

Catalyst 9000スイッチのDHCPのトラブルシューティング

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[関連製品](#)

[トラブルシューティング](#)

[レイヤ2ブリッジとして設定されたスイッチ](#)

[ステップ1: パケットのパスを確認します。](#)

[ステップ2: レイヤ2のパスをチェックする](#)

[ステップ3: スイッチがクライアントポートでDHCP discoverパケットを受信していることを確認します。](#)

[ステップ4: スイッチがDHCPディスカバリを転送していることを確認します。](#)

[リレーエージェントとして設定されたスイッチ](#)

[ステップ1: スイッチがDHCPディスカバリを受信していることを確認します。](#)

[ステップ2: IPヘルパー設定をチェックします。](#)

[ステップ3: DHCPサーバへの接続をチェックします。](#)

[ステップ4: スイッチがDHCPパケットをネクストホップに転送していることを確認します。](#)

[DHCPサーバとして設定されたスイッチ](#)

[ステップ1: 基本設定を確認します。](#)

[ステップ2: スイッチがIPアドレスをリースしていることを確認します。](#)

[関連情報](#)

はじめに

このドキュメントでは、Catalyst 9000スイッチでのDHCPのトラブルシューティング方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Catalyst 9000シリーズスイッチのアーキテクチャ
- ダイナミックホストコンフィギュレーションプロトコル(DHCP)。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- C9200
- C9300
- C9500
- C9400
- C9600

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

関連製品

このドキュメントは、次のバージョンのハードウェアとソフトウェアにも使用できます。

- Cisco IOS® XE 16.xが稼働するCatalyst 3650/3850シリーズスイッチ

トラブルシューティング

DHCP問題のトラブルシューティングを行う際には、問題の原因を切り分けるために確認する必要がある重要な情報があります。送信元から宛先までネットワークのトポロジを描き、その間にあるデバイスとその役割を特定することが非常に重要です。

これらのロールに基づいて、トラブルシューティングを開始するために実行できるアクションがあります。

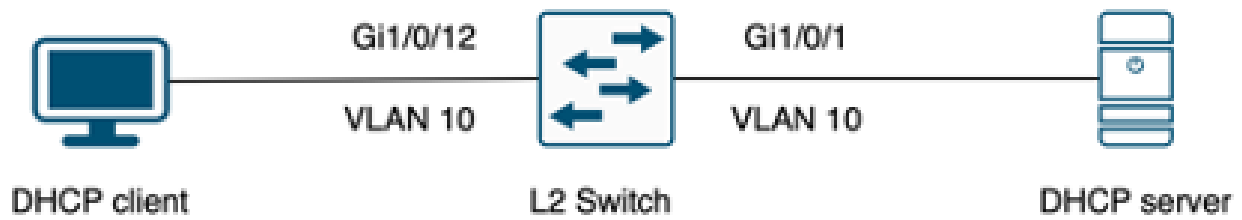
レイヤ2ブリッジとして設定されたスイッチ

このシナリオでは、スイッチはDHCPパケットを変更せずに受信して転送することが想定されています。

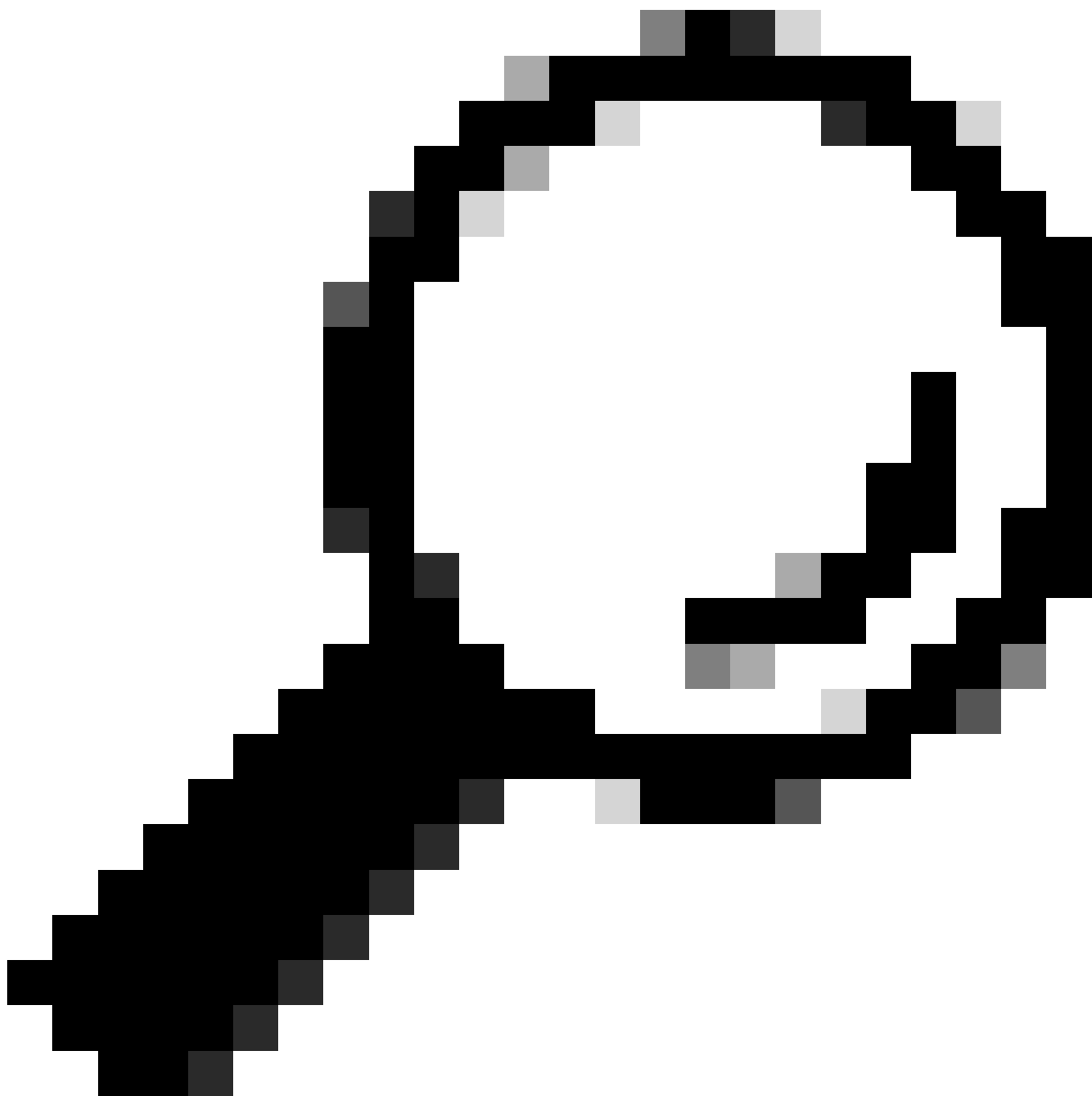
ステップ 1：パケットのパスを確認します。

- クライアントと、DHCPサーバへのネクストホップデバイスが接続されているインターフェイスを特定します。
- 影響を受ける1つまたは複数のVLANを特定します。

例：次のトポロジについて考えてみます。ここでは、C9300スイッチのVLAN 10のインターフェイスGigabitethernet1/0/12に接続されているクライアントが、DHCP経由でIPアドレスを取得できません。DHCPサーバは、VLAN 10のインターフェイスGigabitethernet1/0/1にも接続されています。



クライアントはレイヤ2スイッチに接続されている。



ヒント：問題が複数のデバイスとVLANに影響を与えている場合は、トラブルシューティングを実行するクライアントを1つ選択します。

ステップ 2 : レイヤ2のパスをチェックする

- VLANを作成し、スイッチ上でアクティブにする必要があります。

```
<#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	

- VLANは、入インターフェイスと出インターフェイスで許可されている必要があります。
 -

```
<#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
```

- スイッチは、正しいVLANでクライアントのMACアドレスを学習する必要があります。

```
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

- DHCPスヌーピングが設定されている場合は、信頼インターフェイスが正しく設定されていることを確認します。

ステップ 3 : スイッチがクライアントポートでDHCP discoverパケットを受信していることを確認します。

- Embedded Packet Capture(EPC)ツールを使用できます。
- DHCPパケットだけをフィルタリングするには、ACLを設定します。

```
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
```

- クライアントポートでインバウンド方向のパケットキャプチャを設定し、開始します。

```
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

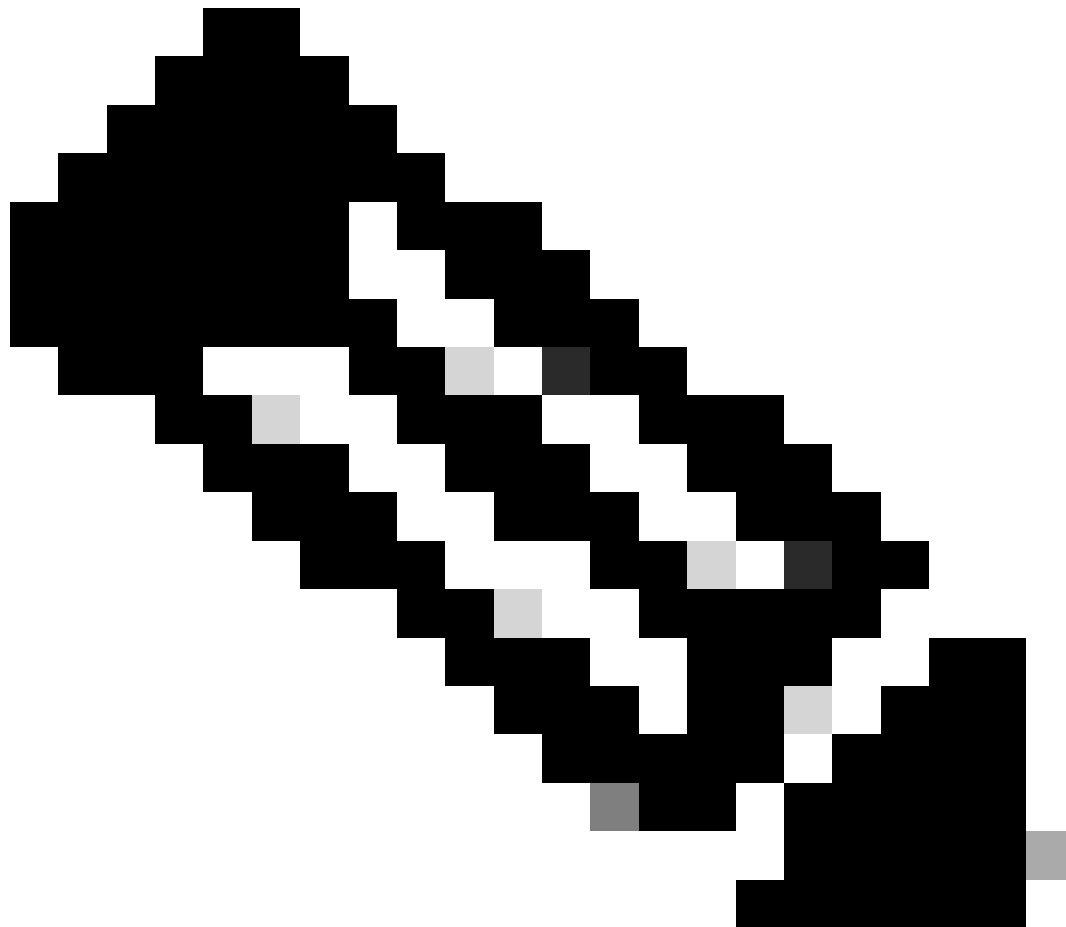
Stopped capture point : cap

- キャプチャの内容を確認します。

```
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
```



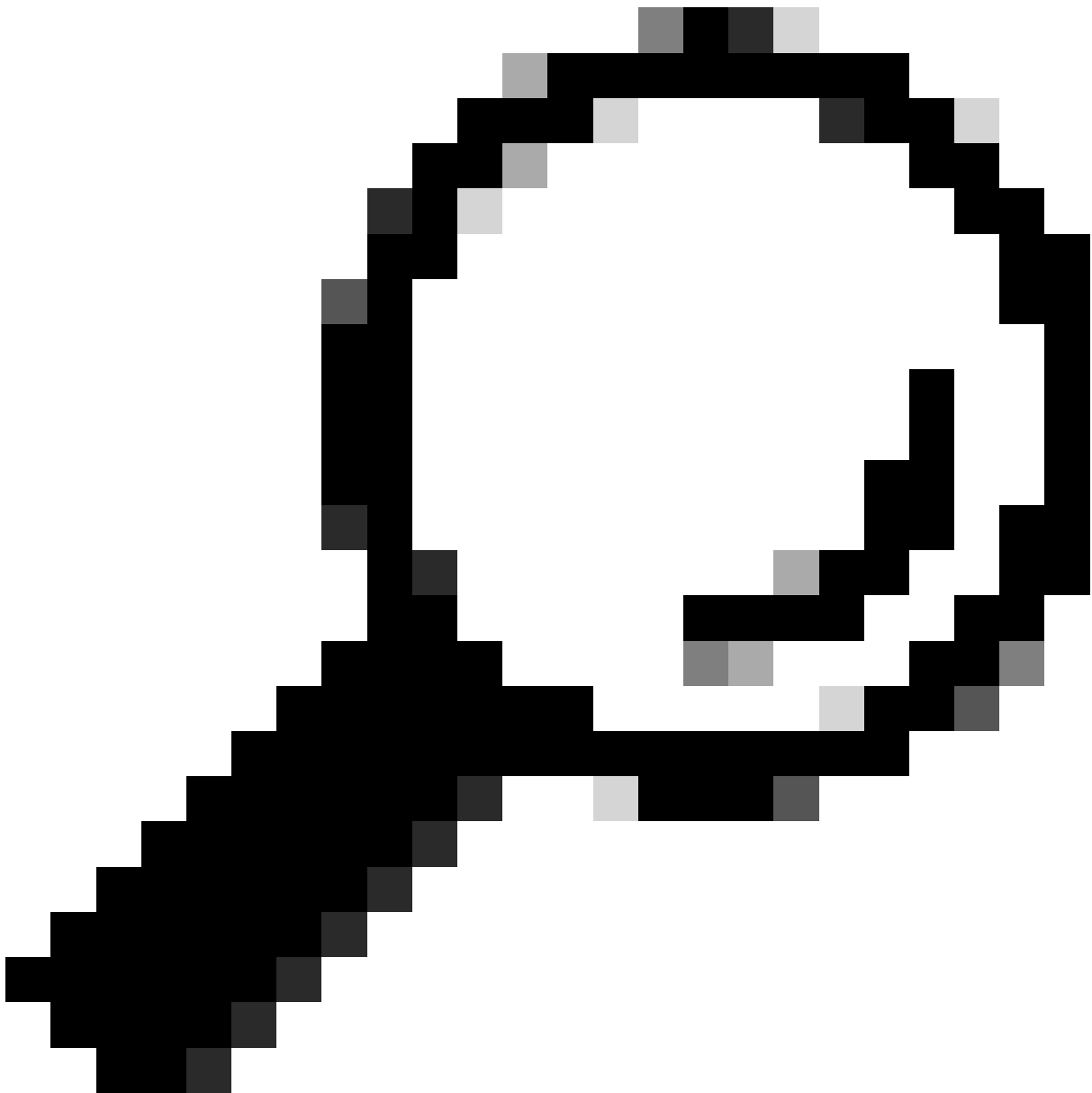
注：通常の状況で、クライアントポートで両方向のEPCを取ると、DORAプロセスが完了していることがわかります。

ステップ 4：スイッチがDHCPディスカバリを転送していることを確認します。

- アウトバウンド方向の出力ポートでキャプチャを取得できます。

```
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
```



ヒント：キャプチャで収集されたDHCP Discoverがトラブルシューティング対象のクライアントに属していることを確認するために、`display-filter`オプションを使用してフィルタ`dhcp.hw.mac_addr`をEPCに適用できます。

この時点で、スイッチがDHCPパケットを転送しており、トラブルシューティングをDHCPサーバに移せることを確認しました。

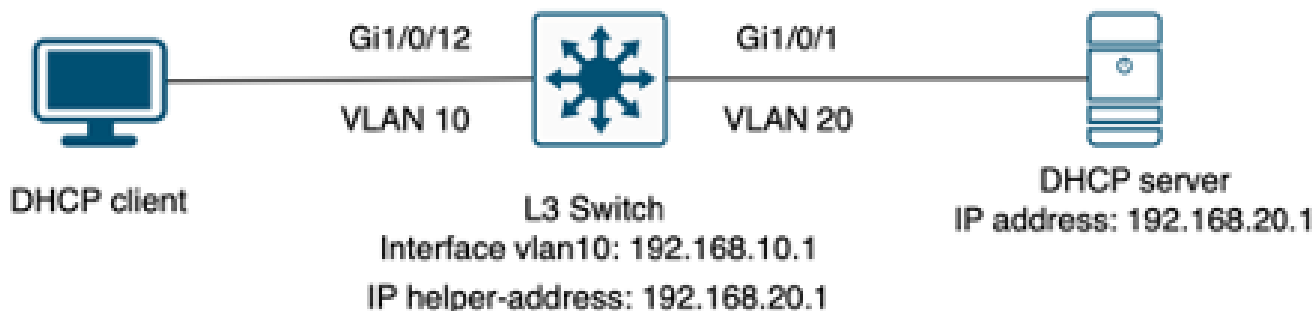
リレーエージェントとして設定されたスイッチ

リレーエージェントは、クライアントとDHCPサーバが同じブロードキャストドメインに属していない場合に使用されます。

スイッチがリレーエージェントとして設定されている場合は、スイッチ内でDHCPパケットが変更されます。クライアントから送信されたパケットの場合は、スイッチが自身の情報（IPアドレ

スおよびMACアドレス)をパケットに追加し、DHCPサーバに向けてネクストホップに送信します。DHCPサーバから受信したパケットはリレーエージェントをポイントし、スイッチはそれらのパケットをクライアントに転送します。

前のシナリオの例を引き続き使用します。クライアントは、DHCP経由でIPアドレスを取得できないVLAN 10のインターフェイスGigabitethernet1/0/12に接続されています。ここで、C9000スイッチはVLAN 10のデフォルトゲートウェイであり、リレーエージェントとして設定されています。DHCPサーバはVLAN 20のインターフェイスGigabitethernet1/0/1に接続されています。



リレーエージェントとして設定されたレイヤ3スイッチに接続されたクライアント。

ステップ 1 : スイッチがDHCPディスカバリを受信していることを確認します。

- クライアントに面するインターフェイスでパケットキャプチャを実行します。前のシナリオのステップ3を参照してください。

ステップ 2 : IPヘルパー設定をチェックします。

- DHCPサービスを有効にする必要があります。

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

- VLAN 10 SVIでIP helperコマンドを実行します。

```
<#root>
```

```
interface vlan10
ip address 192.168.10.1 255.255.255.0

ip helper-address 192.168.20.1
```

ステップ 3 : DHCPサーバへの接続をチェックします。

- スイッチには、クライアントVLANからDHCPサーバへのユニキャスト接続が必要です。pingを使用してテストできます。

```
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
```

ステップ 4 : スイッチがDHCPパケットをネクストホップに転送していることを確認します。

- debug ip dhcp server packet detailを実行できます。

<#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.
```

- パケットキャプチャを取得します。コントロールプレーンでEPCを使用できます。

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

- 出力ポートでSPANを使用することもできます。

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

注：パスにはリレーエージェントを1つだけ設定する必要があります。

DHCPサーバとして設定されたスイッチ

このシナリオでは、スイッチにDHCPスコープがローカルに設定されています。

ステップ 1：基本設定を確認します。

- プールを作成し、ネットワーク、サブネットマスク、デフォルトルータを設定する必要があります。

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

- DHCPサービスを有効にする必要があります。

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

- スイッチには、プールに設定されたネットワークへのユニキャスト接続が必要です。

```
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
```

- 静的に設定されたすべてのIPアドレスをプール範囲から除外する必要があります。

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

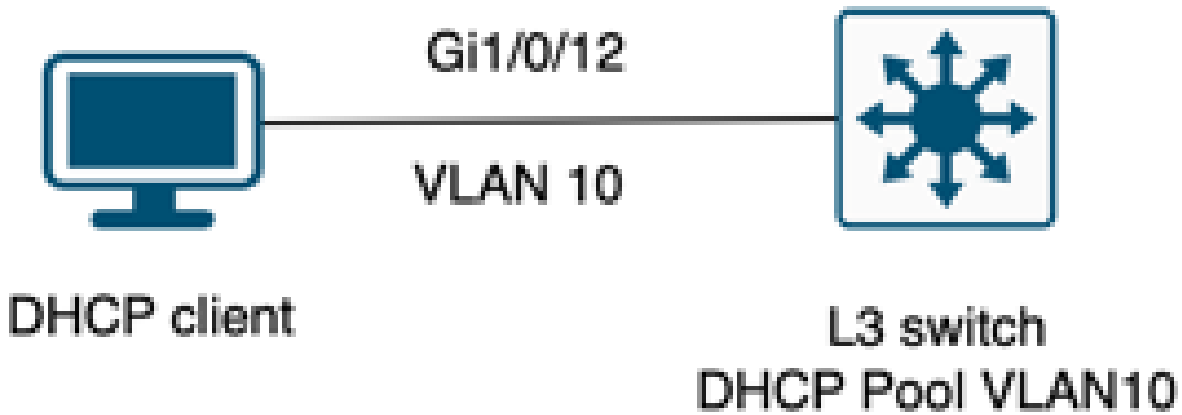


注：スイッチがDHCPサーバまたはリレーエージェントとして設定されている場合は、サービスDHCPを有効にする必要があります。

ステップ 2：スイッチがIPアドレスをリースしていることを確認します。

- `debug ip dhcp server packet detail`を使用できます。

例1：クライアントは、VLAN 10上のDHCPサーバとして設定されたCatalyst 9000スイッチに直接接続されています。



DHCPサーバとして設定されたレイヤ3スイッチに接続されたクライアント。

<#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 Interface 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

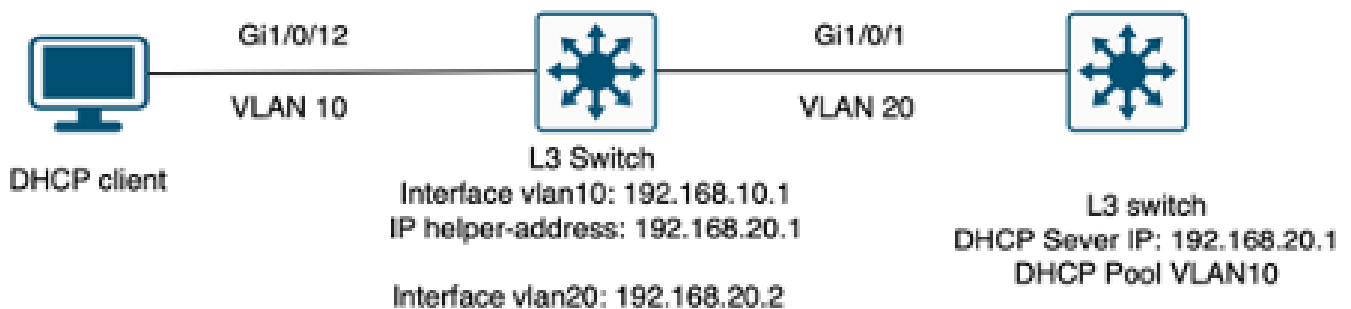
```

*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 Interface Vlan10
*Feb 16 19:03:33.829:
DHCPD: broadcasting BOOTREPLY to client 9c54.16b7.7d64

```

例2：クライアントが、DHCPサーバとして設定されているCatalyst 9000スイッチに直接接続されていない。

このシナリオでは、クライアントはデフォルトゲートウェイおよびリレーエージェントとして設定されたL3スイッチに接続され、DHCPサーバはVLAN 20上の隣接するCatalyst 9000スイッチでホストされています。



DHCPサーバとして動作しているレイヤ3スイッチに直接接続されていないクライアント。

<#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 Interface 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.



注：スイッチが同じVLANのDHCPサーバおよびリレーエージェントとして設定されている場合は、DHCPサーバが優先されます。

関連情報

- [DHCP の設定](#)
- [組み込みパケットキャプチャの設定](#)
- [SPANの設定](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。