Probleemoplossing en verifiëren SD-Access draadloze initiële setup

Inhoud

Inleiding

Dit artikel beschrijft de basisstappen voor probleemoplossing om fundamentele connectiviteitsproblemen in SD-Access draadloze instellingen te identificeren. Hierin worden de items en opdrachten beschreven die moeten worden gecontroleerd om problemen met de draadloze oplossing te isoleren.

Voorwaarden

Vereisten

Kennis van de SD-Access oplossing

Een reeds ingestelde SD-access topologie

Gebruikte componenten

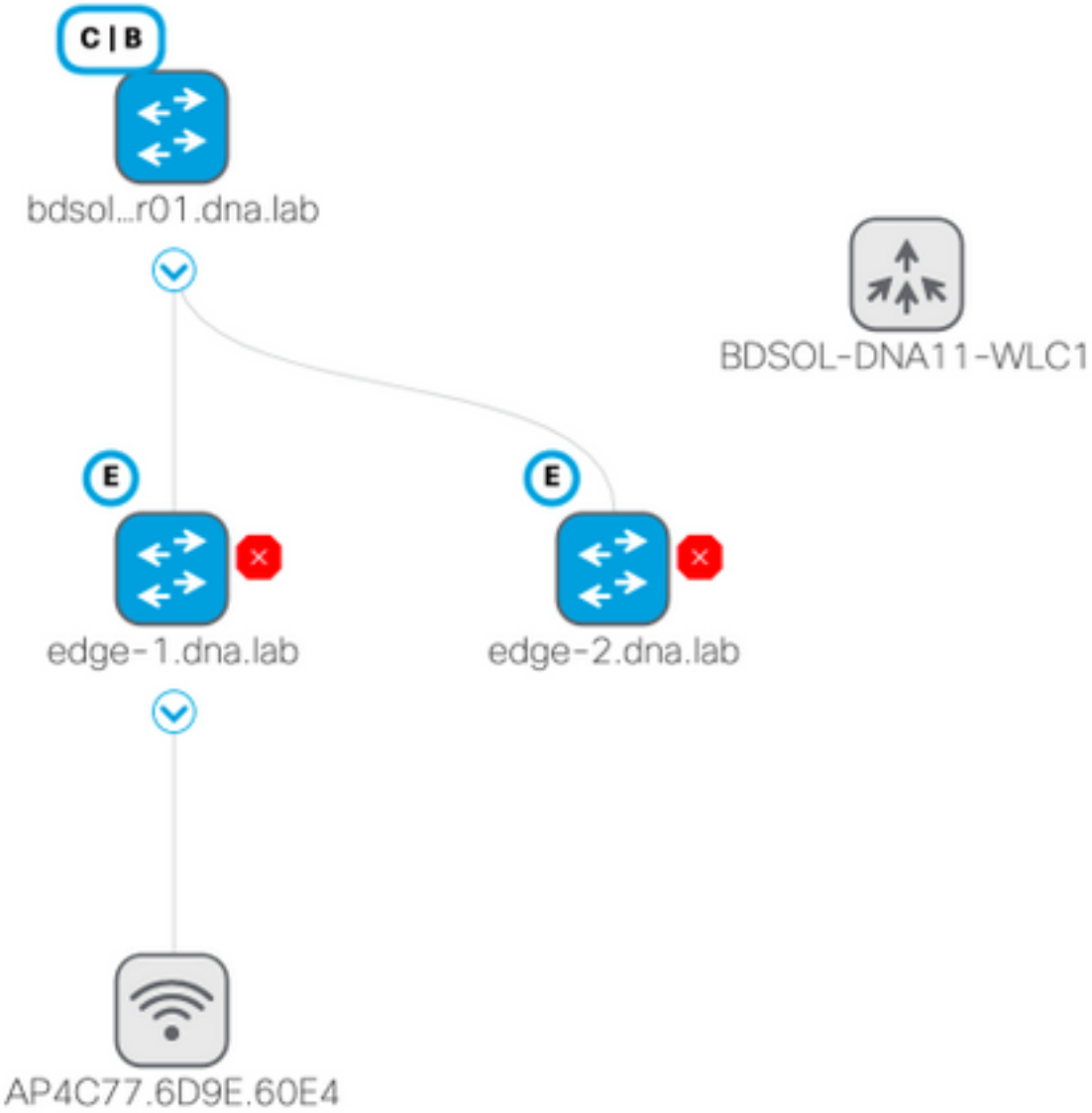
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële

impact van elke opdracht begrijpt. Er zijn andere soorten apparaten ondersteund voor SD-access draadloze, maar dit artikel richt zich op de apparaten beschreven in deze sectie. De opdrachten kunnen per platform en softwareversie verschillen.

8.5.151 draadloze controller

16.9.3 switch 9300 als randknooppunt

Topologie



Probleemoplossing en isoleren

Snelle verificatie

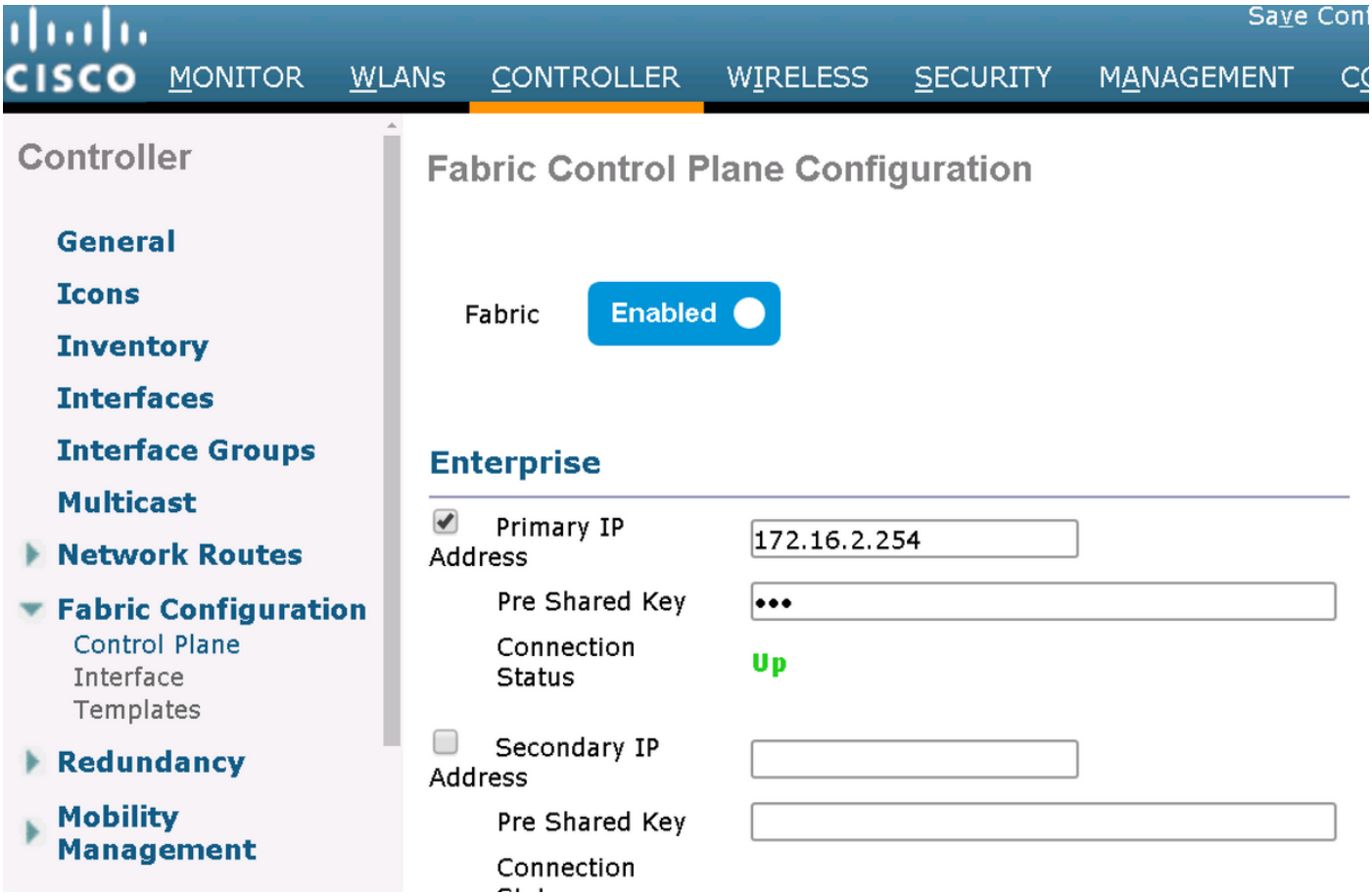
Er is een reeks vereisten in SD-access scenario's die vaak een bron van fouten is, dus verifieer eerst dat aan deze vereisten wordt voldaan:

- Zorg ervoor dat u een specifieke route hebt (en niet de standaardroute gebruiken) die aan

WLC op de LISP-besturingsvlakke knooppunt wijst
- Zorg ervoor dat uw AP's in de Infra VPN zijn, met behulp van de globale routeringstabel
- Zorg ervoor dat APs connectiviteit aan WLC door WLC van AP zelf te pingelen hebben
- Zorg ervoor dat de fabricstatus van het bedieningsvlak op de WLC omhoog is
- Zorg ervoor dat de toegangspunten zich in de voor het weefsel geschikte status bevinden

scenario 1. Controleer WLC registratie met het LISP/MAP server control vliegtuig

Wanneer u de WLC aan de stof in DNA Center toevoegt, worden de opdrachten naar de controller geduwd om een verbinding tot stand te brengen met de knoop die in DNA-C als controlevlak wordt gedefinieerd. De eerste stap is ervoor te zorgen dat deze registratie succesvol is. Als de LISP-configuratie op het besturingsplane op een of andere manier beschadigd is geraakt, kan deze registratie mislukken.



Als deze status zo laat zien, kan het interessant zijn om debugs uit te voeren of een pakketopname tussen de WLC en het besturingsplane. De registratie betreft zowel TCP als UDP op 4342. Als het besturingsplane niet de juiste configuratie kreeg, zou het met een TCP RST op TCP SYN kunnen antwoorden dat door de WLC wordt verzonden.

Dezelfde status kan worden geverifieerd met **toon fabric map-server samenvatting** op de opdrachtregel. Het proces wordt gedebuggd met **debug fabric lisp map-server alles** op de WLC CLI. Om een poging tot herverbinding uit te lokken, kunt u naar DNA Center gaan en ervoor kiezen om de WLC uit de stof te verwijderen en het opnieuw toe te voegen.

Mogelijke redenen ontbreken de configuratie lijnen in het besturingsplane. Hier is een voorbeeld dat werkt configuratie (het belangrijkste deel slechts):

```
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
```

Als de WLC ip ontbreekt (hier 10.241.0.41) of als de passief-open opdracht ontbreekt, zal de CP de WLC-verbinding weigeren.

De debugs die moeten worden uitgevoerd zijn :

- **'debug capwap events activeert'**
- **'debug capswapfouten activeren'**
- **'debug stof ap-connect gebeurtenissen activeren'**
- **'debug fabric ap-connect detail enabled'**
- **'debug fabric lisp map-server all enable'**

Hier is een voorbeeld van het besturingsplane dat de WLC niet beantwoordt

```
*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 list with path /tmp/msif_local_udp_socket_file failed
*osapiBsnTimer: May 07 14:08:15.179: Map-reply timer for MS IP 10.32.47.128 expired for AP IP
10.32.58.36 and VNID 4097
*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 list with path /tmp/msif_local_udp_socket_file failed
*spamApTask0: May 07 14:08:16.084: 00:fc:ba:15:95:00 WTP Event Request from 10.32.58.36:5248
epoch 1525694896
*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
```

Hier is een voorbeeld van de WLC debugs van een AP die zich aansluit in stof gehandicapte staat omdat de stof controle vliegtuig een specifieke route aan WLC mist

```
(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,c0a82700,ffffff00.Count 3

*emWeb: Oct 16 08:55:26.295:
                            Log to TACACS server(if online): fabric vnid create name
192_168_39_0-INFRA_VN l2-vnid 8191 ip 192.168.39.0 subnet 255.255.255.0 l3-vnid 4097

*spamReceiveTask: Oct 16 08:55:26.295: Fabric is supported for AP f4:db:e6:61:24:a0 (Pod3-
AP4800). apType 54
```

```
*spamReceiveTask: Oct 16 08:55:26.295: spamProcessFabricVnidMappingAddRequest: Fabric Adding
vnid mapping for AP Pod3-AP4800 f4:db:e6:61:24:a0,lradIp 192.168.39.100,AP l2_vnid 0, AP l3_vnid
0
*spamReceiveTask: Oct 16 08:55:26.295: Vnid Mapping return from index 2 with entries name
192_168_39_0-INFRA_VN,l2vnid 8191,l3vnid 4097,ip c0a82700,mask ffffff00.Count 3

*spamReceiveTask: Oct 16 08:55:26.295: spamSendFabricMapServerRequest: MS request from AP Pod3-
AP4800 f4:db:e6:61:24:a0,l3vnid 4097,PMS 192.168.30.55,SMS 0.0.0.0,mwarIp 192.168.31.59,lradIp
192.168.39.100
*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-AP3800). apType 52,apModel AIR-AP3802I-B-K9.

*spamApTask6: Oct 16 08:56:51.949: Fabric is supported for AP f4:db:e6:64:02:a0 (Pod3-AP3800).
apType 52,apModel AIR-AP3802I-B-K9.

*spamApTask6: Oct 16 08:56:51.953: Fabric is supported for AP f4:db:e6:64:02:a0 (Pod3-AP3800).
apType 52,apModel AIR-AP3802I-B-K9.

*spamApTask6: Oct 16 08:56:51.953: Fabric is supported for AP f4:db:e6:64:02:a0 (Pod3-AP3800).
apType 52,apModel AIR-AP3802I-B-K9.

*spamApTask6: Oct 16 08:56:51.953: spamSendFabricMapServerRequest: MS request from AP Pod3-
AP3800 f4:db:e6:64:02:a0 can not be sent ,AP vnid mapping does not exist
```

Het is interessant om op te merken dat als er twee besturingsplanes in uw netwerk van de stof zijn, de WLC altijd naar zowel voor registratie als vragen zal reiken. Verwacht wordt dat beide besturingsplane positieve antwoorden geven op registraties, zodat de WLC AP's niet zal registreren in de stof als een van de twee besturingsplane het om welke reden dan ook verwerpt. Eén bedieningsvlak dat niet beantwoordt, is echter aanvaardbaar en het resterende bedieningsvlak wordt gebruikt.

APs bereiken uit aan WLC door de globale routeringstabel, maar LISP wordt nog steeds gebruikt om WLC op te lossen. Het verkeer dat door AP's naar de WLC wordt verzonden is pure CAPWAP-controle (geen VLAN betrokken), maar het retourverkeer dat door de WLC naar de AP wordt verzonden zal over Vxlan op de overlay worden overgebracht. U zult niet in staat zijn om connectiviteit van de AP-gateway SVI aan de rand naar de WLC te testen omdat aangezien het een Anycast-gateway is, dezelfde IP ook bestaat op het grensknooppunt. Om connectiviteit te testen, is het beste van AP zelf te pingelen.

scenario 2. Access points krijgen geen IP-adres

Access points krijgen een IP-adres van de AP Poo, in de Infra VPNI gedefinieerd in DNA Center. Als dit niet gebeurt, betekent dit meestal dat de switchport waar de AP is aangesloten niet naar het juiste VLAN is verplaatst. De switch zal bij het detecteren (via CDP) van een toegangspunt dat wordt aangesloten een switchport-macro toepassen die de switchport in het VLAN instelt dat door DNA-C is gedefinieerd voor de AP-pool. Als de problematische switchport inderdaad niet met de macro is geconfigureerd, kunt u de configuratie handmatig instellen (zodat de AP een ip krijgt, zich aansluit bij de WLC en waarschijnlijk zijn code verbetert en mogelijk een CDP bug oplost) of het CDP-verbindingsproces oplossen. U kunt host-onboarding naar keuze configureren om de poort op DNA-Center op statische wijze te definiëren om een AP te hosten, zodat deze is voorzien van de juiste configuratie.

Smartport-macro's worden niet automatisch ingeschakeld als de switch niet ten minste met één

AP is voorzien, u kunt verifiëren of de AP-macro is voorzien van het juiste VLAN (in plaats van de standaard VLAN 1)

```
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
```

De opdrachten die Cisco DNA-C ingedrukt houdt om deze in te stellen, zijn

```
macro auto execute CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT builtin CISCO_LWAP_AUTO_SMARTPORT
ACCESS_VLAN=2045
macro auto global processing
```

scenario 3. Access points hebben geen VLAN-tunnel naar hun Fabric Edge-knooppunt

Zodra een AP zich bij de WLC aansluit, zal de WLC (als de AP geschikt voor stof is) de AP op het besturingsplane registreren als een speciaal type client. Het besturingsplane zal vervolgens de Fabric Edge-knooppunt opvragen waar de AP is aangesloten om een VLAN-tunnel naar de AP te bouwen.

AP zal slechts vxlan inkapseling gebruiken om cliëntverkeer (en slechts voor cliënten in de staat van de LOOPPAS) te verzenden, daarom is het normaal om geen vxlan informatie te zien over AP tot een stoffenclient verbindt.

Op het toegangspunt zal de opdracht **ip-tunnelstof** tonen de vxlan-tunnelinformatie zodra een client verbinding heeft gemaakt.

```
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 Bytes-out
        1    172.16.2.253 00:00:0C:9F:F4:5E           Forward      VXLAN     39731  4209554
16345   2087073
AP4001.7A03.5736#
```

Voor de knoop van de Rand van de Fabric, zal het bevel **toegang-tunnel samenvatting** tonen de VLAN tunnels die naar de toegangspunten worden gebouwd. De tunnels zullen worden getoond zodra het besturingsplane opdracht gaf tot hun creatie wanneer de AP toetreedt.

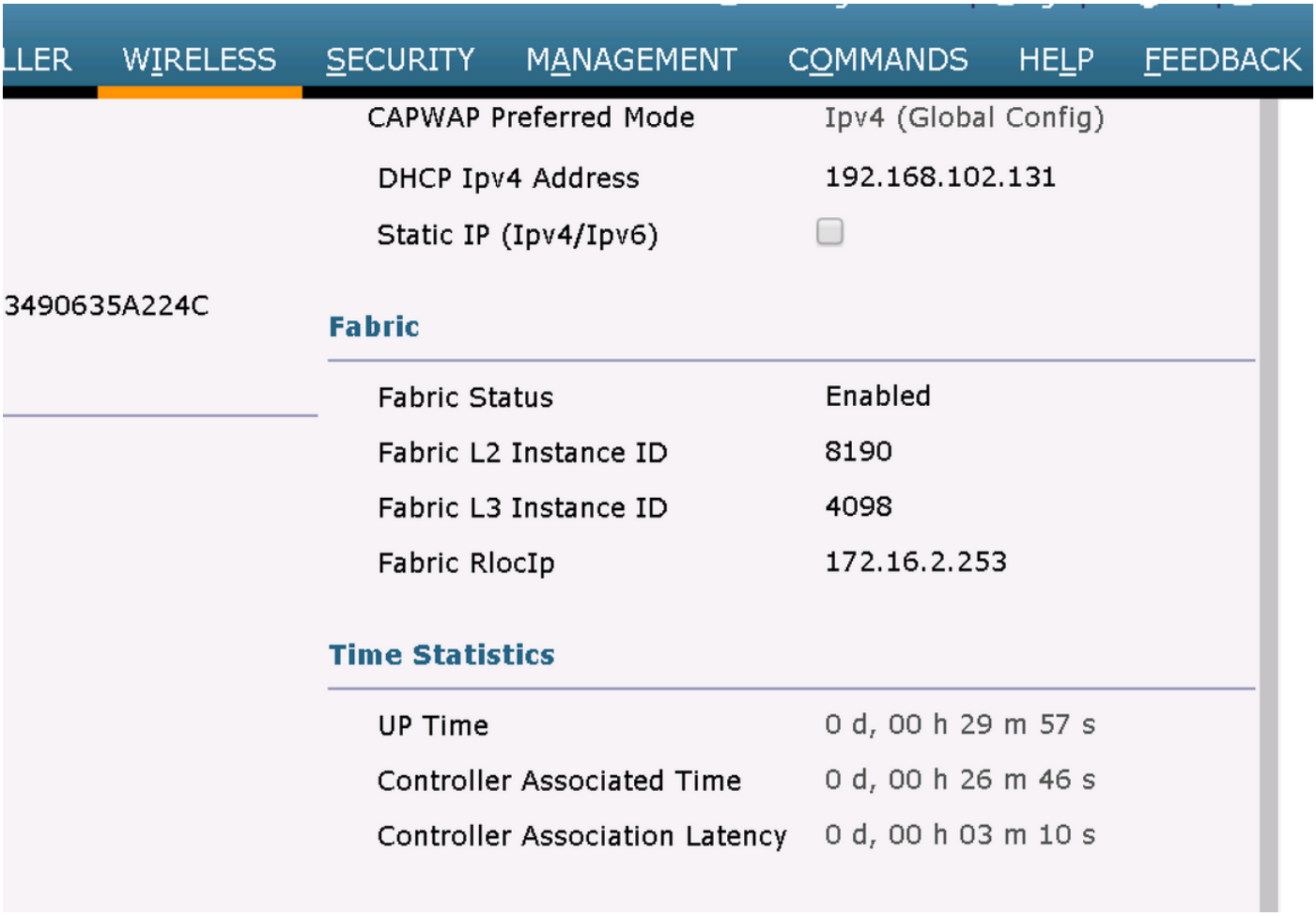
```
edge01#show access-tunnel summ

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
```

U kunt de WLC, op de pagina van het toegangspunt, de L2 LISP-instantienummer controleren die overeenkomt met dat AP en vervolgens de statistieken van die instantie controleren op de Fabric Edge waar deze is aangesloten.




```
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
```

scenario 4. toegangstunnelvermeldingen die na enige tijd ontbreken

Het is mogelijk dat de toegangstunnels met succes de eerste keer worden gemaakt wanneer WLC door Cisco DNA-C wordt geleverd en aan de stof wordt toegevoegd, maar wanneer het opnieuw provisioneren van draadloze configuratie (zoals de WLAN-configuratie) wordt waargenomen dat de toegangstunnelingangen voor AP's missen resulterende draadloze clients niet in staat zijn om IP met succes te verkrijgen.

De topologie is 9500(CP) —> 9300 (Edge) —> AP —> Draadloze client.

De ingangen worden correct geobserveerd in **tonen toegang-tunnel samenvatting** op de randknoop:

```
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
```

Maar bij het controleren **van de toegangstunnel van de switch van de platformsoftware gevoede actieve ifm interfaces, ontbreekt de ingang voor AP of slaagt er niet om in de hardware in dit voorbeeld worden geprogrammeerd.**

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

Voor meer output:

```
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
```

Je moet de verschillende outputs vergelijken en elke tunnel die wordt getoond door de **show access-tunnelsamenvatting** moet in elk van hen aanwezig zijn.

scenario 5. draadloze clients kunnen geen IP-adres verkrijgen

Als de vxlan tunnel aanwezig is en alles ziet er goed uit, maar de draadloze clients zijn systematisch niet in staat om een IP-adres te verkrijgen, bent u misschien geconfronteerd met een optie 82 probleem. Aangezien de DHCP-ONTDEKKING van de client wordt doorgestuurd door de Anycast-gateway op het edge-knooppunt, zou er een probleem zijn voor de DHCP-server OFFER om naar het rechter edge-knooppunt te worden gestuurd door de rand op de terugweg. Dit is de reden waarom de fabric edge die de DHCP Discover doorstuurt een optie 82 veld aan de DHCP ONTDEKT dat de werkelijke fabric RLOC (loopback ip) bevat van de edge knooppunt gecodeerd samen met andere informatie. Dit betekent dat uw DHCP-server optie 82 moet ondersteunen.

Als u het DHCP-proces wilt oplossen, neemt u opnamen op de fabric-knooppunten (met name de client edge-knooppunten) om te verifiëren dat de fabric-rand het optie 82-veld toevoegt.

scenario 6. Gaststof / web authenticatie werkt niet / niet omleiden van clients

Het gastenfabric-scenario is zeer vergelijkbaar met Central Web Verification (CWA) op Flexconnect access points en werkt precies op dezelfde manier (zelfs als de stof AP's niet in flexconnect modus staan).

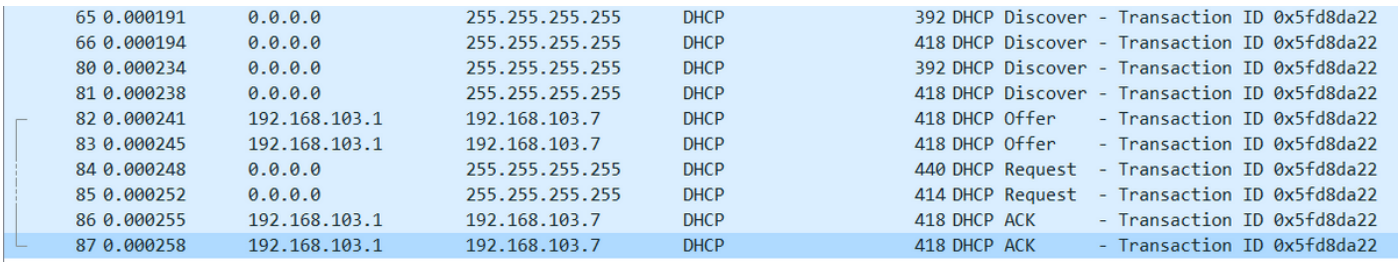
De omleidingsACL en URL moeten door ISE worden geretourneerd in het eerste mac-verificatieresultaat. Controleer die in de ISE-logboeken evenals de pagina met clientdetails op de WLC.

Omleiden ACL moet als Flex ACL op WLC aanwezig zijn en moet "vergunning"verklaringen naar het adres van ISE IP op haven 8443 (minstens) bevatten.

De client moet in "CENTRAL_WEBAUTH_REQ" staat op de client details pagina op de WLC. De client zal niet in staat zijn om zijn standaardgateway te pingen en dit wordt verwacht. Als u niet wordt doorgestuurd kunt u proberen om handmatig een IP-adres in de client web browser (om DNS uit te sluiten, maar ISE hostname zal hoe dan ook moeten worden opgelost). U moet de ISE IP op poort 8443 in de clientbrowser kunnen invoeren en de portaalpagina zien, aangezien deze stroom niet wordt omgeleid. Als dit niet gebeurt, wordt u of geconfronteerd met een ACL-kwestie of een routeringskwestie naar. Verzamel pakketopnamen langs de weg om te zien waar de HTTP-pakketten worden gestopt.

begrijpen

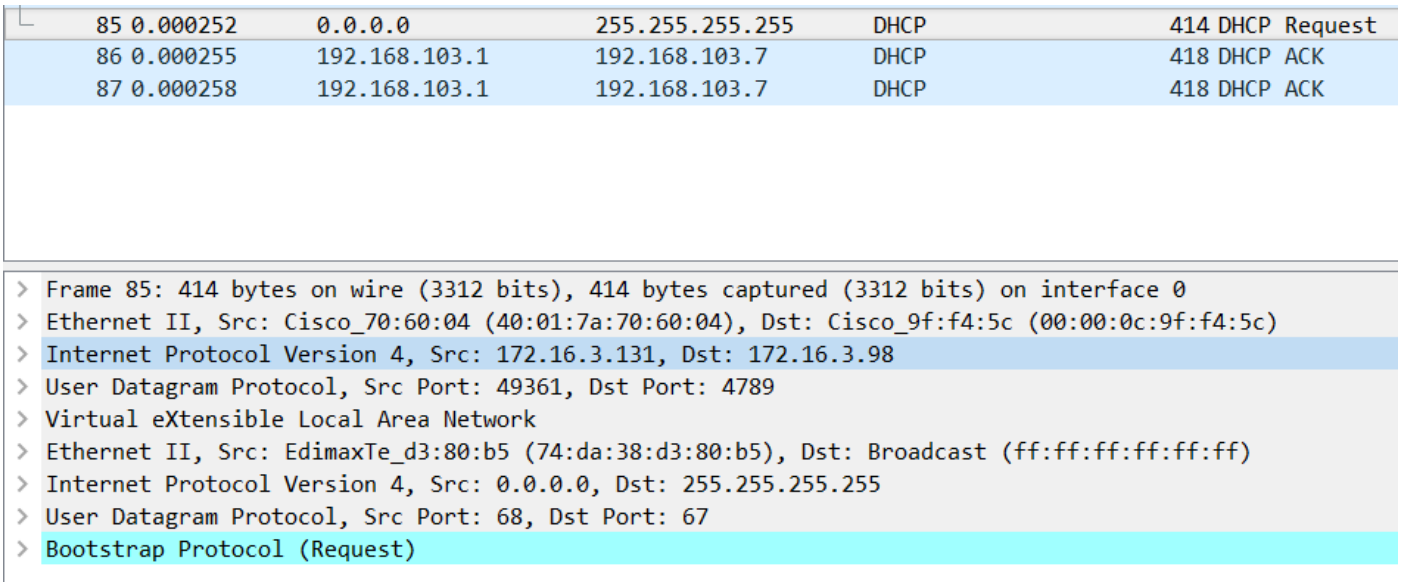
Hoe krijgt een draadloze client een IP-adres in Fabric Architecture



65	0.000191	0.0.0.0	255.255.255.255	DHCP	392	DHCP Discover - Transaction ID 0x5fd8da22
66	0.000194	0.0.0.0	255.255.255.255	DHCP	418	DHCP Discover - Transaction ID 0x5fd8da22
80	0.000234	0.0.0.0	255.255.255.255	DHCP	392	DHCP Discover - Transaction ID 0x5fd8da22
81	0.000238	0.0.0.0	255.255.255.255	DHCP	418	DHCP Discover - Transaction ID 0x5fd8da22
82	0.000241	192.168.103.1	192.168.103.7	DHCP	418	DHCP Offer - Transaction ID 0x5fd8da22
83	0.000245	192.168.103.1	192.168.103.7	DHCP	418	DHCP Offer - Transaction ID 0x5fd8da22
84	0.000248	0.0.0.0	255.255.255.255	DHCP	440	DHCP Request - Transaction ID 0x5fd8da22
85	0.000252	0.0.0.0	255.255.255.255	DHCP	414	DHCP Request - Transaction ID 0x5fd8da22
86	0.000255	192.168.103.1	192.168.103.7	DHCP	418	DHCP ACK - Transaction ID 0x5fd8da22
87	0.000258	192.168.103.1	192.168.103.7	DHCP	418	DHCP ACK - Transaction ID 0x5fd8da22

Packet Capture wordt tussen het fabric-toegangspunt en de Fabric Edge genomen. Pakketten worden gedupliceerd omdat twee DHCP Discover-pakketten zijn verzonden. Het verkeer kwam alleen binnen en werd opgenomen op de Fabric Edge.

Er zijn altijd twee DHCP-pakketten. Een die door CAPWAP rechtstreeks naar de controller wordt gestuurd om het bij te houden. De andere studie wordt door VXLAN naar het Control Node verzonden. Wanneer het toegangspunt bijvoorbeeld een DHCP-aanbieding met VXLAN ontvangt van de DHCP-server, stuurt het een kopie naar de controller met CAPWAP.



Om te zien waar het pakket werd verzonden, moet u op het op Wireshark klikken. Hier kunnen we zien dat de bron onze AP 172.16.3.131 is en het pakket werd verzonden naar de Fabric Edge 172.16.3.98. De Fabric Edge heeft deze doorgestuurd naar het Control Node.

Begrijp de webomleidingsstroom in een fabric scenario

Redirect ACL op WLC bepaalt welk verkeer wordt opnieuw gericht/bij de aanpassing van ontkennen verklaringen (er is impliciet ontkennen aan het eind) wordt onderschept. Dat verkeer dat zal worden opnieuw gericht zal naar WLC binnen capwap inkapseling voor WLC worden verzonden om opnieuw te richten. Bij het matchen van een vergunningsverklaring wordt dat verkeer niet omgeleid en laat het door en door het op de stof (verkeer naar ISE komt in deze categorie).

Logbestanden van de AP die zich bij de WLC aansluiten in een toestand die door het weefsel wordt ingeschakeld

Zodra Access-Point zich registreert bij WLC, zal de controller zijn IP- en MAC-adres registreren in SDA Control Node (LISP Map Server).

De AP sluit zich alleen aan bij de WLC in fabric-enabled-modus als de WLC het LISP RLOC-pakket ontvangt. Dit pakket is verzonden om er zeker van te zijn dat het toegangspunt is verbonden met een Fabric Edge.

De debugs die in dit voorbeeld op de WLC worden gebruikt zijn:

- **'debug capwap events activeert'**
- **'debug capswapfouten activeren'**

- **'debug stof ap-connect gebeurtenissen activeren'**
- **'debug fabric ap-connect detail enabled'**
- **'debug fabric lisp map-server all enable'**

Voor de test wordt het toegangspunt opnieuw opgestart:

```
*spamApTask0: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for Aggregated
Payload 3 sent to 172.16.3.131:5256
*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 BOTH MS
*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 VNID 4097
*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 IP 172.16.3.131 VNID 4097 for MS 172.16.3.254
*msfMsgQueueTask: May 07 13:00:18.804: Set nonce 0x3cd13556-0x81864b7b for AP 172.16.3.131 and
VNID 4097
*msfMsgQueueTask: May 07 13:00:18.804: Nonce 0x3cd13556-0x81864b7b is updated for AP IP
172.16.3.131, VNID 4097 and MS IP 172.16.3.254, db idx 12
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for PHY
payload sent to 172:16:3:131
*msfMsgQueueTask: May 07 13:00:18.804: Build and send map-request for AP IP 172.16.3.131 and
VNID 4097 to MS IP 172.16.3.254
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for
RrmInterferenceCtrl payload sent to 172:16:3:131
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for
RrmInterferenceCtrl payload sent to 172:16:3:131
*msfMsgQueueTask: May 07 13:00:18.804: nonce = 3cd13556-81864b7b lisp_map_request_build
allocating nonce
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for
RrmNeighbourCtrl payload sent to 172.16.3.131
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for
CcxRmMeas payload sent to 172.16.3.131
*msfMsgQueueTask: May 07 13:00:18.804: Sending map-request for AP 172.16.3.131 VNID 4097 to MS
172.16.3.254
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for AP
ext-logging AP ext-logging message sent to 172.16.3.131:5256
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update for Delba sent to
172.16.3.131:5256
*msfMsgQueueTask: May 07 13:00:18.804: Map-request for AP IP 172.16.3.131 VNID 4097 to MS
172.16.3.254 is sent
*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
172.16.3.131
*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 AP IP 172.16.3.131
```

```
*msfMsgQueueTask: May 07 13:00:18.807: Sent received RLOC IP 172.16.3.98 for AP 172.16.3.131 and
VNID 4097 in map-reply to spam task
*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 4097,fabricRLoc 172.16.3.98 apip 172.16.3.131 apRadMac 70:70:8b:20:29:00
```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.