Comprendre la création d'un tunnel d'accès dans SD-Access

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Topologie

Aperçu

Processus de création de tunnel d'accès

Vérification du processus

- Vérifiez si le point d'accès obtient une adresse IP
- Vérification de l'enregistrement MAC Ethernet et IP des points d'accès sur le plan de contrôle LISP
- Vérifiez que le WLC marque le périphérique comme étant compatible avec le fabric
- Vérification de l'enregistrement MAC radio sur le plan de contrôle LISP
- Vérification de la création du tunnel d'accès

Débogages et suivis

Résumé

Introduction

Ce document décrit ce qu'est un tunnel d'accès dans SD-Access, son but, et comment vous pouvez trier la formation du tunnel d'accès.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Protocole LISP (Locator ID Separation Protocol)
- Sans fil

Composants utilisés

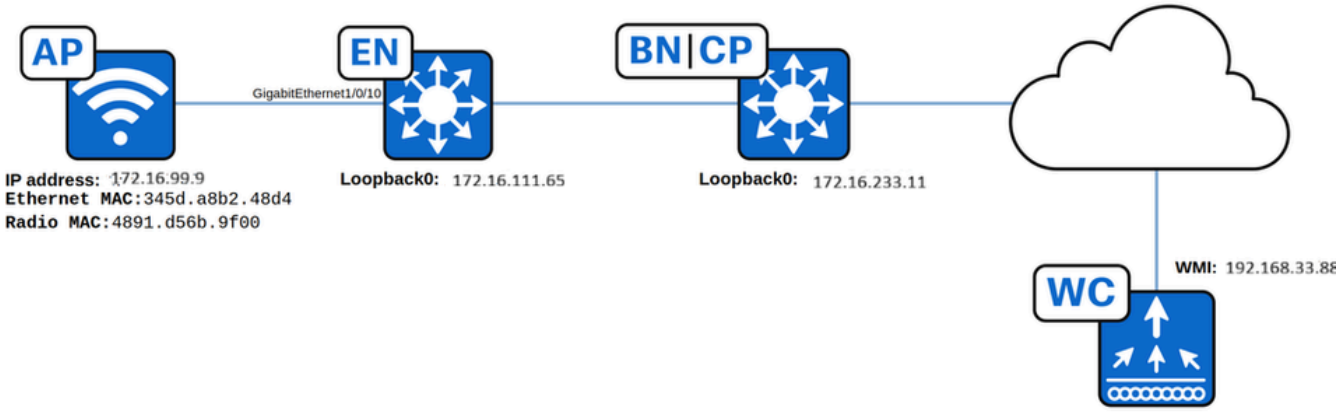
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Contrôleur LAN sans fil Cisco (WLC) - C9800-CL, Cisco IOS® XE 17.12.04
- Noeud de périphérie SDA - C9300-48P, Cisco IOS® XE 17.12.05
- Plan de contrôle/noeud de périphérie SDA - C9500-48P, Cisco IOS® XE 17.12.05

- Point d'accès Cisco - C9130AXI-A, version 17.9.5.47

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.

Topologie



Topologie utilisée dans cet article

Aperçu

Un tunnel d'accès dans Cisco SD-Access est un tunnel de réseau local virtuel extensible (VXLAN) établi entre les noeuds de périphérie de fabric et les points d'accès (AP). Ce tunnel encapsule le trafic client dans VXLAN, permettant une communication transparente au sein du fabric SD-Access. Le tunnel d'accès sert de superposition de plan de données qui achemine le trafic des clients sans fil connectés au point d'accès jusqu'à la périphérie du fabric, assurant ainsi une application et une segmentation cohérentes des politiques sur l'ensemble du réseau.

Processus de création de tunnel d'accès

1. Le point d'accès est branché et mis sous tension via PoE (Power over Ethernet).
2. AP obtient une adresse IP via DHCP dans la superposition. Au cours de ce processus, le point d'accès reçoit également l'option 43 du serveur DHCP pour le contrôleur LAN sans fil.
3. La périphérie du fabric enregistre l'adresse IP et l'adresse MAC Ethernet du point d'accès et met à jour le plan de contrôle LISP.
4. WLC interroge le protocole LISP CP pour savoir si le point d'accès est connecté à un périphérique de fabric .
5. Le plan de contrôle LISP répond au WLC avec le localisateur (IP de bouclage 0) du périphérique de fabric auquel le point d'accès est connecté. S'il y a une réponse, cela signifie que le point d'accès est connecté au fabric et est marqué comme Fabric activé.
6. WLC effectue un enregistrement LISP L2 pour l'AP Radio MAC dans le plan de contrôle LISP avec des informations de métadonnées du WLC au FE.
7. Le plan de contrôle LISP notifie la périphérie du fabric et envoie les métadonnées reçues du

WLC. Ces métadonnées contiennent un indicateur qui indique qu'il s'agit d'un AP et de l'adresse IP de l'AP.

8. La périphérie du fabric traite les informations. Il apprend qu'il s'agit d'un point d'accès et crée un tunnel VXLAN également appelé tunnel d'accès entre le point d'accès et la périphérie du fabric.

Lisez ces étapes pour assurer une formation de tunnel d'accès réussie pour l'intégration d'AP dans SD-Access. Toute défaillance dans ces vérifications peut empêcher la création de tunnels. Si une étape ne produit pas les résultats attendus, concentrez les efforts de dépannage sur le composant associé à cette étape.

Vérification du processus

Vérifiez si le point d'accès obtient une adresse IP

Pour vérifier que le point d'accès reçoit une adresse IP, exécutez cette commande sur le noeud de périphérie :

<#root>

```
Edge#show device-tracking database interface gigabitEthernet 1/0/10


...
     Network Layer Address   Link Layer Address  Interface  vlan prlvl age state     Time left
DH4

172.16.99.9



345d.a8b2.48d4

      Gi1/0/10

99

   0024  15s REACHABLE 237 s try 0(47302 s)
```

D'après le résultat précédent, il peut être confirmé que le point d'accès connecté à l'interface GigabitEthernet 1/0/10 a l'adresse IP 172.16.99.9 sur le VLAN 99, avec l'adresse MAC Ethernet 345d.a8b2.48d4.
Si le résultat est vide, le point d'accès n'a pas réussi à obtenir une adresse IP ou Power over Ethernet (PoE) ne fonctionne pas. Pour vérifier que la technologie PoE est opérationnelle, vérifiez que l'adresse MAC du point d'accès est affichée dans la table d'adresses MAC en exécutant la commande suivante :

<#root>

```
Edge#show mac address-table interface gigabitEthernet 1/0/10


Mac Address Table
-------------------------------------------
```

```
Vlan Mac Address Type Ports
---- ----------- -------- -----
```

99

345d.a8b2.48d4

DYNAMIC

Gi1/0/10

Pour vérifier que l'alimentation en ligne pour PoE est opérationnelle, exécutez cette commande :

<#root>

Edge#show power inline gigabitEthernet 1/0/10

```
Interface  Admin
```

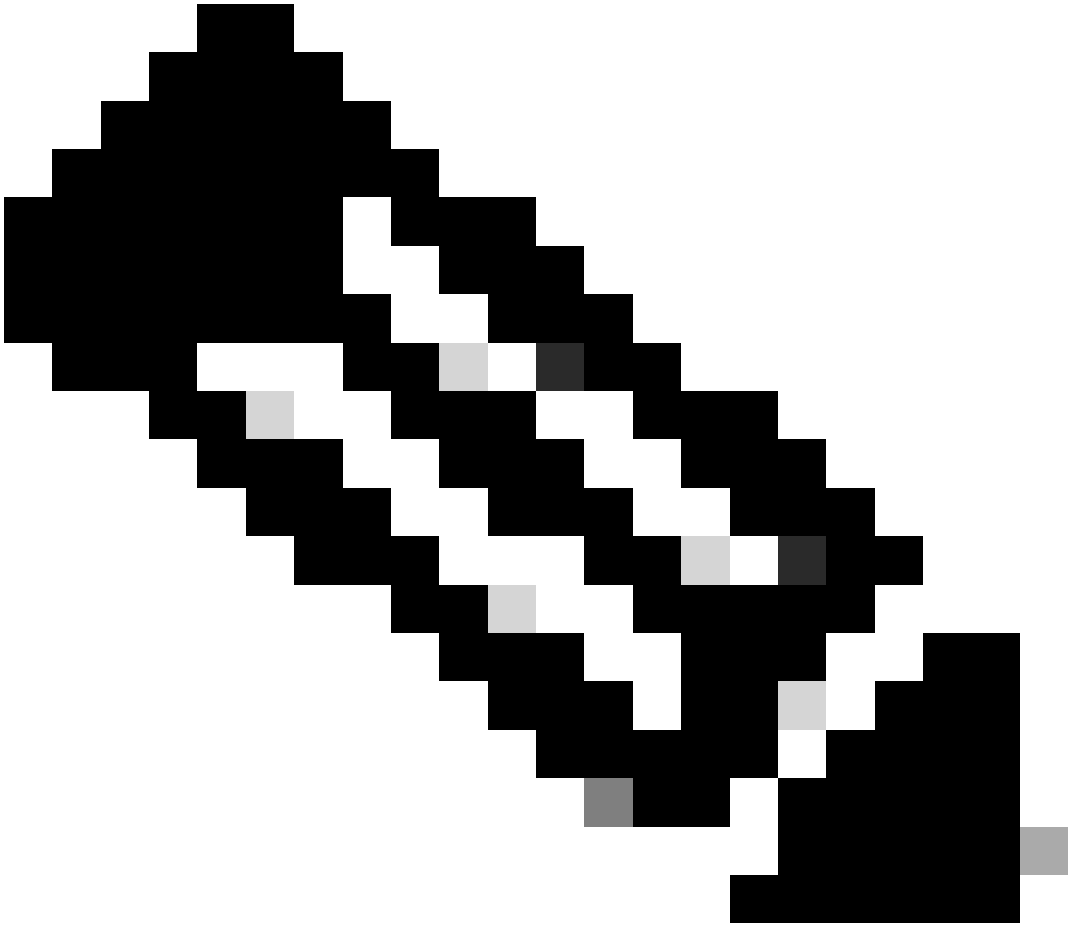
Oper

```
   Power   Device      Class  Max
                         (Watts)
--------- ------ ---------- ------- ------------------ ----- ----
Gi1/0/10    auto
```

on

```
     30.0   C9130AXI-A   4    30.0
```

La technologie PoE est opérationnelle et fonctionne à 30 watts.



Remarque : Après avoir obtenu une adresse IP, le point d'accès tente de se connecter au contrôleur de réseau local sans fil (WLC), comme dans le cas d'un réseau traditionnel. Si le point d'accès n'est pas répertorié lors de l'exécution de la commande show ap summary, dépannez la jonction AP.

Vérification de l'enregistrement MAC Ethernet et IP des points d'accès sur le plan de contrôle LISP

Pour identifier le plan de contrôle, également appelé serveur de mappage, pour l'arête du fabric, exécutez la commande suivante :

<#root>

Edge#show lisp session

```
Sessions for VRF default, total: 1, established: 1
Peer State Up/Down In/Out Users
```

172.16.233.11

:4342 Up 1d02h 326/324 12

Le plan de contrôle est 172.16.233.11, qui serait le loopback0 de ce périphérique.

Pour identifier le plan de contrôle du site de fabric, vous pouvez également exécuter cette commande :

<#root>

Edge#show running-config | section map-server

etr map-server

172.16.233.11

 key 7 050F020C734848514D514117595853732F
etr map-server

172.16.233.11

 proxy-reply
etr map-server

172.16.233.11

 key 7 050F020C734848514D514117595853732F
etr map-server

172.16.233.11

 proxy-reply

Sur le WLC, vous pouvez également vérifier que la session LISP avec le plan de contrôle est dans l'état UP :

<#root>

WLC#show wireless fabric summary

Fabric Status :

Enabled

Control-plane:
Name   IP-address   Key   Status
----
default-control-plane

172.16.233.11

    ddc2df8446e2479d

Up

Utilisez cette commande pour rechercher l'adresse IP de l'AP enregistrée sur le plan de contrôle :

<#root>

Border#show lisp instance-id 4097 ipv4 server 172.16.99.9

LISP Site Registration Information
...

EID-prefix: 172.16.99.9/32 instance-id 4097

First registered: 22:14:34
Last registered: 22:14:34
Routing table tag: 0
Origin: Dynamic, more specific of 172.16.99.0/24
...
TTL: 1d00h

State: complete

Extranet IID: Unspecified
Registration errors:

Authentication failures: 0

Allowed locators mismatch: 0

ETR 172.16.111.65:21839, last registered 22:14:34, proxy-reply, map-notify <-- Last registration

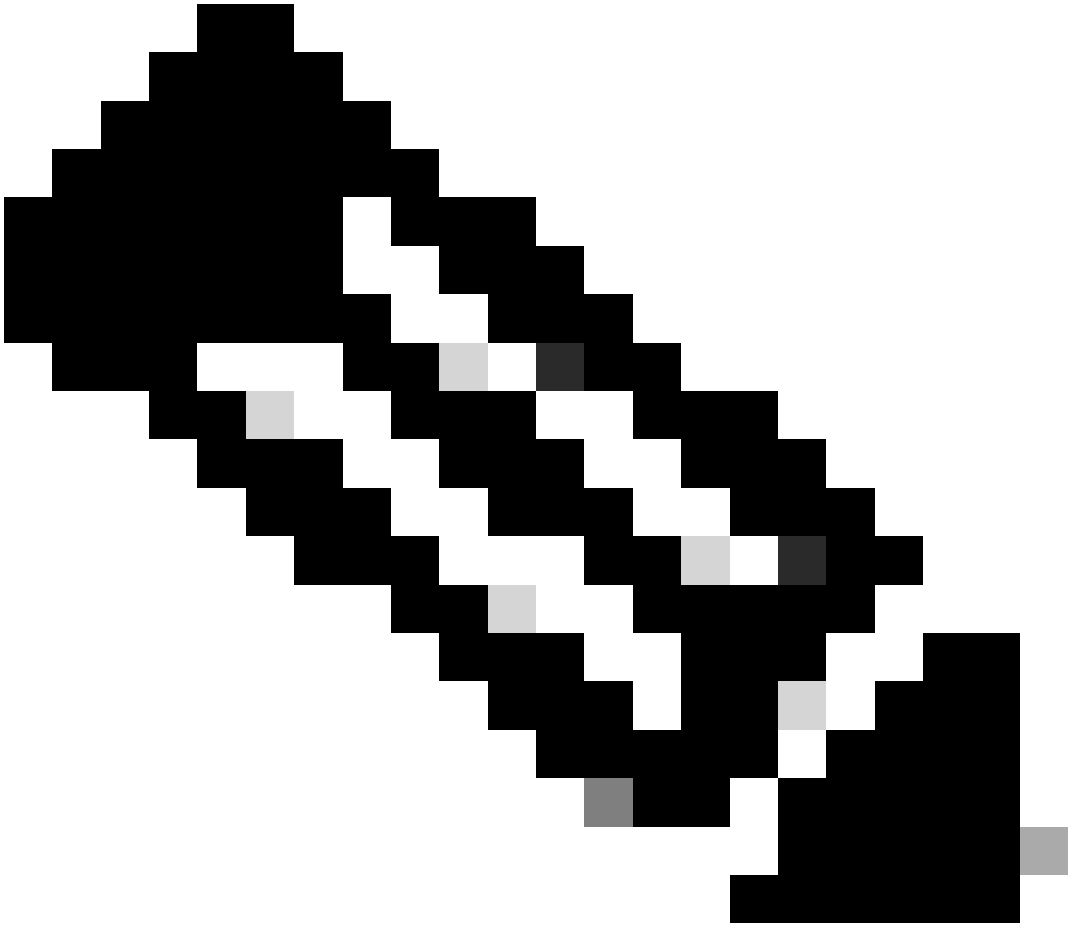
TTL 1d00h, no merge, hash-function sha1
state complete, no security-capability
...
Domain-ID 1559520338
Multihoming-ID unspecified
sourced by reliable transport

Locator

Local State Pri/Wgt Scope

172.16.111.65

yes up 10/10 IPv4 none



Remarque : Les points d'accès utilisent toujours l'INFRA_VN pour la couche 3, et cet INFRA_VN est toujours mappé à l'ID d'instance 4097.

L'enregistrement est terminé pour le point d'accès avec l'adresse IP 172.16.99.9. Il n'y a pas d'échec d'authentification et il est connecté au noeud de périphérie 172.13.111.65 (localisateur).

Pour vérifier si l'adresse MAC est enregistrée sur le plan de contrôle, identifiez d'abord l'ID d'instance de couche 2 pour le VLAN auquel le point d'accès est connecté. Utilisez les commandes suivantes :

<#root>

```
Edge#show vlan id 99

VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------

99

 AP_VLAN active
```

```
L2LI0:8188

, Gi1/0/10, Ac0
...
```

Le VLAN 99 est mappé à l'ID d'instance 8188. À l'aide de cet ID d'instance, exécutez cette commande pour confirmer si l'adresse MAC Ethernet est enregistrée sur le plan de contrôle :

<#root>

```
Border#show lisp instance-id 8188 ethernet server 345d.a8b2.48d4


LISP Site Registration Information
...

EID-prefix: 345d.a8b2.48d4/48 instance-id 8188


First registered: 22:57:39
Last registered: 22:57:39
Routing table tag: 0
Origin: Dynamic, more specific of any-mac
...

State: complete


Extranet IID: Unspecified
Registration errors:

Authentication failures: 0


Allowed locators mismatch: 0

ETR 172.16.111.65:21839, last registered 22:57:39, proxy-reply, map-notify


   TTL 1d00h, no merge, hash-function sha1
   state complete, no security-capability
   ...
   Domain-ID 1559520338
   Multihoming-ID unspecified
   sourced by reliable transport

Locator

      Local State Pri/Wgt Scope

172.16.111.65

 yes   up    10/10   IPv4 none
```

L'enregistrement de l'adresse MAC Ethernet du point d'accès 345d.a8b2.48d4 est terminé sans échec d'authentification et est connecté au noeud de périphérie 172.13.111.65 (localisateur).

Vérifiez que le WLC marque le périphérique comme étant compatible avec le fabric

<#root>

```
WLC#show fabric ap summary

Number of Fabric AP : 1

AP Name           Slots  AP Model
Ethernet MAC


Radio MAC

        Location Country
IP Address

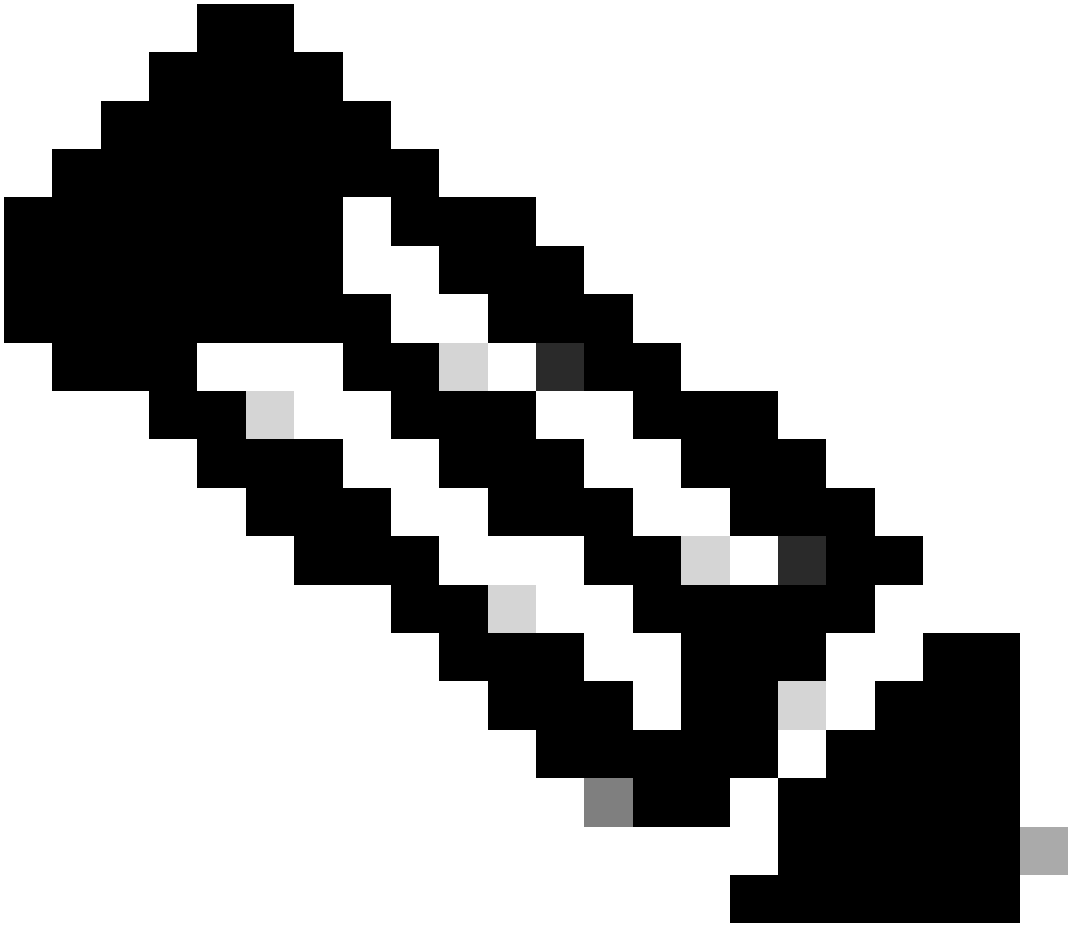
  State
-----------------------------------------------------------------------------------------------------------
AP345D.A8B2.48D4  3      C9130AXI-A
345d.a8b2.48d4


4891.d56b.9f00

   default location MX
172.16.99.9

 Registered
```

Le point d'accès avec l'adresse IP 172.16.99.9 est correctement marqué comme point d'accès de fabric. Si le point d'accès n'est pas répertorié, cela indique que le WLC n'a pas pu recevoir de réponse du plan de contrôle LISP. Dans ce résultat, l'adresse MAC radio pour le point d'accès est 4891.d56b.9f00.



Remarque : Si le point d'accès est enregistré sur le plan de contrôle, mais n'est pas marqué comme Fabric-enabled, assurez-vous qu'aucun pare-feu ne bloque le trafic LISP sur le port UDP 4342.

Vérification de l'enregistrement MAC radio sur le plan de contrôle LISP

Utilisez la même commande que celle utilisée pour vérifier l'enregistrement de l'adresse MAC Ethernet, mais remplacez l'adresse MAC Ethernet par l'adresse MAC radio :

<#root>

```
Border#show lisp instance-id 8188 ethernet server 4891.d56b.9f00

LISP Site Registration Information
...
EID-prefix: 4891.d56b.9f00/48 instance-id 8188
```

```
First registered: 22:49:43
Last registered: 22:49:43
Routing table tag: 0
Origin: Dynamic, more specific of any-mac
...
State: complete
Extranet IID: Unspecified
Registration errors:
```

Authentication failures: 0

```
Allowed locators mismatch: 0
ETR 192.168.33.88:59019, last registered 22:49:43, no proxy-reply, no map-notify
   TTL 1d00h, no merge, hash-function sha2
   state complete, no security-capability
   ...
   sourced by reliable transport
   Affinity-id: 0 , 0
```

WLC AP bit: Set

Locator

```
       Local State Pri/Wgt Scope
```

172.16.111.65

```
 yes   up    0/0     IPv4 none
```

L'adresse MAC radio est entièrement enregistrée sans échec d'authentification et est connectée au noeud de périphérie 172.16.111.65 (localisateur). Le résultat montre également le bit d'AP WLC : Définissez un indicateur utilisé par le plan de contrôle LISP pour indiquer au noeud d'extrémité que cet enregistrement appartient à un point d'accès sur son RLOC 172.16.111.65.

Vérification de la création du tunnel d'accès

La dernière étape consiste à vérifier la création du tunnel d'accès sur la périphérie du fabric. Comme indiqué précédemment, c'est l'objectif ultime de l'intégration des points d'accès dans SD-Access. Pour vérifier la création du tunnel d'accès, exécutez cette commande :

<#root>

Edge#show access-tunnel summary

```
Access Tunnels General Statistics:
Number of AccessTunnel Data Tunnels = 1
Name   RLOC IP(Source)   AP IP(Destination) VRF ID Source Port Destination Port
------ --------------- ------------------ ------ ----------- ----------------
```

Ac0

172.16.111.65

172.16.99.9

0 N/A 4789

Name IfId Uptime
------ ---------- --------------------

Ac0 0x00000058 0 day, 00:00:51

Le tunnel d'accès 0 connecte le point d'accès 172.16.99.9 au localisateur de noeud de périphérie 172.16.111.65 et est actif depuis 51 secondes. Le minuteur est défini sur 0 après chaque réinitialisation.

Vous pouvez également confirmer que le tunnel est programmé au niveau de la couche d'abstraction FED (Forwarding Engine Driver), qui assure l'interface directe avec le matériel du commutateur :

<#root>

Edge#show platform software fed switch active ifm interfaces access-tunnel

Interface IF_ID State

Ac0

0x00000058

READY

À l'aide de IF_ID, vous pouvez trouver plus d'informations sur ce tunnel :

<#root>

Edge#show platform software fed switch active ifm if-id 0x00000058

Interface IF_ID : 0x0000000000000058
Interface Name : Ac0
Interface Block Pointer : 0x73d6c83dc6f8

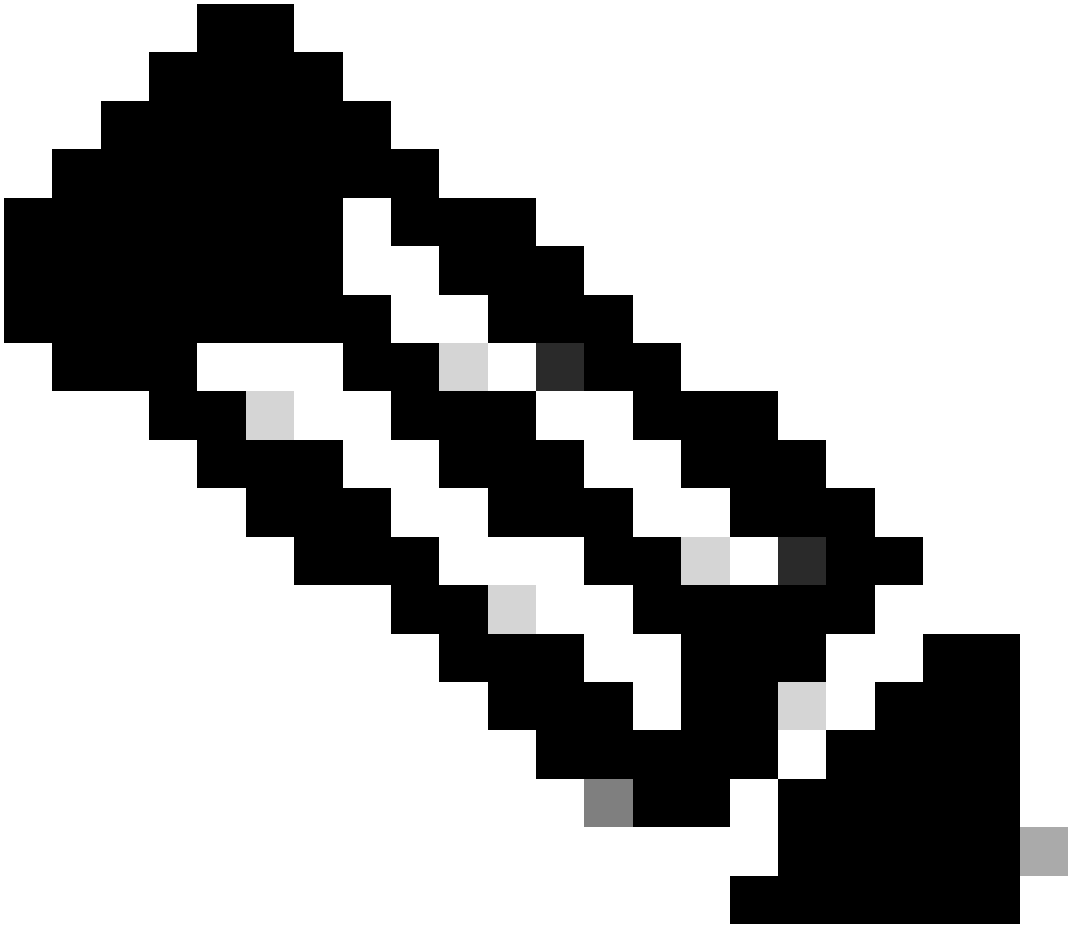
Interface Block State : READY

Interface State : Enabled

```
...
Interface Type : ACCESS_TUNNEL


...
Tunnel Type : L2Lisp
Encap Type : VxLan
...
```

Il s'agit d'un tunnel lisp de couche 2 utilisant l'encapsulation VXLAN et le type d'interface est access-tunnel.



Remarque : Il est important que le nombre de tunnels d'accès corresponde dans le résultat de la commande show access-tunnel summary et de la commande FED. Une non-correspondance peut indiquer une erreur de programmation.

Sur l'AP, vous pouvez vérifier la création du tunnel d'accès avec cette commande :

<#root>

AP#show ip tunnel fabric

```
Fabric GWs Information:
Tunnel-Id GW-IP         GW-MAC            Adj-Status Encap-Type Packet-In
  Bytes-In Packet-Out Bytes-out
        1
```

172.16.111.65

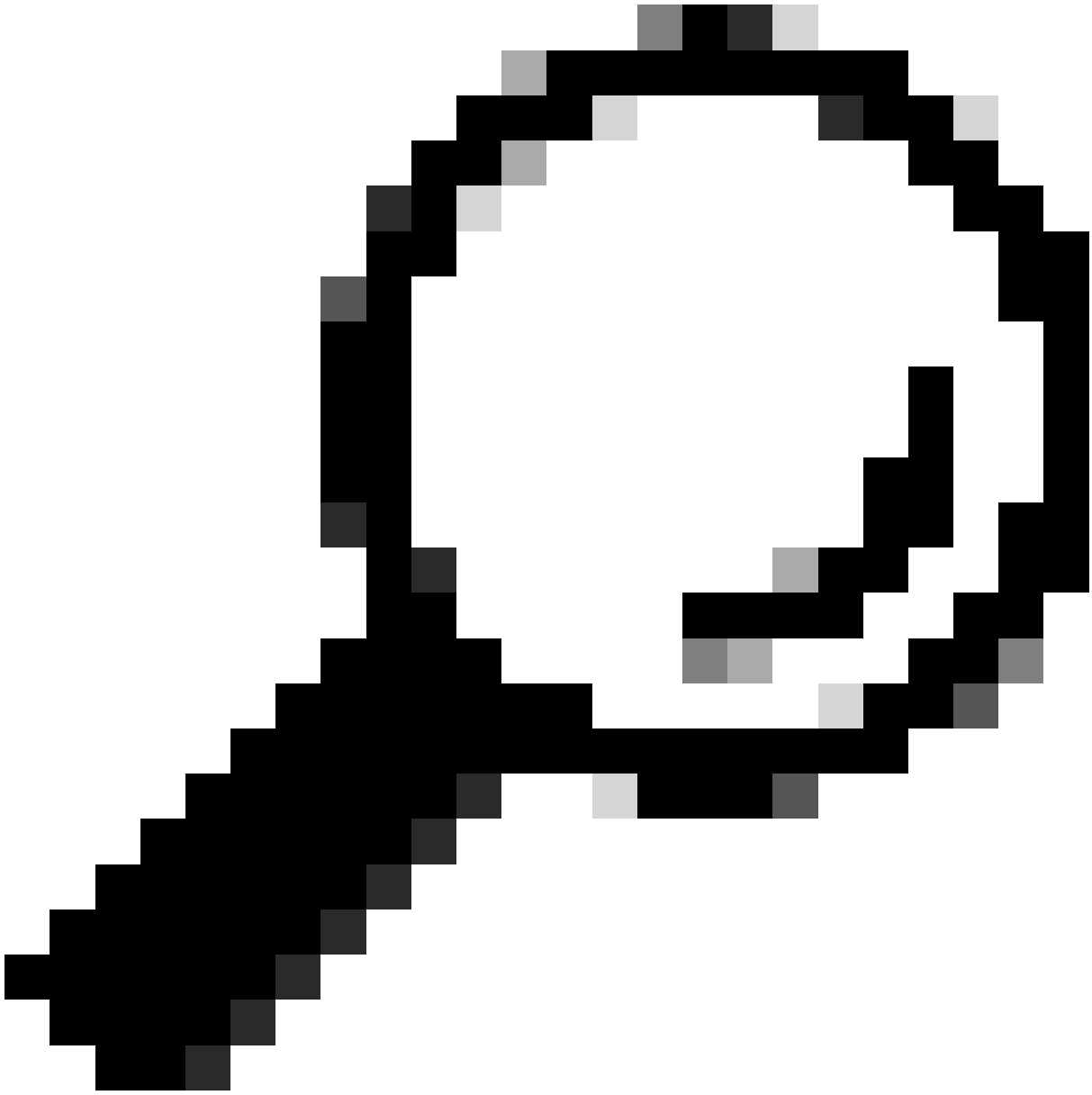
00:00:0C:9F:F2:80

Forward

VXLAN

```
      121
   17096    239       35041
AP APP Fabric Information:
GW_ADDR ENCAP_TYPE VNID SGT FEATURE_FLAG GW_SRC_MAC GW_DST_MAC
```

Le point d'accès a un tunnel d'accès pointant vers le localisateur du noeud de périphérie 172.16.111.65. L'adresse MAC 00:00:0C:9F:F2:80 appartient à l'interface virtuelle de commutateur (SVI) 99, qui est le VLAN où le point d'accès est connecté. Le type d’encapsulation est VXLAN.



Conseil : Le tunnel n'apparaît sur le point d'accès que lorsqu'un client actif est connecté. Sinon, la commande renvoie une sortie vide.

Débogages et suivis

Pour un débogage plus avancé de la création du tunnel d'accès, activez ces traces sur la périphérie du fabric :

```
set platformsoftware trace forwarding-manager switch active R0 access-tunnel debug
set platform software trace forwarding-manager switch active F0 access-tunnel debug
set platform software trace forwarding-manager switch active access-tunnel noise
request plat sof trace rotate all
show pla sof trace message forwarding-manager switch active R0 reverse
show pla sof trace message forwarding-manager switch active F0 reverse
```

```
show pla sof trace message fed sw active reverse
```

Commandes dépendant de la plate-forme du tunnel d’accès du Catalyst 9000 pour vérifier la programmation du tunnel d’accès à la périphérie du fabric :

```
show platform software fed switch active ifm interfaces access-tunnel
show platform software access-tunnel switch active R0
show platform software access-tunnel switch active R0 statistics
show platform software access-tunnel switch active F0
show platform software access-tunnel switch active F0 statistics
show platform software fed switch active ifm if-id <if-id>
```

Pour le débogage, le processus pour le tunnel d'accès sur le WLC, activez ces commandes :

```
set platform software trace wncd chassis active r0 lisp-agent-api
set platform software trace wncd chassis active r0 lisp-agent-db
set platform software trace wncd chassis active r0 lisp-agent-fsm
set platform software trace wncd chassis active r0 lisp-agent-ha
set platform software trace wncd chassis active r0 lisp-agent-internal g
set platform software trace wncd chassis active r0 lisp-agent-lib
set platform software trace wncd chassis active r0 lisp-agent-lispmsg
set platform software trace wncd chassis active r0 lisp-agent-shim
set platform software trace wncd chassis active r0 lisp-agent-transport
```

Débogages pour le processus d'enregistrement. Ces commandes peuvent être exécutées sur le noeud de périphérie pour vérifier s'il tente d'enregistrer l'adresse IP et l'adresse MAC Ethernet du point d'accès, et sur le plan de contrôle pour confirmer si l'enregistrement s'effectue correctement.

```
debug lisp filter eid <mac-or-ip>
debug lisp control-plane all
```

Résumé

- Les tunnels d'accès dans SD-Access sont des tunnels VXLAN entre des noeuds de périphérie de fabric et des points d'accès qui transportent le trafic client dans le fabric encapsulé dans VXLAN.
- Ils permettent des plans de données sans fil unifiés et l'application cohérente des politiques, car l'étiquette de groupe de sécurité (SGT) est étiquetée au niveau du point d'accès pour les terminaux sans fil.
- La vérification et le triage impliquent la vérification de l'enregistrement sur le plan de contrôle du fabric, la confirmation de la création sur les noeuds de périphérie du fabric et la vérification de l'état du fabric pour le point d'accès sur le WLC à l'aide de commandes show spécifiques.
- Le dépannage consiste à s'assurer que les tunnels sont correctement créés et restent stables après les modifications de configuration.

- Le tunnel d'accès est l'objectif final lors de l'intégration d'un nouveau point d'accès à SD-Access.

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.