排除故障並驗證SD-Access無線初始設定

目錄

簡介

本文介紹確定SD-Access無線設定中的基本連線問題的基本故障排除步驟。它將說明檢查的專案和命令，以找出與無線相關的解決方案中的問題。

必要條件

需求

瞭解SD-Access解決方案

已設定SD訪問拓撲

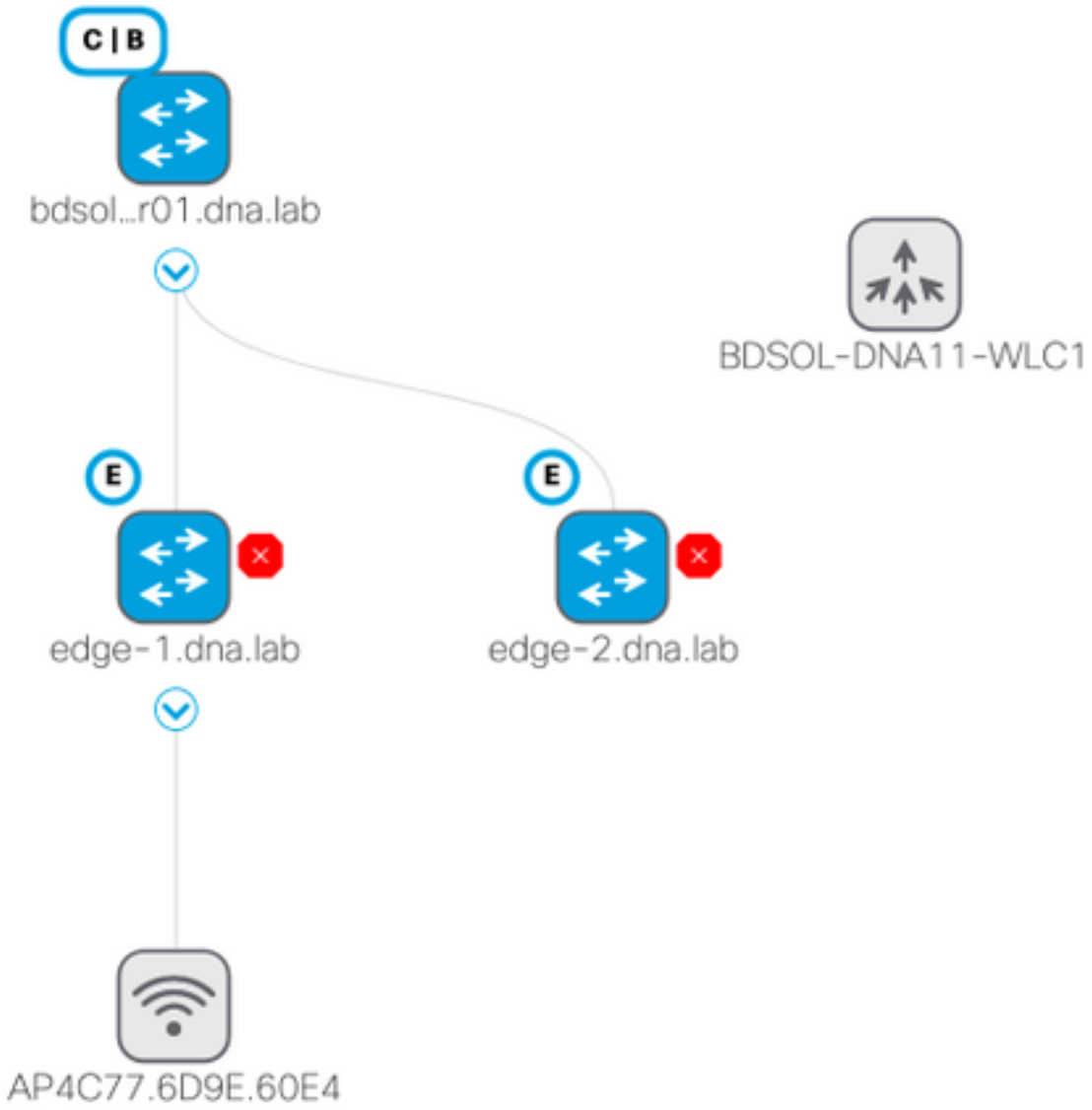
採用元件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。SD-access無線支援其他型別的裝置，但本文重點介紹本節中介紹的裝置。命令可能因平台和軟體版本而異。

8.5.151無線控制器

16.9.3 9300交換機作為邊緣節點

拓撲



故障排除和隔離

快速驗證

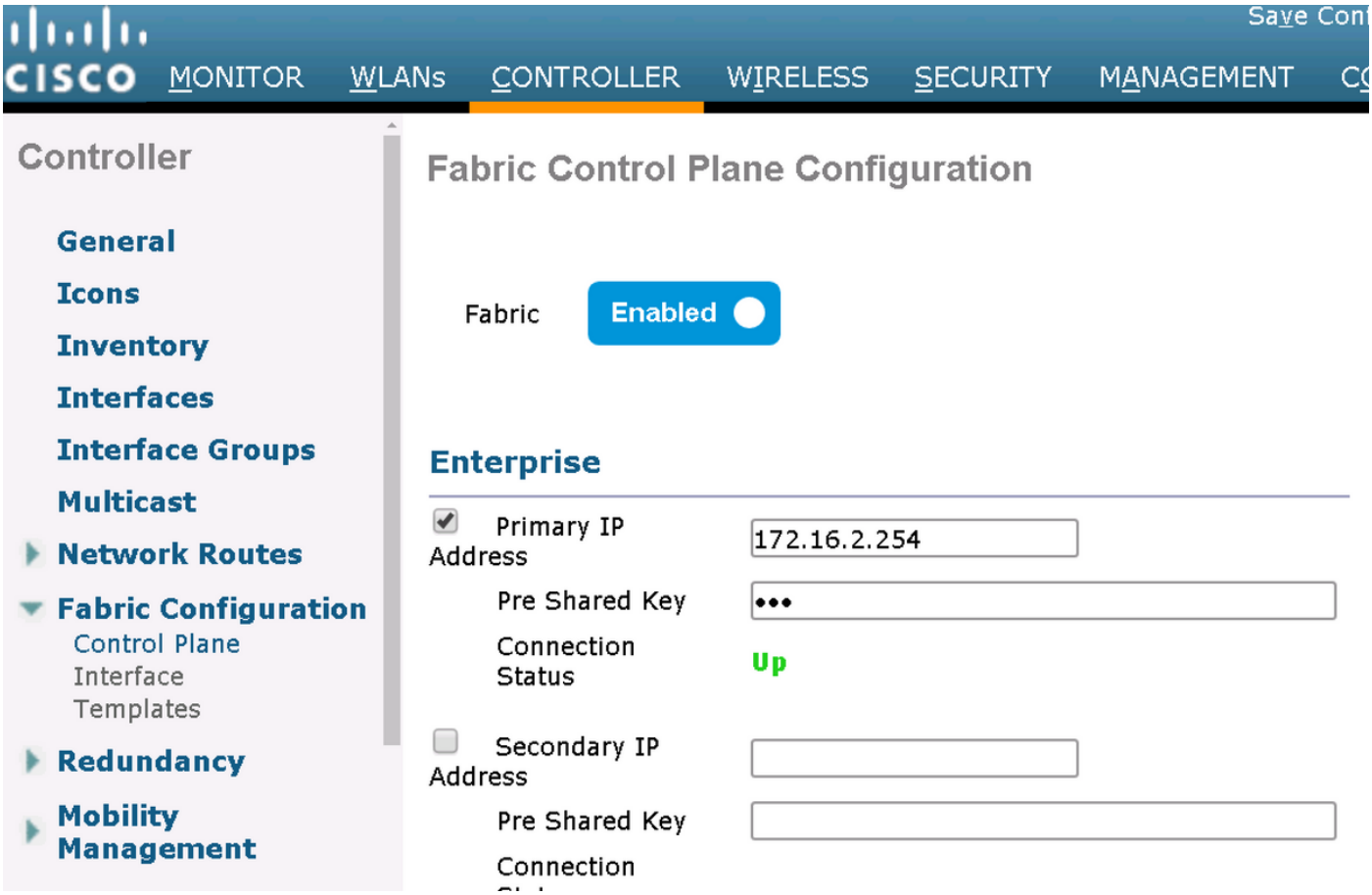
SD訪問方案中存在一系列要求，這些要求通常是錯誤源，因此請首先驗證這些要求是否滿足：

- 請確保在LISP控制平面節點上有指向WLC的特定路由（並且不使用預設路由）
- 使用全域性路由表確保您的AP位於基礎設施VN中
- 從AP本身ping WLC，確保AP與WLC連通
- 確保WLC上控制平面的光纖狀態為開啟
- 確保AP處於支援結構的狀態

案例 1.驗證使用LISP/MAP伺服器控制平面的WLC註冊

將WLC新增到DNA Center中的交換矩陣時，會向控制器推送命令，以便建立與DNA-C中定義為控制平面的節點的連線。第一步是確保此註冊成功。如果控制平面上的LISP配置以某種方式損壞，則

此註冊可能會失敗。



如果此狀態顯示為「down」，則可能需要在WLC和控制平面之間運行調試或資料包捕獲。註冊過程包括4342上的TCP和UDP。如果控制平面沒有取得適當的組態，它可能會使用TCP RST回覆WLC傳送的TCP SYN。

在命令列上使用**show fabric map-server summary**可以驗證相同的狀態。此程式在WLC CLI上使用**debug fabric lisp map-server all**進行調試。若要引發重新連線嘗試，您可以前往DNA Center，並選擇從光纖中移除WLC並再次新增。

可能的原因是控制平面中缺少配置行。以下是工作設定範例（只有最重要的部分）：

```
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
```

如果缺少WLC ip（此處為10.241.0.41）或缺少passive-open命令，CP將拒絕WLC連線。

要運行的調試程式為：

- **'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'**

WLC

```
*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
```

以下範例顯示由於光纖控制平面缺少到WLC的特定路由而加入光纖停用狀態的AP的WLC偵錯

```
(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
```

值得注意的是，如果交換矩陣網路中有兩個控制平面，WLC將始終聯絡這兩個平面進行註冊或查詢。預期兩個控制平面都會在註冊時提供正回覆，因此，如果兩個控制平面中的其中一個由於任何原因拒絕了AP，WLC將無法在交換矩陣中註冊AP。一個控制平面不應答是可接受的，但將使用其餘的控制平面。

AP通過全域性路由表連線到WLC，但LISP仍用於解析WLC。AP傳送到WLC的流量是純CAPWAP控制（不涉及vxlan），但WLC傳送到AP的返回流量將在重疊上透過Vxlan傳輸。您將無法測試從邊緣的AP網關SVI到WLC的連線，因為它是任播網關，邊界節點上也存在相同的IP。為了測試連線，最好的方法是從AP本身執行ping。

案例 2.接入點未獲取IP地址

接入點需要從AP池獲取IP地址，該地址位於DNA中心定義的Infra VNI中。如果沒有發生這種情況，通常意味著AP所連線的交換機埠沒有移動到正確的VLAN。當檢測到（通過CDP）連線的接入點時，交換機將應用一個交換機埠宏，該宏將在AP池的DNA-C定義的vlan中設定交換機埠。如果確實沒有使用宏配置有問題的switchport，您可以手動設定配置（使AP獲得ip、加入WLC並可能升級其代碼並可能解決任何CDP錯誤）或排除CDP連線過程故障。或者，您可以配置主機自註冊，以靜態定義DNA-Center上的埠來託管AP，以便為其調配正確的配置。

如果交換機未調配至少一個AP，則Smartport宏不會自動啟動，您可以驗證AP宏是否調配了正確的VLAN（而不是預設的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
```

Cisco DNA-C推送的用於設定此值的命令是

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

案例 3.接入點沒有針對其Fabric Edge節點構建的vxlan隧道

一旦AP加入WLC，WLC（如果AP支援交換矩陣）將在控制平面上將AP註冊為特殊型別的客戶端。然後，控制平面將請求連線AP的交換矩陣邊緣節點，以構建通向AP的VXLAN隧道。

AP將僅使用vxlan封裝來傳送使用者端流量（且僅適用於處於RUN狀態的使用者端），因此，在交換矩陣使用者端連線之前，在AP上看不到任何vxlan資訊是正常的。

在AP上，客戶端連線後，**show ip tunnel fabric**命令將顯示vxlan隧道資訊。

```
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#
```

在Fabric Edge節點上，**show access-tunnel summary**命令將顯示針對接入點構建的vxlan隧道。當AP加入時，一旦控制平面命令建立隧道，隧道就會顯示。

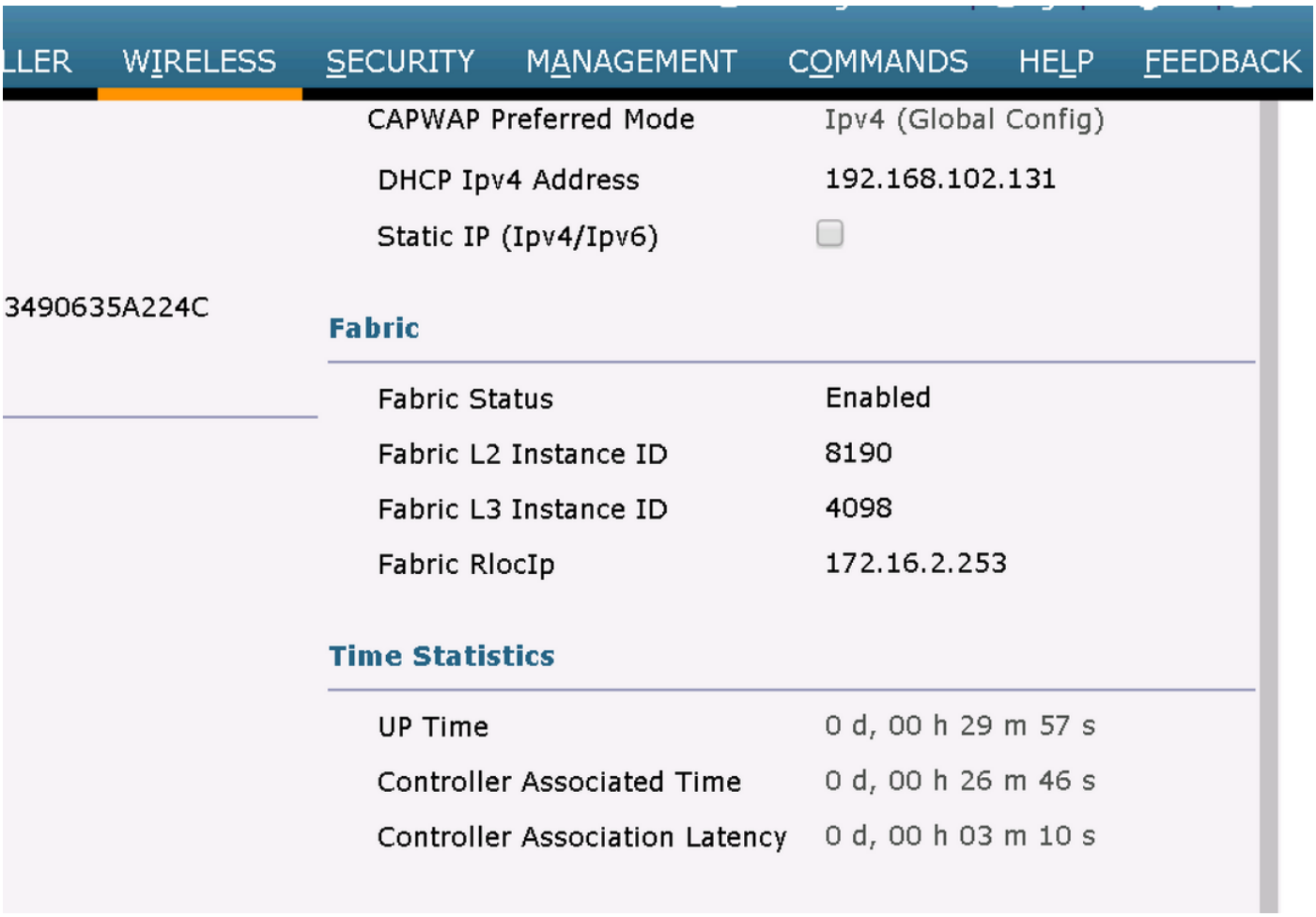
```
edge01#show access-tunnel summ

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
```

您可以在WLC的AP頁面上檢查與該AP對應的L2 LISP例項ID，然後在連線該AP的交換矩陣邊緣上檢查該例項的統計資訊。




```
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
```

案例4.一段時間後遺失存取通道專案

第一次通過Cisco DNA-C布建WLC並將其新增到交換矩陣時，可能會成功建立存取通道，但重新布建無線組態（例如WLAN組態）時，會發現AP的存取通道專案遺失，因此無線使用者端無法成功取得IP。

拓撲是9500(CP)—> 9300（邊緣） — > AP —>無線客戶端。

在邊緣節點上的**show access-tunnel summary**中正確觀察到了條目：

```
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
```

但是，在檢查**show platform software fed switch active ifm interfaces access-tunnel**時，此示例中的硬體中丟失或未能程式設計AP的條目。

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

更多輸出：

```
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
```

您需要比較不同的輸出，並且**show access-tunnel summary**顯示的每個隧道必須存在於每個輸出中。

場景5.無線客戶端無法獲取IP地址

如果存在vxlan隧道，並且所有看起來都正常，但無線客戶端系統無法獲取IP地址，則可能會遇到選項82問題。由於客戶端的DHCP DISCOVER由邊緣節點上的任播網關轉發，因此返回時邊界會將DHCP伺服器OFFER傳送到正確的邊緣節點。這就是轉發DHCP DISCOVER的交換矩陣邊緣向DHCP DISCOVER附加選項82欄位的原因，該選項包含邊緣節點的實際交換矩陣RLOC（環回IP）以及其他資訊編碼後的內容。這意味著您的DHCP伺服器必須支援選項82。

要對DHCP過程進行故障排除，請在交換矩陣節點（尤其是客戶端邊緣節點）上捕獲資料，以驗證交換矩陣邊緣是否附加了選項82欄位。

案例 6.訪客交換矩陣/Web驗證無法正常工作/未重定向客戶端

訪客交換矩陣方案與Flexconnect接入點上的中央Web身份驗證(CWA)極為相似，並且工作方式完全相同（即使交換矩陣AP未處於flexconnect模式）。

重定向ACL和URL必須由ISE在第一個mac身份驗證結果中返回。驗證ISE日誌中的日誌以及WLC上的客戶端詳細資訊頁面中的日誌。

重定向ACL必須以Flex ACL的形式出現在WLC上，並且必須包含對埠8443上的ISE IP地址的「允許」語句（至少）。

在WLC上的使用者端詳細資訊頁面中，使用者端應處於「CENTRAL_WEBAUTH_REQ」狀態。客戶端將無法ping通其預設網關，這是預期的。如果沒有重定向，您可以嘗試在客戶端Web瀏覽器中手動鍵入IP地址（以排除DNS，但無論如何都必須解析ISE主機名）。您應該能夠在客戶端瀏覽器中的埠8443上輸入ISE IP，並檢視門戶頁面，因為此流量將不會被重定向。如果不發生這種情況，您可能會面臨ACL問題或路由問題。沿途收集資料包捕獲，檢視HTTP資料包的停止位置。

瞭解

無線客戶端如何獲得交換矩陣架構中的IP地址

```
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
```

資料包捕獲在交換矩陣AP和交換矩陣邊緣之間進行。資料包重複，因為傳送了兩個DHCP發現資料包。流量僅在交換矩陣邊緣上輸入和捕獲。

始終有兩個DHCP資料包。一個由CAPWAP直接傳送到控制器以保持其更新。另一個由VXLAN傳送到控制節點。例如，當AP通過DHCP伺服器收到帶有VXLAN的DHCP提供時，它會使用CAPWAP將副本傳送到控制器。

```
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)
```

要檢視資料包的傳送位置，您需要在Wireshark上按一下它。此處我們可以看到來源是我們的AP 172.16.3.131，資料包被傳送到交換矩陣邊緣172.16.3.98。交換矩陣邊緣將其轉發到控制節點。

瞭解交換矩陣方案中的Web重定向流程

WLC上的重新導向ACL會定義在相符的deny陳述式上重新導向/攔截哪些流量（結尾有隱含的deny）。要重定向的流量將傳送到WLC的CAPWAP封裝內的WLC以進行WLC重定向。當匹配permit語句時，它不會重定向該流量，而是允許該流量通過交換矩陣並在交換矩陣上轉發該流量（指向ISE的流量進入此類別）。

以啟用結構的狀態加入WLC的AP的日誌

一旦存取點註冊到WLC，控制器就會在SDA控制節點（LISP對映伺服器）中註冊其IP和MAC位址。

只有當WLC收到LISP RLOC封包時，AP才會以支援光纖的模式加入WLC。傳送此資料包是為了確保AP已連線到交換矩陣邊緣。

在此範例中，WLC上使用的偵錯如下：

- **'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'**

對於測試，AP重新啟動：

```
*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
```

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。