Understand And Troubleshoot Central Web-Authentication (CWA) In Guest Anchor Set-Up

Contents

Introduction

This document describes how central webauth works in a guest anchor setup and some of the common issues seen in a production network and how they can be fixed.

Prerequisites

Requirements

Cisco recommends that you have knowledge on how to configure central webauth on the Wireless LAN Controller (WLC).

This document provides steps with regards to configuration of central webauth: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html

Components Used

The information in this document is based on these software and hardware versions:

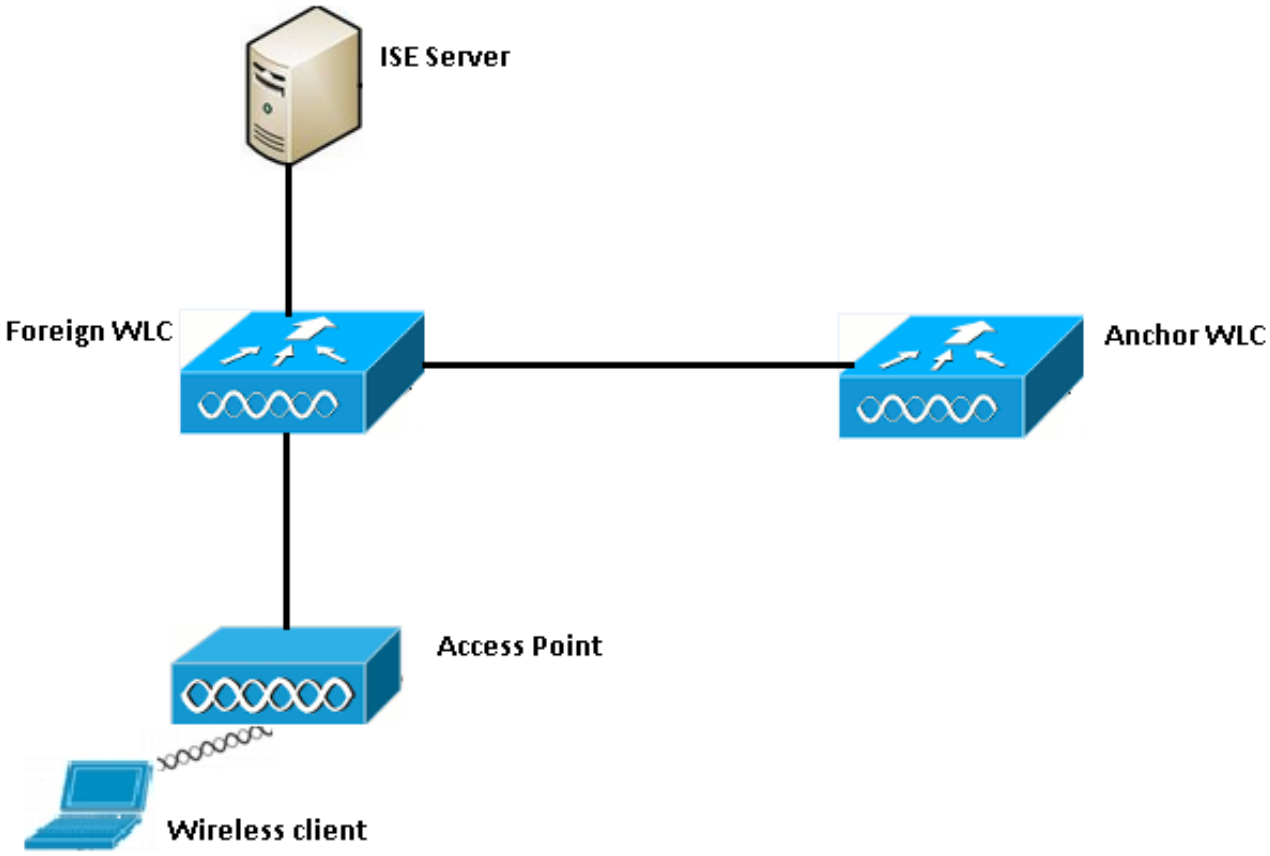
- WLC 5508 running version 7.6
- Identity Services Engine (ISE) running version 1.4

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of

any command

Basic flow

This section shows the basic workflow of central webauth in a guest anchor setup as shown in the image:



Step 1. Client starts the connection when it sends an association request.

Step 2. WLC begins the MAC authentication process when it sends an authentication request to the ISE server configured.

Step 3. Based on the authorization policy configured on ISE, the Access-Accept message is sent back to the WLC with the redirect URL and redirect Access Control List (ACL) entries.

Step 4. The foreign WLC then sends an association response to the client.

Step 5. This information is passed on by the foreign WLC to the anchor WLC in mobility handoff messages. You need to ensure that the redirect ACL's are configured on both the anchor and foreign WLC's.

Step 6. At this stage, the client moves into Run state on the foreign WLC.

Step 7. Once the client initiates web-auth with a URL in the browser, the anchor starts the redirection process.

Step 8. Once the client is successfully authenticated, the client moves into **RUN** state on the

anchor WLC.

Central Webauth Flow for Successful Client Connection Attempt

You can now analyze the basic flow described above in detail when you go through the debugs. These debugs have been collected on both the anchor and foreign WLC to help with your analysis:

```
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
```

These details are used here:

```
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
```

Step 1. The client begins the connection process when it sends an association request. This is seen on the foreign controller:

```
*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
```

Step 2. The WLC sees that the Wireless LAN (WLAN) is mapped for MAC authentication and moves the client to **AAA pending** status. It also begins the authentication process when it sends an authentication request to ISE:

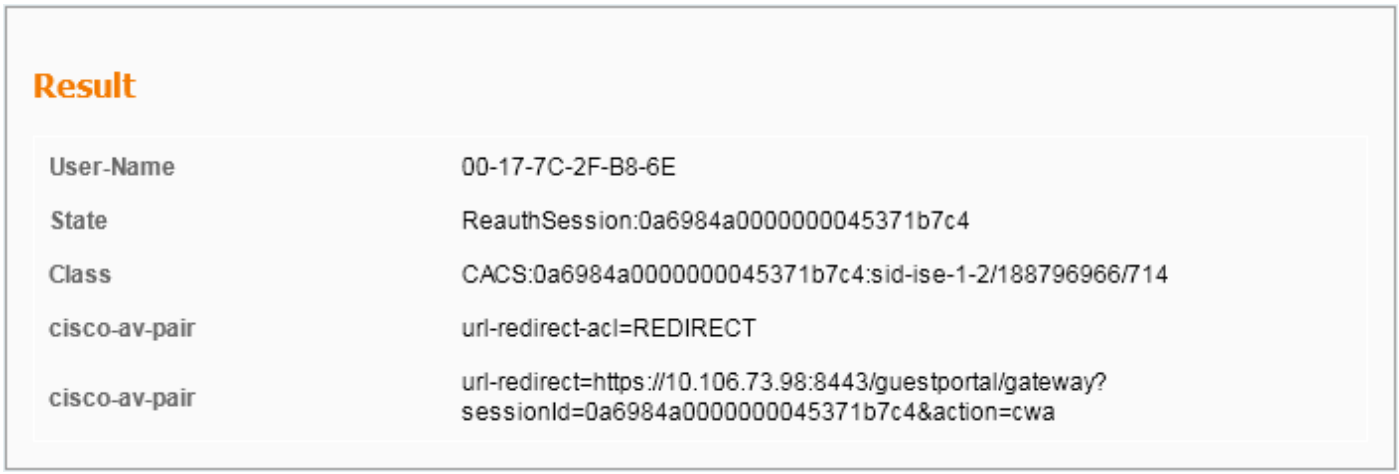
```
*apfMsConnTask_6: May 08 12:10:35.898: 00:17:7c:2f:b8:6e apfProcessAssocReq (apf_80211.c:8221)
Changing state for mobile 00:17:7c:2f:b8:6e on AP dc:a5:f4:ec:df:30 from Idle to AAA Pending
*aaaQueueReader: May 08 12:10:35.898: AuthenticationRequest: 0x2b6bf574

*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
```

Step 3. On the ISE, MAC authentication bypass is configured and it returns the redirect URL and ACL after MAC authentication. You can see these parameters sent in the authorization response:

```
*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)
```

You can see the same information under the ISE logs. Navigate to **Operations >Authentications** and click **Client session details** as shown in the image:



Step 4. The foreign WLC then changes the state to L2 auth complete and sends the association response to the client.

> **Note**: With MAC authentication enabled, association response is not sent until this is completed.

```
*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
```

Step 5: The foreign then initiates the handoff process to the anchor. This is seen the debug mobility handoff output:

```
*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
```

Step 6. You can see that the client moves into RUN state on the foreign WLC. The correct status of the client can now be seen only on the anchor. Here is a snippet of the show client detail output collected from the foreign (only relevant information is shown):

```
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
```

Step 7. The foreign controller initiates a handoff request with the anchor. You can now see the handoff messages below:

```
*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
```

Step 8. The anchor controller then moves the client to DHCP required state. Once the client gets an IP address, the controller continues to process and move the client into central webauth required state. You can see the same in the show client detail output collected on the anchor:

```
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
```

Step 9. The foreign WLC simultaneously starts the accounting process once it moves the client into run state. It sends the accounting start message to ISE:

```
*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)
```

Note: Accounting only needs to be configured on the foreign WLC.

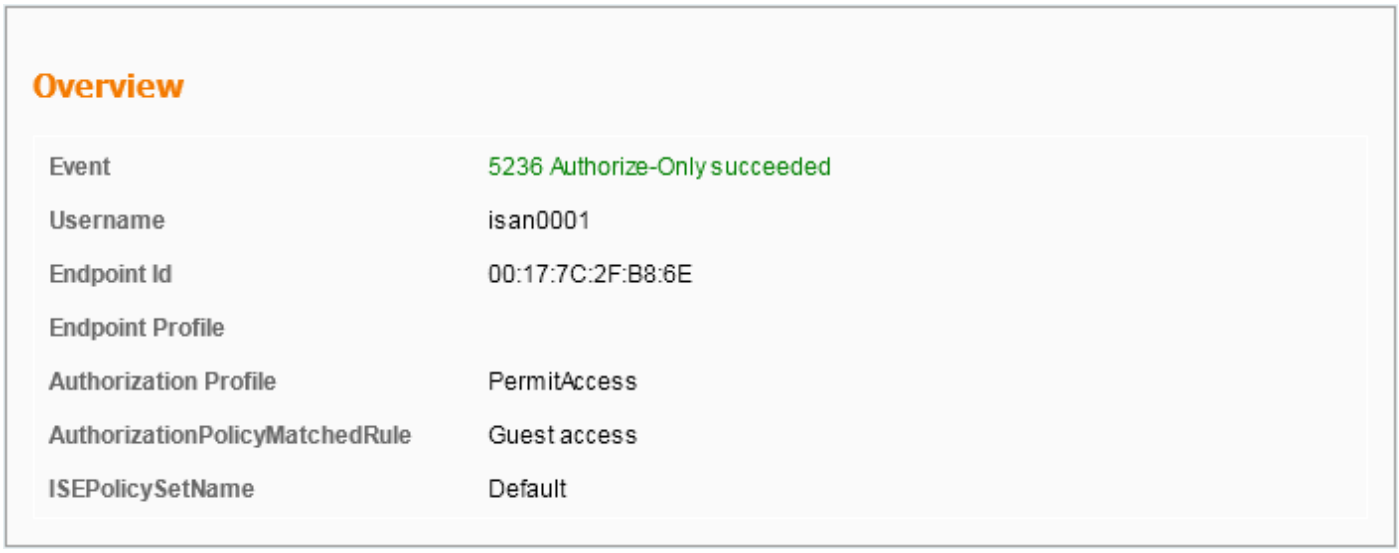
Step 10. The user then initiates the web-auth redirect process by entering a URL in the browser. You can see the relevant debugs on the anchor controller:

```
*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
```

Step 11. We can also see that the authentication part in the webauth process is handled at the foreign WLC and not at the anchor. You can see the same in the debug AAA outputs on the foreign:

```
*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)
```

The same can be verified on ISE as shown in the image:



Step 12. This information is passed onto the anchor WLC. This handshake is not clearly visible in the debugs and you can make this out by the anchor which applies a post handoff policy as shown here:

```
*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.
```

The best way to verify that authentication is complete is to verify the passed logs on ISE and collect the output of show client detail on the controller which should show the client in **RUN** state as shown here:

```
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
```

Another important check is the fact that the anchor sends a gratuitous Address Resolution Protocol (ARP) after successful authentication:

```
*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
```

From here the client is free to send all types of traffic which is forwarded out by the anchor controller.

Central Webauth Flow when Client Gets Disconnected

When a client entry needs to be removed from the WLC either due to a session/idle timeout or when we manually remove the client from the WLC, these steps take place:

Foreign WLC sends a de-authenticate message to the client and schedules it for deletion:

```
*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
```

It then sends a radius stop accounting message to inform the ISE server that the client authentication session has ended:

```
*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)
```

It also sends a mobility handoff message to the anchor WLC to inform it to terminate the client session. This can be seen in the mobility debugs on the anchor WLC:

```
*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)
```

Client Account Suspended on ISE

ISE has the ability to suspend a guest user account which signals the WLC to terminate the client session. This is useful for administrators who do not need to check which WLC the client is connected to and simply terminate the session. You can now see what happens when the guest user account is suspended/expired on ISE:

The ISE server sends a Change of Authorization message to the foreign controller which indicates that the client connection needs to be removed. This can be seen in the debug outputs:

```
*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
```

Foreign WLC then sends a de-authenticate message to the client:

```
*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)
```

It also sends an accounting stop message to the accounting server to end the client authentication session on its side:

```
*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)
```

A handoff message is also sent to the anchor WLC to terminate the client session. You can see this on the anchor WLC:

```
*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
```

Troubleshoot Central Webauth in Guest Anchor Set-Up

Let’s now have a look at some of the common issues seen when you use CWA and what can be done to fix it.

Scenario 1. Client Stuck in START State and Does Not Get IP Address

In a central webauth scenario since MAC authentication is enabled, association responses are sent after a MAC authentication is completed. In this case, if there is a communication failure between the WLC and the radius server or there is a misconfig on the radius server which causes it to send access-rejects, you can see the client stuck in an association loop where it repeatedly gets an association reject. There is also a chance that the client gets excluded as well if client exclusion is enabled.

The radius server reachability can be verified with the **test aaa radius** command which is available in code 8.2 and above.

The below reference link shows how to use this:
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/212473-verify-radius-server-connectivity-with-t.html

Scenario 2. Client is Unable to Get IP Address

There are a few reasons why a client can fail to get an IP address in a CWA guest anchor setup.

- **SSID config on the anchor and foreign does not match**

It is ideal to have SSID config same between the anchor and foreign WLC's. Some of the aspects for which a strict check is done are L2/L3 security config, DHCP config and AAA override parameters. In case this is not the same, a handoff to the anchor fails and you can see these messages in the anchor debugs:

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

In order to mitigate this, you need to ensure that the SSID config is the same anchor and foreign.

- **Mobility tunnel between anchor and foreign WLC's are down/flapping**

All client traffic is sent in mobility data tunnel which uses IP protocol 97. If the mobility tunnel is not up then you can see that the handoff does not complete and client does not move into RUN state on the foreign. The mobility tunnel status needs to show as **UP** and can be seen under **Controller >Mobility Management >Mobility Groups** as shown in the image.

If there is only one controller mapped as a member (either foriegn or anchor), then you can also check the global mobility statistics under **Monitor >Statistics > Mobility Statistics.**

- **Redirect ACL not configured on either the anchor or foreign controllers:**

When the name of the redirect ACL sent by the radius server does not match what is configured on the foreign WLC, then even though MAC authentication is completed, the client is rejected and does not proceed to do DHCP. It is not mandatory to configure the individual ACL rules as client traffic is terminated on the anchor. As long as there is an ACL created with the same name as the redirect ACL, the client is handed off to the anchor. The anchor needs to have the ACL name and rules configured correctly for the client to move to webauth required state.

Scenario 3. Client Does not Get Redirected to Web Page

There are again a few different reasons why a webauth page can fail to get displayed. Some of the common WLC side issues are covered here:

- **DNS server issues**

DNS server reachability/misconfig issues are one of the most common reasons why clients fail to get redirected. This can also be hard to catch as it does not show up in any WLC logs or debugs. The user needs to verify if the DNS server config pushed from the DHCP server is correct and whether it is reachable from the wireless client. A simple DNS lookup from the non-working client is the easiest way to check this.

- **Default gateway un-reachable when you use internal DHCP server on anchor:**

When you use internal DHCP servers, it is important to ensure that the default-gateway config is correct and the VLAN is allowed on the switchport which connects to the anchor WLC. If not, the client gets an IP address, but it won't be able to access anything. You can check the ARP table on the client for the gateway's MAC address. It is a quick way to verify the L2 connectivity to the gateway and that it is reachable.