了解访客锚点设置中的中心Web身份验证(CWA)并对其进行故障排除

目录

简介

本文档介绍中心Webauth如何在访客锚点设置中工作，以及生产网络中出现的一些常见问题，以及如何解决这些问题。

先决条件

要求

思科建议您了解如何在无线LAN控制器(WLC)上配置中心Webauth。

本文档提供有关中央Webauth配置的步骤：
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html

使用的组件

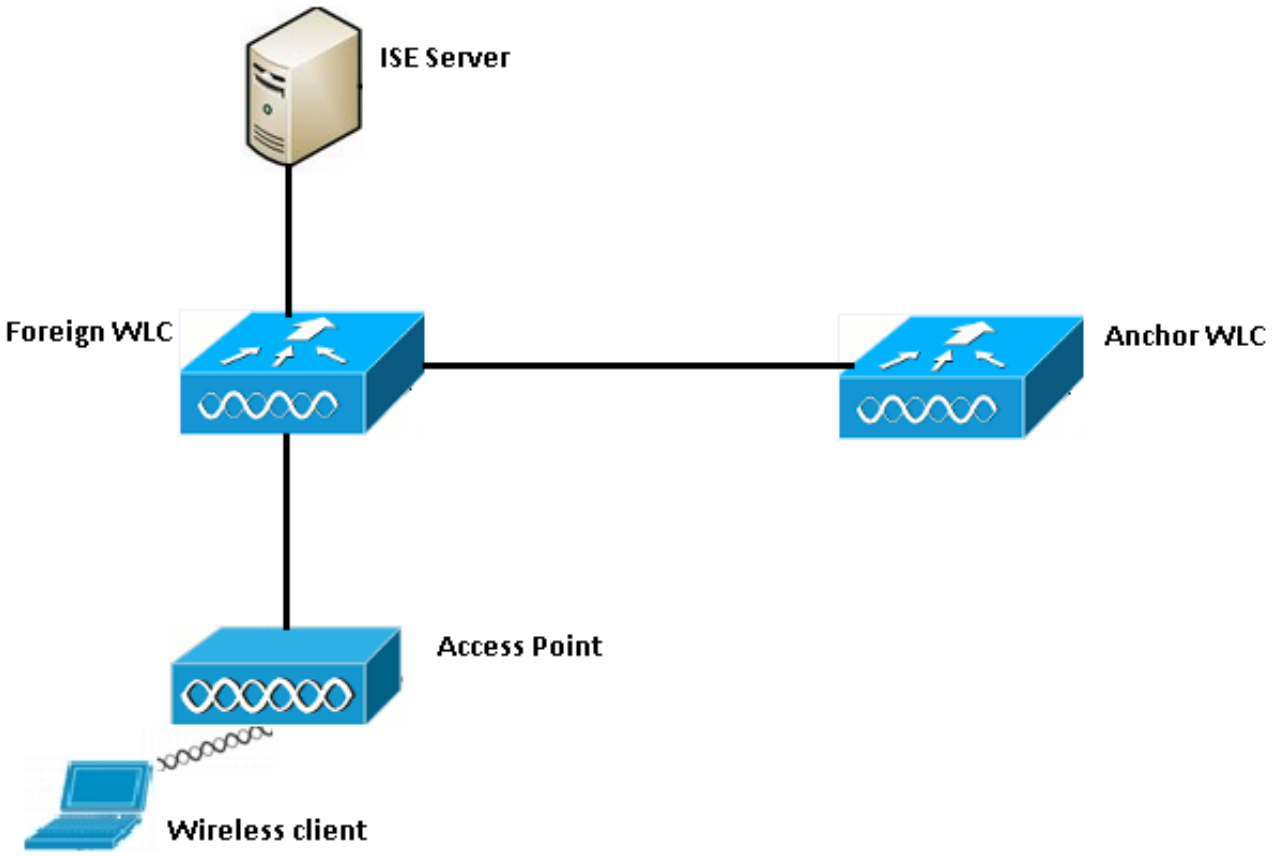
本文档中的信息基于以下软件和硬件版本：

- 运行版本7.6的WLC 5508
- 运行版本1.4的身份服务引擎(ISE)

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，请确保您了解任何命令的潜在影响

基本流

本节显示访客锚点设置中中心Webauth的基本工作流程，如图所示：



步骤1.客户端在发送关联请求时启动连接。

步骤2.当WLC向配置的ISE服务器发送身份验证请求时，WLC开始MAC身份验证过程。

步骤3.根据在ISE上配置的授权策略，Access-Accept消息将通过重定向URL和重定向访问控制列表(ACL)条目发回WLC。

步骤4.然后，外部WLC向客户端发送关联响应。

步骤5.此信息由外部WLC在移动切换消息中传递到锚点WLC。您需要确保在锚点和外部WLC上都配置了重定向ACL。

步骤6.在此阶段，客户端在外部WLC上进入“运行”状态。

步骤7.一旦客户端在浏览器中使用URL启动Web身份验证，锚点将启动重定向过程。

步骤8.客户端成功通过身份验证后，客户端在锚点WLC**上进**入RUN状态。

成功客户端连接尝试的中心Webauth流

现在，在进行调试时，您可以详细分析上述基本流。已在锚点和外部WLC上收集这些调试，以帮助您进行分析：

```
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
```

这些详细信息用于：

```
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
```

步骤1.客户端在发送关联请求时开始连接过程。在外部控制器上可以看到：

```
*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
```

步骤2. WLC发现无线局域网(WLAN)已映射以进行MAC身份验证，并将客户端移至AAA**挂起**状态。当它向ISE发送身份验证请求时，也会开始身份验证过程：

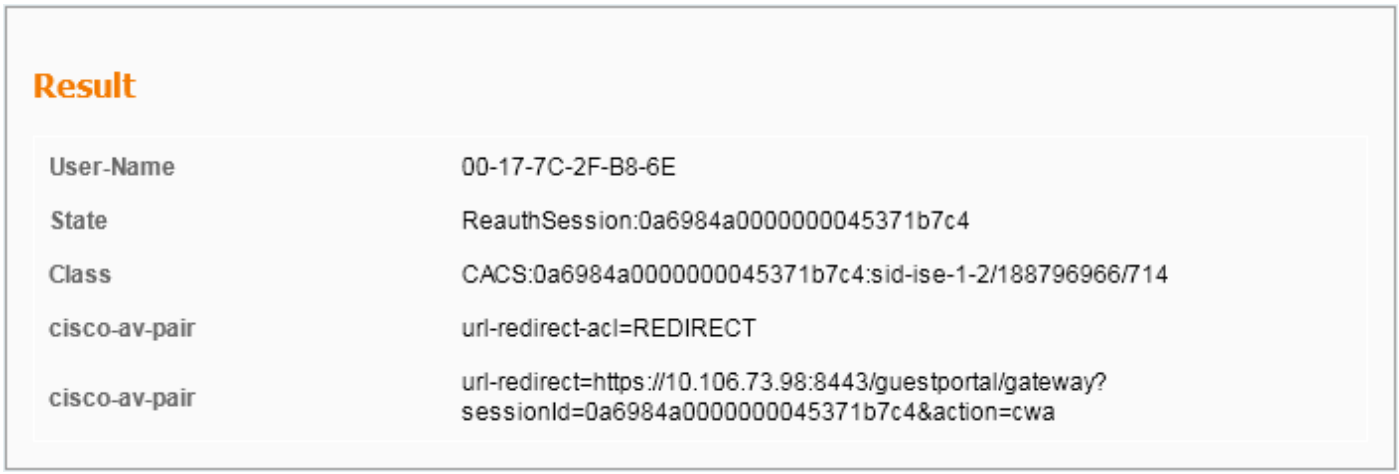
```
*apfMsConnTask_6: May 08 12:10:35.898: 00:17:7c:2f:b8:6e apfProcessAssocReq (apf_80211.c:8221)
Changing state for mobile 00:17:7c:2f:b8:6e on AP dc:a5:f4:ec:df:30 from Idle to AAA Pending
*aaaQueueReader: May 08 12:10:35.898: AuthenticationRequest: 0x2b6bf574

*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
```

步骤3.在ISE上，配置了MAC身份验证绕行，并在MAC身份验证后返回重定向URL和ACL。您可以在授权响应中看到以下参数发送：

```
*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)
```

您可以在ISE日志下看到相同的信息。导航至“操**作”>“身份**验证”，然**后单击“客**户端会话详细信息”，如图所示：



步骤4.然后，外部WLC将状态更改为L2身份验证完成，并将关联响应发送到客户端。

注意：启用MAC身份验证后，在完成此操作之前不会发送关联响应。

```
*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
```

步骤 5：然后，外部发起到锚的切换过程。以下是debug mobility handfort输出：

```
*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
```

步骤6.您可以看到客户端在外部WLC上进入RUN状态。客户端的正确状态现在只能在锚点上查看。以下是从外部收集的show client detail输出的片段（仅显示相关信息）：

```
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
```

步骤7.外部控制器发起与锚点的切换请求。您现在可以看到以下切换消息：

```
*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
```

步骤8.然后锚点控制器将客户端移至DHCP所需状态。一旦客户端获得IP地址，控制器将继续处理并将客户端移至中央Webauth必需状态。在锚点上收集的show client detail输出中，您可以看到相同的内容：

```
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
```

步骤9.外部WLC在将客户端移至运行状态后，会同时启动记帐过程。它向ISE发送记帐开始消息：

```
*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)
```

注意：只需在外部WLC上配置记帐。

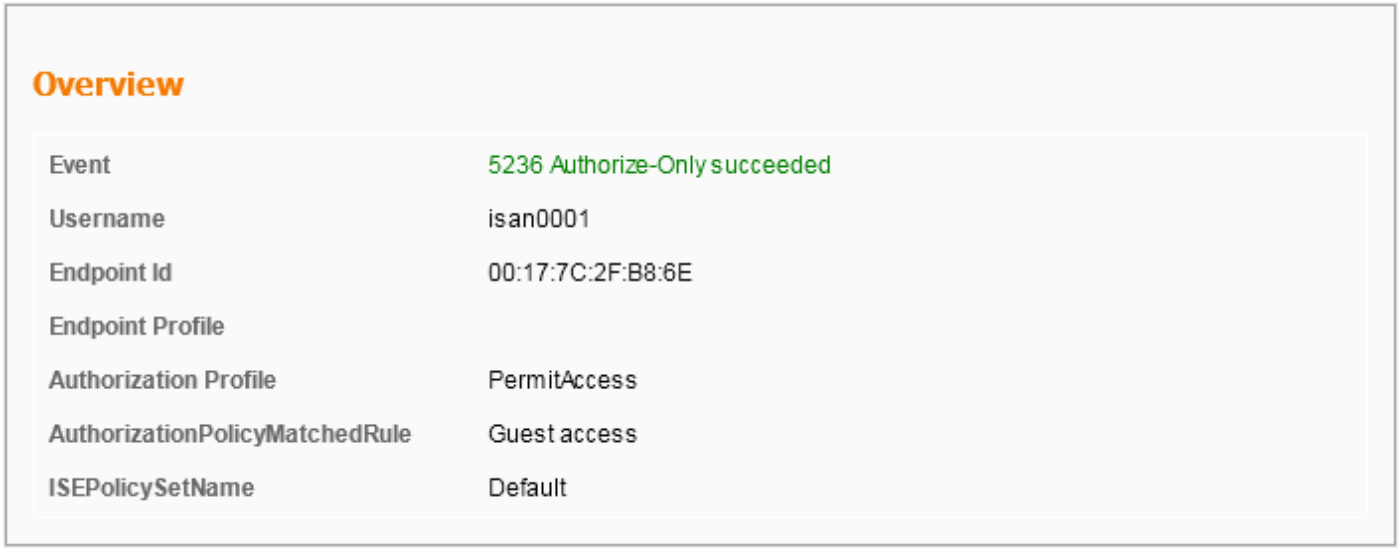
步骤10.然后，用户通过在浏览器中输入URL来启动网络身份验证重定向过程。您可以在锚点控制器上看到相关调试：

```
*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
```

步骤11.我们还可以看到，Webauth进程中的身份验证部分在外部WLC处理，而不是在锚点处理。在外部的调试AAA输出中，您可以看到相同的结果：

```
*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)
```

ISE上也可以验证，如图所示：



步骤12.此信息将传递到锚点WLC。此握手在调试中不明显可见，您可以通过应用后切换策略的锚点进行此操作，如下所示：

```
*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.
```

验证身份验证是否完成的最佳方法是验证ISE上通过的日志，并收集控制器上show client detail的输出，该输出应显示客户端处于**RUN**状态，如下所示：

```
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
```

另一个重要检查是锚点在成功进行身份验证后发送无偿地址解析协议(ARP):

```
*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
```

客户端可以从此处自由发送锚点控制器转发出去的所有类型的流量。

客户端断开连接时的中心Webauth流

当由于会话/空闲超时而需要从WLC中删除客户端条目，或者当我们手动从WLC中删除客户端时，将执行以下步骤：

外部WLC向客户端发送取消身份验证消息并安排其删除：

```
*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
```

然后，它会发送RADIUS停止记帐消息，通知ISE服务器客户端身份验证会话已结束：

```
*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)
```

它还向锚点WLC发送移动切换消息以通知它终止客户端会话。在锚点WLC上的移动调试中可以看到：

```
*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上的客户端帐户已暂停

ISE能够暂停访客用户帐户，该帐户指示WLC终止客户端会话。这对于无需检查客户端连接到哪个WLC并简单终止会话的管理员非常有用。您现在可以看到访客用户帐户在ISE上暂停/过期时会发生什么情况：

ISE服务器向外部控制器发送授权更改消息，该消息指示需要删除客户端连接。在调试输出中可以看到以下内容：

```
*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
```

然后，外部WLC向客户端发送取消身份验证消息：

```
*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)
```

它还向记帐服务器发送记帐停止消息以结束其端的客户端身份验证会话：

```
*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)
```

切换消息也发送到锚点WLC以终止客户端会话。您可以在锚点WLC上看到以下内容：

```
*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
```

对访客锚点设置中的中心Webauth进行故障排除

现在，我们来了解一下在使用CWA时遇到的一些常见问题，以及可以采取哪些措施来解决它。

场景1.客户端停滞在START状态且未获取IP地址

在中心Webauth场景中，自MAC身份验证启用后，在MAC身份验证完成后发送关联响应。在这种情况下，如果WLC与RADIUS服务器之间出现通信故障，或RADIUS服务器上配置错误导致其发送访问拒绝，您会看到客户端陷入关联循环，在该循环中，客户端会重复获得关联拒绝。如果启用了客户端排除，也有可能排除客户端。

可使用代码8.2及更高版本中**的test aaa radius命**令验证RADIUS服务器的可达性。

以下参考链接显示如何使用：
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/212473-verify-radius-server-connectivity-with-t.html

场景2.客户端无法获取IP地址

客户端在CWA访客锚点设置中无法获取IP地址的原因有几个。

- **锚点上的SSID配置与外部不匹配**

锚点和外部WLC之间的SSID配置相同是理想之选。严格检查的一些方面包括L2/L3安全配置、DHCP配置和AAA覆盖参数。如果情况不同，切换到锚点将失败，您可以在锚点调试中看到以下消息：

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

为了缓解这种情况，您需要确保SSID配置是相同的锚点和外部。

- **锚点和外部WLC之间的移动隧道关闭/摆动**

所有客户端流量都在使用IP协议97的移动数据隧道中发送。如果移动隧道未启用，则您可以看到切换未完成，并且客户端在外部不进入RUN状态。移动隧道状态需要显示为**UP**，并可在**Controller >Mobility Management >Mobility Groups下看**到，如图所示。

如果只有一个控制器映射为成员（外部或锚点），则还可以在“监控”>“统计”>“移动统计”下检查全**局移动统计信息。**

- **在锚点或外部控制器上未配置重定向ACL:**

当RADIUS服务器发送的重定向ACL的名称与外部WLC上配置的名称不匹配时，即使MAC身份验证完成，客户端也会被拒绝，并且不会继续执行DHCP。客户端流量在锚点上终止时，不必配置单个ACL规则。只要创建的ACL与重定向ACL的名称相同，客户端就会被转移到锚点。锚点需要正确配置ACL名称和规则，以便客户端转到webauth必需状态。

场景3.客户端未重定向到网页

Webauth页面无法显示的原因同样有几个。下面介绍一些常见的WLC侧问题：

- **DNS服务器问题**

DNS服务器可达性/配置错误问题是客户端无法重定向的最常见原因之一。这也很难捕捉，因为它不会出现在任何WLC日志或调试中。用户需要验证从DHCP服务器推送的DNS服务器配置是否正确以及是否可从无线客户端访问。从非工作客户端进行简单的DNS查找是检查此情况的最简单方法。

- **在锚点上使用内部DHCP服务器时，默认网关不可达：**

使用内部DHCP服务器时，必须确保默认网关配置正确，并且在连接到锚点WLC的交换机端口上允许VLAN。如果没有，客户端将获得IP地址，但无法访问任何内容。您可以在客户端的ARP表中查找网关的MAC地址。它是检验L2与网关的连接以及该网关是否可达的快速方法。