Fehlerbehebung und Überprüfung der ursprünglichen Einrichtung des SD-Access Wireless-Netzwerks

Inhalt

Einleitung

In diesem Artikel werden die grundlegenden Schritte zur Fehlerbehebung beschrieben, um grundlegende Verbindungsprobleme in SD-Access Wireless-Konfigurationen zu identifizieren. Es beschreibt die Elemente und Befehle, die überprüft werden müssen, um Probleme in der Wireless-Lösung zu isolieren.

Voraussetzungen

Anforderungen

Kenntnis der SD-Access-Lösung

Eine bereits eingerichtete SD-Zugriffstopologie

Verwendete Komponenten

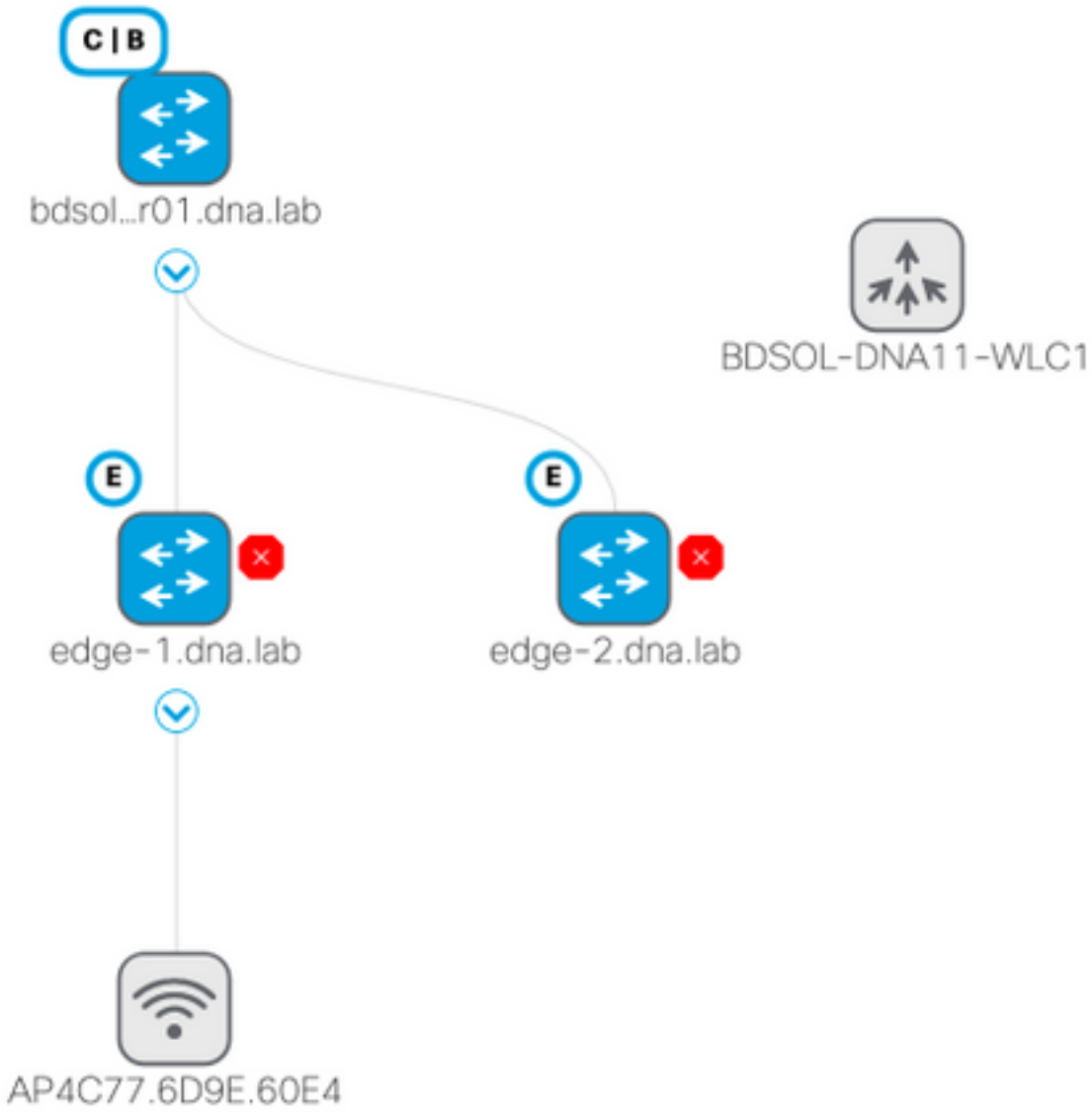
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten

Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen. Es gibt andere Gerätetypen, die für SD-Wireless-Zugriff unterstützt werden, aber dieser Artikel konzentriert sich auf die in diesem Abschnitt beschriebenen Geräte. Die Befehle können je nach Plattform und Softwareversion variieren.

8.5.151 Wireless-Controller

16.9.3 9300 Switch als Edge-Knoten

Topologie



Fehlerbehebung und Isolierung

Schnelle Überprüfungen

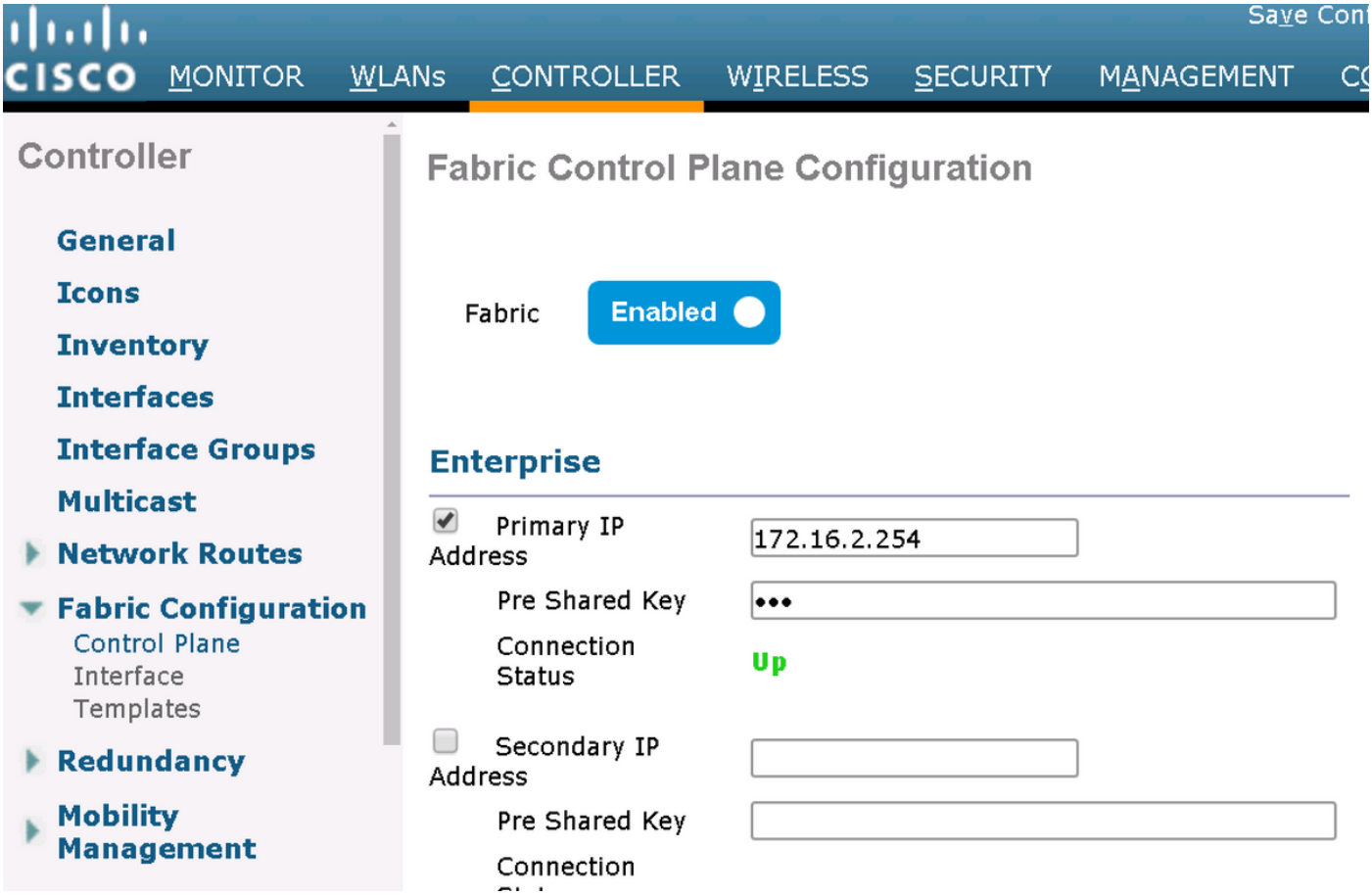
In Szenarien mit SD-Zugriff gibt es eine Reihe von Anforderungen, die häufig eine Fehlerquelle

darstellen. Stellen Sie daher zunächst sicher, dass diese Anforderungen erfüllt sind:

- Vergewissern Sie sich, dass eine bestimmte Route (die nicht die Standardroute verwendet) zum WLC auf dem LISP-Steuerungsebenenknoten verläuft.
- Vergewissern Sie sich mithilfe der globalen Routing-Tabelle, dass sich Ihre APs im Infra VN befinden.
- Stellen Sie sicher, dass die APs über eine Verbindung zum WLC verfügen, indem Sie den WLC vom AP aus pingen.
- Sicherstellen, dass der Fabric-Status der Kontrollebene auf dem WLC aktiv ist
- Stellen Sie sicher, dass sich die APs im Fabric-aktivierten Zustand befinden.

szenario 1. Überprüfen der WLC-Registrierung auf der LISP-/MAP-Server-Kontrollebene

Wenn Sie den WLC zum Fabric im DNA-Center hinzufügen, werden Befehle an den Controller gesendet, um eine Verbindung zu dem Knoten herzustellen, der als Kontrollebene in DNA-C definiert ist. Der erste Schritt besteht darin, sicherzustellen, dass diese Registrierung erfolgreich ist. Wenn die LISP-Konfiguration auf der Steuerungsebene beschädigt wurde, kann diese Registrierung fehlschlagen.



Wenn dieser Status als ausgefallen angezeigt wird, ist es möglicherweise interessant, zwischen dem WLC und der Kontrollebene Debug-Vorgänge oder eine Paketerfassung auszuführen. Die Registrierung bezieht sich auf TCP und UDP auf 4342. Wenn die Kontrollebene nicht die richtige Konfiguration erhält, antwortet sie möglicherweise mit einer TCP-RST auf das vom WLC gesendete TCP-SYN.

Derselbe Status kann mithilfe von **show fabric map-server summary** in der Befehlszeile überprüft

werden. Der Prozess wird mit **debug fabric lisp map-server** auf der WLC-CLI debuggt. Um einen erneuten Verbindungsversuch zu provozieren, können Sie zum DNA Center gehen und den WLC aus dem Gewebe entfernen und ihn erneut hinzufügen.

Mögliche Gründe sind fehlende Konfigurationszeilen auf der Kontrollebene. Hier ist ein Beispiel für eine funktionierende Konfiguration (nur der wichtigste Teil):

```
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
```

Wenn die WLC-IP fehlt (hier 10.241.0.41) oder der Befehl "passiv-open" fehlt, lehnt der CP die WLC-Verbindung ab.

Die auszuführenden Debugs sind:

- **'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"**

Hier ist ein Beispiel dafür, wie die Kontrollebene den WLC nicht beantwortet.

```
*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
```

Im Folgenden finden Sie ein Beispiel für die WLC-Fehlerbehebung eines Access Points, der im deaktivierten Zustand der Fabric beitritt, weil der Fabric-Kontrollebene eine bestimmte Route zum WLC fehlte.

```
(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
```

Wenn Ihr Fabric-Netzwerk über zwei Kontrollebenen verfügt, wendet sich der WLC bei Registrierungen oder Fragen stets an beide. Es wird erwartet, dass beide Kontrollebenen bei Registrierungen positive Antworten geben, sodass der WLC die APs in der Fabric nicht registrieren kann, wenn eine der beiden Kontrollebenen die Registrierung aus irgendeinem Grund ablehnt. Eine nicht antwortende Kontrollebene kann jedoch verwendet werden, und die verbleibende Kontrollebene wird verwendet.

APs wenden sich über die globale Routing-Tabelle an den WLC, aber LISP wird nach wie vor zur Auflösung des WLC verwendet. Der von den APs an den WLC gesendete Datenverkehr stellt eine reine CAPWAP-Steuerung dar (keine VXLANs beteiligt). Der vom WLC an den AP gesendete Datenrückverkehr wird jedoch über VXLAN auf dem Overlay übertragen. Sie können die Verbindung vom AP-Gateway SVI am Edge zum WLC nicht testen, da es sich um ein Anycast-Gateway handelt und die gleiche IP auch am Grenzknoten vorhanden ist. Um die Verbindung zu testen, ist es am besten, vom Access Point aus zu pingen.

szenario 2. Access Points erhalten keine IP-Adresse.

Es wird erwartet, dass die Access Points eine IP-Adresse vom AP-Pool im Infra-VNI erhalten, das im DNA-Center definiert ist. Geschieht dies nicht, wird der Switch-Port, an dem der AP angeschlossen ist, normalerweise nicht in das richtige VLAN verschoben. Wenn der Switch erkennt, dass (über CDP) ein Access Point verbunden ist, wendet er ein Switch-Port-Makro an,

das den Switch-Port in das VLAN setzt, das durch DNA-C für den AP-Pool definiert ist. Wenn der problematische Switch-Port nicht mit dem Makro konfiguriert ist, können Sie die Konfiguration entweder manuell festlegen (sodass der AP eine IP erhält, dem WLC beitritt und wahrscheinlich seinen Code aktualisiert und möglicherweise einen CDP-Fehler behebt) oder den CDP-Verbindungsprozess beheben. Optional können Sie das Host-Onboarding so konfigurieren, dass der Port im DNA-Center zum Hosten eines AP statisch definiert wird, sodass dieser mit der richtigen Konfiguration bereitgestellt wird.

Smartport-Makros werden nicht automatisch aktiviert, wenn der Switch nicht mit mindestens einem Access Point ausgestattet war. Sie können überprüfen, ob das Access Point-Makro mit dem richtigen VLAN ausgestattet wurde (anstatt mit dem Standard-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
```

Die von Cisco DNA-C hierfür bereitgestellten Befehle sind:

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

szenario 3. Access Points verfügen nicht über einen zu ihrem Fabric Edge-Knoten aufgebauten VXLAN-Tunnel

Sobald ein AP dem WLC beitritt, registriert der WLC den AP (sofern der AP Fabric-fähig ist) auf der Kontrollebene als speziellen Client-Typ. Die Kontrollebene fordert dann den Fabric Edge-Knoten an, an den der AP angeschlossen ist, um einen VXLAN-Tunnel zum AP zu erstellen.

Der WAP verwendet nur die VXLAN-Kapselung zum Senden von Client-Datenverkehr (und nur für Clients im RUN-Zustand). Daher werden VXLAN-Informationen auf dem WAP normalerweise erst angezeigt, wenn ein Fabric-Client eine Verbindung herstellt.

Auf dem AP zeigt der Befehl **show ip tunnel fabric** die VXLAN-Tunnelinformationen an, sobald ein Client eine Verbindung hergestellt hat.

```
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#
```

Auf dem Fabric Edge-Knoten zeigt der Befehl **show access-tunnel summary** die zu den Access Points aufgebauten VXLAN-Tunnel an. Die Tunnel werden angezeigt, sobald die Kontrollebene ihre Erstellung beim Beitritt des Access Points angeordnet hat.

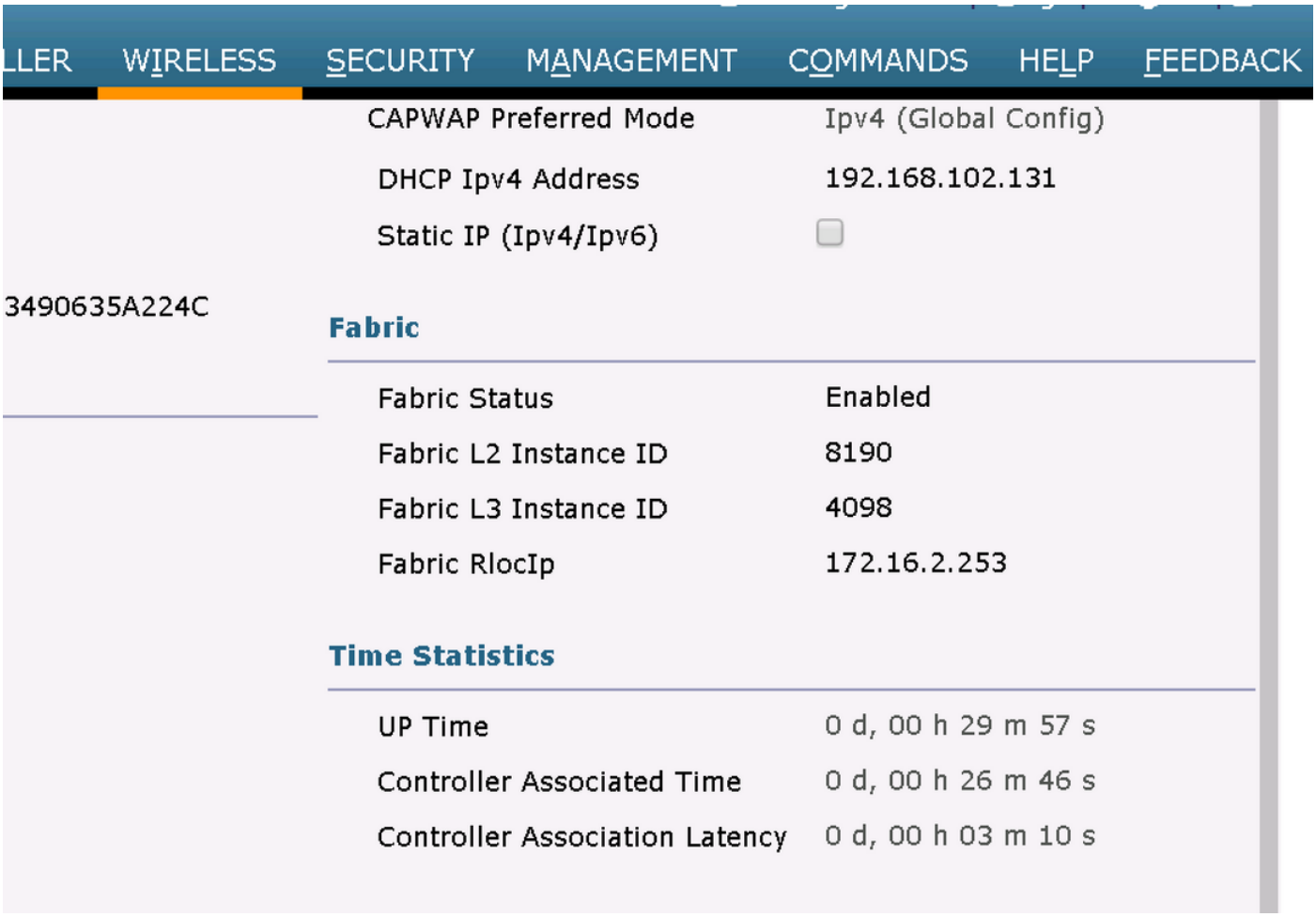
```
edge01#show access-tunnel summ
```

```
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
```

Sie können auf dem WLC auf der Seite für den Access Point die L2-LISP-Instanz-ID für diesen AP überprüfen und dann die Statistiken dieser Instanz am Fabric Edge überprüfen, mit dem sie verbunden ist.




```
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
```

Szenario 4. Nach einer Weile fehlen die Zugriffstunneleinträge

Es ist möglich, dass die Zugriffstunnel beim ersten Mal erfolgreich erstellt werden, wenn der WLC über Cisco DNA-C bereitgestellt und der Fabric hinzugefügt wird. Beim erneuten Bereitstellen der Wireless-Konfiguration (wie bei der WLAN-Konfiguration) stellt sich jedoch heraus, dass Zugriffstunnel-Einträge für APs fehlen, was dazu führt, dass die Wireless-Clients IP nicht erfolgreich erhalten können.

Die Topologie ist 9500(CP) —> 9300(Edge) —> AP —> Wireless Client.

Die Einträge werden in der **Übersicht zum Zugriffstunnel anzeigen** am Edge-Knoten korrekt angezeigt:

```
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
```

Beim Überprüfen von **show platform software fed switch active ifm interfaces access-tunnel fehlt in diesem Beispiel der Eintrag für den Access Point oder wurde in der Hardware nicht programmiert.**

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

Weitere Informationen:

```
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
```

Sie müssen die verschiedenen Ausgänge vergleichen und jeder Tunnel, der durch die **show access-tunnel summary** angezeigt wird, muss in jedem von ihnen vorhanden sein.

Szenario 5. Wireless-Clients können keine IP-Adresse abrufen.

Wenn der VXLAN-Tunnel vorhanden ist und alles gut aussieht, aber die Wireless-Clients systematisch keine IP-Adresse abrufen können, haben Sie möglicherweise ein Problem mit Option 82. Da die DHCP DISCOVER des Clients vom Anycast Gateway auf dem Edge-Knoten weitergeleitet wird, könnte es beim Rückweg zu Problemen kommen, wenn der DHCP-Server OFFER an den rechten Edge-Knoten über die Grenze gesendet wird. Aus diesem Grund fügt der Fabric-Edge, der den DHCP DISCOVER weiterleitet, ein Feld der Option 82 an den DHCP DISCOVER an, das den tatsächlichen Fabric-RLOC (Loopback-IP) des Edge-Knotens enthält, der zusammen mit anderen Informationen verschlüsselt ist. Das bedeutet, dass Ihr DHCP-Server Option 82 unterstützen muss.

Zur Fehlerbehebung beim DHCP-Prozess führen Sie auf den Fabric-Knoten (insbesondere dem Client-Edge-Knoten) Erfassungen durch, um zu überprüfen, ob der Fabric-Edge das Feld für die Option 82 anhängt.

szenario 6. Guest Fabric/Web-Authentifizierung funktioniert nicht/Clients werden nicht umgeleitet

Das Gast-Fabric-Szenario ähnelt stark der zentralen Webauthentifizierung (CWA) auf Flexconnect Access Points und funktioniert genauso (auch wenn sich die Fabric-APs nicht im Flexconnect-Modus befinden).

Die Umleitungs-ACL und die URL müssen von der ISE im ersten MAC-Authentifizierungsergebnis zurückgegeben werden. Überprüfen Sie die Einträge in den ISE-Protokollen und auf der Client-Detailseite des WLC.

Die Umleitungs-ACL muss als Flex-ACL auf dem WLC vorhanden sein und (mindestens) "permit"-Anweisungen zur ISE-IP-Adresse an Port 8443 enthalten.

Der Client muss sich im Status "CENTRAL_WEBAUTH_REQ" auf der Client-Detailseite des WLC befinden. Der Client kann keinen Ping an sein Standard-Gateway senden. Dies wird erwartet. Wenn Sie nicht umgeleitet werden, können Sie versuchen, manuell eine IP-Adresse in den Client-Webbrowser einzugeben (um DNS auszuschließen, aber ISE-Hostname muss trotzdem aufgelöst werden). Sie sollten die ISE-IP auf Port 8443 im Client-Browser eingeben können und die Portalseite sehen, da dieser Fluss nicht umgeleitet wird. Wenn dies nicht geschieht, liegt entweder ein Problem mit der Zugriffskontrollliste oder ein Routing-Problem in Richtung vor. Sammeln Sie auf dem Weg erfasste Pakete, um festzustellen, wo die HTTP-Pakete gestoppt werden.

Verstehen

Wie erhält ein Wireless-Client eine IP-Adresse in der Fabric-Architektur?

```
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
```

Die Paketerfassung erfolgt zwischen Fabric-AP und Fabric-Edge. Pakete werden dupliziert, da zwei DHCP Discover-Pakete gesendet wurden. Der Datenverkehr wurde nur am Fabric-Edge empfangen und erfasst.

Es sind immer zwei DHCP-Pakete vorhanden. Eine wird von CAPWAP direkt an den Controller gesendet, um ihn auf dem neuesten Stand zu halten. Das andere wird vom VXLAN an den Steuerungsknoten gesendet. Wenn der WAP beispielsweise ein DHCP-Angebot mit VXLAN vom DHCP-Server erhält, sendet er eine Kopie an den Controller mit CAPWAP.

```
85 0.000252    0.0.0.0          255.255.255.255    DHCP    414 DHCP Request
86 0.000255    192.168.103.1    192.168.103.7      DHCP    418 DHCP ACK
87 0.000258    192.168.103.1    192.168.103.7      DHCP    418 DHCP ACK
```

```
> Frame 85: 414 bytes on wire (3312 bits), 414 bytes captured (3312 bits) on interface 0
> Ethernet II, Src: Cisco_70:60:04 (40:01:7a:70:60:04), Dst: Cisco_9f:f4:5c (00:00:0c:9f:f4:5c)
> Internet Protocol Version 4, Src: 172.16.3.131, Dst: 172.16.3.98
> User Datagram Protocol, Src Port: 49361, Dst Port: 4789
> Virtual eXtensible Local Area Network
> Ethernet II, Src: EdimaxTe_d3:80:b5 (74:da:38:d3:80:b5), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Bootstrap Protocol (Request)
```

Um zu sehen, wohin das Paket gesendet wurde, müssen Sie in Wireshark darauf klicken. Hier sehen wir, dass die Quelle unser AP 172.16.3.131 ist und das Paket an den Fabric Edge 172.16.3.98 gesendet wurde. Der Fabric-Edge leitete sie an den Steuerungsknoten weiter.

Analyse des Web-Umleitungsflusses in einem Fabric-Szenario

Die Umleitungs-ACL auf dem WLC definiert, welcher Datenverkehr bei übereinstimmenden deny-Anweisungen umgeleitet/abgefangen wird (am Ende gibt es eine implizite deny-Anweisung). Der umzuleitende Datenverkehr wird an den WLC innerhalb der CAPWAP-Kapselung gesendet, damit dieser ihn umleiten kann. Beim Abgleich mit einer permit-Anweisung wird dieser Datenverkehr nicht umgeleitet, sondern durchgelassen und an die Fabric weitergeleitet (der Datenverkehr an die ISE geht in diese Kategorie ein).

Protokolle des Access Points, die dem WLC im Fabric-fähigen Zustand beitreten

Sobald sich der Access Point beim WLC registriert hat, registriert der Controller seine IP- und MAC-Adresse im SDA Control Node (LISP Map Server).

Der WAP tritt dem WLC im Fabric-fähigen Modus nur bei Empfang des LISP RLOC-Pakets bei. Dieses Paket wird gesendet, um sicherzustellen, dass der Access Point mit einem Fabric Edge verbunden ist.

Die im WLC für dieses Beispiel verwendeten Debugging-Funktionen sind:

- **'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"**

Für den Test wird der Access Point neu gestartet:

```
*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**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.