ゲストアンカーセットアップの中央Web認証(CWA)の理解とトラブルシューティング

内容

概要

このドキュメントでは、ゲストアンカーのセットアップで中央Web認証がどのように動作するか、および実稼働ネットワークで発生する一般的な問題の一部と、それらの修正方法について説明します。

前提条件

要件

ワイヤレスLANコントローラ(WLC)での中央Web認証の設定方法に関する知識があることが推奨されます。

このドキュメントでは、中央Web認証の設定に関する手順について説明します。
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html

使用するコンポーネント

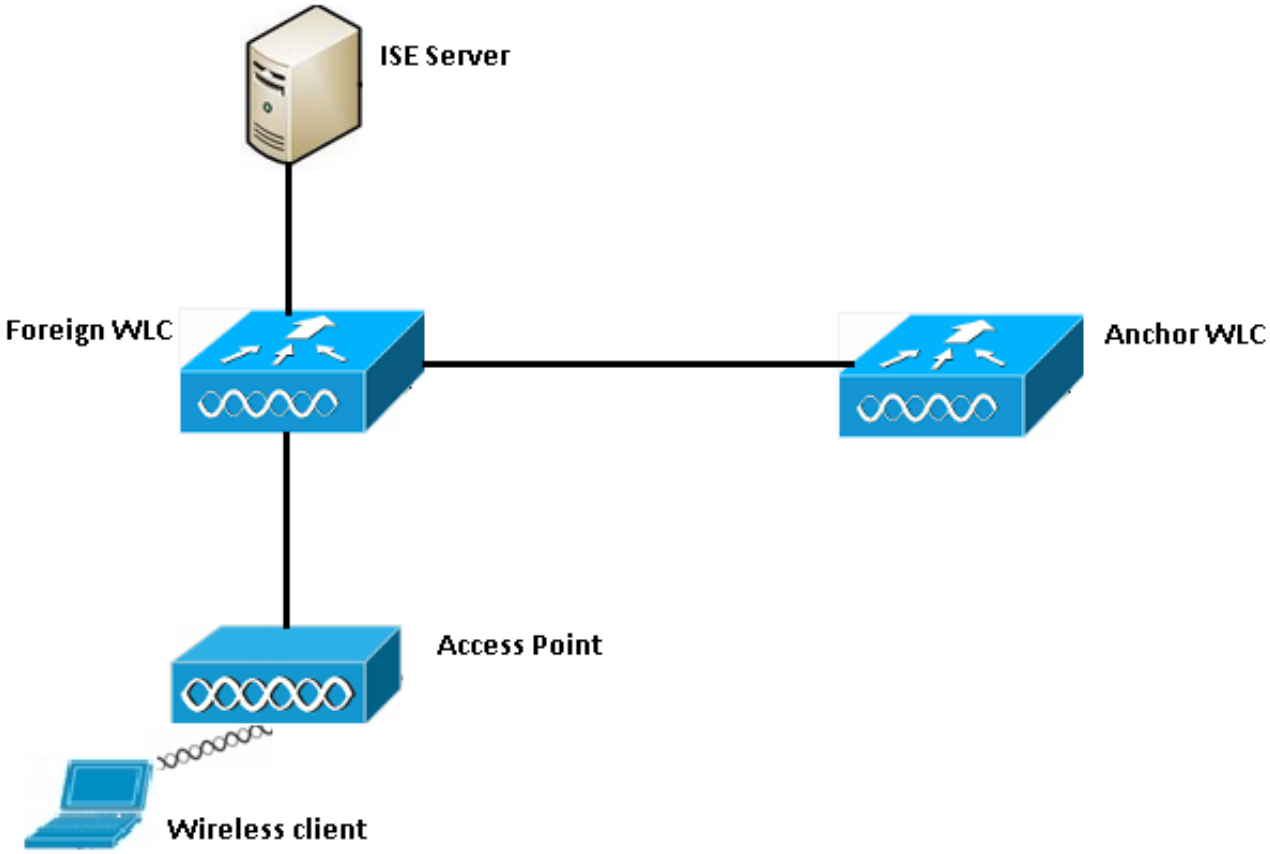
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- バージョン7.6が稼働するWLC 5508
- バージョン1.4を実行するIdentity Services Engine(ISE)

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、初期（デフォルト）設定の状態から起動しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響について確実に理解しておく必要があります

基本フロー

このセクションでは、図に示すように、ゲストアンカー設定での中央webauthの基本的なワークフローを示します。



ステップ1：クライアントがアソシエーション要求を送信すると、接続が開始されます。

ステップ2:WLCは、設定されたISEサーバに認証要求を送信すると、MAC認証プロセスを開始します。

ステップ3:ISEで設定された認可ポリシーに基づいて、リダイレクトURLとリダイレクトのアクセスコントロールリスト(ACL)エントリを使用してAccess-Acceptメッセージが WLCに返信されます。

ステップ4：外部WLCはクライアントにアソシエーション応答を送信します。

ステップ5：この情報は、モビリティハンドオフメッセージで外部WLCからアンカーWLCに渡されます。リダイレクトACLがアンカーWLCと外部WLCの両方で設定されていることを確認する必要があります。

ステップ6：この段階で、クライアントは外部WLCで実行状態に移行します。

ステップ7：クライアントがブラウザでURLを使用してWeb認証を開始すると、アンカーはリダイレクトプロセスを開始します。

ステップ8：クライアントが正常に認証されると、アンカーWLC上でクライアントがRUN状態に移行します。

クライアント接続の試行に成功するための中央Web認証フロー

デバッグを行う際に、上記の基本的なフローを詳細に分析できるようになりました。分析に役立つように、アンカーと外部WLCの両方で次のデバッグが収集されています。

```
debug client 00:17:7c:2f:b8:6e
debug aaa detail enable
debug mobility handoff enable
debug web-auth redirect enable mac 00:17:7c:2f:b8:6e
```

次の詳細を使用します。

```
WLAN name: CWA
WLAN ID: 5
IP address of anchor WLC: 10.105.132.141
IP address of foreign WLC: 10.105.132.160
Redirect ACL used: REDIRECT
Client MAC address: 00:17:7c:2f:b8:6e
New mobility architecture disabled
```

ステップ1：クライアントがアソシエーション要求を送信すると、接続プロセスが開始されます。これは外部コントローラで表示されます。

```
*apfMsConnTask_6: May 08 12:10:35.897: 00:17:7c:2f:b8:6e Association received from mobile on
BSSID dc:a5:f4:ec:df:34
```

ステップ2:WLCは、ワイヤレスLAN(WLAN)がMAC認証用にマッピングされていることを確認し、クライアントを**AAA pendingステータスに移**動します。また、ISEに認証要求を送信すると、認証プロセスが開始されます。

```
*apfMsConnTask_6: May 08 12:10:35.898: 00:17:7c:2f:b8:6e apfProcessAssocReq (apf_80211.c:8221)
Changing state for mobile 00:17:7c:2f:b8:6e on AP dc:a5:f4:ec:df:30 from Idle to AAA Pending
*aaaQueueReader: May 08 12:10:35.898: AuthenticationRequest: 0x2b6bf574

*aaaQueueReader: May 08 12:10:35.898: Callback.....................................0x10166e78
*aaaQueueReader: May 08 12:10:35.898: protocolType.................................0x40000001
*aaaQueueReader: May 08 12:10:35.898:
proxyState.....................................00:17:7C:2F:B8:6E-00:00
```

ステップ3:ISEでMAC認証バイパスが設定され、MAC認証後にリダイレクトURLとACLが返されます。許可応答で送信された次のパラメータを確認できます。

```
*radiusTransportThread: May 08 12:10:35.920: AuthorizationResponse: 0x14c47c58
*radiusTransportThread: May 08 12:10:35.920: structureSize...............................320
*radiusTransportThread: May 08 12:10:35.920: resultCode...................................0
*radiusTransportThread: May 08 12:10:35.920:
protocolUsed.................................0x00000001
*radiusTransportThread: May 08 12:10:35.920:
proxyState.....................................00:17:7C:2F:B8:6E-00:00
*radiusTransportThread: May 08 12:10:35.920: Packet contains 5 AVPs:
*radiusTransportThread: May 08 12:10:35.920: AVP[01] User-
Name.............................00-17-7C-2F-B8-6E (17 bytes)
*radiusTransportThread: May 08 12:10:35.920: AVP[02]
State.................................ReauthSession:0a6984a00000004c536bac7b (38 bytes)
*radiusTransportThread: May 08 12:10:35.920: AVP[03]
```

```
Class.....................................CACS:0a6984a00000004c536bac7b:sid-ise-1-2/188796966/38
(54 bytes)
*radiusTransportThread: May 08 12:10:35.920: AVP[04] Cisco / Url-Redirect-
Acl.................REDIRECT (8 bytes)
*radiusTransportThread: May 08 12:10:35.920: AVP[05] Cisco / Url-
Redirect.....................DATA (91 bytes)
```

ISEログにも同じ情報が表示されます。図に示すように、[Operations] > [Authentications]に移動し、[Client session details]をクリックします。

Result

User-Name	00-17-7C-2F-B8-6E
State	ReauthSession:0a6984a0000000045371b7c4
Class	CACS:0a6984a0000000045371b7c4:sid-ise-1-2/188796966/714
cisco-av-pair	url-redirect-acl=REDIRECT
cisco-av-pair	url-redirect=https://10.106.73.98:8443/guestportal/gateway?sessionId=0a6984a0000000045371b7c4&action=cwa

ステップ4：外部WLCは状態をL2 auth completeに変更し、アソシエーション応答をクライアントに送信します。

> **注**：MAC認証を有効にすると、アソシエーション応答は、これが完了するまで送信されません。

```
*apfReceiveTask: May 08 12:10:35.921: 00:17:7c:2f:b8:6e 0.0.0.0 AUTHCHECK (2) Change state to
L2AUTHCOMPLETE (4)
*apfReceiveTask: May 08 12:10:35.922: 00:17:7c:2f:b8:6e Sending Assoc Response to station on
BSSID dc:a5:f4:ec:df:34 (status 0) ApVapId 5 Slot 0
```

ステップ 5：次に、外部がアンカーへのハンドオフプロセスを開始します。次に、debug mobility handoffの出力を示します。

```
*apfReceiveTask: May 08 12:10:38.799: 00:17:7c:2f:b8:6e Attempting anchor export for mobile
00:17:7c:2f:b8:6e
*apfReceiveTask: May 08 12:10:38.799: 00:17:7c:2f:b8:6e Anchor Export:
Client IP: 0.0.0.0, Anchor IP: 10.105.132.141
*apfReceiveTask: May 08 12:10:38.799: 00:17:7c:2f:b8:6e mmAnchorExportSend: Building
UrlRedirectPayload
*apfReceiveTask: May 08 12:10:38.799: 00:17:7c:2f:b8:6e Anchor Export: Sending url redirect acl
REDIRECT
```

ステップ6：クライアントが外部WLCでRUN状態に移行します。これで、クライアントの正しいステータスは、アンカーでのみ確認できます。外部から収集されたshow client detailの出力の一部を次に示します（関連情報のみを示します）。

```
Client MAC Address.............................. 00:17:7c:2f:b8:6e
Client Username ................................ 00-17-7C-2F-B8-6E
AP MAC Address.................................. dc:a5:f4:ec:df:30
BSSID........................................... dc:a5:f4:ec:df:34
IP Address...................................... Unknown
```

```
Gateway Address.............................. Unknown
Netmask...................................... Unknown
Mobility State............................... Export Foreign
Mobility Anchor IP Address................... 10.105.132.141
Policy Manager State......................... RUN
Policy Manager Rule Created.................. Yes
AAA Override ACL Name........................ REDIRECT
AAA URL
redirect.............................https://10.106.73.98:8443/guestportal/gatewaysessionId=
0a6984a00000004c536bac7b&action=cwa
```

ステップ7：外部コントローラがアンカーでハンドオフ要求を開始します。ハンドオフメッセージは次のように表示されます。

```
*mmListen: May 08 05:52:50.587: 00:17:7c:2f:b8:6e Received Anchor Export request: from Switch
IP: 10.105.132.160
*mmListen: May 08 05:52:50.587: 00:17:7c:2f:b8:6e Adding mobile on Remote AP
00:00:00:00:00:00(0)
*mmListen: May 08 05:52:50.587: 00:17:7c:2f:b8:6e mmAnchorExportRcv:, Mobility role is Unassoc
*mmListen: May 08 05:52:50.587: 00:17:7c:2f:b8:6e mmAnchorExportRcv Ssid=cwa Security
Policy=0x42000
*mmListen: May 08 05:52:50.587: 00:17:7c:2f:b8:6e mmAnchorExportRcv vapId= 5, Ssid=cwa
AnchorLocal=0x0
*mmListen: May 08 05:52:50.588: 00:17:7c:2f:b8:6e mmAnchorExportRcv:Url redirect
https://10.106.73.98:8443/guestportal/gateway?sessionId=0a6984a00000004c536bac7b&action=cwa
*mmListen: May 08 05:52:50.588: 00:17:7c:2f:b8:6e Url redirect ACL REDIRECT

A handoff acknowledgement message is also sent to the foreign and can be seen in the debugs on
foreign:
*mmListen: May 08 12:10:38.802: 00:17:7c:2f:b8:6e Received Anchor Export Ack for client from
Switch IP: 10.105.132.141
*mmListen: May 08 12:10:38.802: 00:17:7c:2f:b8:6e Anchor Mac: d0:c2:82:e2:91:60, Old Foreign
Mac: 30:e4:db:1b:e0:a0 New Foreign Mac: 30:e4:db:1b:e0:a0
```

ステップ8：アンカーコントローラは、クライアントをDHCP required状態に移行します。クライアントがIPアドレスを取得すると、コントローラは処理を続行し、クライアントを中央Web認証の必須状態に移行します。アンカー上で収集されたshow client detailの出力でも同じことが分かります。

```
Client MAC Address........................... 00:17:7c:2f:b8:6e
AP MAC Address............................... 00:00:00:00:00:00
Client State................................. Associated
Wireless LAN Id.............................. 5
IP Address................................... 10.105.132.254
Mobility State............................... Export Anchor
Mobility Foreign IP Address.................. 10.105.132.160
Policy Manager State......................... CENTRAL_WEB_AUTH
AAA Override ACL Name........................ REDIRECT
AAA URL redirect.............................
https://10.106.73.98:8443/guestportal/gateway?sessionId=0a6984a00000004c536bac7b&action=cwa
```

ステップ9：外部WLCは、クライアントを実行状態に移行すると、同時にアカウンティングプロセスを開始します。ISEにアカウンティング開始メッセージを送信します。

```
*aaaQueueReader: May 08 12:10:38.803: AccountingMessage Accounting Start: 0x2b6c0a78
*aaaQueueReader: May 08 12:10:38.803: Packet contains 16 AVPs:
*aaaQueueReader: May 08 12:10:38.803: AVP[01] User-Name.............................00-17-7C-
2F-B8-6E (17 bytes)
```

注：アカウンティングは、外部WLCでのみ設定する必要があります。

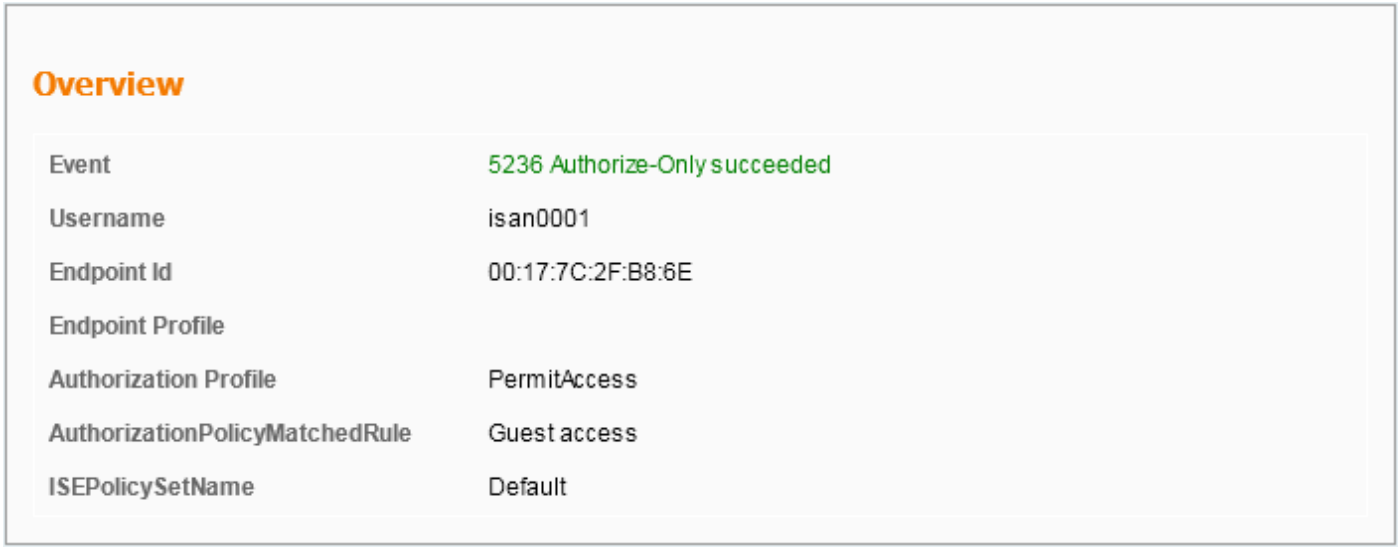
ステップ10：ユーザは、ブラウザにURLを入力して、Web認証リダイレクトプロセスを開始します。アンカーコントローラで関連するデバッグを確認できます。

```
*webauthRedirect: May 08 05:53:05.927: 0:17:7c:2f:b8:6e- received connection
*webauthRedirect: May 08 05:53:05.928: captive-bypass detection disabled, Not checking for wispr
in HTTP GET, client mac=0:17:7c:2f:b8:6e
*webauthRedirect: May 08 05:53:05.928: 0:17:7c:2f:b8:6e- Preparing redirect URL according to
configured Web-Auth type
*webauthRedirect: May 08 05:53:05.928: 0:17:7c:2f:b8:6e: Client configured with AAA overridden
redirect URL
https://10.106.73.98:8443/guestportal/gateway?sessionId=0a6984a00000004c536bac7b&action=cwa
```

ステップ11：また、webauthプロセスの認証部分がアンカーではなく外部WLCで処理されていることも確認できます。外部ルータのdebug AAA出力でも同じことが分かります。

```
*aaaQueueReader: May 08 12:11:11.537: AuthenticationRequest: 0x2b6c0a78
*aaaQueueReader: May 08 12:11:11.537: Callback.....................................0x10166e78
*aaaQueueReader: May 08 12:11:11.537: protocolType.................................0x40000001
*aaaQueueReader: May 08 12:11:11.537:
proxyState.....................................00:17:7C:2F:B8:6E-00:00
*aaaQueueReader: May 08 12:11:11.537: Packet contains 12 AVPs (not shown)
Authorization response from ISE:
*radiusTransportThread: May 08 12:11:11.552: AuthorizationResponse: 0x14c47c58
*radiusTransportThread: May 08 12:11:11.552: structureSize..............................252
*radiusTransportThread: May 08 12:11:11.552: resultCode.................................0
*radiusTransportThread: May 08 12:11:11.552:
protocolUsed................................0x00000001
*radiusTransportThread: May 08 12:11:11.552:
proxyState.....................................00:17:7C:2F:B8:6E-00:00
*radiusTransportThread: May 08 12:11:11.552: Packet contains 6 AVPs:
*radiusTransportThread: May 08 12:11:11.552: AVP[01] User-
Name.............................isan0001 (8 bytes) -----> (Username used for web
authentication)
*radiusTransportThread: May 08 12:11:11.552: AVP[02]
State.....................................ReauthSession:0a6984a00000004c536bac7b (38 bytes)
*radiusTransportThread: May 08 12:11:11.552: AVP[03]
Class.....................................CACS:0a6984a00000004c536bac7b:sid-ise-1-2/188796966/40
(54 bytes)
*radiusTransportThread: May 08 12:11:11.552: AVP[04] Session-
Timeout.........................0x00006e28 (28200) (4 bytes)
*radiusTransportThread: May 08 12:11:11.552: AVP[05] Termination-
Action.....................0x00000000 (0) (4 bytes)
*radiusTransportThread: May 08 12:11:11.552: AVP[06] Message-
Authenticator...................DATA (16 bytes)
```

図に示すように、ISEでも同じことが確認できます。



ステップ12：この情報はアンカーWLCに渡されます。このハンドシェイクはデバッグでは明確に表示されず、次に示すようにポストハンドオフポリシーを適用するアンカーによって確認できます。

```
*mmListen: May 08 05:53:23.337: 00:17:7c:2f:b8:6e Received Anchor Export policy update, valid
mask 0x900:
Qos Level: 0, DSCP: 0, dot1p: 0 Interface Name: , IPv4 ACL Name:
*mmListen: May 08 05:53:23.337: 00:17:7c:2f:b8:6e Applying post-handoff policy for station
00:17:7c:2f:b8:6e - valid mask 0x900
*mmListen: May 08 05:53:23.337: 00:17:7c:2f:b8:6e QOS Level: -1, DSCP: -1, dot1p: -1,
Data Avg: -1, realtime Avg: -1, Data Burst -1, Realtime Burst -1
*mmListen: May 08 05:53:23.337: 00:17:7c:2f:b8:6e Session: 0, User session: 28200, User elapsed
1
Interface: N/A, IPv4 ACL: N/A, IPv6 ACL: N/A.
```

認証が完了したことを確認する最善の方法は、ISEで渡されたログを確認し、次に示すようにクライアントが**RUN状態であることを示すコントローラのshow client detailの出力を収集することです。**

```
Client MAC Address.............................. 00:17:7c:2f:b8:6e
Client State.................................... Associated
Client NAC OOB State............................ Access
Wireless LAN Id................................. 5
IP Address...................................... 10.105.132.254
Mobility State.................................. Export Anchor
Mobility Foreign IP Address..................... 10.105.132.160
Policy Manager State............................ RUN
```

もう1つの重要なチェックは、アンカーが認証に成功した後にgratuitous Address Resolution Protocol(ARP)を送信するという事実です。

```
*pemReceiveTask: May 08 05:53:23.343: 00:17:7c:2f:b8:6e Sending a gratuitous ARP for
10.105.132.254, VLAN Id 20480
```

ここから、クライアントはアンカーコントローラによって転送されるすべてのタイプのトラフィックを自由に送信できます。

クライアントが切断されたときの中央Webauthフロー

セッション/アイドルタイムアウトが原因でクライアントエントリをWLCから削除する必要がある場合、またはWLCからクライアントを手動で削除する場合、次の手順が実行されます。

外部WLCは認証解除メッセージをクライアントに送信し、削除のスケジュールを設定します。

```
*apfReceiveTask: May 08 12:19:21.199: 00:17:7c:2f:b8:6e apfMsExpireMobileStation (apf_ms.c:6634)
Changing state for mobile 00:17:7c:2f:b8:6e on AP dc:a5:f4:ec:df:30 from Associated to
Disassociated
*apfReceiveTask: May 08 12:19:21.199: 00:17:7c:2f:b8:6e Sent Deauthenticate to mobile on BSSID
dc:a5:f4:ec:df:30 slot 0(caller apf_ms.c:6728
```

次に、クライアント認証セッションが終了したことをISEサーバに通知するradius stop accountingメッセージを送信します。

```
*aaaQueueReader: May 08 12:19:21.199: AccountingMessage Accounting Stop: 0x2b6d5684
*aaaQueueReader: May 08 12:19:21.199: Packet contains 24 AVPs:
*aaaQueueReader: May 08 12:19:21.199: AVP[01] User-Name.............................00-17-7C-
2F-B8-6E (17 bytes)
```

また、アンカーWLCにモビリティハンドオフメッセージを送信して、クライアントセッションを終了するように通知します。これは、アンカーWLCのモビリティデバッグで確認できます。

```
*mmListen: May 08 06:01:32.907: 00:17:7c:2f:b8:6e Received Handoff End request for client from
Switch IP: 10.105.132.160
*apfReceiveTask: May 08 06:01:32.907: 00:17:7c:2f:b8:6e apfMmProcessResponse: Handoff end rcvd
for mobile 00:17:7c:2f:b8:6e, delete mobile. reason code = 0
*apfReceiveTask: May 08 06:01:32.908: 00:17:7c:2f:b8:6e 10.105.132.254 RUN (20) mobility role
update request from Export Anchor to Handoff
Peer = 10.105.132.160, Old Anchor = 10.105.132.141, New Anchor = 0.0.0.0
*apfReceiveTask: May 08 06:01:32.908: 00:17:7c:2f:b8:6e apfMmProcessCloseResponse (apf_mm.c:647)
Expiring Mobile!
*apfReceiveTask: May 08 06:01:32.908: 00:17:7c:2f:b8:6e Mobility Response: IP 0.0.0.0 code
Anchor Close (5), reason Normal disconnect (0), PEM State DHCP_REQD, Role Handoff(6)
*apfReceiveTask: May 08 06:01:32.908: 00:17:7c:2f:b8:6e Deleting mobile on AP
00:00:00:00:00:00(0)
```

ISEで中断されたクライアントアカウント

ISEには、WLCにクライアントセッションの終了を通知するゲストユーザアカウントを一時停止する機能があります。これは、クライアントが接続されているWLCを確認する必要がなく、セッションを単純に終了する必要がない管理者に便利です。ゲストユーザアカウントがISEで一時停止または期限切れになった場合の動作を確認できます。

ISEサーバは、クライアント接続を削除する必要があることを示すChange of Authorization(CO)メッセージを外部コントローラに送信します。これはデバッグ出力で確認できます。

```
*radiusCoASupportTransportThread: May 13 02:01:53.446: 00:17:7c:2f:b8 :6e apfMsDeleteByMscb
Scheduling mobile for deletion with deleteReason 6, reason Code 252
*radiusCoASupportTransportThread: May 13 02:01:53.446: 00:17:7c:2f:b8:6e Schedul ing deletion of
Mobile Station: (callerId: 30) in 1 seconds
```

その後、外部WLCは認証解除メッセージをクライアントに送信します。

```
*apfReceiveTask: May 13 02:01:54.303: 00:17:7c:2f:b8:6e Sent Deauthenticate to mobile on BSSID
dc:a5:f4:ec:df:30 slot 0(caller apf_ms.c:5921)
```
また、アカウンティングサーバにアカウンティング停止メッセージを送信して、クライアント認証セッションを終了します。

```
*aaaQueueReader: May 13 02:01:54.303: AccountingMessage Accounting Stop: 0x2b6d2 c7c
*aaaQueueReader: May 13 02:01:54.303: Packet contains 23 AVPs:
*aaaQueueReader: May 13 02:01:54.303: AVP[01] User-Name.....................
.............00177c2fb86e (12 bytes)
```
ハンドオフメッセージは、クライアントセッションを終了するためにアンカーWLCにも送信されます。アンカーWLCでは次の情報が表示されます。

```
*mmListen: May 12 19:42:52.871: 00:17:7c:2f:b8:6e Received Handoff End request for client from
Switch IP: 10.105.132.160
*apfReceiveTask: May 12 19:42:52.872: 00:17:7c:2f:b8:6e apfMmProcessResponse: Handoff end rcvd
for mobile 00:17:7c:2f:b8:6e, delete mobile. reason code = 0
```

ゲストアンカーセットアップでの中央Web認証のトラブルシューティング

次に、CWAを使用する際に発生する一般的な問題とその修正方法について説明します。

シナリオ1.クライアントがSTART状態のままになり、IPアドレスを取得しない

MAC認証が有効であるため、中央Web認証シナリオでは、MAC認証が完了した後にアソシエーション応答が送信されます。この場合、WLCとRADIUSサーバの間で通信障害が発生した場合、またはRADIUSサーバに設定ミスが発生してアクセス拒否が送信された場合、クライアントが関連付けループに留まり、関連付け拒否を繰り返し受します。クライアント除外が有効になっている場合は、クライアントも除外される可能性があります。

radiusサーバの到達可能性は、**test aaa radiusコマンド**を使用して確認できます。このコマンドはコード8.2以降で使用できます。

次の参照リンクは、この使用方法を示しています。
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/212473-verify-radius-server-connectivity-with-t.html

シナリオ2：クライアントがIPアドレスを取得できない

クライアントがCWAゲストアンカーセットアップでIPアドレスの取得に失敗する理由はいくつかあります。

- **アンカーと外部のSSID設定が一致しません**

アンカーと外部WLCの間でSSID設定を同じにするのが理想的です。厳密なチェックが行われる側面には、L2/L3セキュリティ設定、DHCP設定、およびAAAオーバーライドのパラメータがあります。同じでない場合は、アンカーへのハンドオフが失敗し、アンカーデバッグに次のメッセージが表示されます。

```
DHCP dropping packet due to ongoing mobility handshake exchange, (siaddr 0.0.0.0, mobility state
= 'apfMsMmAnchorExportRequested'
```

これを軽減するには、SSID設定が同じアンカーおよび外部であることを確認する必要があります。

- **アンカーと外部WLC間のモビリティトンネルがダウン/フラッピングしている**

すべてのクライアントトラフィックは、IPプロトコル97を使用するモビリティデータトンネルで送信されます。モビリティトンネルがアップしていない場合は、ハンドオフが完了せず、クライアントが外部でRUN状態になりません。モビリティトンネルのステータスは**UP**と表示される必要があり、図に示すように**[Controller] > [Mobility Management] > [Mobility Groups]で確認**できます。

メンバとしてマッピングされているコントローラが1つだけ（foriegnまたはanchor）ある場合は、**[Monitor] > [Statistics] > [Mobility Statistics]でグローバルモビリティ統計情報を確認することもできます。**

- **アンカーまたは外部コントローラで設定されていないリダイレクトACL:**

radiusサーバによって送信されたリダイレクトACLの名前が外部WLCで設定された名前と一致しない場合、MAC認証が完了しても、クライアントは拒否され、DHCPの実行に進みません。クライアントトラフィックがアンカーで終端されるため、個々のACLルールを設定する必要はありません。リダイレクトACLと同じ名前で作成されたACLがある限り、クライアントはアンカーに引き渡されます。アンカーには、クライアントがwebauth required状態に移行できるように、ACL名とルールが正しく設定されている必要があります。

シナリオ3.クライアントがWebページにリダイレクトされない

Web認証ページの表示に失敗する理由もいくつか考えられます。WLC側の一般的な問題の一部を次に示します。

- **DNSサーバの問題**

DNSサーバの到達可能性や設定ミスの問題は、クライアントがリダイレクトに失敗する最も一般的な理由の1つです。また、WLCのログやデバッグには表示されないため、この処理が困難になる可能性があります。ユーザは、DHCPサーバからプッシュされたDNSサーバ設定が正しいかどうか、およびワイヤレスクライアントから到達可能かどうかを確認する必要があります。これを確認する最も簡単な方法は、動作していないクライアントからの単純なDNSルックアップです。

- **アンカーで内部DHCPサーバを使用すると、デフォルトゲートウェイが到達不能になります。**

内部DHCPサーバを使用する場合、デフォルトゲートウェイの設定が正しく、アンカーWLCに接続するスイッチポートでVLANが許可されていることを確認することが重要です。そうでない場合、クライアントはIPアドレスを取得しますが、何もアクセスできません。クライアントのARPテーブルで、ゲートウェイのMACアドレスを確認できます。これは、ゲートウェイへのL2接続と到達可能であることを確認する迅速な方法です。