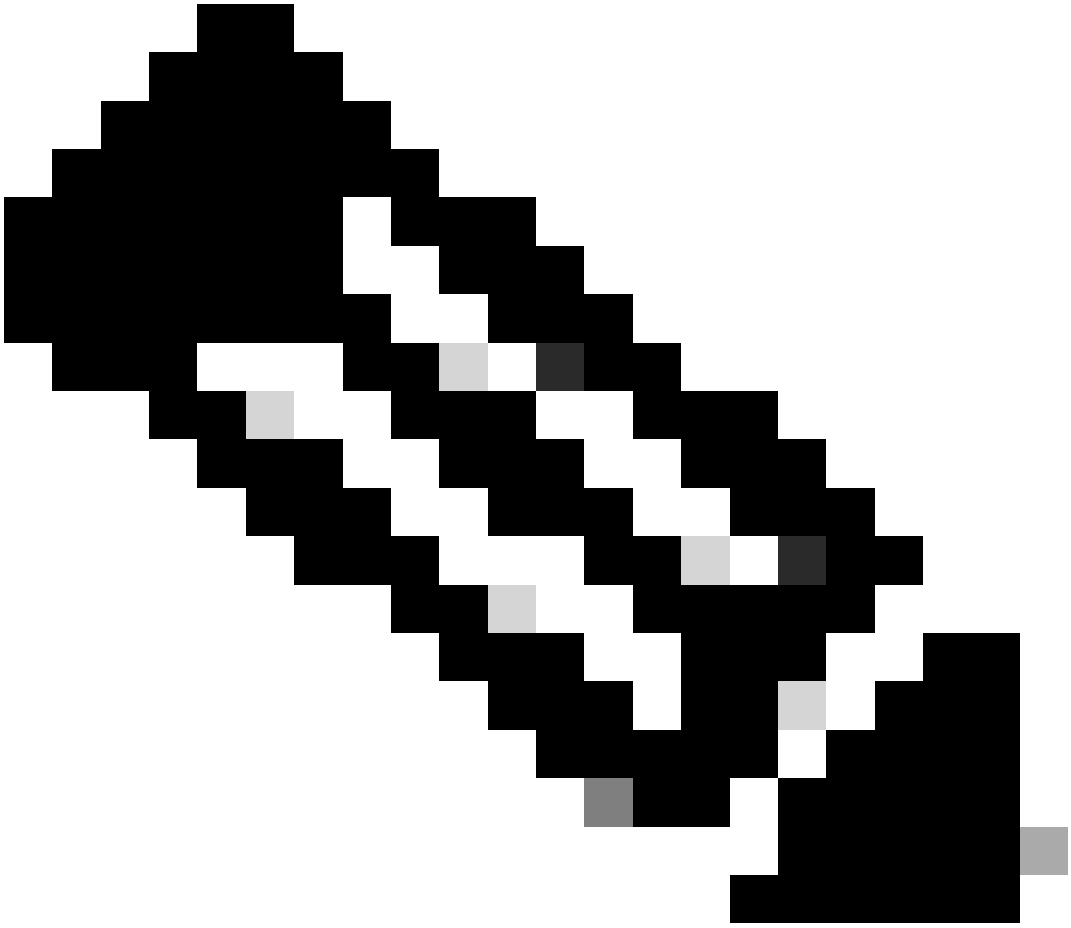
DHCPREQUEST received from client

```
 0063.6973.636f.2d39.6335.342e.3136.6237.2e37.6436.342d.5477.6531.2f30.2f31 on interface Vlan20
*Feb 16 19:56:35.785: DHCPD: Client is Selecting (
```

DHCP Request with Requested IP = 192.168.10.2, Server ID = 192.168.20.1

```
)
*Feb 16 19:56:35.785: DHCPD: Option 125 not present in the msg.
*Feb 16 19:56:35.785: DHCPD: No default domain to append - abort updateDHCPD: Setting only requested pa
*Feb 16 19:56:35.785: DHCPD: Option 125 not present in the msg.
*Feb 16 19:56:35.785: DHCPD: egress Interfce Vlan20
*Feb 16 19:56:35.785:
```

DHCPD: unicasting BOOTREPLY for client 9c54.16b7.7d64 to relay 192.168.10.1.



Nota: se lo switch è configurato come server DHCP e agente di inoltro per la stessa VLAN, il server DHCP ha la precedenza.

Informazioni correlate

- Configurazione di DHCP
- Configurazione di Embedded Packet Capture
- Configurazione di SPAN

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).