Dépannage du relais DHCP dans l'ACI avec les terminaux locaux

Table des matières

Introduction

Abréviations

- Exigences
- Composants utilisés

Recommandations de dépannage

- Apprentissage des terminaux
- Déploiement de politiques
- Accessibilité des hôtes

Apprentissage et routage des terminaux

Validation des stratégies

Suivi des paquets DHCP

Problèmes courants

- Problème 1: Perte silencieuse L3out
- Problème 2: Le serveur DHCP ne prend pas en charge l'option 82

Références

Introduction

Ce document décrit le dépannage du relais DHCP dans les fabrics ACI.

Abréviations

- BD : Domaine Bridge
- EPG : Groupe de terminaux
- ExEPG : Groupe de terminaux externes
- VRF : Routage et transfert virtuels
- ID de classe ou pcTag : Balise qui identifie un EPG
- DHCP : Protocole de configuration d'hôte dynamique
- SVI : Interface virtuelle commutée

Exigences

Pour cet article, nous vous recommandons de disposer de connaissances générales sur les sujets suivants :

- Concepts et workflow DHCP (processus DORA)
- Concepts ACI : Politiques d'accès, apprentissage des terminaux, contrats et L3out

- Les stratégies de relais DHCP doivent être déjà créées

Composants utilisés

Cet exercice de dépannage a été effectué sur la version 6.0(8f) de l'ACI à l'aide des commutateurs Nexus de deuxième génération N9K-C93180YC-EX et N9K-C93240YC-FX2.

Toutes les commandes de cet article ont été exécutées dans un environnement de travaux pratiques et à l'aide de la RFC1819 pour l'adressage IP. Si votre réseau est actif, assurez-vous de comprendre l'impact potentiel de toute commande en vous assurant que vous adaptez la commande en question à vos besoins spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Recommandations de dépannage

Apprentissage des terminaux

Si les points d'extrémité ne sont pas appris, validez les stratégies de port statiques telles que les configurations de commutateur, d'interface et de VLAN. Pour les serveurs virtuels, vérifiez que le groupe de ports est correctement déployé et attribué à la machine virtuelle.

Déploiement de politiques

Assurez-vous que la politique de relais DHCP (dhcpRelayP) et l'étiquette de relais DHCP (dhcpLbl) sont correctement configurées et utilisées par le domaine de pont (BD) approprié. Les règles de propriété des politiques d'étiquette sont :

- Propriété du locataire utilisateur : Seul ce locataire peut utiliser la stratégie
- Propriété commune du locataire : Tous les locataires peuvent utiliser la stratégie, mais le serveur DHCP doit être appris sur un EPG commun
- Propriété du locataire infra : Tous les locataires peuvent utiliser la stratégie et le serveur DHCP peut être appris n'importe où dans le fabric

Si la classe enfant dhcpRtLblDefToRelayP est manquante dans la stratégie parent dhcpRelayP, aucun BD n'utilise la stratégie de relais et une action corrective est requise.

Accessibilité des hôtes

Le client DHCP doit être accessible à partir de l'interface SVI de son BD. En cas d'inaccessibilité, vérifiez les contrats et les configurations de routage pour assurer la connectivité.

Apprentissage et routage des terminaux

Assurez-vous que le serveur DHCP est accessible à partir de l'interface SVI du domaine de pont où réside le 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

Les clients DHCP et les serveurs DHCP doivent être appris en tant que points d'extrémité lorsqu'ils sont configurés sous un EPG. Pour vérifier que ces points d'extrémité sont correctement appris, vous pouvez vérifier la table du gestionnaire de points d'extrémité sur le leaf.

<#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|sclass|timer|

::::
```

Validation des stratégies

Lors de la validation d'une stratégie de relais DHCP, ces attributs clés peuvent être confirmés :

- Name : Identificateur de la politique de relais DHCP.
- Propriétaire : Service partagé sous lequel la stratégie est configurée, indiquant sa portée de visibilité limitée à ce service partagé.
- Adresse : Adresse IP du serveur DHCP vers lequel les requêtes DHCP sont relayées.
- Emplacement du serveur DHCP : Validée via des balises telles que epgDn, bdDefDn et ctxDefDn pour garantir une association correcte avec l'EPG, le domaine de pont et le VRF.
- État de la politique : La stratégie doit être dans un état formé, indiquant qu'elle est correctement déployée et active dans le fabric.

Cette validation est effectuée en exécutant des moqueries sur le contrôleur APIC pour confirmer que les stratégies de relais DHCP sont correctement créées, associées aux locataires appropriés et correctement liées aux domaines de pont appropriés. Cette étape permet d'identifier rapidement les erreurs de configuration, évitant ainsi les échecs de relais DHCP causés par un déploiement de stratégie manquant ou incorrect.

<#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

Une fois qu'une politique de relais DHCP est associée au domaine de pont (BD) du client, une politique d'étiquette DHCP correspondante est automatiquement créée. Cette politique d'étiquette DHCP agit comme une liaison entre la politique de relais DHCP et le BD, activant la fonctionnalité de relais.

Vous pouvez vérifier la politique d'étiquette DHCP à l'aide de la CLI APIC avec une commande telle que :

<#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:

Affiche l'objet Étiquette DHCP associé à la BD.

Si la stratégie de relais DHCP est correctement configurée, elle aura un objet enfant où l'étiquette DHCP est utilisée, qui peut être vérifié avec :

<#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.RtLblDefToRelayP
tDn : uni/bd-[uni/tn-tz/
BD-BD2

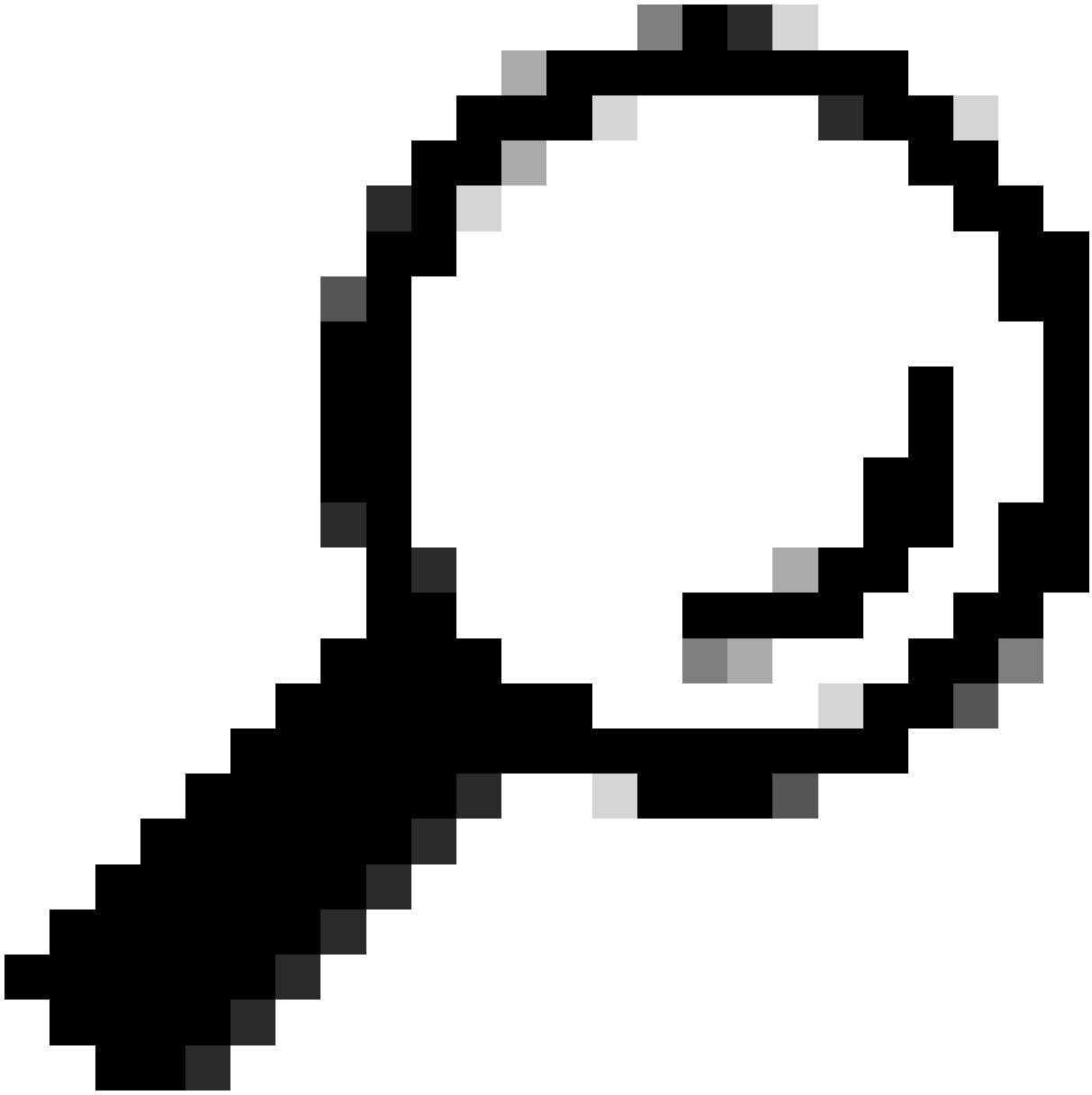
]-isSvc-no/dhcplbldef-tz-DHCP_Relay
childAction : deleteNonPresent
dn : uni/tn-tz/relayp-tz-DHCP_Relay/rtlblDefToRelayP-[uni/bd-[uni/tn-tz/BD-BD2]-isSvc-no/dhcplbldef-tz-
lcOwn : local
modTs : 2025-09-11T16:30:03.106+00:00
rn : rtlblDefToRelayP-[uni/bd-[uni/tn-tz/BD-BD2]-isSvc-no/dhcplbldef-tz-DHCP_Relay]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

Suivi des paquets DHCP

L'ACI consigne tous les paquets DHCP envoyés au processeur dans des fichiers de trace, qui peuvent être analysés pour dépanner le processus DHCP Discover, Offer, Request, and Acknowledge (DORA). Utilisez cette commande pour afficher les traces de paquets DHCP :

<#root>

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



Conseil : Un seul paquet DHCP génère plus de 100 entrées de suivi. Il est fortement recommandé d'utiliser grep avec des expressions régulières pour filtrer les résultats pertinents pour une analyse efficace.

Lors de l'analyse de la trace DHCP dans Cisco ACI, plusieurs attributs clés peuvent être confirmés pour garantir un fonctionnement correct du relais DHCP :

- Ajouter une sous-option ID de circuit :

Indique que l'option DHCP 82 est ajoutée au paquet, ce qui est essentiel pour les informations de l'agent de relais.

- Adresse interne globale:

Représente l'adresse IP du serveur DHCP configurée dans la stratégie de relais DHCP.

- Adresse d'assistance :

Adresse IP SVI utilisée par le relais pour atteindre le serveur DHCP.

- Le client et le serveur se trouvent dans le même VRF :

Confirme que le client et le serveur DHCP appartiennent au même contexte VRF.

- msg :

Type de message DHCP observé, tel que Découverte, Offre, Demande ou Ack.

- nom ctx :

Nom VRF où la stratégie d'étiquette DHCP est configurée.

- Smac :

Adresse MAC du client DHCP.

- Port UDP src/dst :

Ports DHCP utilisés, généralement 68 pour les clients et 67 pour les serveurs.

<#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:
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
```

Problèmes courants

Problème 1: Perte silencieuse L3out

- Problème

Lorsqu'un L3Out utilise une interface vPC pour établir une relation de voisinage avec un routeur adjacent, chaque commutateur envoie des paquets à l'aide de son propre protocole vTEP. Si l'homologue vPC reçoit une offre DHCP avec une adresse vTEP qui n'est pas la sienne, il transfère le paquet à travers le fabric, entraînant le vTEP de l'émetteur à le déposer silencieusement sans journaux d'erreurs.

Pour vérifier de telles pertes, utilisez cette commande :

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

- Solution

Accédez à Locants > [nom du locataire] > Networking > L3out > [nom L3out] > Logical Node Profile > [nom LNP] > Logical Interface Profile [nom LIP] > SVI > [stratégie SVI]

Une fois sur place, créez ou ouvrez l'adresse IP secondaire et activez la case à cocher Activer pour le relais DHCP.



Cela va forcer l'envoi des messages à l'aide de l'adresse vTEP vPC au lieu de l'adresse vTEP locale et les paquets seront transférés comme prévu.

Problème 2: Le serveur DHCP ne prend pas en charge l'option 82

L'option 82 est essentielle dans les environnements VXLAN tels que l'ACI, car elle crée un circuit entre le leaf source et la destination en fonction des adresses vTEP. Elle comprend :

- ID du circuit : Interface entrante, VLAN et VNID EPG où la détection DHCP est vue.
- ID distant : Adresse TEP du commutateur qui a reçu la détection.

Si l'option 82 est manquante, les paquets de relais DHCP sont abandonnés. Validez la présence de l'option 82 sur le leaf connecté au serveur DHCP en recherchant les erreurs dans les journaux de suivi DHCP indiquant que l'option 82 est manquante.

Cette commande valide le commutateur leaf sur lequel le serveur DHCP est connecté et reçoit les offres avec une option DHCP valide 82

<#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 faile
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 faile
1716) 2025 Sep 10 05:08:52.295709 _relayback_response: 929 : dhcp_relayback_response : option 82 not pr
```

Références

[Dépannage approfondi du relais DHCP dans le fabric ACI - TACDCN-2017]

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.