排查并验证SD-Access无线初始设置

目录

简介

本文描述确定SD-Access无线设置中的基本连接问题的基本故障排除步骤。本章将介绍用于检查以查明与无线相关的解决方案中的问题的项目和命令。

先决条件

要求

了解SD-Access解决方案

已设置SD访问拓扑

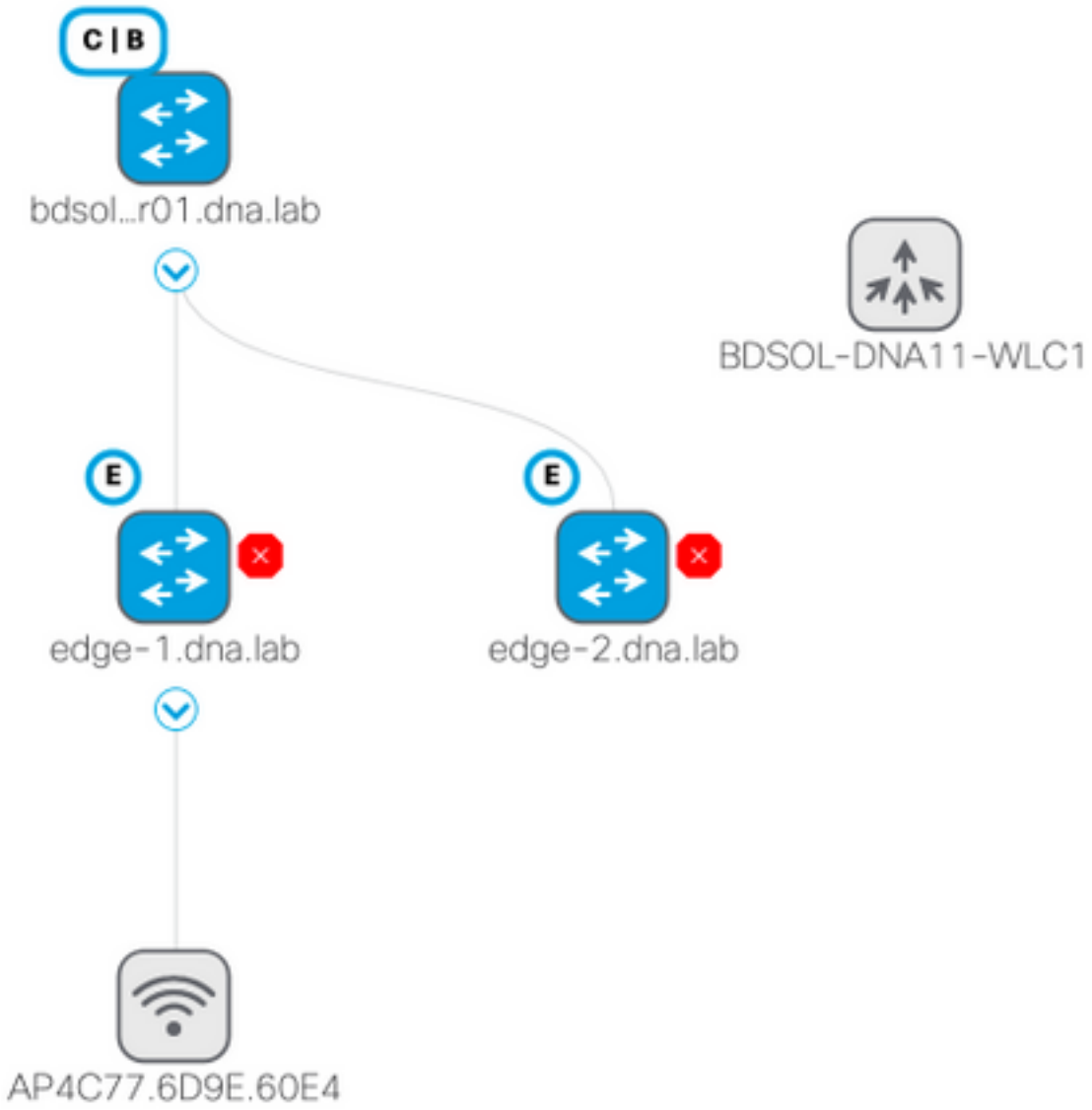
使用的组件

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。SD访问无线支持其它类型的设备，但本文重点介绍本节中介绍的设备。命令可能因平台和软件版本而异。

8.5.151无线控制器

16.9.3 9300交换机作为边缘节点

拓扑



故障排除和隔离

快速验证

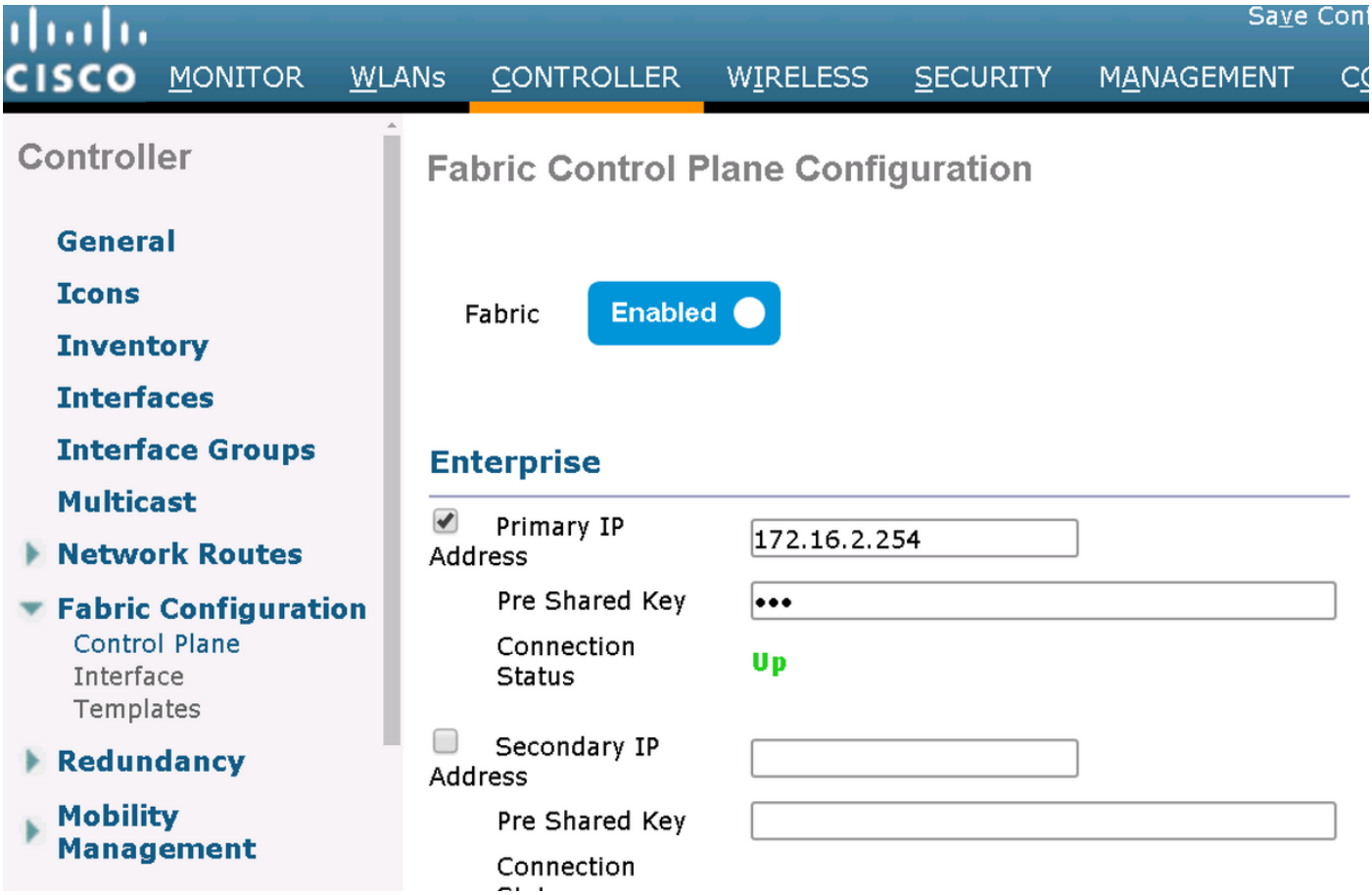
在SD访问场景中有一系列要求，这些要求通常是错误源，因此请首先验证这些要求是否满足：

- 确保您拥有指向LISP控制平面节点上的WLC的特定路由（并且不使用默认路由）
- 使用全局路由表确保您的AP位于基础设施VN中
- 通过从AP本身ping WLC，确保AP与WLC连接
- 确保WLC上控制平面的交换矩阵状态为up
- 确保AP处于交换矩阵启用状态

场景 1.验证与LISP/MAP服务器控制平面的WLC注册

当您将WLC添加到DNA Center中的交换矩阵时，命令会被推送到控制器以建立与DNA-C中定义为控制平面的节点的连接。第一步是确保此注册成功。如果控制平面上的LISP配置在某些方面损坏

，此注册可能会失败。



如果此状态显示为down，则在WLC和控制平面之间运行调试或数据包捕获可能很有意义。4342上的注册包括TCP和UDP。如果控制平面没有获得正确的配置，它可能会使用TCP RST来回复WLC发送的TCP SYN。

在命令行上使用**show fabric map-server summary**可以验证相同的状态。此进程在WLC CLI上使用**debug fabric lisp map-server all**进行调试。若要引发重新连接尝试，您可以转到DNA Center，并选择从交换矩阵中删除WLC，然后重新添加。

可能的原因是控制平面中缺少配置行。以下是工作配置示例（仅最重要的部分）：

```
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WLC ip缺失（此处为10.241.0.41）或缺少passive-open命令，CP将拒绝WLC连接。

要运行的调试程序为：

- **'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
```

以下是AP以交换矩阵禁用状态加入的WLC调试示例，因为交换矩阵控制平面缺少到WLC的特定路由

```
(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，如果您的交换矩阵网络中有两个控制平面，则WLC将始终联系这两个平面进行注册或查询。预期两个控制平面都会在注册时给出正回复，因此，如果两个控制平面中的一个因任何原因拒绝注册AP，WLC将无法注册交换矩阵中的AP。一个控制平面不可应答，但将使用其余控制平面。

AP通过全局路由表连接到WLC，但LISP仍用于解析WLC。AP发送到WLC的流量是纯CAPWAP控制（不涉及vxlan），但是WLC发送到AP的返回流量将在重叠上通过Vxlan传输。您将无法测试从边缘的AP网关SVI到WLC的连接，因为由于它是任播网关，边界节点上也存在相同的IP。为了测试连接，最好的方法是从AP本身执行ping操作。

场景 2：接入点未获得IP地址

接入点需要从AP池获取IP地址，该地址位于DNA中心中定义的Infra VNI中。如果不发生这种情况，通常意味着连接AP的交换机端口没有移至正确的vlan。当检测到连接的接入点（通过CDP）时，交换机将应用switchport宏，该宏将在AP池的DNA-C定义的vlan中设置交换机端口。如果确实没有使用宏配置有问题的交换机端口，您可以手动设置配置（以便AP获得ip、加入WLC并可能升级其代码和解决任何CDP错误），也可以排除CDP连接过程故障。您可以选择配置主机自注册，以静态定义DNA-Center上的端口来托管AP，从而为其调配正确的配置。

如果交换机未调配至少一个AP，Smartport宏不会自动启动，您可以验证AP宏是否调配了正确的vlan（而不是默认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推送的用于设置此值的命令是

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

场景 3：接入点没有建立到其交换矩阵边缘节点的vxlan隧道

一旦AP加入WLC，WLC（如果AP支持交换矩阵）将在控制平面上将AP注册为特殊类型的客户端。然后，控制平面将请求连接AP的交换矩阵边缘节点建立通向AP的vxlan隧道。

AP将仅使用vxlan封装来发送客户端流量（并且仅用于处于RUN状态的客户端），因此，在连接交换矩阵客户端之前，在AP上看不到任何vxlan信息是正常的。

在AP上，客户端连接后，**show ip tunnel fabric**命令将显示vxlan隧道信息。

```
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#
```

在交换矩阵边缘节点上，命令**show access-tunnel summary**将显示构建到接入点的vxlan隧道。当AP加入时，一旦控制平面下令创建隧道，隧道就会显示。

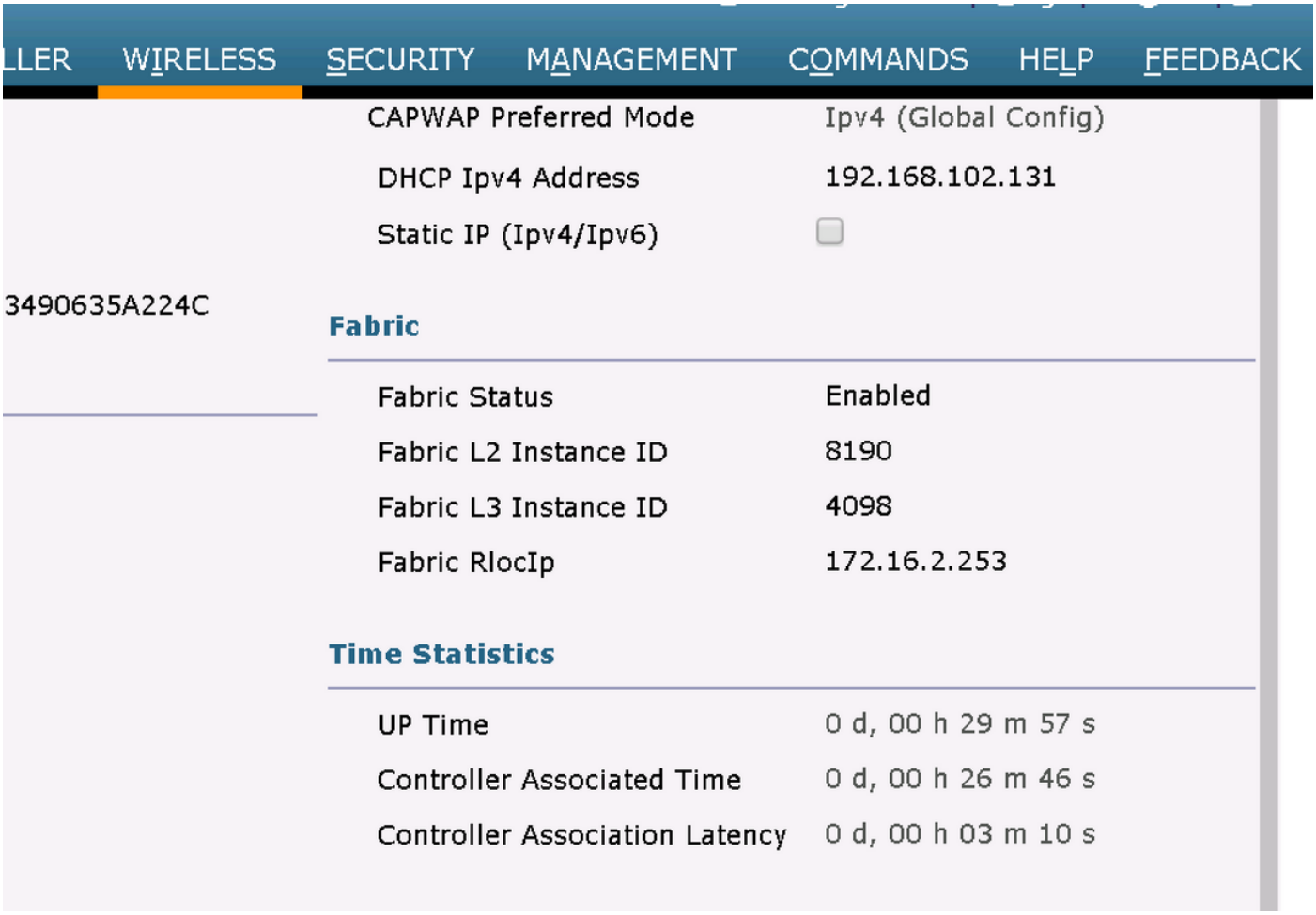
```
edge01#show access-tunnel summ

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页面上检查与该AP对应的L2 LISP实例ID，然后在连接该实例的交换矩阵边缘上检查该实例的统计信息。




```
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
```

场景4.一段时间后缺少访问隧道条目

首次通过Cisco DNA-C调配WLC并添加到交换矩阵时，可能会成功创建访问隧道，但在重新调配无线配置（如WLAN配置）时，会发现AP的访问隧道条目缺失，导致无线客户端无法成功获取IP。

拓扑是9500(CP)—> 9300（边缘） — > AP —>无线客户端。

在边缘节点上的**show access-tunnel summary**中正确观察了条目：

```
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，当检查**show platform software feed switch active ifm interfaces access-tunnel**时，此示例中的硬件中缺少AP条目或无法对其进行编程。

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

更多输出：

```
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
```

您需要比较不同的输出，并且**show access-tunnel summary**显示的每个隧道必须存在于每个输出中。

场景5.无线客户端无法获取IP地址

如果存在vxlan隧道，并且所有看起来都正常，但无线客户端系统无法获取IP地址，则可能面临选项82问题。由于客户端的DHCP DISCOVER是由边缘节点上的任播网关转发的，因此返回时边界会将DHCP服务器OFFER发送到正确的边缘节点会有问题。这就是转发DHCP DISCOVER的交换矩阵边缘向DHCP DISCOVER附加选项82字段的原因，该选项包含边节点的实际交换矩阵RLOC（环回IP）以及其他信息编码。这意味着您的DHCP服务器必须支持选项82。

要排除DHCP过程故障，请捕获交换矩阵节点（尤其是客户端边缘节点）上的捕获信息，以验证交换矩阵边缘是否附加了选项82字段。

方案 6.访客交换矩阵/Web身份验证不起作用/无法重定向客户端

访客交换矩阵场景与Flexconnect接入点上的集中式Web身份验证(CWA)极为相似，并且工作方式完全相同（即使交换矩阵AP不处于flexconnect模式）。

重定向ACL和URL必须由ISE返回第一个mac身份验证结果。在WLC上的ISE日志和客户端详细信息页面中验证这些信息。

重定向ACL必须作为Flex ACL存在于WLC上，并且必须包含对端口8443上的ISE IP地址的“permit”语句（至少）。

在WLC的客户端详细信息页面中，客户端应处于“CENTRAL_WEBAUTH_REQ”状态。客户端将无法ping通其默认网关，这是正常的。如果未重定向，您可以尝试在客户端Web浏览器中手动键入ip地址（以排除DNS，但无论如何都必须解析ISE主机名）。您应该能够在客户端浏览器中的端口8443上输入ISE IP并查看门户页面，因为此流不会重定向。如果不发生这种情况，您可能会面临ACL问题或路由问题。收集沿途的数据包捕获，以查看HTTP数据包的停止位置。

了解

无线客户端如何获得交换矩阵架构中的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
```

数据包捕获在交换矩阵AP和交换矩阵边缘之间进行。数据包重复，因为发送了两个DHCP发现数据包。流量仅在交换矩阵边缘上入口和捕获。

始终有两个DHCP数据包。由CAPWAP直接发送给控制器以保持其更新。另一个由VXLAN发送到控制节点。当AP收到例如DHCP服务器通过VXLAN提供的DHCP提供时，它会通过CAPWAP向控制器发送副本。

```
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)
```

要查看数据包的发送位置，您需要在Wireshark上单击它。在这里，我们可以看到源地址是AP 172.16.3.131，数据包已发送到交换矩阵边缘172.16.3.98。交换矩阵边缘将其转发到控制节点。

了解交换矩阵方案中的Web重定向流程

WLC上的重定向ACL定义在匹配的deny语句上重定向/拦截哪些流量（在末尾存在隐式拒绝）。要重定向的流量将发送到WLC内部的CAPWAP封装，以便WLC进行重定向。当匹配permit语句时，它不会重定向该流量并使其通过交换矩阵并在交换矩阵上转发该流量（指向ISE的流量进入此类别）。

以交换矩阵启用状态加入WLC的AP的日志

接入点注册到WLC后，控制器将在SDA控制节点（LISP映射服务器）中注册其IP和MAC地址。

只有当WLC收到LISP RLOC数据包时，AP才会以交换矩阵启用模式加入WLC。发送此数据包是为了确保AP已连接到交换矩阵边缘。

本示例在WLC上使用的调试是：

- **'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'**

对于测试，AP重新启动：

```
*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
```

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。