Comprender Y Resolver Problemas De Autenticación Web Central (CWA) En Configuración De Anclaje De Invitado

Contenido

Introducción

Este documento describe cómo funciona el webauth central en una configuración de anclaje de invitado y algunos de los problemas comunes que se ven en una red de producción y cómo se pueden corregir.

Prerequisites

Requirements

Cisco recomienda que tenga conocimientos sobre cómo configurar la autenticación web central en el controlador de LAN inalámbrica (WLC).

Este documento proporciona los pasos con respecto a la configuración de webauth central: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

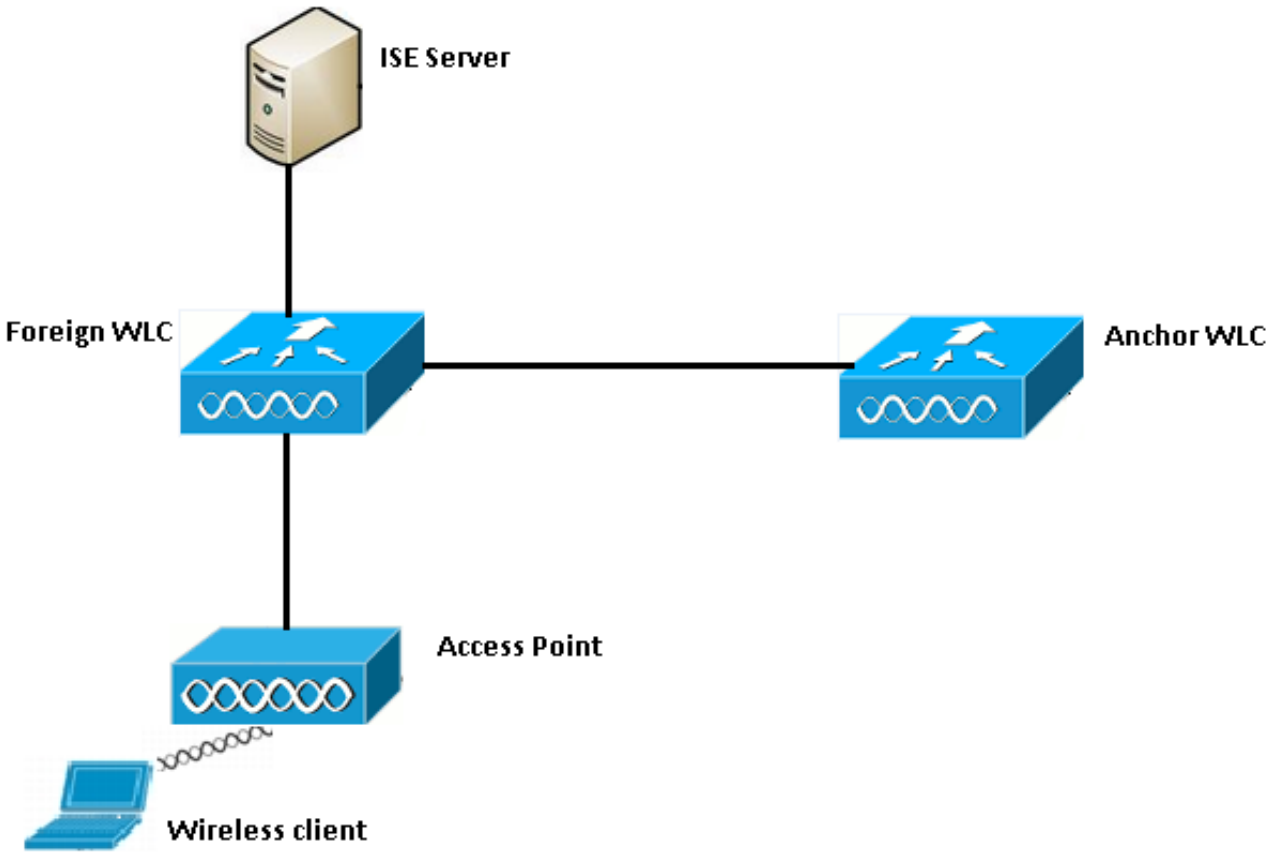
- WLC 5508 que ejecuta la versión 7.6
- Identity Services Engine (ISE) que ejecuta la versión 1.4

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando

Flujo básico

Esta sección muestra el flujo de trabajo básico de webauth central en una configuración de anclaje de invitado como se muestra en la imagen:



Paso 1. El cliente inicia la conexión cuando envía una solicitud de asociación.

Paso 2. El WLC inicia el proceso de autenticación MAC cuando envía una solicitud de autenticación al servidor ISE configurado.

Paso 3. Según la política de autorización configurada en ISE, el mensaje Access-Accept se envía de vuelta al WLC con la URL de redirección y las entradas de la Lista de control de acceso (ACL) de redirección.

Paso 4. El WLC externo entonces envía una respuesta de asociación al cliente.

Paso 5. Esta información es transmitida por el WLC externo al WLC de anclaje en los mensajes de transferencia de movilidad. Debe asegurarse de que las ACL de redirección estén configuradas tanto en el WLC de anclaje como en el WLC externo.

Paso 6. En esta etapa, el cliente pasa al estado Run en el WLC externo.

Paso 7. Una vez que el cliente inicia web-auth con una URL en el navegador, el ancla inicia el proceso de redirección.

Paso 8. Una vez que el cliente se autentica exitosamente, el cliente pasa al estado **RUN** en el WLC de anclaje.

Flujo de Webauth central para un intento de conexión de cliente exitoso

Ahora puede analizar el flujo básico descrito anteriormente detalladamente cuando se realiza la depuración. Estas depuraciones se han recopilado tanto en el WLC de anclaje como en el WLC externo para ayudar con su análisis:

```
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
```

Estos detalles se utilizan aquí:

```
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
```

Paso 1. El cliente inicia el proceso de conexión cuando envía una solicitud de asociación. Esto se ve en el controlador externo:

```
*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
```

Paso 2. El WLC ve que la LAN inalámbrica (WLAN) está asignada para la autenticación MAC y mueve el cliente al estado **AAA pendiente**. También comienza el proceso de autenticación cuando envía una solicitud de autenticación a ISE:

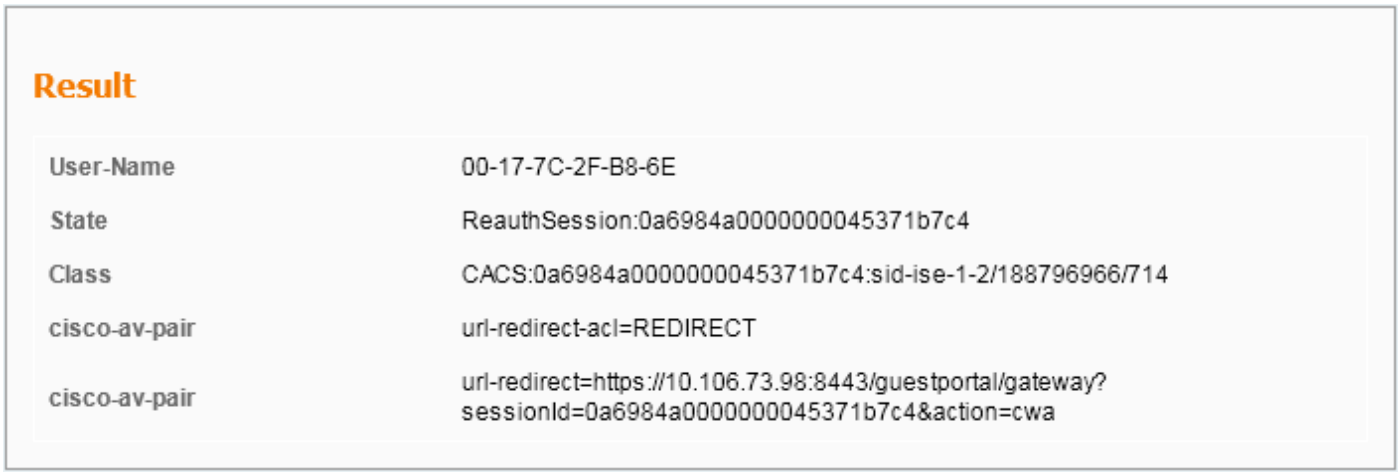
```
*apfMsConnTask_6: May 08 12:10:35.898: 00:17:7c:2f:b8:6e apfProcessAssocReq (apf_80211.c:8221)
Changing state for mobile 00:17:7c:2f:b8:6e on AP dc:a5:f4:ec:df:30 from Idle to AAA Pending
*aaaQueueReader: May 08 12:10:35.898: AuthenticationRequest: 0x2b6bf574

*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
```

Paso 3. En el ISE, se configura el desvío de la autenticación MAC y devuelve la URL de redirección y la ACL después de la autenticación MAC. Puede ver estos parámetros enviados en la respuesta de autorización:

```
*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)
```

Puede ver la misma información en los registros de ISE. Navegue hasta **Operaciones >Autenticaciones** y haga clic en **Detalles de sesión del cliente** como se muestra en la imagen:



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

Paso 4. El WLC externo luego cambia el estado a L2 auth complete y envía la respuesta de asociación al cliente.

> **Nota:** Con la autenticación MAC activada, la respuesta de asociación no se envía hasta que se complete.

```
*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
```

Paso 5: El Foreign inicia luego el proceso de entrega al ancla. Esto se ve en el resultado de debug mobility handoff:

```
*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
```

Paso 6. Puede ver que el cliente se mueve al estado RUN en el WLC externo. El estado correcto del cliente ahora sólo se puede ver en el ancla. A continuación se muestra un fragmento de la

salida show client detail recopilada del archivo externo (sólo se muestra la información relevante):

```
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
```

Paso 7. El controlador externo inicia una solicitud de entrega con el ancla. Ahora puede ver los siguientes mensajes de entrega:

```
*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
```

Paso 8. A continuación, el controlador de anclaje mueve el cliente al estado requerido por DHCP. Una vez que el cliente obtiene una dirección IP, el controlador continúa procesando y trasladando al cliente al estado requerido de webauth central. Puede ver lo mismo en el resultado show client detail recopilado en el ancla:

```
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
```

Paso 9. El WLC externo inicia simultáneamente el proceso de contabilización una vez que mueve

el cliente al estado de ejecución. Envía el mensaje de inicio de contabilización a 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)
```

Nota: La contabilidad sólo necesita ser configurada en el WLC externo.

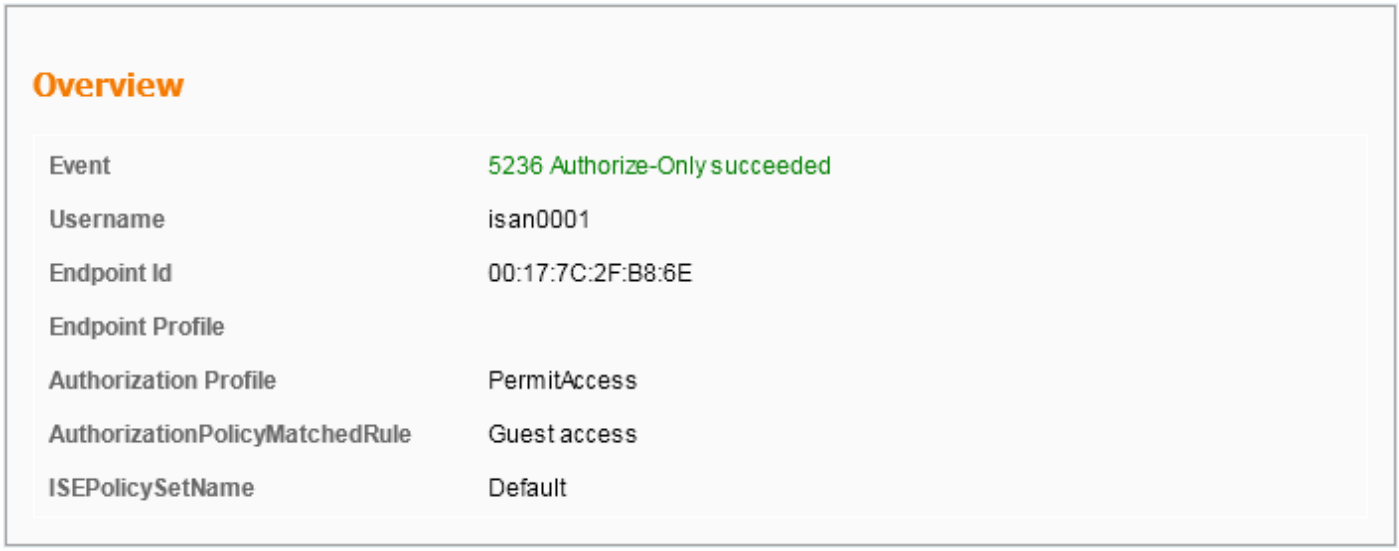
Paso 10. A continuación, el usuario inicia el proceso de redirección de autenticación web introduciendo una dirección URL en el explorador. Puede ver las depuraciones relevantes en el controlador de anclaje:

```
*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
```

Paso 11. También podemos ver que la parte de autenticación en el proceso webauth se maneja en el WLC extranjero y no en el ancla. Puede ver lo mismo en los resultados de debug AAA en el comando outside:

```
*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)
```

Lo mismo se puede verificar en ISE, como se muestra en la imagen:



Paso 12. Esta información se pasa al WLC de anclaje. Este intercambio de señales no está claramente visible en las depuraciones y puede hacerlo mediante el delimitador que aplica una política de transferencia de publicaciones como se muestra aquí:

```
*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.
```

La mejor manera de verificar que la autenticación esté completa es verificar los registros pasados en ISE y recopilar el resultado de show client detail en el controlador que debería mostrar al cliente en el estado **RUN** como se muestra aquí:

```
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
```

Otra comprobación importante es el hecho de que el anclaje envía un protocolo gratuito de resolución de direcciones (ARP) después de una autenticación correcta:

```
*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
```

Desde aquí el cliente es libre de enviar todos los tipos de tráfico que el controlador de anclaje reenvía.

Flujo de Webauth central cuando el cliente se desconecta

Cuando una entrada de cliente necesita ser eliminada del WLC ya sea debido a un tiempo de espera de sesión/inactividad o cuando removemos manualmente al cliente del WLC, estos pasos ocurren:

El WLC externo envía un mensaje de desautenticación al cliente y lo programa para su eliminación:

```
*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
```

A continuación, envía un mensaje de contabilización de detención de RADIUS para informar al servidor ISE de que la sesión de autenticación del cliente ha finalizado:

```
*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)
```

También envía un mensaje de transferencia de movilidad al WLC de anclaje para informarlo de que finalice la sesión del cliente. Esto se puede ver en los debugs de movilidad en el WLC de anclaje:

```
*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)
```

Cuenta de cliente suspendida en ISE

ISE tiene la capacidad de suspender una cuenta de usuario invitado que indica al WLC que termine la sesión del cliente. Esto es útil para los administradores que no necesitan verificar a qué WLC está conectado el cliente y simplemente terminar la sesión. Ahora puede ver qué sucede cuando la cuenta de usuario invitado se suspende o caduca en ISE:

El servidor ISE envía un mensaje de cambio de autorización al controlador externo que indica que la conexión del cliente debe ser eliminada. Esto se puede ver en las salidas de depuración:

```
*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
```

El WLC externo entonces envía un mensaje de desautenticación al cliente:

```
*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)
```

También envía un mensaje de detención de contabilización al servidor de contabilización para finalizar la sesión de autenticación del cliente en su lado:

```
*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)
```

También se envía un mensaje de entrega al WLC de anclaje para terminar la sesión del cliente. Puede ver esto en el WLC de anclaje:

```
*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
```

Solución de problemas de Central Webauth en la configuración de Guest Anchor

Veamos ahora algunos de los problemas habituales que se observan al utilizar CWA y qué se puede hacer para solucionarlos.

Escenario 1. El cliente se bloquea en el estado START y no obtiene la dirección IP

En un escenario webauth central, dado que la autenticación MAC está habilitada, las respuestas de asociación se envían después de que se complete la autenticación MAC. En este caso, si hay una falla de comunicación entre el WLC y el servidor radius o hay una configuración incorrecta en el servidor radius que hace que envíe rechazos de acceso, puede ver al cliente atascado en un loop de asociación donde se obtiene una asociación rechazada repetidamente. También existe la posibilidad de que se excluya al cliente si se habilita la exclusión del cliente.

El alcance del servidor radius se puede verificar con el comando **test aaa radius** disponible en el código 8.2 y superior.

El siguiente enlace de referencia muestra cómo utilizar esto: https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/212473-verify-radius-server-connectivity-with-t.html

Situación hipotética 2. El cliente no puede obtener la dirección IP

Hay algunas razones por las que un cliente no puede obtener una dirección IP en una configuración de anclaje de invitado de CWA.

- **La configuración de SSID en el anclaje y la configuración externa no coincide**

Es ideal tener la configuración SSID igual entre el WLC del anclaje y el WLC externo. Algunos de

los aspectos para los cuales se realiza una verificación estricta son los parámetros de configuración de seguridad L2/L3, configuración DHCP y invalidación AAA. En caso de que esto no sea lo mismo, un traspaso al delimitador falla y puede ver estos mensajes en las depuraciones de anclaje:

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

Para mitigar esto, debe asegurarse de que la configuración de SSID sea la misma ancla y externa.

- **El túnel de movilidad entre el anclaje y el WLC externo está desactivado/inestable**

Todo el tráfico del cliente se envía en el túnel de datos de movilidad que utiliza el protocolo IP 97. Si el túnel de movilidad no está activo, puede ver que la transferencia no se completa y el cliente no pasa al estado RUN en el Foreign. El estado del túnel de movilidad debe mostrarse como **UP** y puede verse en **Controller >Gestión de movilidad >Grupos de movilidad** como se muestra en la imagen.

Si sólo hay un controlador asignado como miembro (ya sea externo o ancla), también puede verificar las estadísticas de movilidad global bajo **Monitor > Statistics > Mobility Statistics.**

- **Redirigir ACL no configurado en el controlador de anclaje o en el controlador externo:**

Cuando el nombre de la ACL de redirección enviada por el servidor RADIUS no coincide con lo que se configura en el WLC externo, a pesar de que la autenticación MAC se complete, el cliente se rechaza y no procede a hacer DHCP. No es obligatorio configurar las reglas de ACL individuales ya que el tráfico del cliente finaliza en el anclaje. Mientras haya una ACL creada con el mismo nombre que la ACL de redirección, el cliente se entrega al anclaje. El ancla necesita tener el nombre de ACL y las reglas configuradas correctamente para que el cliente pase al estado requerido de webauth.

Situación hipotética 3. El cliente no se redirige a la página Web

De nuevo, hay varias razones por las que una página de webauth no puede mostrarse. Algunos de los problemas comunes del WLC se tratan aquí:

- **Problemas del servidor DNS**

Los problemas de disponibilidad/configuración incorrecta del servidor DNS son una de las razones más comunes por las que los clientes no pueden ser redirigidos. Esto también puede ser difícil de detectar ya que no aparece en ningún registro o depuración del WLC. El usuario debe verificar si la configuración del servidor DNS enviada desde el servidor DHCP es correcta y si se puede alcanzar desde el cliente inalámbrico. Una búsqueda de DNS simple del cliente que no funciona es la manera más fácil de verificar esto.

- **El gateway predeterminado es inalcanzable cuando se utiliza el servidor DHCP interno en el anclaje:**

Cuando utiliza servidores DHCP internos, es importante asegurarse de que la configuración del gateway predeterminado sea correcta y que la VLAN esté permitida en el puerto del switch que se conecta al WLC del ancla. Si no, el cliente obtiene una dirección IP, pero no podrá acceder a nada. Puede verificar la tabla ARP en el cliente para la dirección MAC del gateway. Se trata de una forma rápida de verificar la conectividad L2 al gateway y que es accesible.