

SD-Accessワイヤレスの初期設定のトラブルシューティングと確認

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[トポロジ](#)

[トラブルシューティングと切り分け](#)

[迅速な検証](#)

[シナリオ 1.LISP/MAPサーバのコントロールプレーンを使用したWLC登録の確認](#)

[シナリオ 2.アクセスポイントがIPアドレスを取得していない](#)

[シナリオ 3.アクセスポイントには、ファブリックエッジノードに向けて構築されたvxlanトンネルがありません](#)

[シナリオ 4: しばらくするとアクセストンネルエントリが消失する](#)

[シナリオ 5: ワイヤレスクライアントがIPアドレスを取得できない](#)

[シナリオ 6.ゲストファブリック/Web認証が機能しないクライアントをリダイレクトしない](#)

[理解する](#)

[ワイヤレスクライアントがファブリックアーキテクチャでIPアドレスを取得する方法](#)

[ファブリックシナリオにおけるWebリダイレクションフローの理解](#)

[ファブリックが有効な状態でWLCに参加しているAPのログ](#)

はじめに

この記事では、SDアクセスのワイヤレス設定で基本的な接続の問題を特定するための基本的なトラブルシューティング手順について説明します。ワイヤレスに関連するソリューションの問題を切り分けるためにチェックする項目とコマンドについて説明します。

前提条件

要件

SD-Accessソリューションの知識

SDアクセストポロジがすでに設定されている

使用するコンポーネント

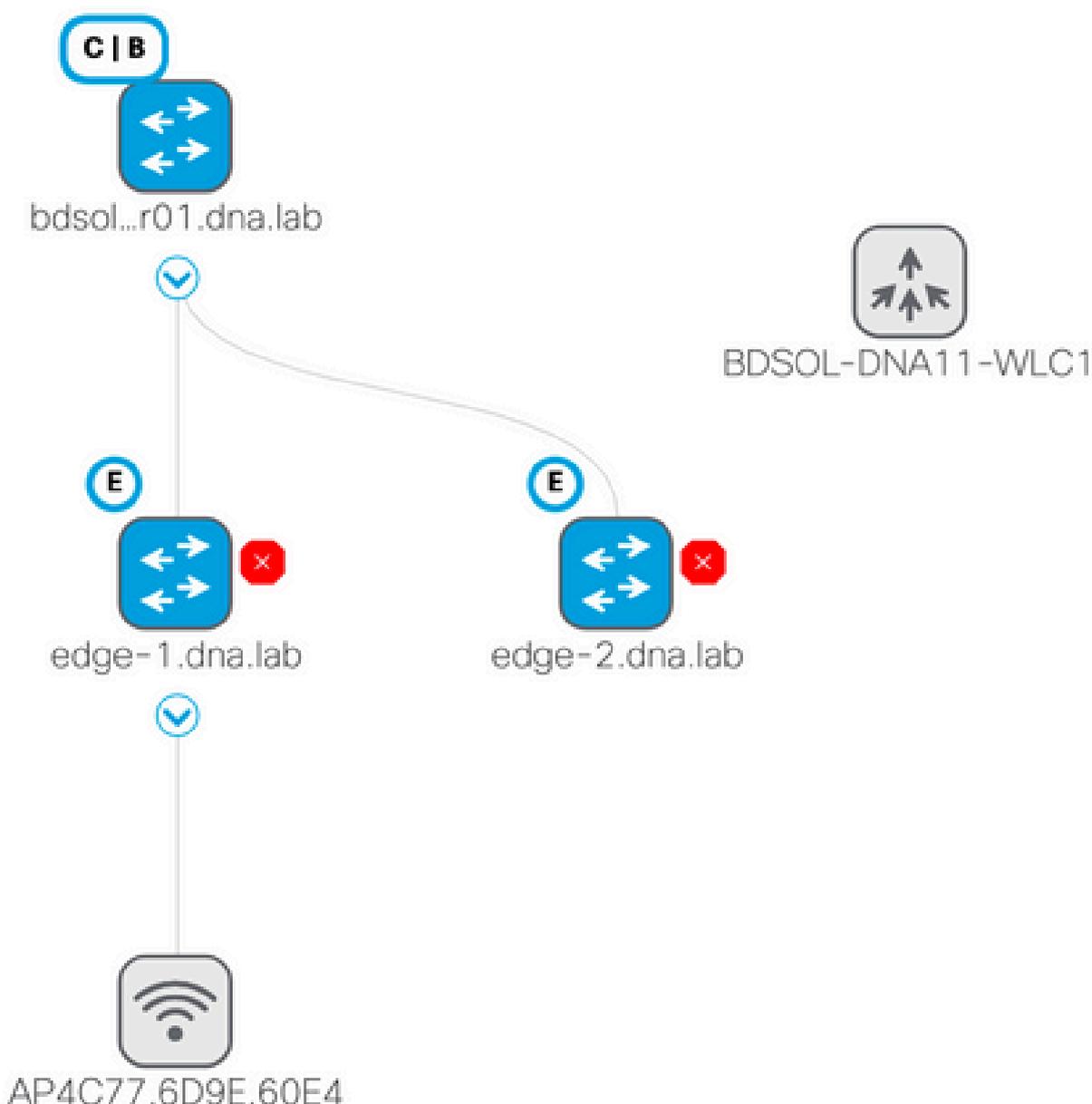
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始していま

す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。SDアクセスワイヤレスでサポートされるデバイスは他のタイプもありますが、この記事では、このセクションで説明するデバイスに焦点を当てています。コマンドは、プラットフォームとソフトウェアのバージョンによって異なります。

8.5.151ワイヤレスコントローラ

エッジノードとしての16.9.3 9300スイッチ

トポロジ



トラブルシューティングと切り分け

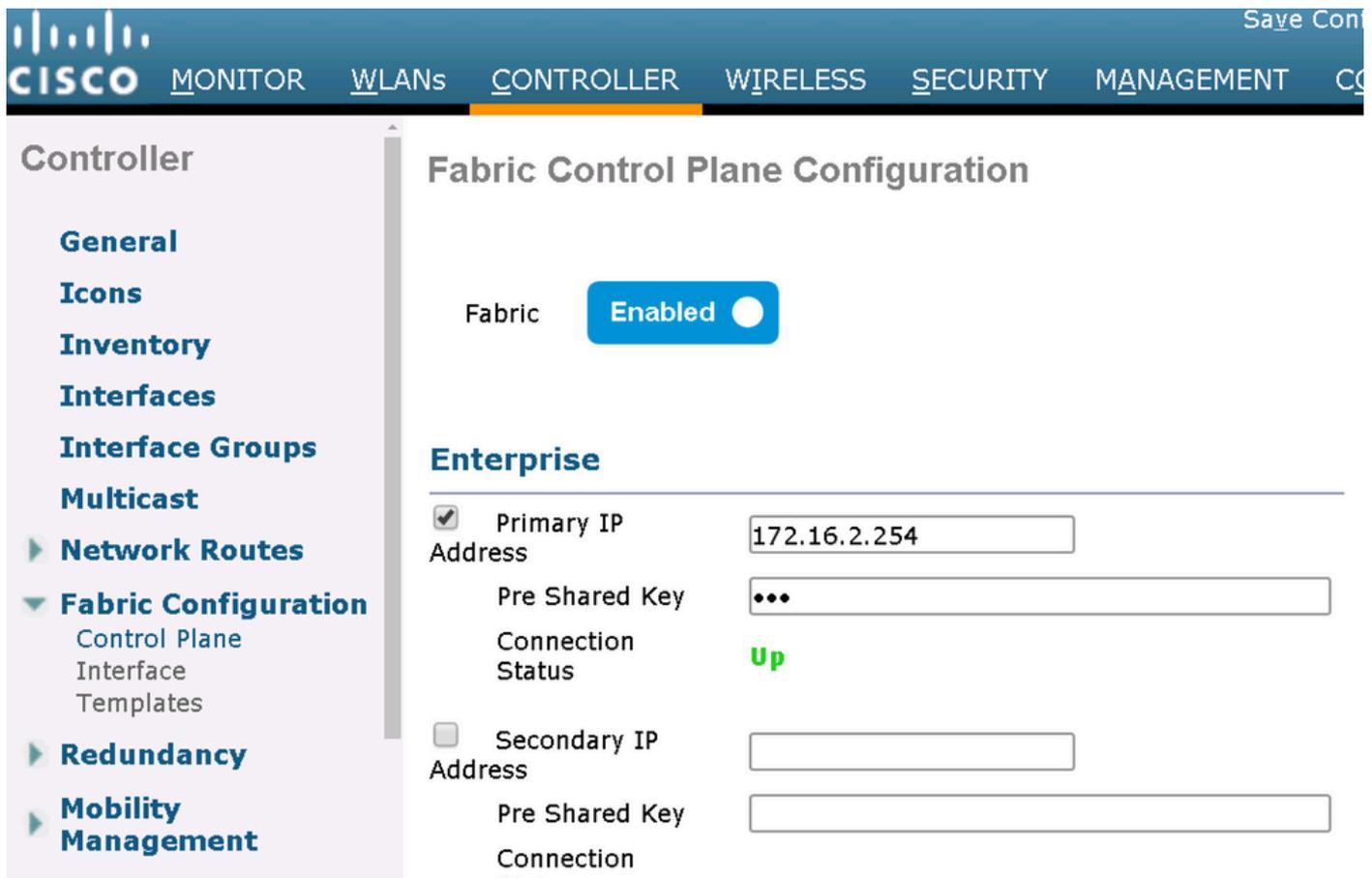
迅速な検証

SDアクセスのシナリオには、多くの場合エラーの原因となる一連の要件があります。最初にこれらの要件が満たされていることを確認してください（SDアクセスのシナリオでは、SDアクセスの要件が満たされていることを確認する必要があります）。

- LISPコントロールプレーンノード上のWLCを指す特定のルートがあることを確認します（デフォルトのルートは使用しません）
- グローバルルーティングテーブルを使用して、APがInfra VNにあることを確認します
- AP自体からWLCにpingを実行して、APがWLCに接続できることを確認します
- WLC上のコントロールプレーンのファブリックステータスがupであることを確認します
- APがファブリック対応状態であることを確認します

シナリオ 1.LISP/MAPサーバのコントロールプレーンを使用したWLC登録の確認

DNA CenterでWLCをファブリックに追加すると、コマンドがコントローラにプッシュされ、DNA-Cでコントロールプレーンとして定義されているノードへの接続が確立されます。最初のステップは、この登録が正常に行われたことを確認することです。コントロールプレーン上のLISP設定が何らかの形で破損した場合、この登録は失敗する可能性があります。



The screenshot displays the Cisco DNA Center interface for configuring the Fabric Control Plane. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', and 'MANAGEMENT'. The left sidebar lists various configuration categories, with 'Fabric Configuration' selected. The main content area shows the 'Fabric Control Plane Configuration' page. The 'Fabric' status is 'Enabled'. Under the 'Enterprise' section, the 'Primary IP Address' is set to 172.16.2.254, and the 'Pre Shared Key' is masked with dots. The 'Connection Status' is 'Up'. There are also fields for 'Secondary IP Address' and 'Pre Shared Key' which are currently empty.

このステータスがdownと表示される場合は、WLCとコントロールプレーンの間でデバッグまたはパケットキャプチャを実行するのが興味深い場合があります。4342での登録にはTCPとUDPの両方が含まれます。コントロールプレーンが適切な設定を取得しなかった場合、コントロールプレーンはWLCによって送信されたTCP SYNにTCP RSTで応答する場合があります。

同じステータスは、コマンドラインでshow fabric map-server summaryを使用して確認できます。このプロセスは、WLC CLIでdebug fabric lisp map-server allを使用してデバッグします。再接

続を試行するには、DNA Centerに移動し、ファブリックからWLCを削除して再度追加することを選択します。

考えられる理由は、コントロールプレーンに設定行がないことです。次に動作設定の例を示します (最も重要な部分のみ)。

```
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
```

WLCのipが欠落している場合 (ここでは10.241.0.41)、またはpassive-openコマンドが欠落している場合、CPはWLCの接続を拒否します。

実行するデバッグは次のとおりです。

- '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'

コントロールプレーンがWLCに応答しない例を次に示します

<#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 10.32.58.36

*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
```

次に、ファブリック制御プレーンにWLCへの特定のルートが欠落しているため、ファブリックが無効な状態で参加しているAPのWLCデバッグの例を示します

```
(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 fffffff0,12vnid 8191,13vnid 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_VN
```

```
*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
```

```
*spamReceiveTask: Oct 16 08:55:26.295: Vnid Mapping return from index 2 with entries name 192_168_39_0-INFRA_VN
```

```
*spamReceiveTask: Oct 16 08:55:26.295: spamSendFabricMapServerRequest: MS request from AP Pod3-AP4800 f4:db:e6:61:24:a0
```

```
*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 54
```

```
*spamApTask6: Oct 16 08:56:51.949: Fabric is supported for AP f4:db:e6:64:02:a0 (Pod3-AP3800). apType 54
```

```
*spamApTask6: Oct 16 08:56:51.953: Fabric is supported for AP f4:db:e6:64:02:a0 (Pod3-AP3800). apType 54
```

```
*spamApTask6: Oct 16 08:56:51.953: Fabric is supported for AP f4:db:e6:64:02:a0 (Pod3-AP3800). apType 54
```

```
*spamApTask6: Oct 16 08:56:51.953: spamSendFabricMapServerRequest: MS request from AP Pod3-AP3800 f4:db:e6:64:02:a0
```

興味深いことに、ファブリックネットワークに2つのコントロールプレーンがある場合、WLCは登録またはクエリのために常に両方に到達します。両方のコントロールプレーンが登録に対して肯定応答を返すので、2つのコントロールプレーンの一方が何らかの理由で拒否した場合、WLCはファブリックへのAPの登録に失敗します。応答しないコントロールプレーンが1つあってもかまわないが、残りのコントロールプレーンが使用される

APはグローバルルーティングテーブルを介してWLCに到達しますが、WLCの解決には引き続きLISPが使用されます。APからWLCに送信されるトラフィックは純粋なCAPWAP制御ですが（vxlanは含まれません）、WLCからAPに送信されるリターントラフィックはオーバーレイ上のVxlanを介して伝送されます。エニーキャストゲートウェイであるため、同じIPがボーダーノードにも存在するため、エッジ上のAPゲートウェイSVIからWLCへの接続をテストできません。接続をテストする最善の方法は、AP自体からpingを実行することです。

シナリオ 2. アクセスポイントがIPアドレスを取得していない

アクセスポイントは、DNA Centerで定義されたインフラストラクチャVNI内のAPプールからIPアドレスを取得することが想定されます。これが発生しない場合、通常はAPが接続されているスイッチポートが正しいVLANに移動しなかったことを意味します。スイッチは、接続されているアクセスポイントを（CDPを介して）検出すると、APプールのDNA-Cで定義されているVLANにスイッチポートを設定するswitchportマクロを適用します。問題のあるスイッチポートが実際にマクロを使用して設定されていない場合は、設定を手動で設定するか（APがIPを取得し、WLCに加入して、おそらくコードをアップグレードし、CDPの不具合を解決できる）、CDP接続プロセスのトラブルシューティングを行うことができます。APをホストするDNA-Center上のポートを静的

に定義して、正しい設定でプロビジョニングされるように、ホストオンボーディングをオプションで設定できます。

スイッチが少なくとも1つのAPでプロビジョニングされていない場合、SmartPortマクロは自動的に起動しません。APマクロが (デフォルトのVLAN 1ではなく) 正しいVLANでプロビジョニングされているかどうかを確認できます

```
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がこれを設定するためにプッシュするコマンドは次のとおりです

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

シナリオ 3.アクセスポイントには、ファブリックエッジノードに向けて構築されたvxlanトンネルがありません

APがWLCに加入すると、WLC (APがファブリック対応の場合) はAPを特別なタイプのクライアントとしてコントロールプレーンに登録します。コントロールプレーンは、APが接続されているファブリックエッジノードを要求して、APに向かうvxlanトンネルを構築します。

APはクライアントトラフィックの送信にのみvxlanカプセル化を使用します (RUN状態のクライアントに対してのみ)。したがって、ファブリッククライアントが接続するまでAP上にvxlan情報が表示されないことは正常です。

クライアントが接続すると、APでコマンドshow ip tunnel fabricを実行すると、vxlanトンネルの情報が表示されます。

```
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#
```

ファブリックエッジノードで、コマンドshow access-tunnel summaryを実行すると、アクセスポイントに対して構築されたvxlanトンネルが表示されます。APが加入すると、コントロールプレ

トンネルの作成を要求するとすぐに、トンネルが表示されます。

```
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

WLCのアクセスポイントページで、そのAPに対応するL2 LISPインスタンスIDを確認し、接続先のファブリックエッジでそのインスタンスの統計情報を確認できます。

WLC configuration page showing CAPWAP Preferred Mode, DHCP Ipv4 Address (192.168.102.131), and Static IP (unchecked). The Fabric section is expanded, showing Fabric Status (Enabled), Fabric L2 Instance ID (8190), Fabric L3 Instance ID (4098), and Fabric RlocIp (172.16.2.253). The Time Statistics section shows UP Time (0 d, 00 h 29 m 57 s), Controller Associated Time (0 d, 00 h 26 m 46 s), and Controller Association Latency (0 d, 00 h 03 m 10 s).

```
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
```

シナリオ4 : しばらくするとアクセストンネルエントリが消失する

WLCがCisco DNA-Cを通じてプロビジョニングされ、ファブリックに追加されたときに、最初にアクセストンネルが正常に作成される可能性があります。ワイヤレス設定 (WLAN設定など) を再プロビジョニングすると、APのアクセストンネルエントリが欠落し、ワイヤレスクライアントがIPを正常に取得できないことが判明します。

トポロジは、9500(CP) → 9300 (エッジ) → AP →ワイヤレスクライアントです。

エントリは、エッジノードのshow access-tunnel summaryで正しく表示されます。

```
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
```

しかし、show platform software fed switch active ifm interfaces access-tunnelをチェックすると、この例ではAPのエントリが欠落しているか、ハードウェアでのプログラムに失敗しています。

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

出力の詳細：

```
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 0x0000 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
```

さまざまな出力を比較する必要があり、show access-tunnel summaryで表示されるすべてのトンネルがそれぞれに存在する必要があります。

シナリオ5：ワイヤレスクライアントがIPアドレスを取得できない

vxlanトンネルが存在し、すべてが正常に見えるが、ワイヤレスクライアントがIPアドレスを取得できない場合は、オプション82の問題に直面している可能性があります。クライアントのDHCP DISCOVERはエッジノード上のエニーキャストゲートウェイによって転送されるため、DHCPサーバOFFERが戻る途中の境界によって右側のエッジノードに送信されるのが問題になります。このため、DHCP DISCOVERを転送するファブリックエッジは、DHCP DISCOVERにオプション82フィールドを追加します。このフィールドには、エッジノードの実際のファブリックRLOC (ループバックIP) が他の情報とともにエンコードされています。これは、DHCPサーバがオプション82をサポートする必要があることを意味します。

DHCPプロセスのトラブルシューティングを行うには、ファブリックノード (特にクライアントエッジノード) でキャプチャを取得し、ファブリックエッジがオプション82フィールドに追加されていることを確認します。

シナリオ 6.ゲストファブリック/Web認証が機能しない/クライアントをリダイレクトしない

ゲストファブリックのシナリオは、Flexconnectアクセスポイントの中央Web認証(CWA)に非常に

よく似ており、ファブリックAPがFlexConnectモードでない場合でも、まったく同じように動作します。

リダイレクトACLとURLは、最初のMAC認証結果でISEから返される必要があります。ISEログとWLCのクライアント詳細ページでこれらを確認します。

リダイレクトACLは、WLC上にFlex ACLとして存在し、ポート8443 (少なくとも) のISE IPアドレスに対する「permit」ステートメントを含む必要があります。

クライアントは、WLCのクライアント詳細ページで「CENTRAL_WEBAUTH_REQ」状態になっている必要があります。クライアントはデフォルトゲートウェイにpingを実行できません。これは正常な動作です。リダイレクトされない場合は、クライアントのWebブラウザに手動でIPアドレスを入力できます (DNSを除外しますが、ISEホスト名は解決する必要があります)。クライアントブラウザのポート8443にISE IPを入力すると、このフローはリダイレクトされないため、ポータルページが表示されます。この問題が発生しない場合は、ACLの問題、またはへのルーティングの問題が発生しています。途中でパケットキャプチャを収集し、HTTPパケットが停止している場所を確認します。

理解する

ワイヤレスクライアントがファブリックアーキテクチャでIPアドレスを取得する方法

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

パケットのキャプチャは、ファブリックAPとファブリックエッジの間で行われます。2つのDHCP Discoverパケットが送信されたため、パケットが重複しています。トラフィックは入力のみで、ファブリックエッジでキャプチャされました。

常に2つのDHCPパケットがあります。1つはCAPWAPによってコントローラに直接送信され、更新された状態を維持します。もう1つはVXLANからコントロールノードに送信されるパケットです。APは、たとえばVXLANを使用したDHCPオファーをDHCPサーバによって受信すると、CAPWAPを使用してコピーをコントローラに送信します。

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)

```

パケットの送信先を確認するには、Wiresharkでパケットをクリックする必要があります。ここでは、送信元がAP 172.16.3.131で、パケットがファブリックエッジ172.16.3.98に送信されたことがわかります。ファブリックエッジは、それをコントロールノードに転送しました。

ファブリックシナリオにおけるWebリダイレクションフローの理解

WLC上のリダイレクトACLは、一致するdenyステートメントでリダイレクト/インターセプトされるトラフィックを定義します（最後に暗黙のdenyがあります）。リダイレクトされるトラフィックは、WLCがリダイレクトできるように、CAPWAPカプセル化の内側のWLCに送信されます。permit文に一致する場合、そのトラフィックはリダイレクトされず、ファブリックを通過して転送されます（ISEへのトラフィックがこのカテゴリに入ります）。

ファブリックが有効な状態でWLCに参加しているAPのログ

アクセスポイントがWLCに登録されるとすぐに、コントローラはそのIPアドレスとMACアドレスをSDAコントロールノード（LISPマップサーバ）に登録します。

APは、WLCがLISP RLOCパケットを受信した場合にのみ、ファブリック対応モードでWLCに加入します。このパケットは、APがファブリックエッジに接続されていることを確認するために送信されます。

この例のWLCで使用されるデバッグは次のとおりです。

- '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'

テストのために、APはリブートされます（APはリブートされます）。

<#root>

```

*spamApTask0: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for Aggregated Payload
*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 V
*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-logging
*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

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。