

Risoluzione dei problemi di inoltro DHCP in ACI con endpoint locali

Sommario

[Introduzione](#)

[Abbreviazioni](#)

[Requisiti](#)

[Componenti usati](#)

[Suggerimenti per la risoluzione dei problemi](#)

[Endpoint Learning](#)

[Distribuzione criteri](#)

[Raggiungibilità dell'host](#)

[Instradamento e apprendimento degli endpoint](#)

[Convalida criteri](#)

[Traccia pacchetto DHCP](#)

[Problemi comuni](#)

[Numero 1: L3out silent drop](#)

[Numero 2: Il server DHCP non supporta l'opzione 82](#)

[Riferimenti](#)

Introduzione

In questo documento viene descritto come risolvere i problemi di inoltro DHCP in ACI Fabric.

Abbreviazioni

- BD: Dominio bridge
- EPG: Gruppo endpoint
- ExEPG: Gruppo endpoint esterno
- VRF: Routing e inoltro virtuale
- ID classe o pcTag: Tag che identifica un EPG
- DHCP: Protocollo Dynamic Host Configuration
- SVI Switched Virtual Interface

Requisiti

Per questo articolo è consigliabile avere una conoscenza generale dei seguenti argomenti:

- Concetti e flusso di lavoro DHCP (processo DORA)
- Concetti ACI: Criteri di accesso, apprendimento degli endpoint, contratti e L3out
- I criteri di inoltro DHCP devono essere già stati creati

Componenti usati

Questo esercizio di risoluzione dei problemi è stato eseguito su ACI versione 6.0(8f) con switch Nexus di seconda generazione N9K-C93180YC-EX e N9K-C93240YC-FX2.

Tutti i comandi di questo articolo sono stati eseguiti in un ambiente lab utilizzando la RFC1819 per l'indirizzamento IP. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi e verificare che i comandi corrispondano alle proprie esigenze specifiche.

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.

Suggerimenti per la risoluzione dei problemi

Endpoint Learning

Se non si imparano gli endpoint, convalidare le policy delle porte statiche, ad esempio le configurazioni di switch, interfaccia e VLAN. Per i server virtuali, verificare che il gruppo di porte sia correttamente distribuito e assegnato alla macchina virtuale.

Distribuzione criteri

Verificare che i criteri di inoltro DHCP (dhcpRelayP) e le etichette di inoltro DHCP (dhcpLbl) siano configurati correttamente e utilizzati dal dominio bridge appropriato. Le regole di proprietà per i criteri di etichetta sono:

- Proprietà tenant utente: Solo il tenant può utilizzare i criteri
- Proprietà tenant comune: Tutti i tenant possono utilizzare il criterio, ma il server DHCP deve essere appreso da un EPG comune
- Proprietà tenant infrarossi: Tutti i tenant possono utilizzare il criterio e il server DHCP può essere appreso in qualsiasi punto dell'infrastruttura

Se la classe figlio dhcpRtLblDefToRelayP non è presente nel criterio padre dhcpRelayP, nessun BD sta utilizzando il criterio di inoltro ed è necessaria un'azione correttiva.

Raggiungibilità dell'host

Il client DHCP deve essere raggiungibile dalla SVI del proprio BD. Se non raggiungibile, verificare i contratti e le configurazioni di routing per garantire la connettività.

Instradamento e apprendimento degli endpoint

Verificare che il server DHCP sia raggiungibile dalla SVI del dominio bridge in cui risiede il client.

<#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
```

I client DHCP e i server DHCP devono essere entrambi identificati come endpoint se configurati con EPG. Per verificare che questi endpoint siano stati appresi correttamente, è possibile controllare la tabella di gestione degli endpoint nella foglia.

<#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|sclass|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|
```

::::

Convalida criteri

Durante la convalida di un criterio di inoltro DHCP, è possibile confermare i seguenti attributi chiave:

- Nome: Identificatore del criterio di inoltro DHCP.
- Proprietario: Il tenant in cui è configurato il criterio, indicando il suo ambito di visibilità limitato a tale tenant.
- Indirizzo: Indirizzo IP del server DHCP a cui vengono inoltrate le richieste DHCP.
- Percorso server DHCP: Convalidato tramite tag quali epdDn, bdDefDn e ctxDefDn per garantire la corretta associazione con EPG, dominio bridge e VRF.
- Stato della politica: Il criterio deve essere in uno stato di formato che ne indica la corretta distribuzione e l'attivazione nell'infrastruttura.

Questa convalida viene eseguita eseguendo query sul server APIC per verificare che i criteri di inoltro DHCP siano stati creati correttamente, associati ai tenant appropriati e collegati correttamente ai domini bridge appropriati. Questo passaggio consente di identificare in anticipo eventuali configurazioni errate, impedendo errori di inoltro DHCP causati da una distribuzione dei criteri mancante o errata.

<#root>

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

<#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

Dopo aver associato un criterio di inoltro DHCP al dominio con bridging (BD) del client, viene creato automaticamente un criterio di etichetta DHCP corrispondente. Questo criterio di etichetta DHCP funge da collegamento tra il criterio di inoltro DHCP e BD, attivando la funzionalità di inoltro.

È possibile verificare il criterio Etichetta DHCP utilizzando APIC CLI con un comando quale:

```
<#root>
```

```
moquery -c dhcpLb1 -f 'dhcp.Lb1.dn*"[ tenant ].*[ DHCP Relay Policy name]"'
```

```
<#root>
```

```
APIC#
```

```
moquery -c dhcpLb1 -f 'dhcp.Lb1.dn*"tz.*Relay"'
```

```
Total Objects shown: 1
```

```
# dhcp.Lb1
```

```
name : tz-DHCP_Relay
```

```
annotation :
```

```
childAction :
```

```
descr :
```

```
dn : uni/tn-tz/BD-BD2/dhcp1b1-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 : dhcp1b1-tz-DHCP_Relay
```

```
status : modified
```

```
tag : yellow-green
```

```
uid : 15374
```

```
userdom : :all:
```

Visualizza l'oggetto Etichetta DHCP associato a BD.

Se il criterio di inoltro DHCP è configurato correttamente, avrà un oggetto figlio in cui viene utilizzata l'etichetta DHCP, che può essere verificato con:

```
<#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/rt1b1DefToRelayP-[uni/bd-[uni/tn-tz/BD-BD2]-isSvc-no/dhcp1b1def-tz-
```

```
lcOwn : local
```

```
modTs : 2025-09-11T16:30:03.106+00:00
```

```
rn : rt1b1DefToRelayP-[uni/bd-[uni/tn-tz/BD-BD2]-isSvc-no/dhcp1b1def-tz-DHCP_Relay]
```

```
status :
```

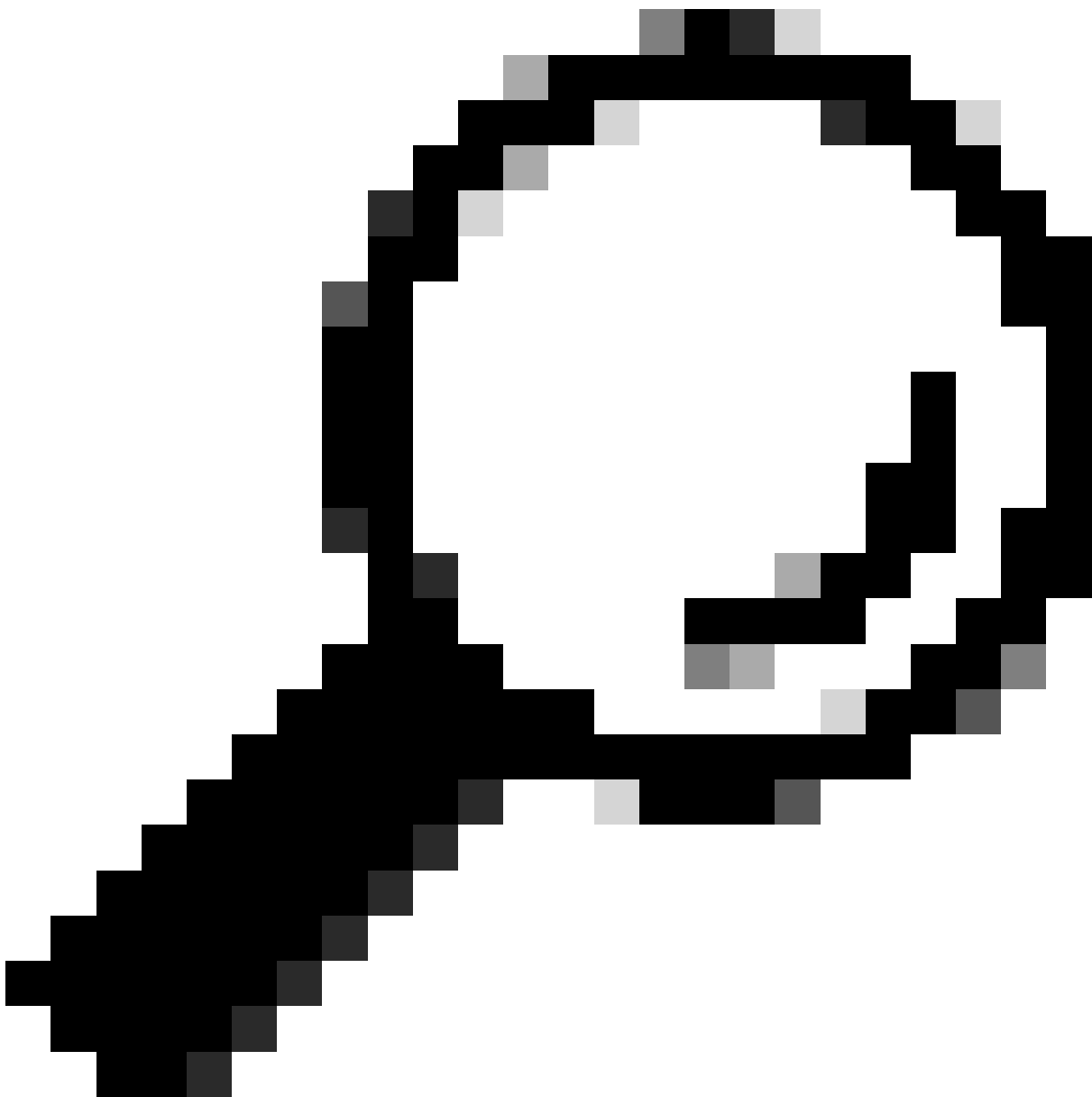
```
tCl : dhcpLb1Def
```

Traccia pacchetto DHCP

ACI registra tutti i pacchetti DHCP inviati alla CPU nei file di traccia, che possono essere analizzati per risolvere i problemi relativi al processo DHCP Discover, Offer, Request, and Acknowledge (DORA). Utilizzare questo comando per visualizzare le tracce dei pacchetti DHCP:

```
<#root>
```

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



Suggerimento: Un singolo pacchetto DHCP genera oltre 100 voci di traccia. Si consiglia di utilizzare GREP con espressioni regolari per filtrare l'output rilevante ai fini di un'analisi efficiente.

Durante l'analisi della traccia DHCP in Cisco ACI, è possibile confermare diversi attributi chiave per garantire il corretto funzionamento dell'inoltro DHCP:

- Aggiungi opzione secondaria ID circuito:

Indica che l'opzione DHCP 82 viene aggiunta al pacchetto, che è essenziale per le informazioni dell'agente di inoltro.

- indirizzo gi:

Rappresenta l'indirizzo IP del server DHCP configurato nei criteri di inoltro DHCP.

- Indirizzo helper:

L'indirizzo IP SVI utilizzato dal relay per raggiungere il server DHCP.

- Client e server si trovano nello stesso VRF:

Conferma che il client DHCP e il server appartengono allo stesso contesto VRF.

- messaggio:

Tipo di messaggio DHCP osservato, ad esempio Discover, Offre, Request o Ack.

- nome ctx:

Nome VRF in cui è configurato il criterio Etichetta DHCP.

- Smac:

Indirizzo MAC del client DHCP.

- Porta src/dst UDP:

Porte DHCP utilizzate, in genere 68 per i client e 67 per i server.

<#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

```

Problemi comuni

Numero 1: L3out silent drop

- Problema

Quando un'uscita L3G utilizza un'interfaccia vPC per formare una relazione di tipo adiacente con un router adiacente, ciascuno switch invia i pacchetti utilizzando il proprio vTEP. Se il peer vPC riceve un'offerta DHCP con un indirizzo vTEP diverso dal proprio, inoltra il pacchetto tramite l'infrastruttura, causando la cancellazione invisibile all'utente del vTEP mittente senza errori nei log.

Per verificare la presenza di tali rilasci, utilizzare questo comando:

```
<#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
```

- Soluzione

Passare a Tenant > [nome tenant] > Rete > L3outs > [Nome L3out] > Profilo nodo logico > [Nome LNP] > Profilo interfaccia logica [Nome LIP] > SVI > [Criteri SVI]

Al termine, creare o aprire la casella di controllo Indirizzo IP secondario e abilitare Abilita inoltre DHCP.

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

In questo modo i messaggi verranno inviati utilizzando l'indirizzo vTEP vPC anziché il vTEP locale e i pacchetti verranno inoltrati come previsto.

Numero 2: Il server DHCP non supporta l'opzione 82

L'opzione 82 è fondamentale in ambienti VXLAN come ACI, in quanto crea un circuito tra la foglia di origine e la destinazione basato sugli indirizzi vTEP. Esso comprende:

- ID circuito: Interfaccia in ingresso, VLAN ed EPG VNID dove viene rilevato il rilevamento DHCP.
- ID remoto: Indirizzo TEP dello switch che ha ricevuto il rilevamento.

Se l'opzione 82 non è disponibile, i pacchetti di inoltro DHCP vengono scartati. Convalidare la presenza dell'opzione 82 sulla foglia connessa al server DHCP verificando nei registri di traccia DHCP la presenza di errori che indicano la mancanza dell'opzione 82.

Questo comando convalida lo switch foglia a cui è connesso il server DHCP e riceve le offerte con un'opzione DHCP 82 valida

```
<#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
```

Riferimenti

[Risoluzione profonda dei problemi relativi all'inoltro DHCP in ACI Fabric - TACDCN-2017](#)

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).