Entienda y resuelva problemas la autenticación Web central (CWA) en configuración del ancla del invitado

Contenido

Introducción

Este documento describe cómo el webauth central trabaja en un ancla del invitado puesta y algunos de los problemas frecuentes considerados en una red de producción y cómo pueden ser reparados.

Prerequisites

Requisitos

Cisco recomienda que usted tiene conocimiento en cómo configurar el webauth central en el regulador del Wireless LAN (WLC).

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

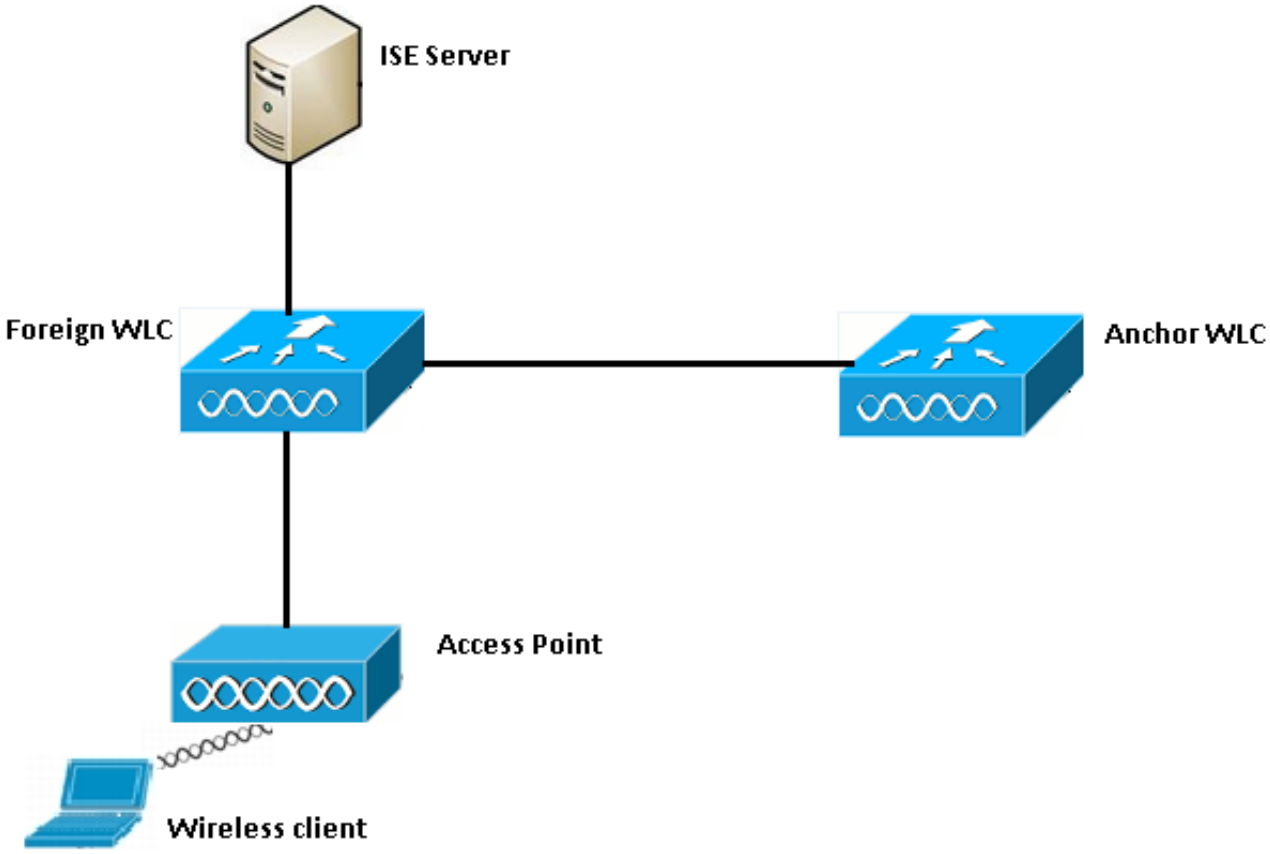
Componentes Utilizados

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

- Versión 7.6 corriente del WLC 5508
- Versión 1.4 corriente del Identity Services Engine (ISE)

Flujo básico

Esta sección muestra el flujo de trabajo básico del webauth central en un ancla del invitado puesta tal y como se muestra en de la imagen:



Paso 1. El cliente comienza la conexión cuando envía una petición de la asociación.

Paso 2. El WLC comienza el proceso de autenticación de MAC cuando envía un pedido de autenticación al servidor ISE configurado.

Paso 3. De acuerdo con la directiva de la autorización configurada en el ISE, el mensaje del access-accept se devuelve al WLC con la reorientación URL y reorienta las entradas de lista de control de acceso (ACL).

Paso 4. El WLC no nativo entonces envía una respuesta de la asociación al cliente.

Paso 5. Esta información es pasada encendido por el WLC no nativo al WLC del ancla en los mensajes de las manos de la movilidad. Usted necesita asegurarse de que la reorientación ACL esté configurada en el ancla y WLC no nativos.

Paso 6. En esta etapa, el cliente se traslada al estado de funcionamiento en el WLC no nativo.

Paso 7. Una vez que el cliente inicia el red-auth con un URL en el navegador, el ancla comienza el proceso de redireccionamiento.

Paso 8. Una vez que autentican al cliente con éxito, el cliente se traslada al estado de **FUNCIONAMIENTO** en el WLC del ancla.

Flujo central de Webauth para la tentativa acertada de la conexión cliente

Usted puede ahora analizar el flujo básico descrito arriba detalladamente cuando usted pasa con los debugs. Estos debugs se han recogido en el ancla y el WLC no nativo 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 comienza el proceso de la conexión cuando envía una petición de la asociación. Esto se ve en el regulador no nativo:

```
*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 el Wireless LAN (red inalámbrica (WLAN)) está asociado para la autenticación de MAC y mueve al cliente al **estado pendiente AAA**. También comienza el proceso de autenticación cuando envía un pedido de autenticación al ISE:

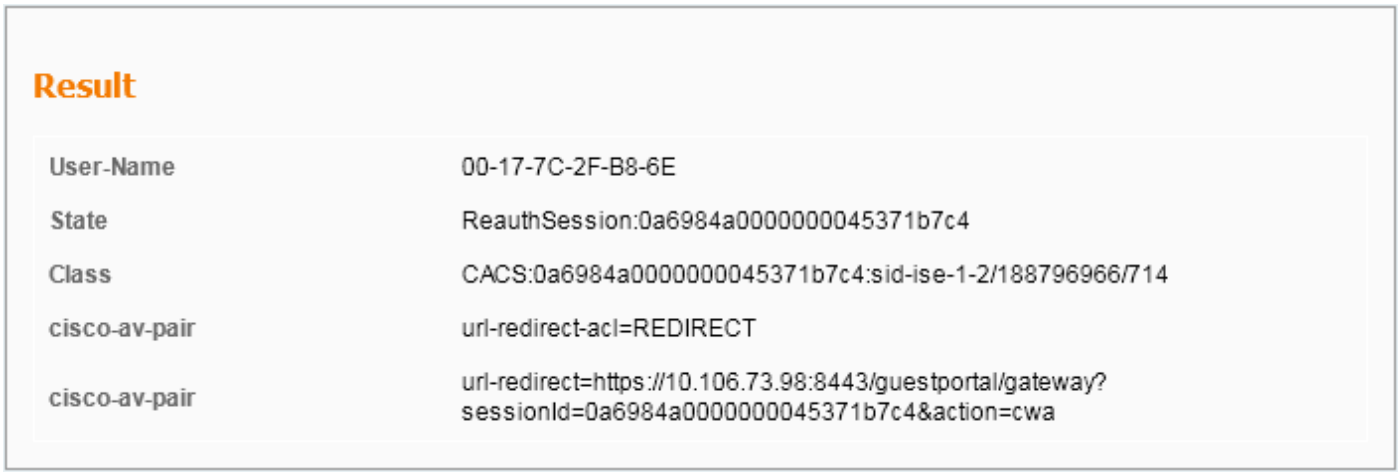
```
*apfMsConnTask_6: May 08 12:10:35.898: 00:17:7c:2f:b8:6e apfProcessAssocReq (apf_80211.c:8221)
Changing state for mobile 00:17:7c:2f:b8:6e on AP dc:a5:f4:ec:df:30 from Idle to AAA Pending
*aaaQueueReader: May 08 12:10:35.898: AuthenticationRequest: 0x2b6bf574

*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 puente de la autenticación de MAC y vuelve la reorientación URL y ACL después de la autenticación de MAC. Usted 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)
```

Usted puede ver la misma información bajo los registros ISE. Navegue a los **>Authentications de las operaciones** y haga clic a los **detalles de la sesión de cliente** tal y como se muestra en de 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 no nativo después cambia el estado al auth L2 completo y envía la respuesta de la asociación al cliente.

> **Note**: Con la autenticación de MAC habilitada, la respuesta de la asociación no se envía hasta que se complete esto.

```
*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 no nativo entonces inicia el proceso de las manos al ancla. Éste es visto las manos de la movilidad del debug hechas salir:

```
*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. Usted puede ver que el cliente se traslada al estado de FUNCIONAMIENTO en el WLC no nativo. El estado correcto del cliente puede ahora ser considerado solamente en el ancla. Aquí está un snippet de la salida del detalle del cliente de la demostración recogida del no nativo (solamente se muestra la información pertinente):

```
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 regulador no nativo inicia una petición de las manos con el ancla. Usted puede ahora ver los mensajes de las manos abajo:

```
*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. El regulador del ancla entonces mueve al cliente al estado requerido DHCP. Una vez que el cliente consigue una dirección IP, el regulador continúa procesando y trasladándose al cliente al estado requerido webauth central. Usted puede ver lo mismo en la salida del detalle del cliente de la demostración recogida 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 no nativo comienza simultáneamente el proceso de las estadísticas una vez que se traslada al cliente al estado de funcionamiento. Envía el mensaje del comienzo de las estadísticas al 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: El considerar necesita solamente ser configurado en el WLC no nativo.

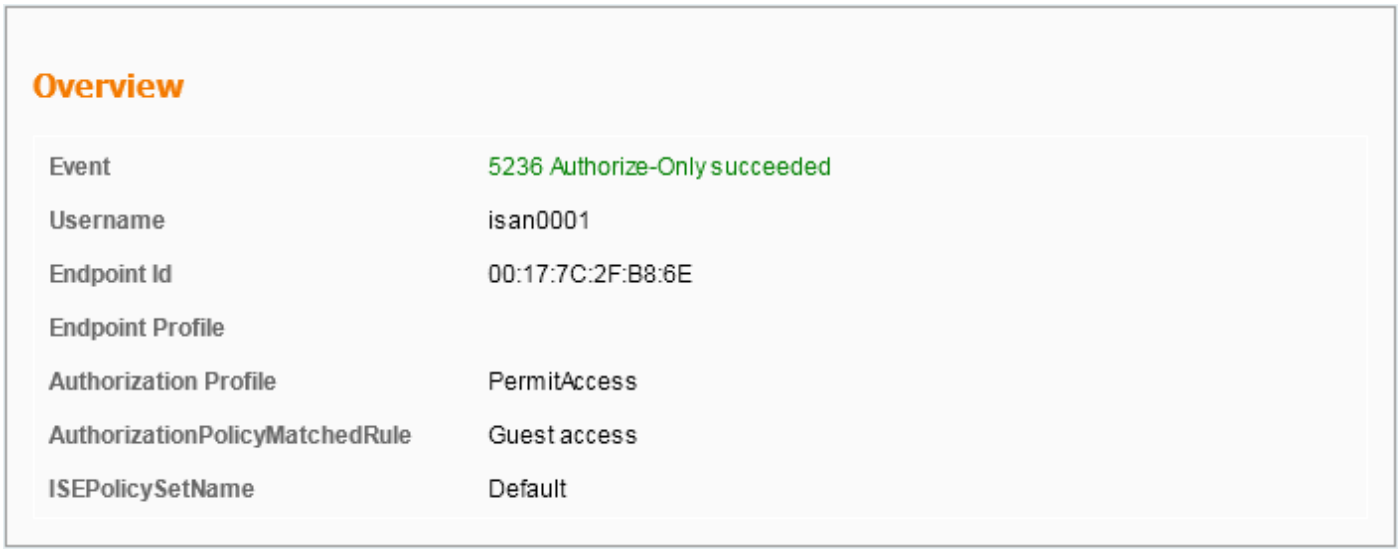
Paso 10. El usuario entonces inicia el red-auth reorienta el proceso ingresando un URL en el hojeador. Usted puede ver los debugs relevantes en el regulador del ancla:

```
*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. Podemos también ver que la pieza de la autenticación en el proceso del webauth está manejada en el WLC no nativo y no en el ancla. Usted puede ver lo mismo en las salidas del debug AAA en el no nativo:

```
*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 pueden verificar en el ISE tal y como se muestra en de la imagen:



Paso 12. Esta información se pasa sobre el WLC del ancla. Este apretón de manos no es claramente visible en los debugs y usted puede hacer esto por el ancla que aplica una directiva de las manos del poste 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 sea completa es verificar pasajero abre una sesión el ISE y recoge la salida del detalle del cliente de la demostración en el regulador que debe mostrar al cliente en el estado de **FUNCIONAMIENTO** 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
```

Otro control importante es el hecho de que el ancla envía un (ARP) del Address Resolution Protocol gratuito después de la autenticación satisfactoria:

```
*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
```

Aquí del cliente está libre de enviar todos los tipos de tráfico que es remitido hacia fuera por el regulador del ancla.

Flujo central de Webauth cuando el cliente consigue disconnected

Cuando una entrada del cliente necesita ser quitada del WLC o debido a una sesión/a un tiempo de inactividad o cuando quitamos manualmente al cliente del WLC, estos pasos ocurren:

El WLC no nativo envía un mensaje de la de-autenticidad al cliente y lo programa para la cancelacíon:

```
*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
```

Entonces envía un mensaje de las estadísticas de la parada del radio para informar al servidor ISE que la sesión de la autenticación de cliente ha terminado:

```
*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 las manos de la movilidad al WLC del ancla para informarle para terminar a la sesión de cliente. Esto se puede ver en los debugs de la movilidad en el WLC del ancla:

```
*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 del cliente suspendida en el ISE

El ISE tiene la capacidad de suspender una cuenta de Usuario invitado que señale el WLC para terminar a la sesión de cliente. Esto es útil para los administradores que no necesitan marcar con que el WLC el cliente está conectado y terminar simplemente la sesión. Usted puede ahora ver qué sucede cuando la cuenta de Usuario invitado se suspende/se expira en el ISE:

El servidor ISE envía un cambio del mensaje de la autorización al regulador no nativo que indica que la conexión cliente necesita ser quitada. Esto se puede ver en las salidas de los debugs:

```
*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 no nativo entonces envía un mensaje de la de-autenticidad 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 la parada de las estadísticas al servidor de contabilidad para terminar la sesión de la autenticación de cliente sobre 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)
```

Un mensaje de las manos también se envía al WLC del ancla para terminar a la sesión de cliente. Usted puede ver esto en el WLC del ancla:

```
*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
```

Troubleshooting Webauth central en configuración del ancla del invitado

Ahora tengamos una mirada en algunos de los problemas frecuentes vistos cuando usted utiliza CWA y qué se puede hacer para repararlo.

El cliente del escenario 1. se pegó en el estado del COMIENZO y no consigue la dirección IP

En un escenario central del webauth puesto que se habilita la autenticación de MAC, se envían las respuestas de la asociación después de que se complete una autenticación de MAC. En este caso, si hay una falla de comunicación entre el WLC y el servidor de RADIUS o hay un misconfig en el servidor de RADIUS que lo hace enviar los rechazos de acceso, usted puede ver al cliente pegado en una asociación para colocar donde consigue en varias ocasiones un rechazo de la asociación. Hay también una ocasión que el cliente consigue excluido también si se habilita la exclusión del cliente.

El accesibilidad del servidor de RADIUS se puede verificar con el comando de la **prueba RADIUS AAA** que está disponible en el código 8.2 y arriba.

El link de referencia abajo 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

El cliente del escenario 2. no puede conseguir la dirección IP

Hay algunas razones por las que un cliente puede no poder conseguir una dirección IP en una configuración del ancla del invitado CWA.

- **El config SSID en el ancla y no nativo no hace juego**

Es ideal tener config SSID lo mismo entre el ancla y los WLC no nativos. Algunos de los aspectos para los cuales se hace una evaluación estricta son config de la Seguridad L2/L3, DHCP config y

los parámetros de la invalidación AAA. En caso de que éste no sea lo mismo, las manos al ancla fallan y usted puede ver estos mensajes en los debugs del ancla:

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

Para atenuar esto, usted necesita asegurarse de que el config SSID sea el la misma ancla y no nativo.

- **El túnel de la movilidad entre el ancla y WLC no nativos es abajo de/cambio**

Todo el tráfico del cliente se envía en el túnel de los datos de la movilidad que las aplicaciones protocolo IP 97. Si el túnel de la movilidad no está encima de entonces usted puede ver que las manos no completan y el cliente no se traslada al estado de FUNCIONAMIENTO en el no nativo. El estado del túnel de la movilidad necesita mostrar como **PARA ARRIBA** y puede ser considerado bajo **grupos del >Mobility de la Administración del >Mobility del regulador** tal y como se muestra en de la imagen.

Si hay solamente un regulador asociado como miembro (no nativo o ancla), después usted puede también marcar las estadísticas globales de la movilidad conforme a las **estadísticas del >Statistics > de la movilidad del monitor.**

- **Reoriente el ACL no configurado en el ancla o los reguladores no nativos:**

Cuando el nombre de la reorientación ACL enviada por el servidor de RADIUS no hace juego qué se configura en el WLC no nativo, después aunque se completa la autenticación de MAC, rechazan y no procede al cliente a hacer el DHCP. No es obligatorio configurar las reglas ACL individuales pues el tráfico del cliente se termina en el ancla. Mientras haya un ACL creado con el mismo nombre que la reorientación ACL, dan el cliente apagado al ancla. El ancla necesita tener el nombre y reglas ACL configurados correctamente para que el cliente se mueva al estado requerido webauth.

El cliente del escenario 3. no consigue reorientado a la página web

Hay otra vez algunas diversas razones por las que una página del webauth puede no poder conseguir visualizada. Algunos de los problemas laterales del WLC común se cubren aquí:

- **Problemas del servidor DNS**

El accesibilidad del servidor DNS/los problemas del misconfig es una de la mayoría de las razones comunes por las que los clientes no pueden conseguir reorientados. Esto puede también ser duro de coger pues no aparece en ningunos registros o debugs del WLC. El usuario necesita verificar si el config del servidor DNS avanzado del servidor DHCP está correcto y si es accesible del cliente de red inalámbrica. Una búsqueda de DNS simple del cliente festivo es la manera más fácil de marcar esto.

- **Default gateway inalcanzable cuando usted utiliza al servidor DHCP interno en el ancla:**

Cuando usted utiliza a los servidores DHCP internos, es importante asegurarse de que el config del gateway predeterminado está correcto y el VLA N está permitido en el switchport que conecta con el WLC del ancla. Si no, el cliente consigue una dirección IP, pero no podrá acceder cualquier cosa. Usted puede marcar la tabla ARP en el cliente para la dirección MAC del gateway. Es un modo rápido verificar la Conectividad L2 al gateway y eso es accesible.