# Dépannage et vérification de la configuration initiale sans fil SD-Access

## Table des matières


Introduction

Conditions préalables

- Exigences
- Composants utilisés
- Topologie

Dépannage et isolation

- Vérifications rapides
- Scénario 1. Vérifier l'enregistrement du WLC avec le plan de contrôle du serveur LISP/MAP
- scénario 2. Les points d'accès n'obtiennent pas d'adresse IP
- scénario 3. Les points d'accès n'ont pas de tunnel vxlan construit vers leur noeud de périphérie de fabric
- scénario 4. entrées de tunnel d'accès manquantes après un certain temps
- scénario 5. Les clients sans fil ne peuvent pas obtenir d'adresse IP
- scénario 6. Fabric invité/authentification Web ne fonctionne pas/ne redirige pas les clients

Comprendre

- Comment un client sans fil obtient-il une adresse IP dans l'architecture de fabric ?
- Comprendre le flux de redirection Web dans un scénario de fabric
- Journaux de l'AP joignant le WLC dans l'état activé par le fabric


## Introduction

Cet article décrit les étapes de dépannage de base permettant d'identifier les problèmes de connectivité de base dans les configurations sans fil SD-Access. Il décrit les éléments et les commandes à vérifier pour isoler les problèmes de la solution relatifs au réseau sans fil.

## Conditions préalables

### Exigences

Connaissance de la solution SD-Access

Une topologie d'accès SD déjà configurée

### Composants utilisés

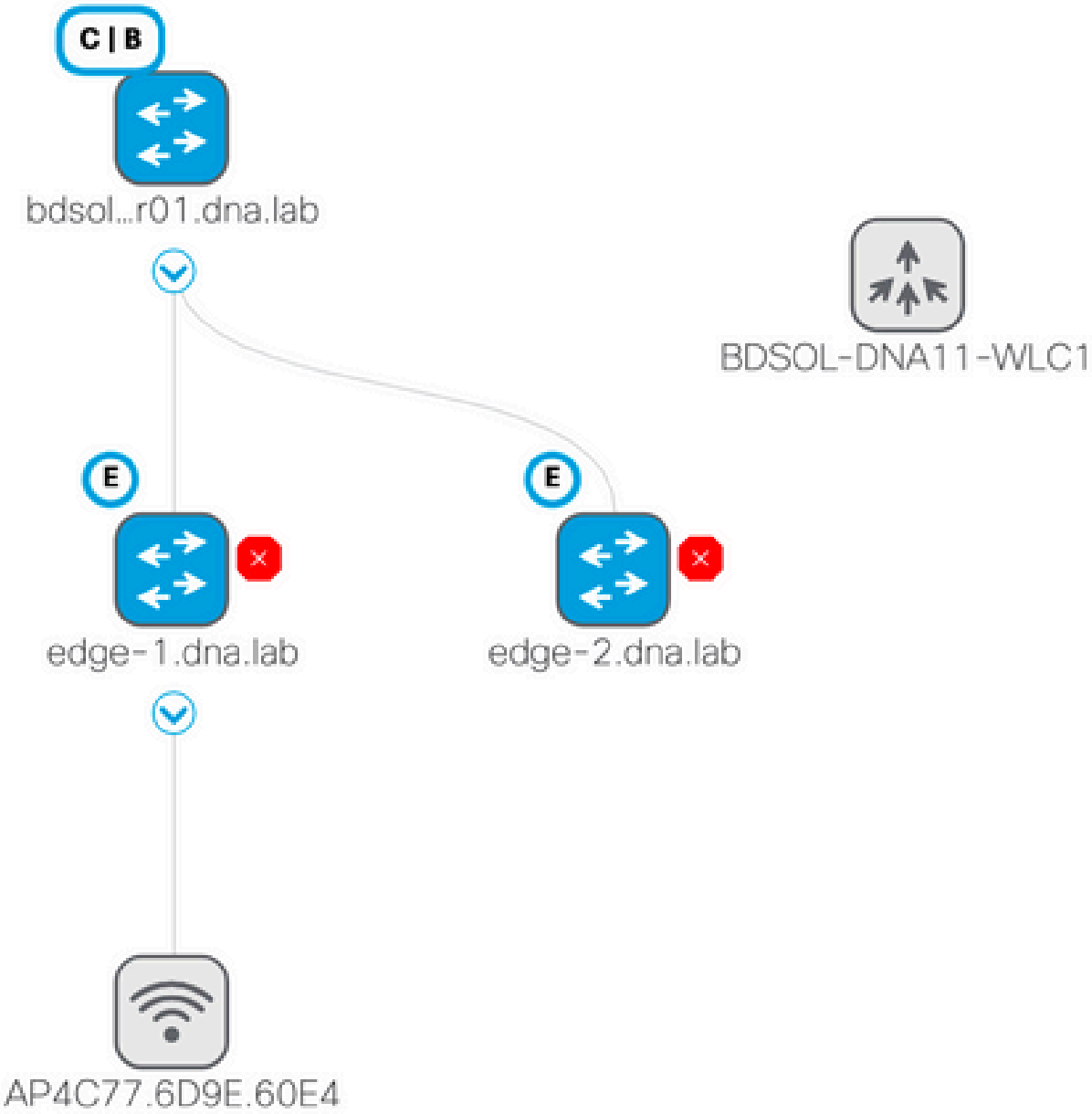
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau

est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes. Il existe d'autres types de périphériques pris en charge pour l'accès sans fil SD, mais cet article se concentre sur les périphériques décrits dans cette section. Les commandes peuvent varier selon la plate-forme et la version du logiciel.

8.5.151 Contrôleur sans fil

16.9.3 Commutateur 9300 en tant que noeud de périphérie

### Topologie




## Dépannage et isolation

### Vérifications rapides

Il y a une série d'exigences dans les scénarios d'accès SD qui est souvent une source d'erreurs, donc s'il vous plaît vérifier d'abord que ces exigences sont respectées :

- Assurez-vous que vous disposez d'une route spécifique (et que vous n'utilisez pas la route par défaut) pointant vers le WLC sur le noeud du plan de contrôle LISP
- Assurez-vous que vos AP se trouvent dans le VPN infrarouge, en utilisant la table de routage globale
- Assurez-vous que les AP ont la connectivité au WLC en envoyant une requête ping au WLC à partir de l'AP lui-même
- Assurez-vous que l'état du fabric du plan de contrôle sur le WLC est up
- Assurez-vous que les points d'accès sont à l'état activé par le fabric

## Scénario 1. Vérifier l'enregistrement du WLC avec le plan de contrôle du serveur LISP/MAP

Lorsque vous ajoutez le WLC au fabric dans DNA Center, les commandes sont envoyées au contrôleur pour établir une connexion au noeud défini comme plan de contrôle dans DNA-C. La première étape consiste à s'assurer que cette inscription est réussie. Si la configuration LISP sur le plan de contrôle a été corrompue d'une certaine manière, cet enregistrement pourrait échouer.


Si cet état indique « down », il peut être intéressant d'exécuter des débogages ou une capture de paquets entre le WLC et le plan de contrôle. L'enregistrement implique à la fois TCP et UDP sur le routeur 4342. Si le plan de contrôle n'a pas obtenu la configuration appropriée, il peut répondre avec un TCP RST au TCP SYN envoyé par le WLC.

Le même état peut être vérifié avec show fabric map-server summary sur la ligne de commande. Le processus est débogué avec debug fabric lisp map-server all sur l'interface de ligne de commande WLC. Pour provoquer une tentative de reconnexion, vous pouvez accéder à DNA Center et choisir de retirer le WLC du fabric et de l'ajouter à nouveau.

Des raisons possibles sont l'absence de lignes de configuration dans le plan de contrôle. Voici un exemple de configuration de travail (la partie la plus importante uniquement) :

```
rtr-cp-mer-172_16_200_4#show run | s WLC
 locator-set WLC
  10.241.0.41
  exit-locator-set
 map-server session passive-open WLC
```

Si le WLC ip est manquant (10.241.0.41 ici) ou si la commande passive-open est manquante, le PC refusera la connexion WLC.

Les débogages à exécuter sont :

- **'debug capwap events enable'**
- **'debug capwap errors enable'**
- **'debug fabric ap-join events enable'**
- **'debug fabric ap-join detail enable'**
- **'debug fabric lisp map-server all enable'**

Voici un exemple du plan de contrôle ne répondant pas au WLC

<#root>

```
*msfMsgQueueTask: May 07 14:08:10.080: Sent map-request to MS 10.32.47.128 for AP 10.32.58.36 VNID 4097
*msfMsgQueueTask: May 07 14:08:10.080: No messages are present in the Client list for Local UDP socket
*msfMsgQueueTask: May 07 14:08:10.080: msfSendLocalUDPSocketMessage:637 Message get for UDP file socket

*osapiBsnTimer: May 07 14:08:15.179: Map-reply timer for MS IP 10.32.47.128 expired for AP IP 10.32.58.3


*msfMsgQueueTask: May 07 14:08:15.179: msfQueue: recieved LISP_MAP_SERVER_TIMEOUT_QUEUE_MSG
*msfMsgQueueTask: May 07 14:08:15.179: Found entry AP 10.32.58.36 vnid 4097

*msfMsgQueueTask: May 07 14:08:15.179: Added AP 10.32.58.36 VNID 4097 for long retry map-request

*msfMsgQueueTask: May 07 14:08:15.179: Found entry AP 10.32.58.36 vnid 4097
*msfMsgQueueTask: May 07 14:08:15.179: No messages are present in the Client list for Local UDP socket
*msfMsgQueueTask: May 07 14:08:15.179: msfSendLocalUDPSocketMessage:637 Message get for UDP file socket
*spamApTask0: May 07 14:08:16.084: 00:fc:ba:15:95:00 WTP Event Request from 10.32.58.36:5248 epoch 1525
*spamApTask0: May 07 14:08:16.084: 00:fc:ba:15:95:00 WTP Event Response sent to 10.32.58.36:5248
*osapiBsnTimer: May 07 14:08:17.839: NAK Timer expiry callback
*msfMsgQueueTask: May 07 14:08:17.839: msfQueue: recieved LISP_MAP_SERVER_NAK_TIMEOUT_QUEUE_MSG
*msfMsgQueueTask: May 07 14:08:17.839: Started periodic NAK processing timer

*msfMsgQueueTask: May 07 14:08:17.839: Process list of AP (1) for which RLOC is not received
```

Voici un exemple des débogages WLC d'un AP se joignant dans l'état de fabric désactivé parce

que le plan de contrôle de fabric n'avait pas de route spécifique vers le WLC

```
(POD3-WLC1) >*emWeb: Oct 16 08:54:21.593: Fabric is supported for apType 54

*emWeb: Oct 16 08:54:21.593: Fabric is supported for apType 54

*emWeb: Oct 16 08:55:26.295: ip c0a82700,subnet ffffff00,l2vnid 8191,l3vnid 1001
*emWeb: Oct 16 08:55:26.295: Vnid Mapping added at index 2 with entries 192_168_39_0-INFRA_VN,8191,4097

*emWeb: Oct 16 08:55:26.295:
                             Log to TACACS server(if online): fabric vnid create name 192_168_39_0-INFRA

*spamReceiveTask: Oct 16 08:55:26.295: Fabric is supported for AP f4:db:e6:61:24:a0 (Pod3-AP4800). apTyp

*spamReceiveTask: Oct 16 08:55:26.295: spamProcessFabricVnidMappingAddRequest: Fabric Adding vnid mappi
*spamReceiveTask: Oct 16 08:55:26.295: Vnid Mapping return from index 2 with entries name 192_168_39_0-

*spamReceiveTask: Oct 16 08:55:26.295: spamSendFabricMapServerRequest: MS request from AP Pod3-AP4800 f4
*emWeb: Oct 16 08:55:29.944:
                             Log to TACACS server(if online): save


(POD3-WLC1) >*spamApTask6: Oct 16 08:56:49.243: Fabric is supported for AP f4:db:e6:64:02:a0 (Pod3-AP380

*spamApTask6: Oct 16 08:56:51.949: Fabric is supported for AP f4:db:e6:64:02:a0 (Pod3-AP3800). apType 53

*spamApTask6: Oct 16 08:56:51.953: Fabric is supported for AP f4:db:e6:64:02:a0 (Pod3-AP3800). apType 53

*spamApTask6: Oct 16 08:56:51.953: Fabric is supported for AP f4:db:e6:64:02:a0 (Pod3-AP3800). apType 53

*spamApTask6: Oct 16 08:56:51.953: spamSendFabricMapServerRequest: MS request from AP Pod3-AP3800 f4:db
```

Il est intéressant de noter que s'il y a deux plans de contrôle dans votre réseau de fabric, le WLC tentera toujours d'atteindre les deux pour l'enregistrement ou les requêtes. Il est prévu que les deux plans de contrôle donnent des réponses positives sur les enregistrements, de sorte que le WLC ne pourra pas enregistrer les AP dans le fabric si l'un des deux plans de contrôle le rejette pour une raison quelconque. Un plan de contrôle ne répondant pas est cependant acceptable et le plan de contrôle restant sera utilisé.

Les AP atteignent le WLC via la table de routage globale, mais LISP est toujours utilisé pour résoudre le WLC. Le trafic envoyé par les AP au WLC est un contrôle CAPWAP pur (aucun vxlan impliqué), mais le trafic de retour envoyé par le WLC au AP sera transporté sur Vxlan sur la superposition. Vous ne pourrez pas tester la connectivité de la passerelle AP SVI sur la périphérie vers le WLC parce que comme il s'agit d'une passerelle Anycast, la même IP existe également sur le noeud de frontière. Pour tester la connectivité, le mieux est d'envoyer une requête ping à partir du point d'accès lui-même.

## scénario 2. Les points d'accès n'obtiennent pas d'adresse IP

Les points d'accès doivent obtenir une adresse IP du point d'accès, dans l'Infra VNI défini dans le centre DNA. Si cela ne se produit pas, cela signifie généralement que le port de commutation où

l'AP est connecté ne s'est pas déplacé vers le VLAN droit. Lors de la détection (via CDP) d'un point d'accès connecté, le commutateur applique une macro switchport qui définit le port de commutation dans le VLAN défini par DNA-C pour le pool AP. Si le port de commutation problématique n'est en effet pas configuré avec la macro, vous pouvez soit définir la configuration manuellement (afin que l'AP obtienne une adresse IP, rejoigne le WLC et mette probablement à niveau son code et éventuellement résoudre tout bogue CDP) ou dépanner le processus de connexion CDP. Vous pouvez éventuellement configurer l'intégration de l'hôte pour définir statiquement le port sur DNA-Center pour héberger un AP afin qu'il soit provisionné avec la bonne configuration.

Les macros SmartPort ne s'activent pas automatiquement si le commutateur n'a pas été configuré avec un point d'accès au moins, vous pouvez vérifier si la macro AP a été configurée avec le bon VLAN (au lieu du VLAN 1 par défaut)

```
Pod3-Edge1#show macro auto device
Device:lightweight-ap
Default Macro:CISCO_LWAP_AUTO_SMARTPORT
Current Macro:CISCO_LWAP_AUTO_SMARTPORT
Configurable Parameters:ACCESS_VLAN
Defaults Parameters:ACCESS_VLAN=1
Current Parameters:ACCESS_VLAN=2045
```

Les commandes envoyées par Cisco DNA-C pour définir ce paramètre sont les suivantes :

```
macro auto execute CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT builtin CISCO_LWAP_AUTO_SMARTPORT ACCESS_VLAN=20
macro auto global processing
```

## scénario 3. Les points d'accès n'ont pas de tunnel vxlan construit vers leur noeud de périphérie de fabric

Une fois qu'un AP rejoint le WLC, le WLC (si l'AP est compatible avec le fabric) enregistrera l'AP sur le plan de contrôle comme un type spécial de client. Le plan de contrôle demande ensuite au noeud de périphérie du fabric où le point d'accès est connecté de construire un tunnel vxlan vers le point d'accès.

Le point d’accès utilise uniquement l’encapsulation vxlan pour envoyer le trafic client (et uniquement pour les clients en état d’exécution). Par conséquent, il est normal de ne voir aucune information vxlan sur le point d’accès tant qu’un client de fabric ne se connecte pas.

Sur le point d'accès, la commande show ip tunnel fabric affichera les informations de tunnel vxlan une fois qu'un client s'est connecté.

```
AP4001.7A03.5736#show ip tunnel fabric
```

```
Fabric GWs Information:
Tunnel-Id           GW-IP            GW-MAC        Adj-Status Encap-Type Packet-In Bytes-In Packet-Out
        1    172.16.2.253 00:00:0C:9F:F4:5E           Forward      VXLAN     39731  4209554      16345
AP4001.7A03.5736#
```

Sur le noeud Périphérie du fabric, la commande show access-tunnel summary affiche les tunnels vxlan construits vers les points d'accès. Les tunnels s'afficheront dès que le plan de contrôle a ordonné leur création quand l'AP se joint.

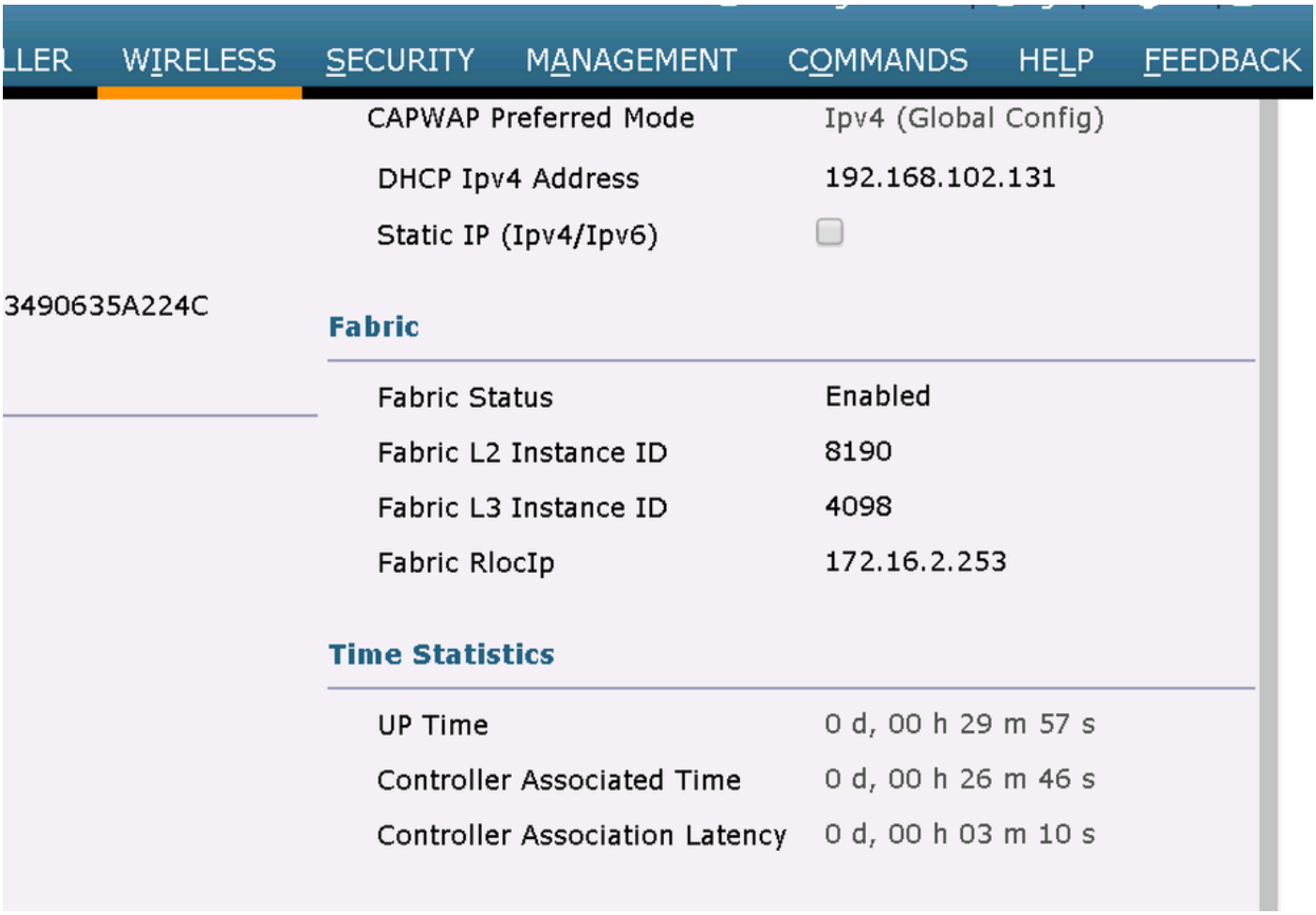
```
edge01#show access-tunnel summ

Access Tunnels General Statistics:
  Number of AccessTunnel Data Tunnels       = 2


Name   SrcIP           SrcPort DestIP          DstPort VrfId
------ --------------- ------- --------------- ------- ----
Ac1    172.16.2.253    N/A     192.168.102.130 4789    2
Ac0    172.16.2.253    N/A     192.168.102.131 4789    2


Name   IfId            Uptime
------ ---------- --------------------
Ac1    0x0000003B 1 days, 22:53:48
Ac0    0x0000003A 0 days, 22:47:06
```

Vous pouvez vérifier sur le WLC, sur la page du point d'accès, l'ID d'instance LISP de couche 2 correspondant à ce point d'accès, puis vérifier les statistiques de cette instance sur la périphérie de fabric où elle est connectée.




```
SDA-D-6880-1#show lisp instance-id 8188 ethernet statistics
LISP EID Statistics for instance ID 8188 - last cleared: never
Control Packets:
  Map-Requests in/out:                      0/0
    Encapsulated Map-Requests in/out:       0/0
    RLOC-probe Map-Requests in/out:         0/0
    SMR-based Map-Requests in/out:          0/0
    Map-Requests expired on-queue/no-reply  0/0
    Map-Resolver Map-Requests forwarded:    0
    Map-Server Map-Requests forwarded:      0
  Map-Reply records in/out:                 0/0
    Authoritative records in/out:           0/0
    Non-authoritative records in/out:       0/0
    Negative records in/out:                0/0
    RLOC-probe records in/out:              0/0
    Map-Server Proxy-Reply records out:     0
  Map-Register records in/out:              24/0
    Map-Server AF disabled:                 0
    Authentication failures:                0
  Map-Notify records in/out:                0/0
    Authentication failures:                0
  Deferred packet transmission:             0/0
    DDT referral deferred/dropped:          0/0
    DDT request deferred/dropped:           0/0
```

## scénario 4. entrées de tunnel d’accès manquantes après un certain temps

Il est possible que les tunnels d'accès soient créés avec succès la première fois que le WLC est provisionné via Cisco DNA-C et ajouté au fabric, mais lors du re-provisionnement de la configuration sans fil (comme la configuration WLAN), il est observé que les entrées de tunnel d'accès pour les points d'accès sont manquantes, ce qui empêche les clients sans fil d'obtenir IP avec succès.

La topologie est 9500(CP) —> 9300 (Edge) —> AP —> Client sans fil.

Les entrées sont correctement observées dans show access-tunnel summary sur le noeud de périphérie :

```
edge_2#show access-tunnel summary

Access Tunnels General Statistics:
Number of AccessTunnel Data Tunnels = 1


Name SrcIP SrcPort DestIP DstPort VrfId
------ --------------- ------- --------------- ------- ----
Ac0 172.16.3.98 N/A 172.16.3.131 4789 0


Name IfId Uptime
------ ---------- --------------------
Ac0 0x0000003C 5 days, 18:19:37
```

Mais lors de la vérification de show platform software fed switch active ifm interfaces access-tunnel, l'entrée pour l'AP est manquante ou n'a pas pu être programmée dans le matériel dans cet exemple.

```
edge_2#show platform software fed switch active ifm interfaces access-tunnel
Interface IF_ID State
----------------------------------------------------------------
Ac0 0x0000003c FAILED
```

Pour plus de sorties :

```
edge_2#sh platform software access-tunnel switch active F0
Name SrcIp DstIp DstPort VrfId Iif_id Obj_id Status
-------------------------------------------------------------------------------------------
```

```
Ac0 98.3.16.172 131.3.16.172 0x12b5 0x000 0x00003c 0x00585f Done


edge_2#sh platform software access-tunnel switch active R0
Name SrcIp DstIp DstPort VrfId Iif_id
------------------------------------------------------------------------
Ac0 172.16.3.98 172.16.3.131 0x12b5 0x0000 0x00003c
```

Vous devez comparer les différentes sorties et chaque tunnel montré par le résumé show access-tunnel doit être présent dans chacune d'elles.

## scénario 5. Les clients sans fil ne peuvent pas obtenir d’adresse IP

Si le tunnel vxlan est présent et que tout semble correct mais que les clients sans fil sont systématiquement incapables d'obtenir une adresse IP, vous êtes peut-être confronté à un problème d'option 82. Puisque la découverte DHCP du client est transmise par la passerelle Anycast sur le noeud de périphérie, il serait difficile pour le serveur DHCP OFFER d'être envoyé au noeud de périphérie droit par la frontière sur le chemin de retour. C'est pourquoi l'arête de fabric qui transfère le DHCP DISCOVER ajoute un champ d'option 82 au DHCP DISCOVER qui contient le RLOC de fabric réel (loopback ip) du noeud d'arête codé avec d'autres informations. Cela signifie que votre serveur DHCP doit prendre en charge l'option 82.

Pour dépanner le processus DHCP, effectuez des captures sur les noeuds du fabric (en particulier le noeud de périphérie client) pour vérifier que la périphérie du fabric ajoute le champ de l'option 82.

## scénario 6. Fabric invité/authentification Web ne fonctionne pas/ne redirige pas les clients

Le scénario de fabric invité est extrêmement similaire à l'authentification Web centrale (CWA) sur les points d'accès Flexconnect et fonctionne exactement de la même manière (même si les points d'accès de fabric ne sont pas en mode Flexconnect).

La liste de contrôle d'accès et l'URL de redirection doivent être renvoyées par ISE dans le premier résultat d'authentification MAC. Vérifiez ces informations dans les journaux ISE ainsi que dans la page de détails du client sur le WLC.

La liste de contrôle d'accès de redirection doit être présente sous la forme d'une liste de contrôle d'accès Flex sur le WLC et doit contenir des instructions « permit » vers l'adresse IP ISE sur le port 8443 (au moins).

Le client doit être à l'état « CENTRAL_WEBAUTH_REQ » dans la page des détails du client sur le WLC. Le client ne pourra pas envoyer de requête ping à sa passerelle par défaut, ce qui est normal. Si vous n'êtes pas redirigé, vous pouvez essayer de taper manuellement une adresse IP dans le navigateur Web du client (pour exclure le DNS, mais le nom d'hôte ISE devra être résolu de toute façon). Vous devriez pouvoir entrer l'adresse IP ISE sur le port 8443 dans le navigateur client et voir la page du portail car ce flux ne sera pas redirigé. Si cela ne se produit pas, vous êtes

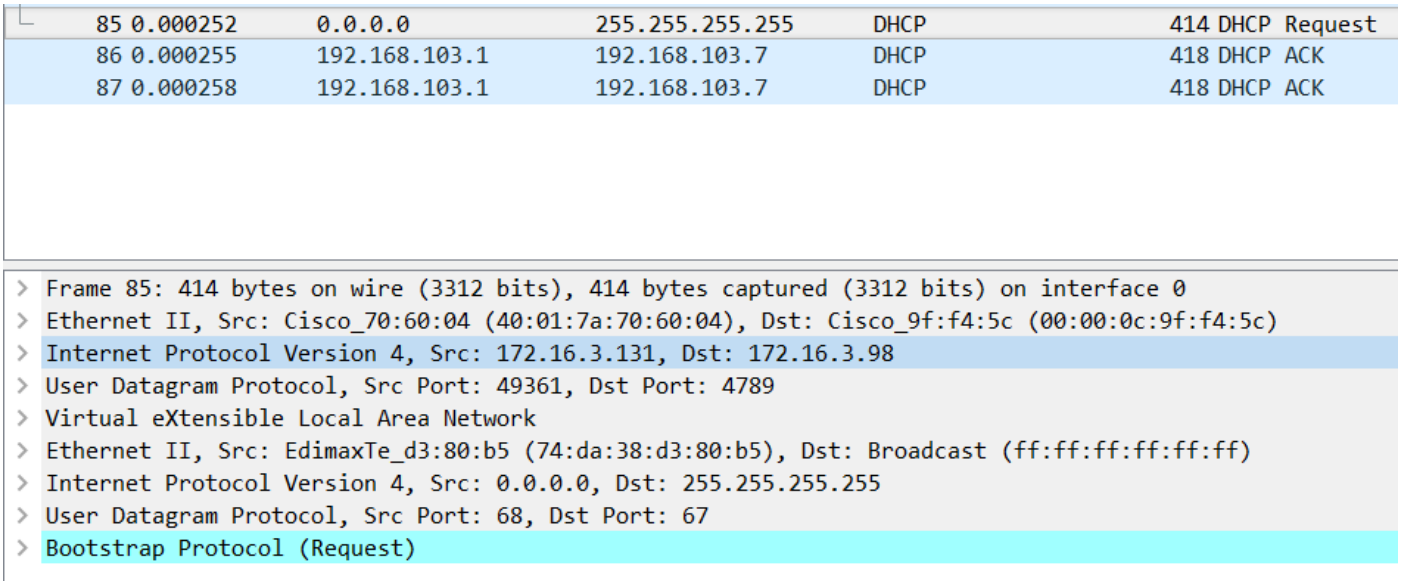
confronté à un problème de liste de contrôle d'accès ou de routage vers. Collectez les captures de paquets en cours de route pour voir où les paquets HTTP sont arrêtés.

# Comprendre

## Comment un client sans fil obtient-il une adresse IP dans l'architecture de fabric ?

La capture de paquets est effectuée entre le point d'accès du fabric et la périphérie du fabric. Les paquets sont dupliqués car deux paquets de détection DHCP ont été envoyés. Le trafic était uniquement en entrée et capturé sur la périphérie du fabric.

Il y a toujours deux paquets DHCP. Un message envoyé par CAPWAP directement au contrôleur pour le tenir à jour. L'autre est envoyé par VXLAN au noeud de contrôle. Lorsque l'AP reçoit par exemple une Offre DHCP avec VXLAN par le serveur DHCP, il envoie une copie au contrôleur avec CAPWAP.




Pour voir où le paquet a été envoyé, vous devez cliquer dessus sur Wireshark. Ici, nous pouvons voir la source est notre AP 172.16.3.131 et le paquet a été envoyé à la périphérie de fabric 172.16.3.98. La périphérie du fabric l'a transféré au noeud de contrôle.

## Comprendre le flux de redirection Web dans un scénario de fabric

La liste de contrôle d'accès de redirection sur le WLC définit quel trafic est redirigé/intercepté sur les instructions de refus correspondantes (il y a un refus implicite à la fin). Ce trafic à rediriger sera envoyé au WLC à l'intérieur de l'encapsulation CAPWAP pour le WLC à rediriger. Lors de la mise en correspondance d'une instruction permit, il ne redirige pas ce trafic et le laisse passer et le transfère sur le fabric (le trafic vers ISE entre dans cette catégorie).

## Journaux de l'AP joignant le WLC dans l'état activé par le fabric

Dès que le point d'accès s'enregistre auprès du WLC, le contrôleur enregistre son adresse IP et MAC dans le noeud de contrôle SDA (serveur de mappage LISP).

Le point d'accès rejoint le WLC en mode Fabric-enabled uniquement si le WLC reçoit le paquet LISP RLOC. Ce paquet est envoyé pour s'assurer que le point d'accès est connecté à une périphérie de fabric.

Les débogages utilisés sur le WLC pour cet exemple sont :

- **'debug capwap events enable'**
- **'debug capwap errors enable'**
- **'debug fabric ap-join events enable'**
- **'debug fabric ap-join detail enable'**
- **'debug fabric lisp map-server all enable'**

Pour le test, le point d'accès est redémarré :

<#root>

```
*spamApTask0: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for Aggregated Payloa
*msfMsgQueueTask: May 07 13:00:18.804: NAK list count becoming 0
*msfMsgQueueTask: May 07 13:00:18.804: NAK list count becoming 0
*msfMsgQueueTask: May 07 13:00:18.804: Cleaned up AP RLOC NAK entry for AP 172.16.3.131 vnid 4097 for B
*msfMsgQueueTask: May 07 13:00:18.804: Inserted entry for AP IP 172.16.3.131 and VNID 4097, db idx 12
*msfMsgQueueTask: May 07 13:00:18.804: Map-reply timer started for AP IP 172.16.3.131 and VNiD 4097
*msfMsgQueueTask: May 07 13:00:18.804: Creating new timer for AP IP 172.16.3.131 and VNID 4097
*msfMsgQueueTask: May 07 13:00:18.804: Map-reply Timer Started Successfully for AP IP 172.16.3.131 and
*msfMsgQueueTask: May 07 13:00:18.804: Not able to find nonce 0x3cd13556-0x81864b7b avl entry
*msfMsgQueueTask: May 07 13:00:18.804: FAIL: not able to find avl entry
*msfMsgQueueTask: May 07 13:00:18.804: Nonce 0x3cd13556-0x81864b7b inserted into nonce aVL tree for AP
*msfMsgQueueTask: May 07 13:00:18.804: Set nonce 0x3cd13556-0x81864b7b for AP 172.16.3.131 and VNID 409
*msfMsgQueueTask: May 07 13:00:18.804: Nonce 0x3cd13556-0x81864b7b is updated for AP IP 172.16.3.131, V
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for PHY payload s
*msfMsgQueueTask: May 07 13:00:18.804: Build and send map-request for AP IP 172.16.3.131 and VNID 4097
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for RrmInterferen
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for RrmInterferen
*msfMsgQueueTask: May 07 13:00:18.804: nonce = 3cd13556-81864b7b lisp_map_request_build allocating nonc
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for RrmNeighbourC
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for CcxRmMeas pay

*msfMsgQueueTask: May 07 13:00:18.804: Sending map-request for AP 172.16.3.131 VNID 4097 to MS 172.16.3.

*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for AP ext-loggin
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update for Delba sent to 172.16.

*msfMsgQueueTask: May 07 13:00:18.804: Map-request for AP IP 172.16.3.131 VNID 4097 to MS 172.16.3.254 i

*msfMsgQueueTask: May 07 13:00:18.804: Sent map-request to MS 172.16.3.254 for AP 172.16.3.131 VNID 4097

*msfMsgQueueTask: May 07 13:00:18.804: Invalid secondary MS IP 0.0.0.0 for map-request for AP IP 172.16
*msfMsgQueueTask: May 07 13:00:18.804: No messages are present in the Client list for Local UDP socket
*msfTcpTask: May 07 13:00:18.807: Sending the UDP control packet to queue task
*msfMsgQueueTask: May 07 13:00:18.807: msfQueue: recieved LISP_MAP_SERVER_UDP_PACKET_QUEUE_MSG
*msfMsgQueueTask: May 07 13:00:18.807: Mapping Record has locators and actions
*msfMsgQueueTask: May 07 13:00:18.807: Mapping record address 172.16.3.98 EID address 172.16.3.98
*msfMsgQueueTask: May 07 13:00:18.807: Got AVL entry for nonce 0x3cd13556-0x81864b7b in map-reply for A

*msfMsgQueueTask: May 07 13:00:18.807: Sent received RLOC IP 172.16.3.98 for AP 172.16.3.131 and VNID 40

*msfMsgQueueTask: May 07 13:00:18.807: Added RLOC 172.16.3.98 for AP IP 172.16.3.131

*spamReceiveTask: May 07 13:00:18.807: Recieved Fabric rloc response from msip 172.16.3.254 with apvnid
```

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.