

ローカルエンドポイントを使用したACIでのDHCPリレーのトラブルシューティング

内容

[はじめに](#)

[略語](#)

[要件](#)

[使用するコンポーネント](#)

[トラブルシューティングの推奨事項](#)

[エンドポイント学習](#)

[ポリシーの導入](#)

[ホスト到達可能性](#)

[エンドポイントの学習とルーティング](#)

[ポリシーの検証](#)

[DHCPパケットトレース](#)

[一般的な問題](#)

[問題1:L3outのサイレントドロップ](#)

[問題2: DHCPサーバがオプション82をサポートしていない](#)

[参考資料](#)

はじめに

このドキュメントでは、ACIファブリックのDHCPリレーのトラブルシューティングについて説明します。

略語

- BD : ブリッジドメイン
- EPG : エンドポイントグループ
- ExEPG : 外部エンドポイントグループ
- VRF:Virtual Routing and Forwarding(VRF)
- クラスIDまたはpcTag:EPGを識別するタグ
- DHCP:Dynamic Host Configuration Protocol (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)
- SVI:Switched Virtual Interface (相手先選択接続)

要件

この記事では、次の項目に関する一般的な知識を持っていることが推奨されます。

- DHCPの概念とワークフロー (DORAプロセス)

- ACIの概念：アクセスポリシー、エンドポイントラーニング、契約、およびL3out
- DHCPリレーポリシーがすでに作成されている必要があります

使用するコンポーネント

このトラブルシューティングの演習は、第2世代のNexusスイッチN9K-C93180YC-EXおよびN9K-C93240YC-FX2を使用するACIバージョン6.0(8f)で行われました。

この記事に記載されているすべてのコマンドは、ラボ環境で実行され、RFC1819を使用してIPアドレスリングが行われました。対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解し、特定のニーズに合わせて適切なコマンドを用意してください。

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。

トラブルシューティングの推奨事項

エンドポイント学習

エンドポイントが認識されない場合は、スイッチ、インターフェイス、VLAN設定などの静的ポートポリシーを検証します。仮想サーバの場合は、ポートグループが適切に導入され、VMに割り当てられていることを確認します。

ポリシーの導入

DHCPリレーポリシー(dhcpRelayP)とDHCPリレーラベル(dhcpLbl)が正しく設定され、適切なブリッジドメイン(BD)によって使用されていることを確認します。ラベルポリシーの所有権ルールは次のとおりです。

- ユーザテナントの所有権：そのテナントだけがポリシーを使用できます
- 共通テナントの所有権：すべてのテナントがポリシーを使用できますが、DHCPサーバは共通のEPGで学習する必要があります
- インフラストラクチャテナントの所有権：すべてのテナントがポリシーを使用でき、DHCPサーバはファブリック内のどこからでも学習できます

dhcpRelayP親ポリシーの下にdhcpRtLblDefToRelayP子クラスが存在しない場合、BDはリレーポリシーを消費しないため、修正措置が必要です。

ホスト到達可能性

DHCPクライアントは、そのBDのSVIから到達可能である必要があります。到達不能な場合は、契約とルーティング設定を確認して接続を確認します。

エンドポイントの学習とルーティング

クライアントが存在するブリッジドメインのSVIからDHCPサーバに到達できることを確認します。

```
<#root>
```

```
iping -V [ tenant : VRF ] -S [ SVI IP of the Client ] [ DHCP server IP]
```

```
<#root>
```

```
Leaf101#
```

```
iping -V tz:VRF1 -S 172.16.19.1 172.16.18.100
```

```
PING 172.16.18.100 (172.16.18.100) from 172.16.19.1: 56 data bytes
64 bytes from 172.16.18.100: icmp_seq=0 ttl=64 time=0.912 ms
64 bytes from 172.16.18.100: icmp_seq=1 ttl=64 time=0.706 ms
64 bytes from 172.16.18.100: icmp_seq=2 ttl=64 time=0.643 ms
64 bytes from 172.16.18.100: icmp_seq=3 ttl=64 time=0.689 ms
64 bytes from 172.16.18.100: icmp_seq=4 ttl=64 time=0.717 ms
```

```
--- 172.16.18.100 ping statistics ---
```

```
5 packets transmitted, 5 packets received, 0.00% packet loss
```

```
round-trip min/avg/max = 0.643/0.733/0.912 ms
```

EPGで設定する場合、DHCPクライアントとDHCPサーバの両方をエンドポイントとして学習する必要があります。これらのエンドポイントが正しく学習されているかどうかを確認するには、リーフのエンドポイントマネージャテーブルを確認します。

```
<#root>
```

```
show system internal epm endpoint [ip | mac] [ DHCP server IP | DHCP client MAC]
```

```
<#root>
```

```
Leaf101# show system internal epm endpoint ip 172.16.18.100
```

```
MAC : 0050.56b7.80cf ::: Num IPs : 1
```

```
IP# 0 : 172.16.18.100
```

```
::: IP# 0 flags : ::: l3-sw-hit: No
Vlan id : 12 ::: Vlan vnid : 8535 ::: VRF name : tz:VRF1
```

```

BD vnid : 15400880 ::: VRF vnid : 2981888
Phy If : 0x1a02c000 ::: Tunnel If : 0
Interface : Ethernet1/45
Flags : 0x80004c04 ::: sclass : 16402 ::: Ref count : 5
EP Create Timestamp : 09/11/2025 17:37:15.158380
EP Update Timestamp : 09/11/2025 19:17:41.261985
EP Flags : local|IP|MAC|sc|timer|

::::

...

Leaf101# show system internal epm endpoint mac 0050.56b7.33ee

MAC : 0050.56b7.33ee ::: Num IPs : 0

```

```

Vlan id : 25 ::: Vlan vnid : 8494 ::: VRF name : tz:VRF1
BD vnid : 15630228 ::: VRF vnid : 2981888
Phy If : 0x1a02c000 ::: Tunnel If : 0
Interface : Ethernet1/45
Flags : 0x80004804 ::: sclass : 32780 ::: Ref count : 4
EP Create Timestamp : 09/11/2025 17:33:36.158122
EP Update Timestamp : 09/11/2025 19:17:41.258478
EP Flags : local|MAC|sc|timer|

::::

```

ポリシーの検証

DHCPリレーポリシーを検証する際、次の重要な属性を確認できます。

- 名前：DHCPリレーポリシーの識別子。
- 所有者：ポリシーが設定されているテナント。その可視性の範囲は、そのテナントに限定されます。
- Address:DHCP要求がリレーされるDHCPサーバのIPアドレス。
- DHCPサーバのロケーション：epgDn、bdDefDn、ctxDefDnなどのタグを使用して検証され、EPG、ブリッジドメイン、およびVRFとの正しい関連付けが保証されます。
- ポリシーの状態：ポリシーは、ファブリック内で正しく展開され、アクティブであることを示す形式の状態である必要があります。

この検証は、APICでmoqueriesを実行して、DHCPリレーポリシーが正しく作成され、適切なテナントに関連付けられ、関連するブリッジドメインに適切にリンクされていることを確認することによって実行されます。この手順は、設定ミスを早期に特定し、ポリシー展開の欠落や誤りが原因で発生するDHCPリレー障害を防止するのに役立ちます。

<#root>

```
moquery -c dhcpRelayP -f 'dhcp.RelayP.dn*"[ tenant name ].*[ DHCP Relay Policy name ]"' -x rsp-subtree=c
```

<#root>

APIC#

moquery -c dhcpRelayP -f 'dhcp.RelayP.dn*"tz.*Relay"' -x rsp-subtree=children

Total Objects shown: 1

dhcp.RelayP

name : tz-DHCP_Relay

<-- cut for brevity-->

dn : uni/tn-tz/relayp-tz-DHCP_Relay

<-- cut for brevity-->

owner : tenant

<-- cut for brevity-->

rn : relayp-tz-DHCP_Relay

dhcp.ProvDhcp

epgDn : uni/tn-tz/ap-AP1/epg-EPG1

addr : 172.16.18.100

bdDefDn : uni/bd-[uni/tn-tz/BD-BD1]-isSvc-no

<-- cut for brevity-->

ctxDefDn : uni/ctx-[uni/tn-tz/ctx-VRF1]

ctxDefStQual : none

ctxSeg : 2981888

descr :

dn : uni/tn-tz/relayp-tz-DHCP_Relay/provdhcp-[uni/tn-tz/ap-AP1/epg-EPG1]

l3CtxEncap : vxlan-2981888

<-- cut for brevity-->

name : EPG1

<-- cut for brevity-->

pcTag : 16402

<-- cut for brevity-->

dhcp.RsProv

tDn : uni/tn-tz/ap-AP1/epg-EPG1

addr : 172.16.18.1

<-- cut for brevity-->

state : formed

DHCPリレーポリシーがクライアントのブリッジドメイン(BD)に関連付けられると、対応するDHCPラベルポリシーが自動的に作成されます。このDHCPラベルポリシーは、DHCPリレーポリシーとBD間のリンクとして機能し、リレー機能を有効にします。

APIC CLIを使用してDHCPラベルポリシーを確認するには、次のようなコマンドを使用します。

```
<#root>
```

```
moquery -c dhcpLbl -f 'dhcp.Lbl.dn*"[ tenant ].*[ DHCP Relay Policy name]"'
```

```
<#root>
```

```
APIC#
```

```
moquery -c dhcpLbl -f 'dhcp.Lbl.dn*"tz.*Relay"'
```

```
Total Objects shown: 1
```

```
# dhcp.Lbl
```

```
name : tz-DHCP_Relay
```

```
annotation :
```

```
childAction :
```

```
descr :
```

```
dn : uni/tn-tz/BD-BD2/dhcpLbl-tz-DHCP_Relay
```

```
extMngdBy :
```

```
lcOwn : local
```

```
modTs : 2025-09-11T16:30:03.016+00:00
```

```
monPolDn : uni/tn-common/monepg-default
```

```
nameAlias :
```

```
owner : tenant
```

```
ownerKey :
```

```
ownerTag :
```

```
rn : dhcpLbl-tz-DHCP_Relay
```

```
status : modified
```

```
tag : yellow-green
```

```
uid : 15374
```

```
userdom : :all:
```

これは、BDに関連付けられたDHCP Labelオブジェクトを示します。

DHCPリレーポリシーが正しく設定されている場合、DHCPラベルが使用される子オブジェクトが存在することになります。これは次のコマンドで確認できます。

```
<#root>
```

```
APIC#
```

```
moquery -c dhcpRelayP -f 'dhcp.RelayP.dn*"tz.*Relay"' -x rsp-subtree=children rsp-subtree-class=dhcpRtLb
```

Total Objects shown: 1

```
# dhcp.RelayP
```

```
name : tz-DHCP_Relay
```

```
annotation :
childAction :
descr :
dn : uni/tn-tz/relayp-tz-DHCP_Relay
extMngdBy :
lcOwn : local
modTs : 2025-09-11T16:10:56.421+00:00
mode : visible
monPolDn : uni/tn-common/monepg-default
nameAlias :
```

```
owner : tenant
```

```
ownerKey :
ownerTag :
rn : relayp-tz-DHCP_Relay
status : modified
uid : 15374
userdom : :all:
```

```
# dhcp.RtLb1DefToRelayP
tDn : uni/bd-[uni/tn-tz/
```

```
BD-BD2
```

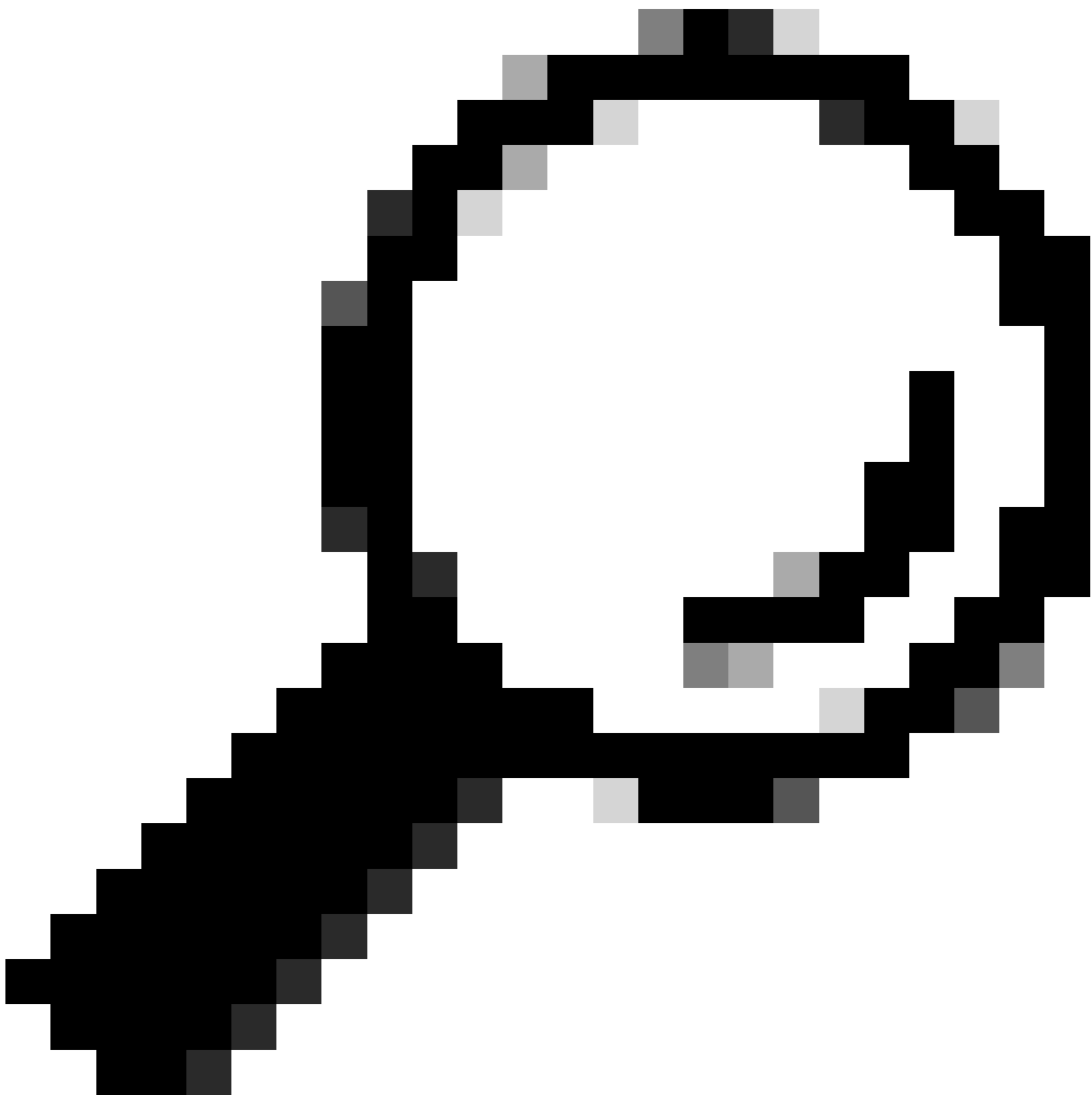
```
] -isSvc-no/dhcp1b1def-tz-DHCP_Relay
childAction : deleteNonPresent
dn : uni/tn-tz/relayp-tz-DHCP_Relay/rtl1b1DefToRelayP-[uni/bd-[uni/tn-tz/BD-BD2]-isSvc-no/dhcp1b1def-tz-
lcOwn : local
modTs : 2025-09-11T16:30:03.106+00:00
rn : rtl1b1DefToRelayP-[uni/bd-[uni/tn-tz/BD-BD2]-isSvc-no/dhcp1b1def-tz-DHCP_Relay]
status :
tCl : dhcpLb1Def
```

DHCPパケットトレース

ACIは、CPUに送信されるすべてのDHCPパケットをトレースファイルに記録します。このファイルを分析して、DHCP Discover, Offer, Request, and Acknowledge(DORA)プロセスのトラブルシューティングを行うことができます。DHCPパケットトレースを表示するには、次のコマンドを使用します。

```
<#root>
```

```
show dhcp internal event-history traces
```



ヒント:1つのDHCPパッケージが100を超えるトレースエントリを生成します。効率的な分析のために、正規表現を使用して関連する出力をフィルタリングすることを強くお勧めします。

Cisco ACIのDHCPトレース分析中に、DHCPリレーが適切に動作していることを確認するために、次の重要な属性を確認できます。

- 回線IDサブオプションの追加：

DHCPオプション82がパッケージに追加されていることを示します。これは、リレーエージェント情報に不可欠です。

- GI アドレス:

DHCPリレーポリシーで設定されているDHCPサーバのIPアドレスを表します。

- ヘルパーアドレス :

リレーがDHCPサーバに到達するために使用するSVI IPアドレス。

- クライアントとサーバが同じVRFにある場合 :

DHCPクライアントとサーバが同じVRFコンテキストに属していることを確認します。

- msg:

確認されたDHCPメッセージのタイプ (Discover、Offer、Request、Ackなど) 。

- ctx名 :

DHCPラベルポリシーが設定されているVRF名。

- SMAC:

DHCPクライアントのMACアドレス。

- UDP送信元/宛先ポート :

使用されるDHCPポート。通常は、クライアント用に68、サーバ用に67。

<#root>

Leaf101# s

```
how dhcp internal event-history traces | grep -A34 -B70 "00 50 56 b7 33 ee" | egrep "(Rec.*pkt.*intf|ip
```

```
2) 2025 Sep 11 04:14:46.660433 _relay_handle_packet_from_pkt_mgr: 480 : Relaying the DHCP pkt on intf: V
28) 2025 Sep 11 04:14:46.659985 _relay_add_circuitid_rmtid_msiteinfo: 3354 :
```

Add circuit id suboption

```
: if_index: Ethernet1/45 (1a02c000) , svlan: 24, option def id: 0 epg_vnid 8529.
```

```
..
31) 2025 Sep 11 04:14:46.659934 _relay_add_option82: 3151 : Mac addr is 28:6f:7f:eb:54:9f
32) 2025 Sep 11 04:14:46.659930 _relay_add_option82: 3147 : Adding option82 suboptions
35) 2025 Sep 11 04:14:46.659924 _relay_send_packet: 1975 :
```

gi address is 172.16.18.1

..

```
37) 2025 Sep 11 04:14:46.659921 _relay_send_packet: 1965 :
```

Helper address is 172.16.18.100

```
38) 2025 Sep 11 04:14:46.659918 _relay_send_packet: 1956 :
```

Client and Server are in the same VRF

```
39) 2025 Sep 11 04:14:46.659793 _relay_send_packet: 1898 : ifindex is Vlan24
```

```
40) 2025 Sep 11 04:14:46.659786 _relay_send_packet: 1833 : dhcp_relay_send_packet: relayback_ifindex is
```

```

..
42) 2025 Sep 11 04:14:46.659730 _relay_handle_packet_from_pkt_mgr: 447 :
DHCPDISCOVER msg

43) 2025 Sep 11 04:14:46.659728 _relay_handle_packet_from_pkt_mgr: 438 : ifindex is Vlan24
..
61) 2025 Sep 11 04:14:46.657274 _snoop_handle_istack_packet: 1763 :
ctx name is tz:VRF1

64) 2025 Sep 11 04:14:46.657062 _snoop_handle_istack_packet: 1751 :
Smac = [00 50 56 b7 33 ee ]

65) 2025 Sep 11 04:14:46.657057 _snoop_handle_istack_packet: 1749 : Dmac = [ff ff ff ff ff ff ];
68) 2025 Sep 11 04:14:46.657050 _snoop_handle_istack_packet: 1737 : Logical interface: Vlan24
72) 2025 Sep 11 04:14:46.657044 _snoop_handle_istack_packet: 1721 : Physical interface: Ethernet1/45
..
86) 2025 Sep 11 04:14:46.657024 _snoop_handle_istack_packet: 1669 :
UDP src port 68 UDP dst port 67

88) 2025 Sep 11 04:14:46.657021 _snoop_handle_istack_packet: 1577 : destination ip address 255.255.255.
89) 2025 Sep 11 04:14:46.657018 _snoop_handle_istack_packet: 1574 : source ip address 0.0.0.0
95) 2025 Sep 11 04:14:46.656991 _snoop_handle_istack_packet: 1533 : Received pkt on Vlan 25 intf Ether

```

一般的な問題

問題1:L3outのサイレントドロップ

- 問題

L3OutがvPCインターフェイスを使用して隣接ルータとのネイバー関係を形成する場合、各スイッチは独自のvTEPを使用してパケットを送信します。vPCピアは、自身のアドレスではないvTEPアドレスを持つDHCPオファラーを受信すると、パケットをファブリック経由で転送します。これにより、発信元vTEPは障害ログなしでパケットをサイレントにドロップします。

このようなドロップを確認するには、次のコマンドを使用します。

```
<#root>
```

```
show
```

```
dhcp
```

```
internal event-history traces |
```

```
egrep
```

```
"(
```

```
failed|Drop
```

```
). *packet" | head
```

```
<#root>
```

```
Leaf101#
```

```
show dhcp internal event-history traces | egrep "(failed|Drop).*packet" | head
```

```
53) 2025 Sep 10 04:14:26.685020 _snoop_handle_istack_packet: 1881 : Drop DHCP DISCOVER/REQUEST packet b
172) 2025 Sep 10 04:14:23.792669 _snoop_handle_istack_packet: 1881 : Drop DHCP DISCOVER/REQUEST packet l
239) 2025 Sep 10 04:14:22.516679 _snoop_handle_istack_packet: 1881 : Drop DHCP DISCOVER/REQUEST packet l
444) 2025 Sep 10 04:14:17.055216 _snoop_handle_istack_packet: 1881 : Drop DHCP DISCOVER/REQUEST packet l
563) 2025 Sep 10 04:14:14.450437 _snoop_handle_istack_packet: 1881 : Drop DHCP DISCOVER/REQUEST packet l
736) 2025 Sep 10 04:14:09.056993 _snoop_handle_istack_packet: 1881 : Drop DHCP DISCOVER/REQUEST packet l
803) 2025 Sep 10 04:14:07.344467 _snoop_handle_istack_packet: 1881 : Drop DHCP DISCOVER/REQUEST packet l
906) 2025 Sep 10 04:14:06.290135 _snoop_handle_istack_packet: 1881 : Drop DHCP DISCOVER/REQUEST packet l
1025) 2025 Sep 10 04:14:03.770388 _snoop_handle_istack_packet: 1881 : Drop DHCP DISCOVER/REQUEST packet l
1094) 2025 Sep 10 04:14:03.234017 _snoop_handle_istack_packet: 1881 : Drop DHCP DISCOVER/REQUEST packet l
```

- 解決方法

Tenants > [tenant name] > Networking > L3outs > [L3out name] > Logical Node Profile > [LNP name] > Logical Interface Profile [LIP name] > SVI > [SVI policy]に移動します。

セカンダリIPアドレスが表示されたら、セカンダリIPアドレスを作成または開き、enable for DHCP Relayチェックボックスをオンにします。

Create Secondary IP address

Address: 192.168.1.1/24

Enable for DHCP Relay: ☒

Use the Secondary IP Address as DHCP Relay Gateway Address

Cancel Submit

これにより、ローカルvTEPの代わりにvPC vTEPアドレスを使用してメッセージが強制的に送信され、予期したとおりにパケットが転送されるようになります。

問題2: DHCPサーバがオプション82をサポートしていない

ACIなどのVXLAN環境では、vTEPアドレスに基づいてソースリーフと宛先の間の回線を作成するため、オプション82が重要です。内容は以下を含みます。

- 回線ID：着信インターフェイス、VLAN、およびDHCPディスカバリが検出されるEPG VNID。
- リモートID：ディスカバリを受信したスイッチのTEPアドレス。

オプション82が欠落している場合、DHCPリレーパケットはドロップされます。DHCPトレースログでOption 82の欠落を示すエラーをチェックすることにより、DHCPサーバに接続されているリーフ上のOption 82の存在を検証します。

このコマンドは、DHCPサーバが接続されているリーフスイッチが、有効なDHCPオプション82を持つオフアを受信することを確認します

```
<#root>
```

```
Leaf101#
```

```
show
```

```
dhcp
```

```
internal event-history traces |
```

```
egrep
```

```
"(
```

```
failed|Drop
```

```
). *packet" | head
```

```
67) 2025 Sep 10 05:16:52.336785 _relay_handle_packet: 1478 : dhcp_relay_handle_packet: DHCP UDP failed
68) 2025 Sep 10 05:16:52.336772 _relayback_response: 929 : dhcp_relayback_response : option 82 not pres
479) 2025 Sep 10 05:11:07.308085 _relay_handle_packet: 1478 : dhcp_relay_handle_packet: DHCP UDP failed
480) 2025 Sep 10 05:11:07.308073 _relayback_response: 929 : dhcp_relayback_response : option 82 not pre
891) 2025 Sep 10 05:10:22.312386 _relay_handle_packet: 1478 : dhcp_relay_handle_packet: DHCP UDP failed
892) 2025 Sep 10 05:10:22.312374 _relayback_response: 929 : dhcp_relayback_response : option 82 not pre
1303) 2025 Sep 10 05:09:37.309888 _relay_handle_packet: 1478 : dhcp_relay_handle_packet: DHCP UDP failed
1304) 2025 Sep 10 05:09:37.309874 _relayback_response: 929 : dhcp_relayback_response : option 82 not pr
1715) 2025 Sep 10 05:08:52.295721 _relay_handle_packet: 1478 : dhcp_relay_handle_packet: DHCP UDP failed
1716) 2025 Sep 10 05:08:52.295709 _relayback_response: 929 : dhcp_relayback_response : option 82 not pr
```

参考資料

[ACIファブリックにおけるDHCPリレーの高度なトラブルシューティング：TACDCN-2017](#)

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。