Fehlerbehebung bei DHCP auf Catalyst Switches der Serie 9000

Inhalt

Einleitung

In diesem Dokument wird die Fehlerbehebung bei DHCP auf Catalyst 9000-Switches beschrieben.

Voraussetzungen

Anforderungen

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

- Catalyst Switches der Serie 9000
- Dynamic Host Configuration Protocol (DHCP)

Verwendete Komponente

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-

Versionen:

- C9200
- C9300
- C9500
- C9400
- C9600

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.

Verwandte Produkte

Dieses Dokument kann auch mit folgenden Hardware- und Softwareversionen verwendet werden:

- Catalyst Switches der Serien 3650/3850 mit Cisco IOS® XE 16.x

Fehlerbehebung

Wenn Sie DHCP-Probleme beheben, müssen Sie die wichtigen Informationen bestätigen, um die Ursache des Problems zu identifizieren. Es ist sehr wichtig, eine Topologie des Netzwerks von der Quelle bis zum Ziel zu zeichnen und die dazwischen liegenden Geräte und deren Rollen zu identifizieren.

Basierend auf diesen Rollen gibt es Aktionen, die ergriffen werden können, um die Fehlerbehebung zu starten.

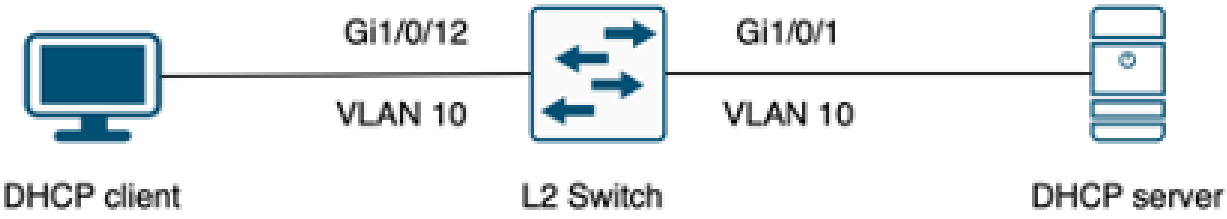
Switch als Layer-2-Bridge konfiguriert

In diesem Szenario wird erwartet, dass der Switch das DHCP-Paket ohne Änderungen empfängt und weiterleitet.

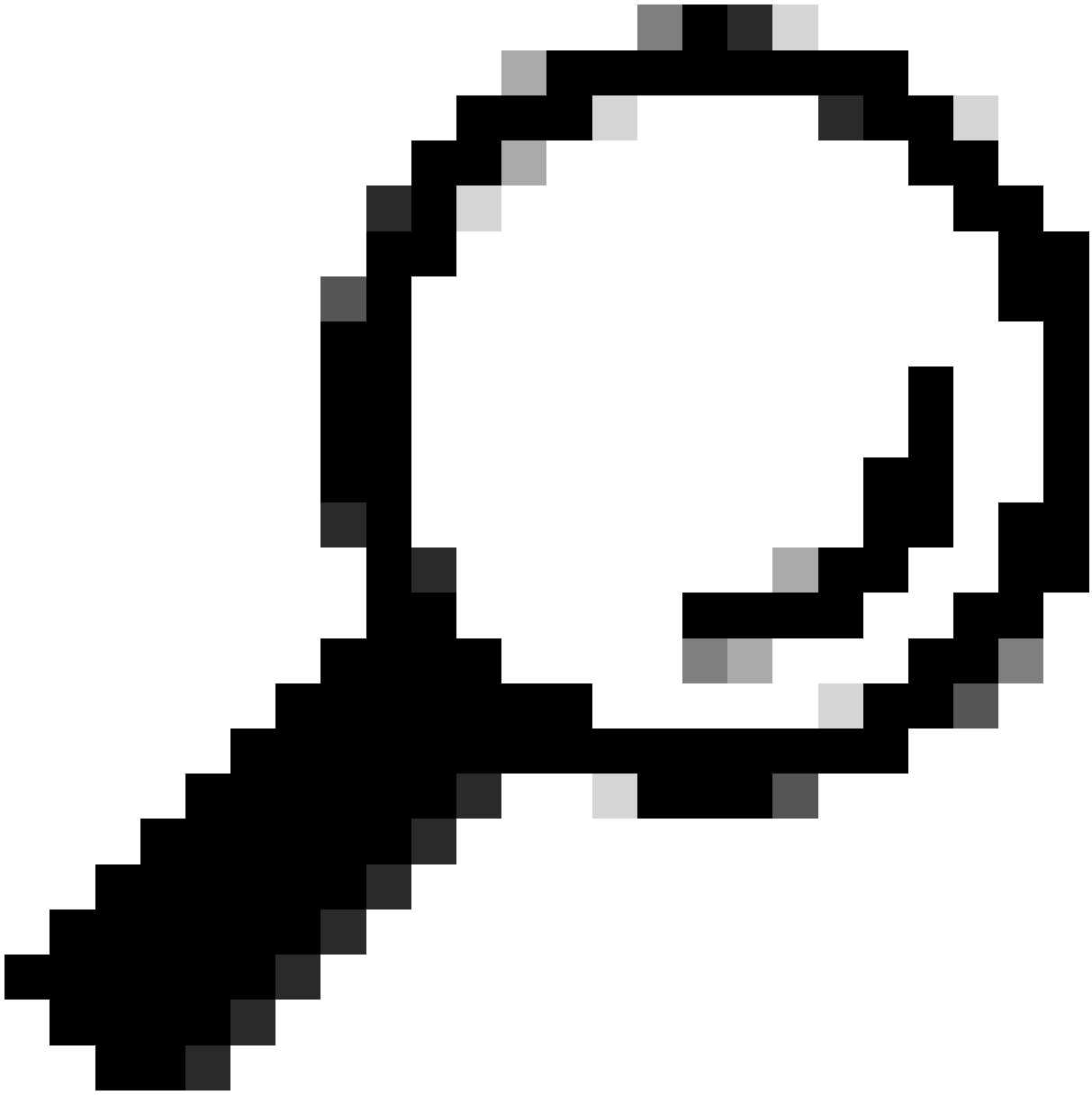
Schritt 1: Bestätigen Sie den Pfad des Pakets.

- Identifizieren Sie die Schnittstellen, über die der Client und das Next-Hop-Gerät mit dem DHCP-Server verbunden sind.
- Identifizieren Sie das betroffene VLAN oder die betroffenen VLANs.

Beispiel: Betrachten Sie die Topologie unten, bei der der Client, der mit der GigabitEthernet1/0/12-Schnittstelle in VLAN 10 auf einem C9300-Switch verbunden ist, keine IP-Adresse über DHCP empfangen kann. Der DHCP-Server ist an die Schnittstelle GigabitEthernet1/0/1 sowie an VLAN 10 angeschlossen.



Mit einem Layer-2-Switch verbundener Client.



Tipp: Wenn das Problem mehrere Geräte und VLANs betrifft, wählen Sie einen Client zur Fehlerbehebung aus.

Schritt 2: Überprüfen Sie den Layer-2-Pfad.

- Das VLAN muss auf dem Switch erstellt und aktiviert werden.

<#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
```

- Das VLAN muss an den Eingangs- und Ausgangsschnittstellen zugelassen werden.

<#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
```

- Der Switch muss die MAC-Adresse des Clients im richtigen VLAN abrufen.

```
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
```

- Wenn DHCP-Snooping konfiguriert ist, stellen Sie sicher, dass die vertrauenswürdige Schnittstelle richtig eingestellt ist.

Schritt 3: Stellen Sie sicher, dass der Switch die DHCP-Ermittlungspakete auf dem Client-Port empfängt.

- Sie können das EPC-Tool (Embedded Packet Capture) verwenden.
- Um nur die DHCP-Pakete zu filtern, konfigurieren Sie eine 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
```

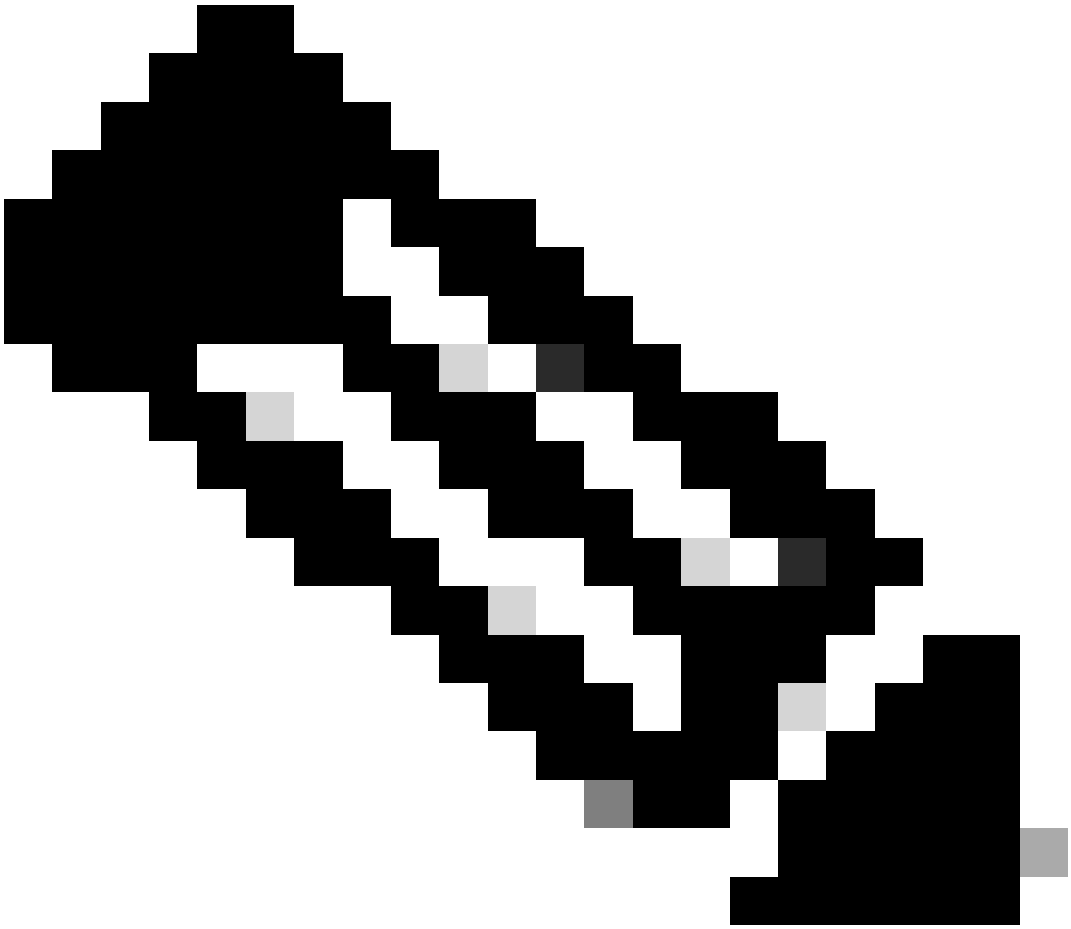
- Konfigurieren und starten Sie die Paketerfassung in eingehender Richtung auf dem Client-Port.

```
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
```

- Überprüfen Sie den Inhalt der Aufzeichnung.

```
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
```

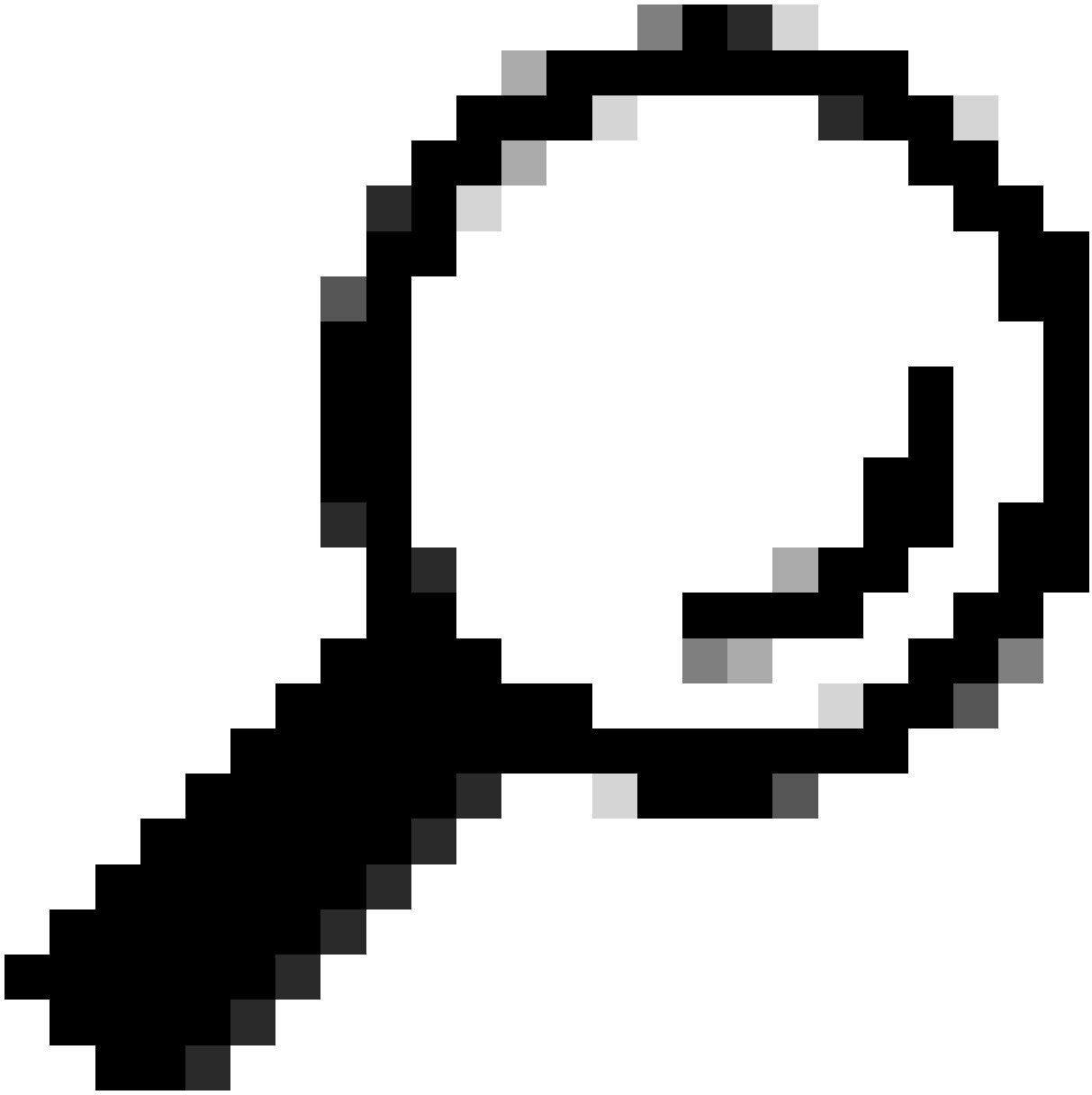


Hinweis: Wenn Sie einen EPC in BEIDE Richtungen auf dem Client-Port nehmen, sehen Sie unter normalen Umständen, dass der DORA-Prozess abgeschlossen ist.

Schritt 4: Stellen Sie sicher, dass der Switch die DHCP-Erkennung weiterleitet.

- Sie können eine Erfassung am Ausgangsport in ausgehender Richtung durchführen.

```
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
```



Tipp: Um zu bestätigen, dass die DHCP-Erkennung, die in der Erfassung erfasst wird, zu dem Client gehört, für den die Fehlerbehebung durchgeführt wird, können Sie den Filter dhcp.hw.mac_addr mithilfe der Option display-filter auf den EPC anwenden.

An diesem Punkt haben wir bestätigt, dass der Switch die DHCP-Pakete weiterleitet. Die Fehlerbehebung kann auf den DHCP-Server verschoben werden.

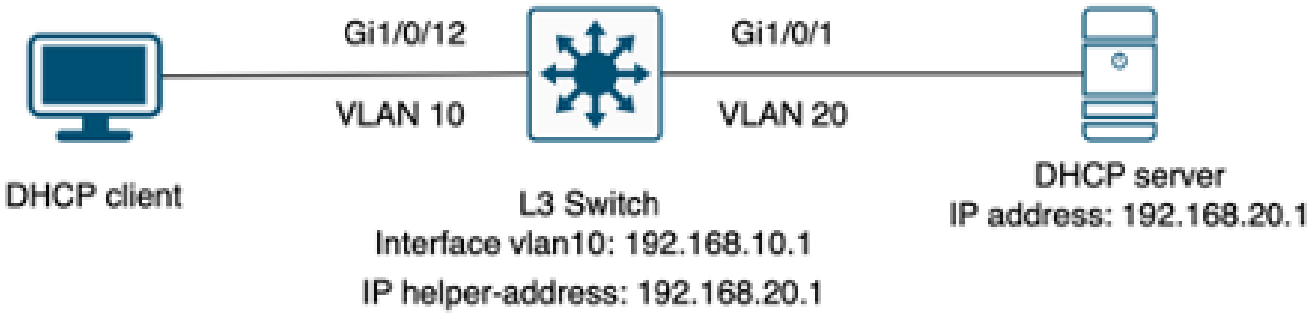
Als Relay Agent konfigurierter Switch

Der Relay-Agent wird verwendet, wenn die Clients und die DHCP-Server nicht zur gleichen Broadcast-Domäne gehören.

Wenn der Switch als Relay Agent konfiguriert ist, werden die DHCP-Pakete im Switch geändert. Bei vom Client gesendeten Paketen fügt der Switch dem Paket seine eigenen Informationen (IP-

Adresse und MAC-Adresse) hinzu und sendet es an den nächsten Hop zum DHCP-Server. Die vom DHCP-Server empfangenen Pakete werden an den Relay Agent weitergeleitet, und der Switch leitet sie dann zurück an den Client.

Fahren Sie mit dem Beispiel aus dem vorherigen Szenario fort: Ein Client, der mit der Schnittstelle Gigabitethernet1/0/12 im VLAN 10 verbunden ist, kann keine IP-Adresse über DHCP abrufen. Der C9000-Switch ist jetzt das Standard-Gateway für VLAN 10 und wird als Relay Agent konfiguriert. Der DHCP-Server ist mit der Schnittstelle Gigabitethernet1/0/1 im VLAN 20 verbunden.



Client, der mit einem als Relay Agent konfigurierten Layer-3-Switch verbunden ist.

Schritt 1: Bestätigen Sie, dass der Switch die DHCP-Erkennung empfängt.

- Führen Sie eine Paketerfassung an der Schnittstelle zum Client aus. Siehe Schritt 3 im vorherigen Szenario.

Schritt 2: Überprüfen der IP-Hilfskonfiguration

- Der DHCP-Dienst muss aktiviert sein.

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

- IP-Hilfsbefehl unter VLAN 10 SVI.

<#root>

```
interface vlan10
 ip address 192.168.10.1 255.255.255.0

ip helper-address 192.168.20.1
```

Schritt 3: Überprüfen der Verbindung zu den DHCP-Servern

- Der Switch muss über Unicast-Verbindungen zum DHCP-Server vom Client-VLAN verfügen. Sie können mit einem Ping testen.

```
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
```

Schritt 4: Vergewissern Sie sich, dass der Switch die DHCP-Pakete an den nächsten Hop weiterleitet.

- Sie können ein debug ip dhcp server packet detail ausführen.

<#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:
```

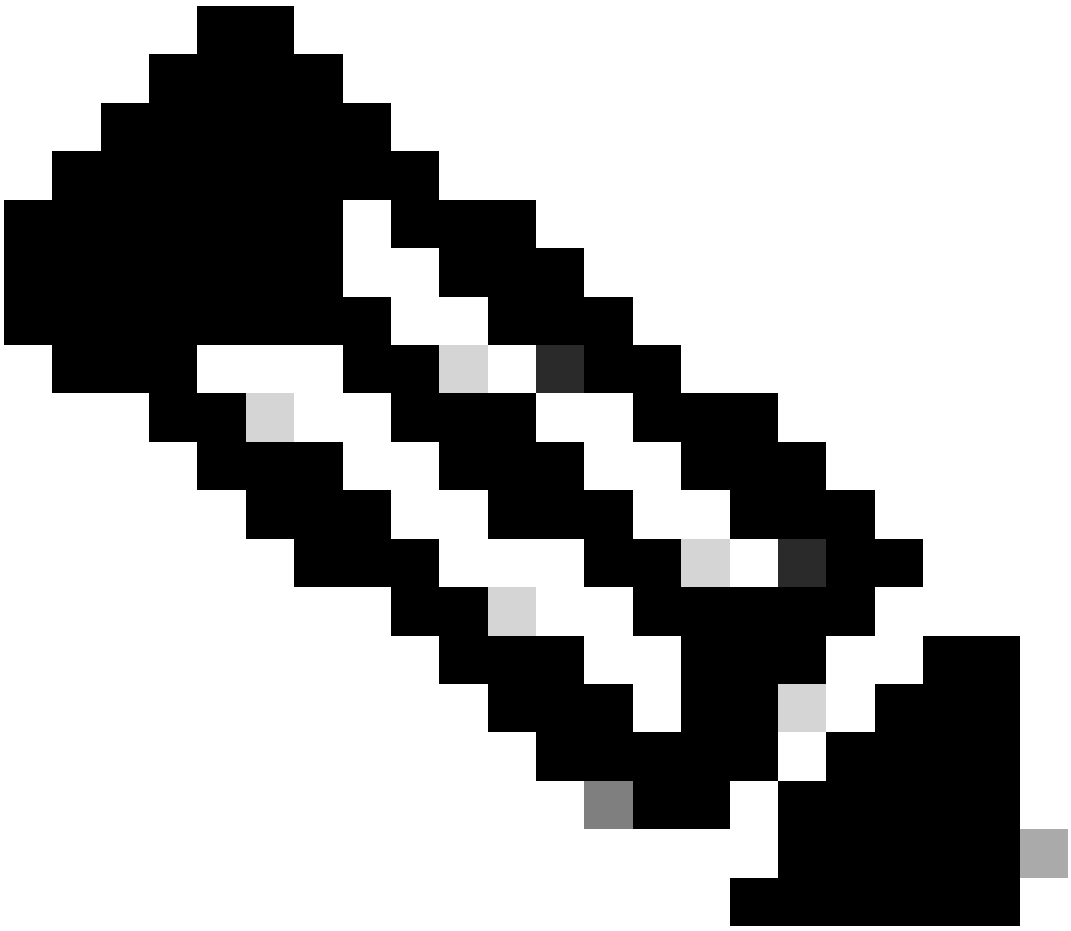
DHCPD: BOOTREQUEST from 0170.18a7.e84f.46 forwarded to 192.168.20.1.

- Nehmen Sie Paketerfassungen. Sie können EPC auf Kontrollebene verwenden.

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

- Sie können auch ein SPAN im Ausgangsport verwenden.

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



Hinweis: Sie müssen nur einen Relay-Agenten auf dem Pfad konfigurieren.

Switch als DHCP-Server konfiguriert

In diesem Szenario wird der DHCP-Bereich des Switches lokal konfiguriert.

Schritt 1: Überprüfen der Basiskonfiguration

- Der Pool muss erstellt werden, und das Netzwerk, die Subnetzmaske und der Standardrouter müssen konfiguriert sein.

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

- DHCP-Dienste müssen aktiviert sein.

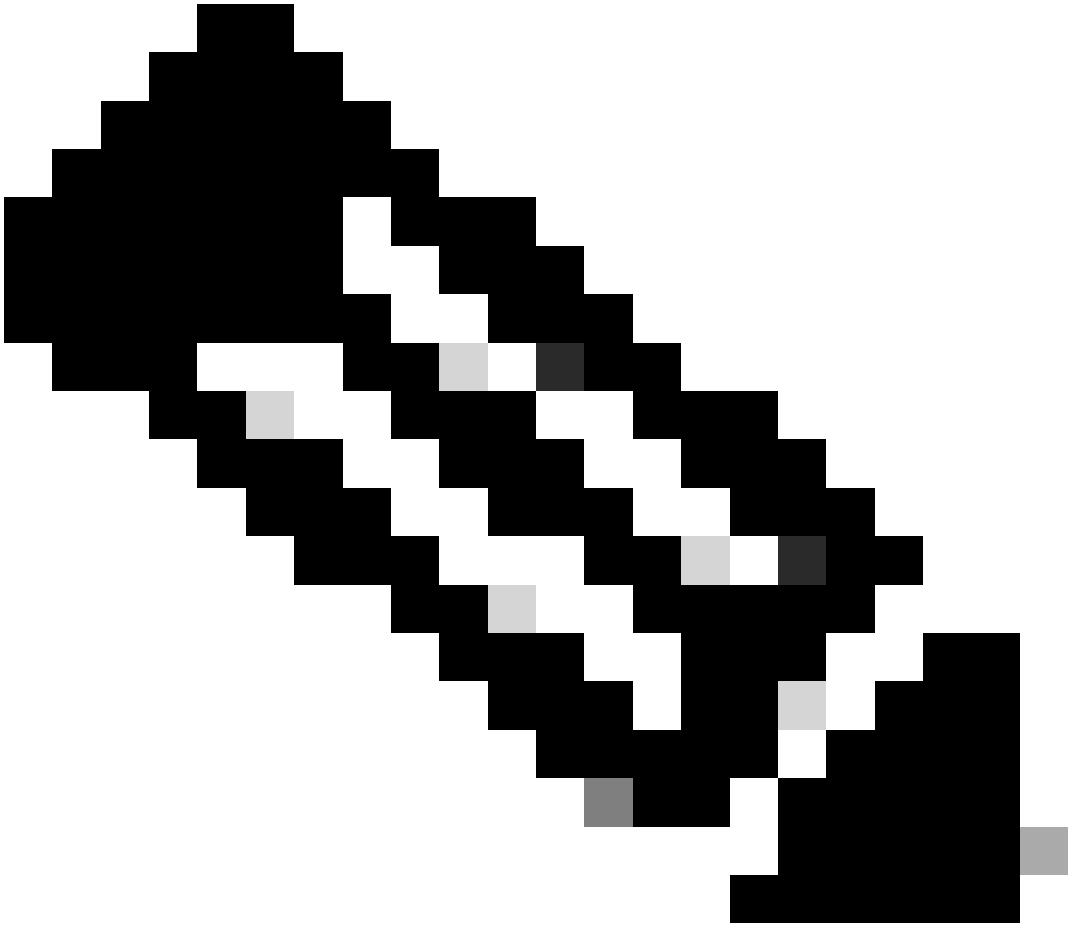
```
show run all | in dhcp
service dhcp
```

- Der Switch muss über Unicast-Verbindungen zu den in den Pools konfigurierten Netzwerken verfügen.

```
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
```

- Alle statisch konfigurierten IP-Adressen müssen aus dem Pool-Bereich ausgeschlossen werden.

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

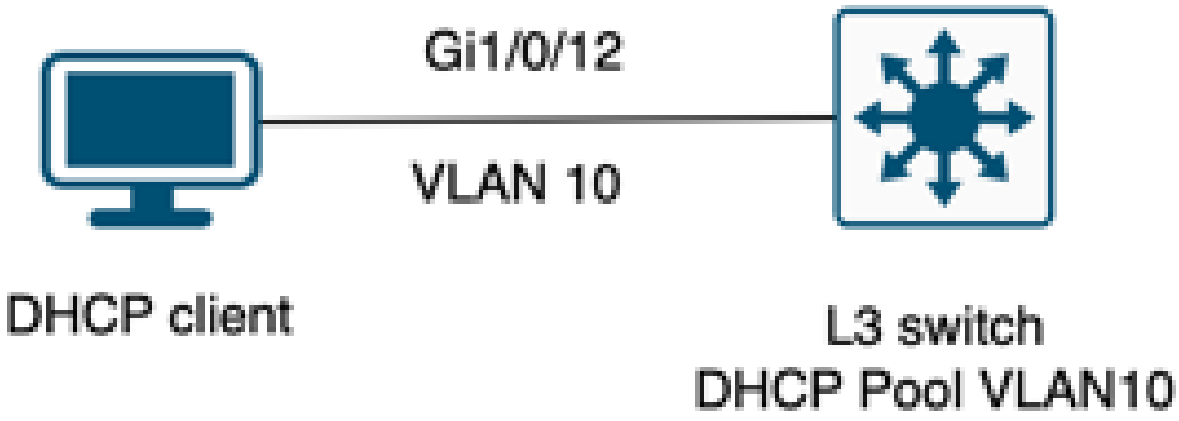


Hinweis: Service-DHCP muss aktiviert sein, wenn der Switch als DHCP-Server oder Relay-Agent konfiguriert ist.

Schritt 2: Überprüfen Sie, ob der Switch IP-Adressen geleast.

- Sie können debug ip dhcp server packet detail verwenden.

Beispiel 1: Der Client stellt eine direkte Verbindung mit dem Catalyst 9000-Switch her, der als DHCP-Server im VLAN 10 konfiguriert ist.



Client, der mit einem als DHCP-Server konfigurierten Layer-3-Switch verbunden ist.

<#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

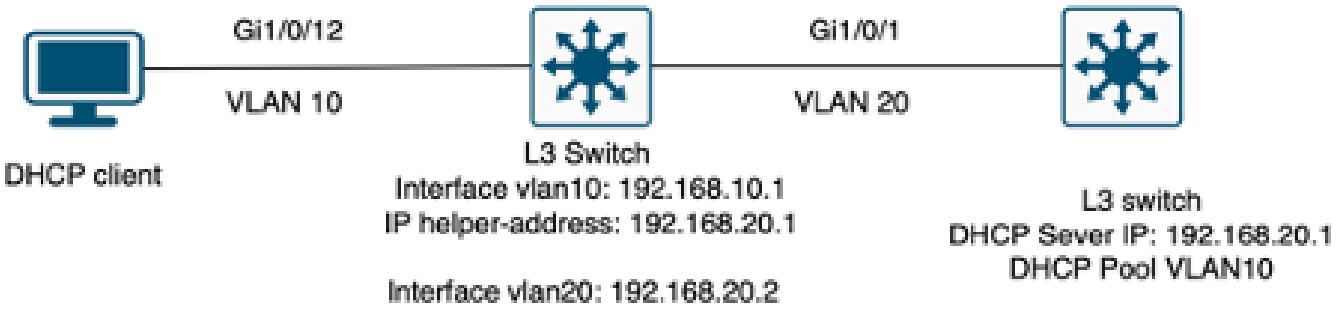
0063.6973.636f.2d39.6335.342e.3136.6237.2e37.6436.342d.5477.6531.2f30.2f31

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
```

Beispiel 2: Der Client ist nicht direkt mit dem als DHCP-Server konfigurierten Catalyst 9000-Switch verbunden.

In diesem Szenario ist der Client mit einem L3-Switch verbunden, der als Standard-Gateway und Relay-Agent festgelegt ist, und der DHCP-Server wird auf einem benachbarten Catalyst 9000-Switch im VLAN 20 gehostet.



Client, der nicht direkt mit dem Layer-3-Switch verbunden ist und als DHCP-Server fungiert

<#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:
```

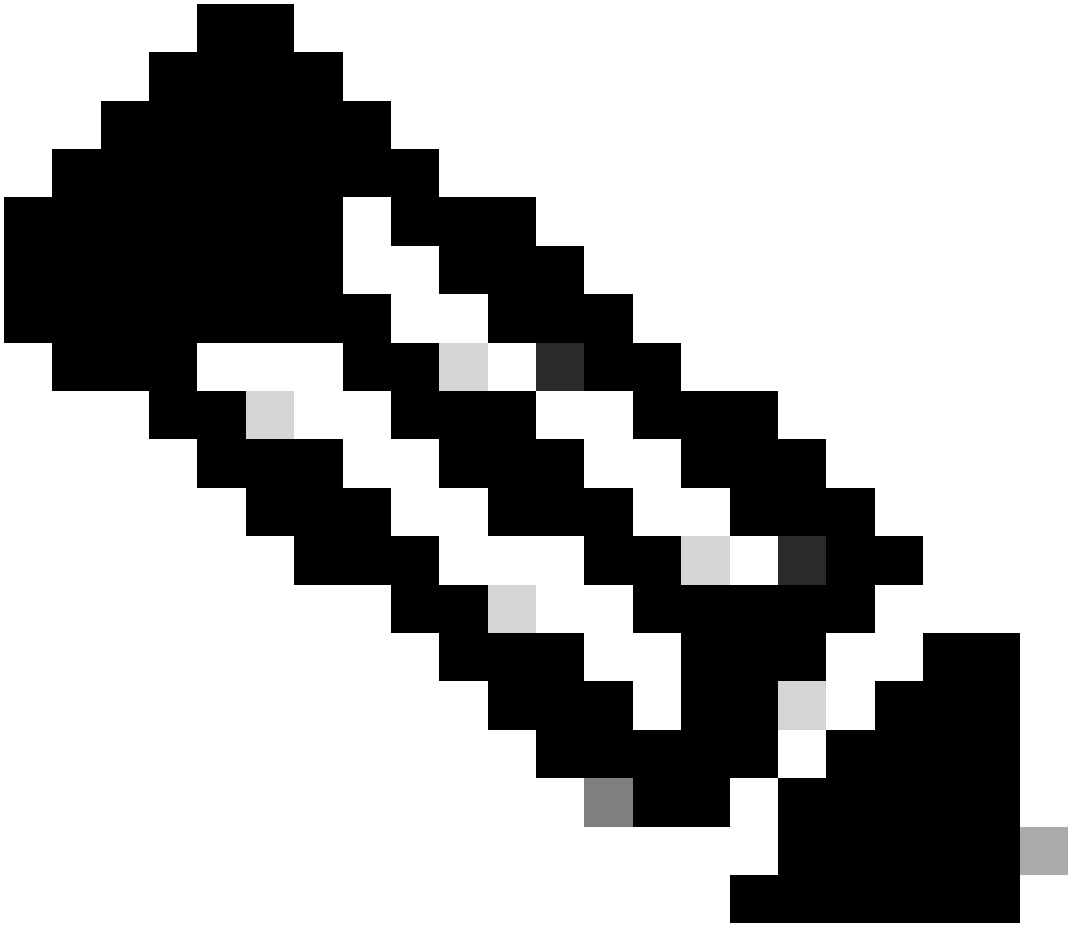
DHCPREQUEST received from client

```
 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.



Hinweis: Wenn der Switch als DHCP-Server und Relay-Agent für dasselbe VLAN konfiguriert ist, hat der DHCP-Server Vorrang.

Zugehörige Informationen

- Konfigurieren von DHCP
- Konfigurieren der eingebetteten Paketerfassung
- Konfigurieren von SPAN

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.