Ejemplo de Modos H-REAP de Configuración de Funcionamiento

Contenido

Introducción

Este documento presenta el concepto de Hybrid Remote Edge Access Point (H-REAP) y explica sus diversos modos de funcionamiento con un ejemplo de configuración.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento de los Controladores de LAN Inalámbricos (WLC) y cómo configurar los

parámetros básicos del WLC
- Conocimiento del REAP

Componentes Utilizados

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

- WLC de la serie Cisco 4400 que ejecuta la versión de firmware 7.0.116.0
- Punto de acceso ligero (LAP) Cisco 1131AG
- Routers de la serie Cisco 2800 que ejecutan la versión 12.4(11)T.
- Cisco Aironet 802.11a/b/g Client Adapter que ejecuta la versión de firmware 4.0
- Cisco Aironet Desktop Utility versión 4.0
- Cisco Secure ACS que ejecuta la versión 4.0

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, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

H-REAP es una solución inalámbrica para implementaciones en sucursales y oficinas remotas. H-REAP permite a los clientes configurar y controlar los puntos de acceso (AP) en una sucursal u oficina remota desde la oficina corporativa a través de un enlace WAN sin implementar un controlador en cada oficina.

H-REAP puede hacer switching de tráfico de datos de clientes de manera local y realizar autenticación de clientes de manera local al perderse la conexión con el controlador. Cuando están conectados con el controlador, los H-REAPs también pueden tunelizar de nuevo el tráfico hacia el controlador. En el modo conectado, el AP de REAP híbrido también puede realizar la autenticación local.

El H-REAP se soporta solamente en:

- AP 1130AG, 1140, 1240, 1250, 1260, AP801, AP 802, 1040 y AP3550
- Controladores de las series 5500, 4400, 2100, 2500 y Flex 7500 de Cisco
- Switch de controlador integrado Catalyst 3750G
- Módulo de servicios inalámbricos (WiSM) Catalyst serie 6500
- Wireless LAN Controller Module (WLCM) para routers de servicios integrados (ISR)

El tráfico del cliente en los H-REAPs puede conmutarse localmente en el AP o tunelizarse nuevamente a un controlador. Esto depende de la configuración por WLAN. Además, el tráfico del cliente conmutado localmente en el H-REAP puede estar etiquetado 802.1Q para proporcionar separación del lado cableado. Durante la interrupción de la WAN, el servicio en todas las WLAN localmente conmutadas y autenticadas persiste.

Nota: Si los AP están en el modo H-REAP y se conmutan localmente en el sitio remoto, la asignación dinámica de usuarios a una VLAN específica basada en la configuración del servidor RADIUS no se soporta. Sin embargo, debería poder asignar usuarios a VLAN específicas basadas en la VLAN estática para la asignación de identificador de conjunto de servicios (SSID) que se realiza localmente en el AP. Por lo tanto, un usuario que pertenece a un SSID determinado puede ser asignado a una VLAN específica a la cual el SSID se mapea localmente en el AP.

Nota: Si la voz sobre WLAN es importante, los AP deben ejecutarse en el modo local para obtener compatibilidad con CCKM y Control de admisión de conexión (CAC), que no se admiten en el modo H-REAP.

H-REAP sobre REAP

Consulte Ejemplo de Configuración de Remote-Edge AP (REAP) con Lightweight APs y Wireless LAN Controllers (WLCs) para obtener más información para ayudar a entender REAP.

El H-REAP se introdujo como resultado de estas deficiencias del REAP:

- REAP no tiene separación del lado cableado. Esto se debe a la falta de compatibilidad con 802.1Q. Los datos de las WLAN aterrizan en la misma subred cableada.
- Durante una falla de WAN, un AP REAP cesa el servicio ofrecido en todas las WLAN, excepto el primero especificado en el controlador.

Así es como H-REAP supera estas dos deficiencias:

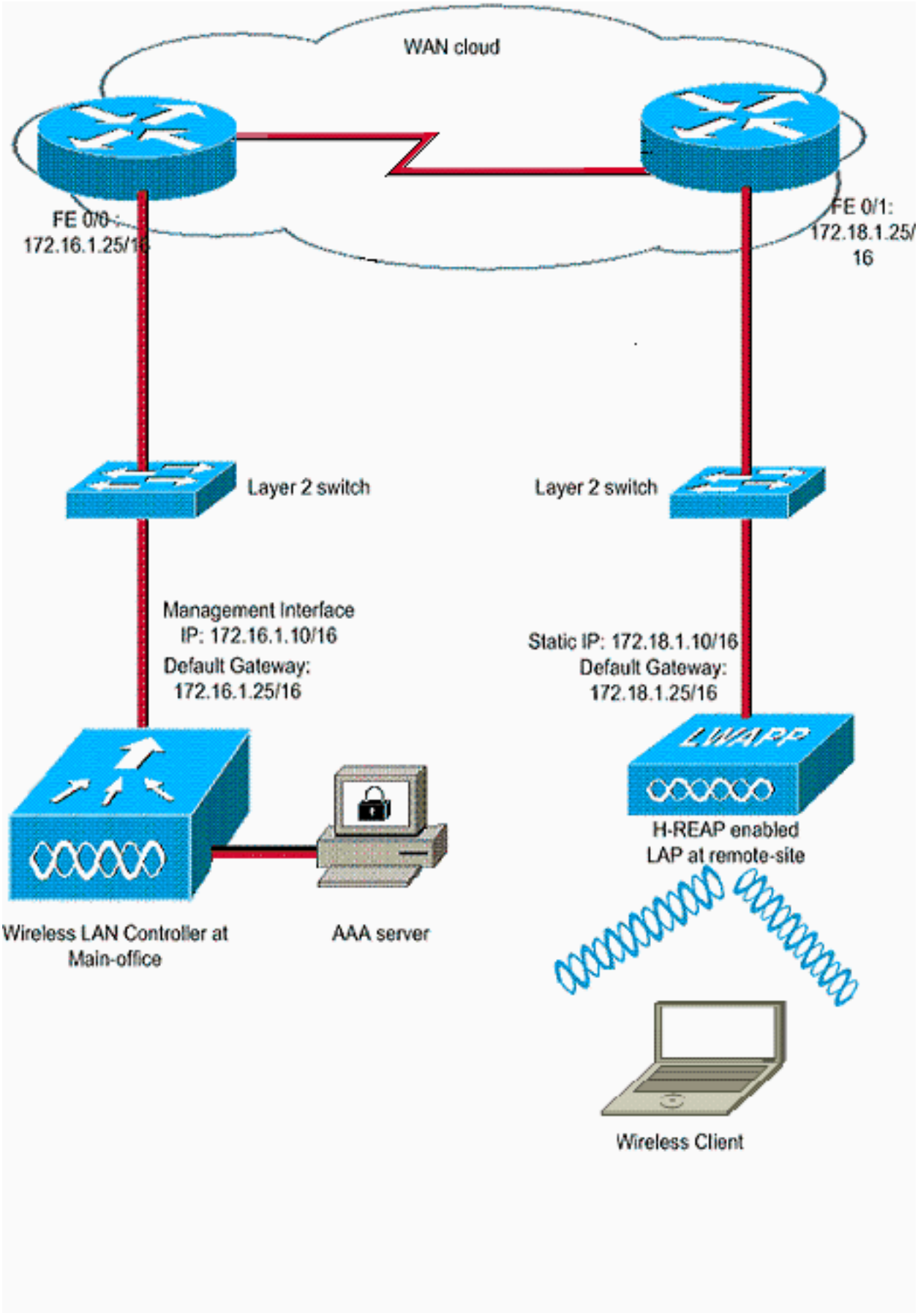
- Proporciona soporte dot1Q y asignación de VLAN a SSID. Esta asignación de VLAN a SSID debe hacerse en H-REAP. Mientras realiza esto, asegúrese de que las VLAN configuradas estén permitidas correctamente a través de los puertos en los switches y routers intermedios.
- Proporciona servicio continuo a todas las WLAN configuradas para el switching local.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuración

Este ejemplo asume que el controlador ya está configurado con configuraciones básicas. El controlador utiliza estas configuraciones:

- Dirección IP de la interfaz de administración: 172.16.1.10/16
- Dirección IP de la interfaz del administrador de AP: 172.16.1.11/16
- Dirección IP del router de gateway predeterminado: 172.16.1.25/16
- Dirección IP de gateway virtual: 1.1.1.1

Nota: Este documento no muestra las configuraciones de WAN y la configuración de routers y switches disponibles entre el H-REAP y el controlador. Esto supone que es consciente de la encapsulación WAN y de los protocolos de ruteo que se utilizan. Además, este documento asume que usted entiende cómo configurarlos para mantener la conectividad entre el H-REAP y el controlador a través del link WAN. En este ejemplo, se utiliza la encapsulación HDLC en el link WAN.

Primar el AP con un controlador y configurar H-REAP

Si desea que el AP detecte un controlador desde una red remota donde los mecanismos de detección CAPWAP no están disponibles, puede utilizar la inicialización. Este método le permite especificar el controlador al que el AP debe conectarse.

Para priorizar un AP compatible con H-REAP, conecte el AP a la red cableada en la oficina principal. Durante su inicio, el AP habilitado para H-REAP busca primero una dirección IP para sí mismo. Una vez que adquiere una dirección IP a través de un servidor DHCP, se inicia y busca un controlador para realizar el proceso de registro.

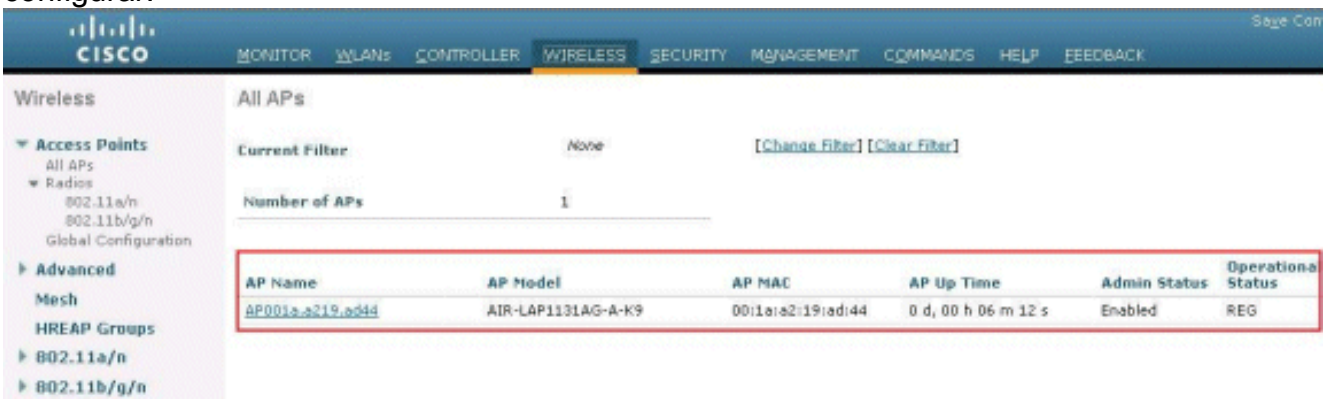
Un AP H-REAP puede aprender la dirección IP del controlador de cualquiera de las maneras explicadas en el registro del AP ligero (LAP) a un controlador de LAN inalámbrica (WLC).

Nota: También puede configurar el LAP para detectar el controlador a través de los comandos CLI en el AP. Refiérase a Detección del Controlador H-REAP usando comandos CLI para obtener más información.

El ejemplo en este documento utiliza el procedimiento de la opción DHCP 43 para que el H-REAP aprenda la dirección IP del controlador. Luego se une al controlador, descarga la imagen de software y la configuración más recientes del controlador, e inicializa el link de radio. Guarda la configuración descargada en la memoria no volátil para su uso en el modo autónomo.

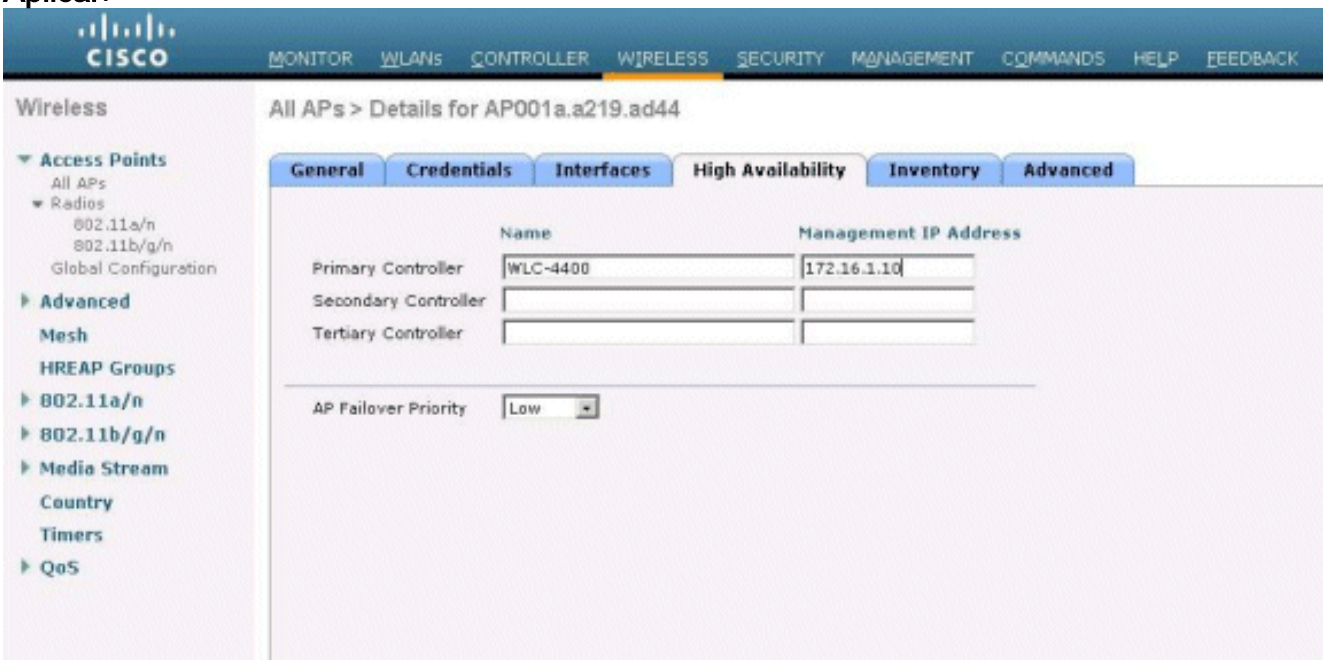
Una vez que el LAP se registra con el controlador, complete estos pasos:

1. En la GUI del controlador, elija **Wireless>Access Points**.Muestra el LAP registrado con este controlador.
2. Haga clic en el AP que desea configurar.



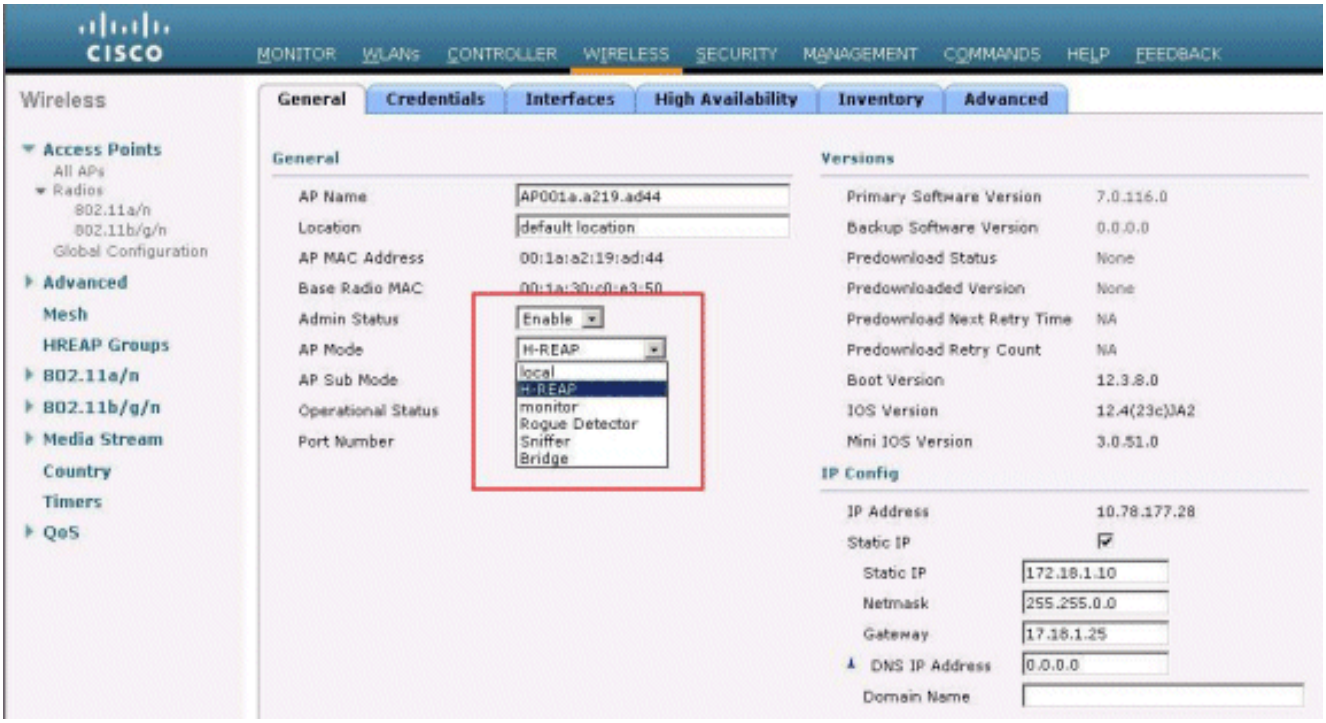
3. En la ventana APs>Detalles, haga clic en la pestaña Alta Disponibilidad, defina los nombres

de controlador que los APs usarán para registrarse y luego haga clic en **Aplicar**.



Puede definir hasta tres nombres de controlador (primario, secundario y terciario). Los AP buscan el controlador en el mismo orden que usted provee en esta ventana. Debido a que este ejemplo utiliza sólo un controlador, el ejemplo define el controlador como el controlador principal.

4. Configure el LAP para H-REAP.Para configurar el LAP para que funcione en el modo H-REAP, en la ventana AP>Detalles, en la pestaña General, elija el **modo AP** como H-REAP del menú desplegable correspondiente.Esto configura el LAP para que funcione en el modo H-
REAP.



Nota: En este ejemplo, puede ver que la dirección IP del AP se cambia al modo estático y la dirección IP estática 172.18.1.10 se ha asignado. Esta asignación se produce porque ésta es la subred que se utilizará en la oficina remota. Por lo tanto, usted utiliza la dirección IP del servidor DHCP, pero sólo durante la primera vez a través de la etapa de registro. Después

de registrar el AP en el controlador, usted cambia la dirección a una dirección IP estática.

Ahora que su LAP se prepara con el controlador y se configura para el modo H-REAP, el siguiente paso es configurar H-REAP en el lado del controlador y discutir los estados de conmutación H-REAP.

Teoría de las operaciones de H-REAP

El LAP habilitado para H-REAP funciona en estos dos modos diferentes:

- Modo **conectado**:Se dice que un H-REAP está en modo conectado cuando su link de plano de control CAPWAP al WLC está activo y en funcionamiento. Esto significa que el link WAN entre el LAP y el WLC no está inactivo.
- Modo **autónomo**:Se dice que un H-REAP está en el modo autónomo cuando su link WAN al WLC está inactivo. Por ejemplo, cuando este H-REAP ya no tiene conectividad con el WLC conectado a través del link WAN.

El mecanismo de autenticación utilizado para autenticar un cliente puede definirse como **Central** o **Local**.

- **Autenticación central**: se refiere al tipo de autenticación que implica el proceso del WLC desde el sitio remoto.
- **Autenticación local**: se refiere a los tipos de autenticación que no implican ningún procesamiento del WLC para la autenticación.

Nota: Todo el procesamiento de autenticación y asociación 802.11 ocurre en el H-REAP, sin importar en qué modo esté el LAP. Durante el modo conectado, H-REAP proxia estas asociaciones y autenticaciones al WLC. En el modo autónomo, el LAP no puede informar al WLC de tales eventos.

Cuando un cliente se conecta a un AP H-REAP, el AP reenvía todos los mensajes de autenticación al controlador. Después de una autenticación exitosa, sus paquetes de datos se conmutan localmente o se tunelizan nuevamente al controlador. Esto se realiza de acuerdo con la configuración de la WLAN a la que está conectada.

Con H-REAP, las WLANs configuradas en un controlador pueden funcionar en dos modos diferentes:

- **Switching central:**Se dice que una WLAN en H-REAP funciona en el modo de conmutación central si el tráfico de datos de esa WLAN está configurado para ser tunelizado al WLC.
- **Conmutación local:**Se dice que una WLAN en H-REAP funciona en el modo de conmutación local si el tráfico de datos de esa WLAN termina localmente en la interfaz cableada del LAP mismo, sin ser tunelizada al WLC.**Nota:** Sólo se pueden configurar las WLANs 1 a 8 para el H-REAP Local Switching porque solamente estas WLANs se pueden aplicar a los APs de las series 1130, 1240 y 1250 que soportan la funcionalidad de H-REAP.

Estados de switching H-REAP

Combinado con los modos de autenticación y conmutación mencionados en la sección anterior, un H-REAP puede funcionar en cualquiera de estos estados:

- Autenticación central, conmutación central

- autentificación desactivada, conmutación desactivada
- Autenticación central, conmutación local
- Autenticación desactivada, conmutación local
- Autenticación local, conmutación local

Autenticación central, conmutación central

En este estado, para la WLAN dada, el AP reenvía todas las solicitudes de autenticación del cliente al controlador y tuneliza todos los datos del cliente al WLC. Este estado es válido solamente cuando el H-REAP está en el modo conectado. Cualquier WLAN configurada para funcionar en este modo se pierde durante la interrupción de la WAN, independientemente del método de autenticación.

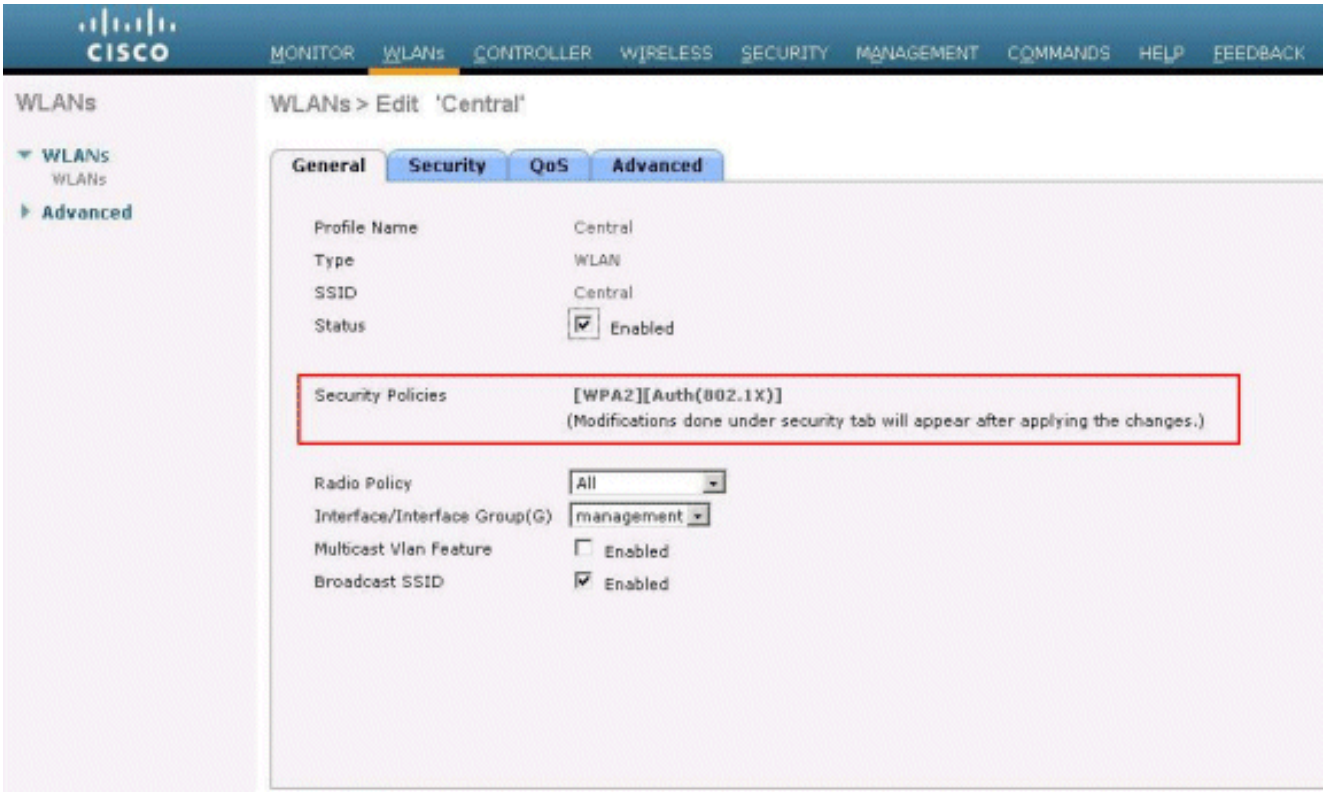
Este ejemplo utiliza estos valores de configuración:

- Nombre de WLAN/SSID: **Central**
- Seguridad de capa 2: **WPA2**
- H-REAP Local Switching: **inhabilitado**

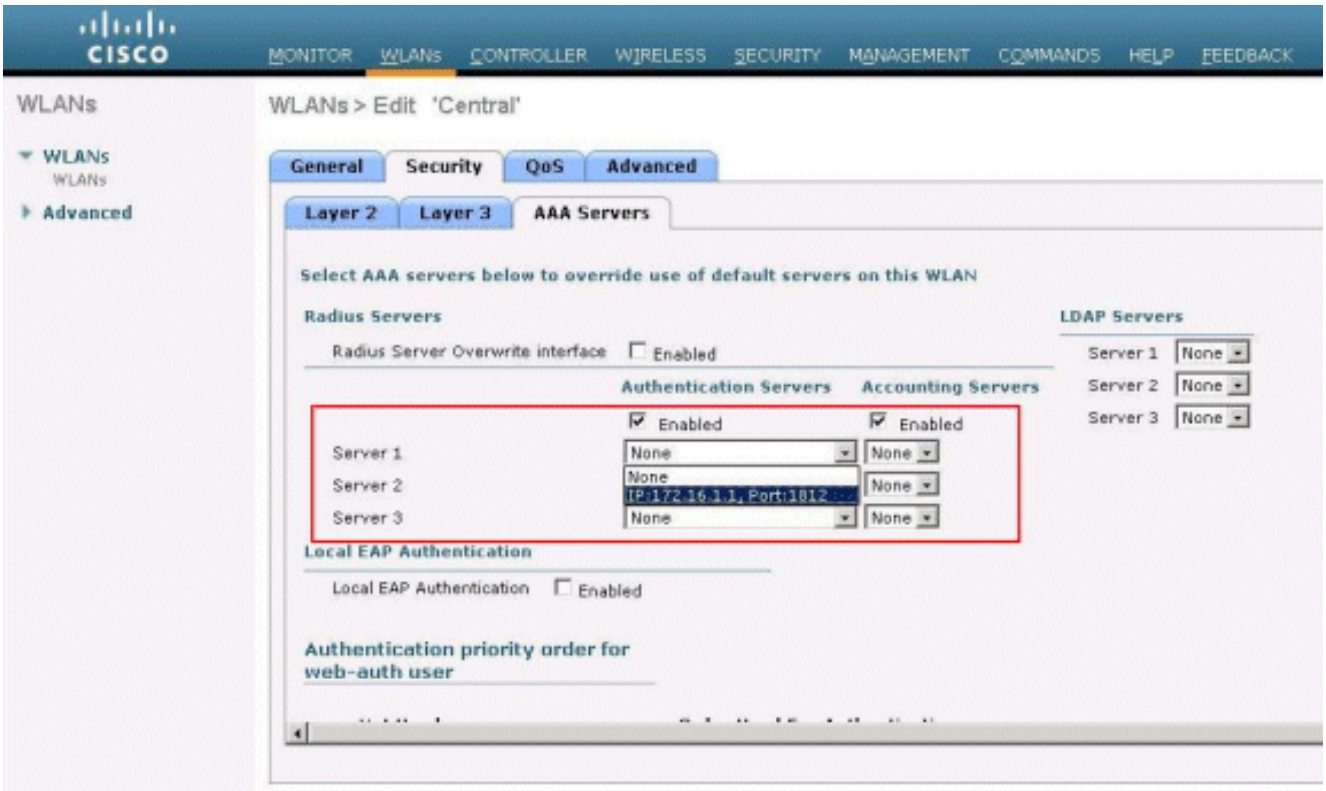
Complete estos pasos para configurar el WLC para la autenticación central, conmutación central usando la GUI:

1. Haga clic en **WLANs** para crear una nueva WLAN denominada **Central** y luego haga clic en **Aplicar**.

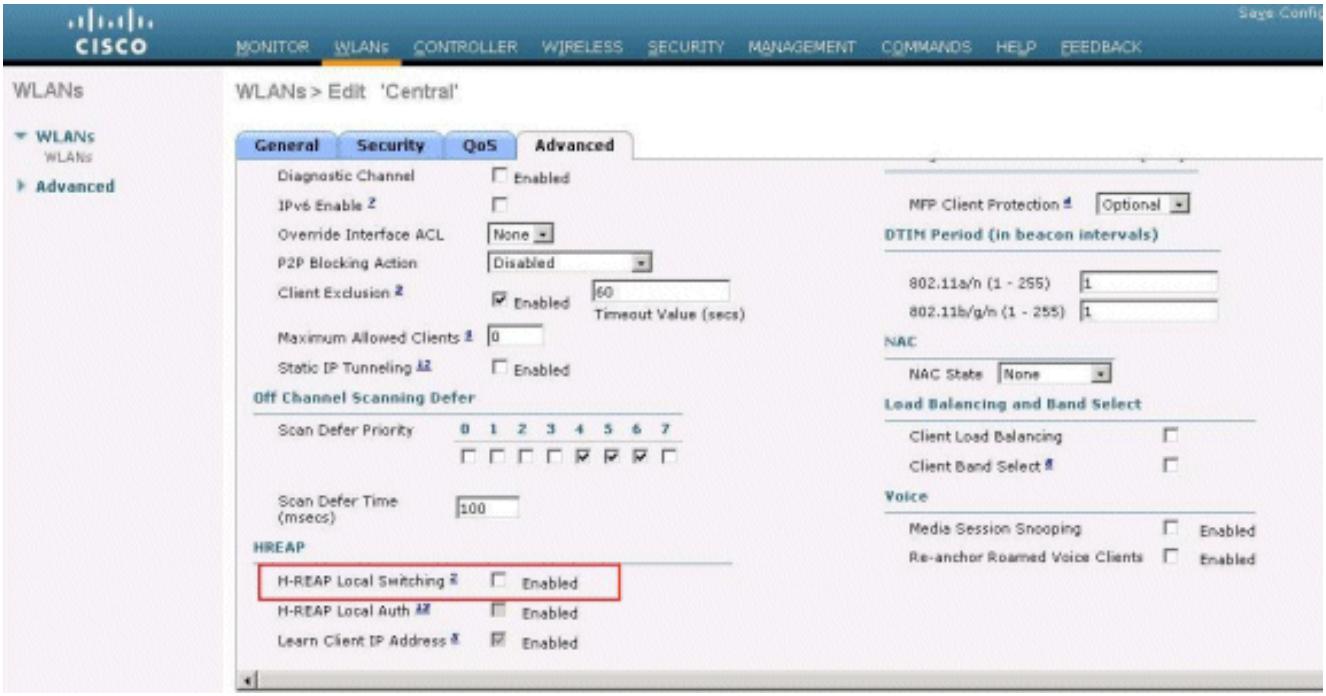
2. Debido a que esta WLAN utiliza la autenticación central, utilizamos la autenticación WPA2 en el campo Layer 2 Security . WPA2 es la seguridad de capa 2 predeterminada para una WLAN.



3. Elija la pestaña Servidores AAA y luego elija el servidor apropiado configurado para la autenticación.



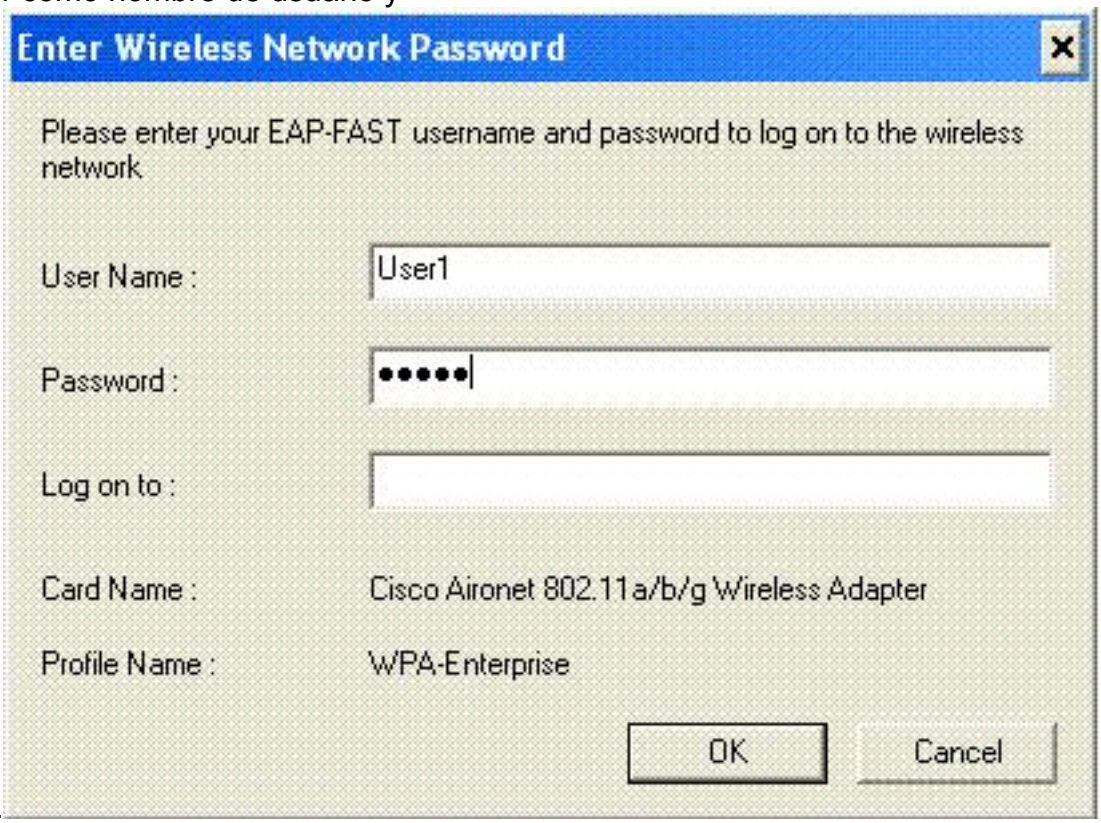
4. Debido a que esta WLAN utiliza conmutación central, debe asegurarse de que la casilla de verificación H-REAP Local Switching esté inhabilitada (es decir, la casilla de verificación Local Switching no está seleccionada). A continuación, haga clic en **Aplicar**.



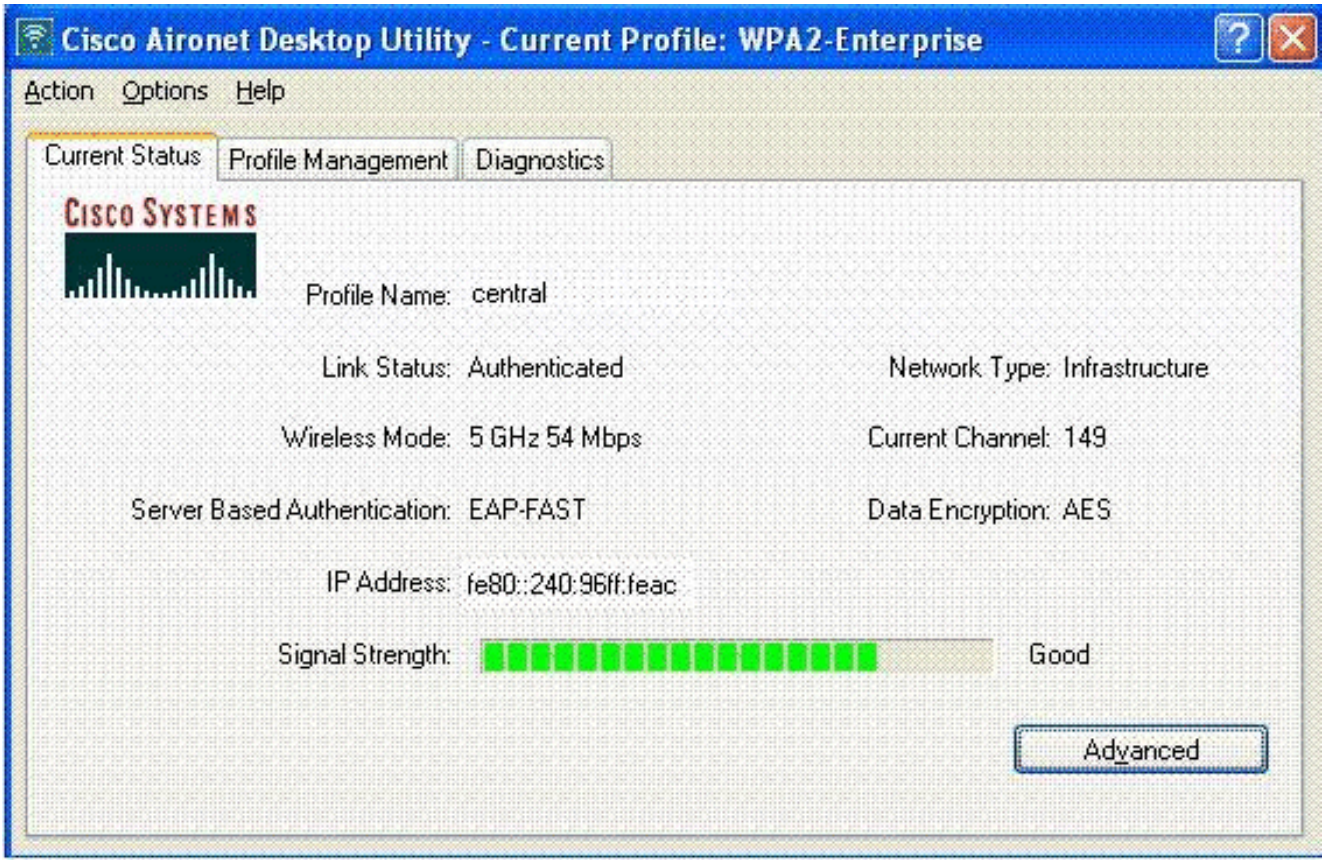
Verificación de la autenticación central, conmutación central

Complete estos pasos:

1. Configure el cliente inalámbrico con el mismo SSID y las mismas configuraciones de seguridad.En este ejemplo, el SSID es *Central* y el método de seguridad es *WPA2*.
2. Ingrese el nombre de usuario y la contraseña tal como se configuraron en el servidor RADIUS>Configuración de usuario para activar el SSID central en el cliente.Este ejemplo utiliza *User1* como nombre de usuario y



contraseña.El cliente es autenticado centralmente por el servidor RADIUS y está asociado con el AP H-REAP. El H-REAP se encuentra ahora en **autenticación central, conmutación central**.



autentificación desactivada, conmutación desactivada

Con la misma configuración explicada en la sección Autenticación central, conmutación central, inhabilite el link WAN que conecta el controlador. Ahora, el controlador espera una respuesta de latido desde el AP. Una respuesta de latido es similar a los mensajes de señal de mantenimiento. El controlador prueba cinco latidos consecutivos, cada uno cada segundo.

Debido a que no se recibe con una respuesta de latido del H-REAP, el WLC desregistra el LAP.

Ejecute el comando **debug capwap events enable** desde la CLI del WLC para verificar el proceso de anulación del registro. Este es el ejemplo de salida de este comando **debug**:

```
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Did not receive heartbeat reply from
AP 00:15:c7:ab:55:90
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte
xt: Down capwap event for AP 00:15:c7:ab:55:90 slot 0
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte
xt: Deregister capwap event for AP 00:15:c7:ab:55:90 slot 0
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte
xt: Down capwap event for AP 00:15:c7:ab:55:90 slot 1
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte
xt: Deregister capwap event for AP 00:15:c7:ab:55:90 slot 1
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Received capwap Down event for AP 00:
15:c7:ab:55:90 slot 0!
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Deregister capwap event for AP 00:15:
c7:ab:55:90 slot 0
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Received capwap Down event for AP 00:
15:c7:ab:55:90 slot 1!
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Deregister capwap event for AP 00:15:
c7:ab:55:90 slot 1
```

El H-REAP entra en el modo autónomo.

Debido a que esta WLAN se autenticó previamente de forma centralizada y se conmutó de forma centralizada, tanto el tráfico de datos como de control se tunelizaron de nuevo al controlador. Por lo tanto, sin el controlador, el cliente no puede mantener la asociación con el H-REAP y se desconecta. Este estado de H-REAP con la asociación de cliente y la autenticación inactivas se denomina Autenticación inactiva, Conmutación inactiva.

Autenticación central, conmutación local

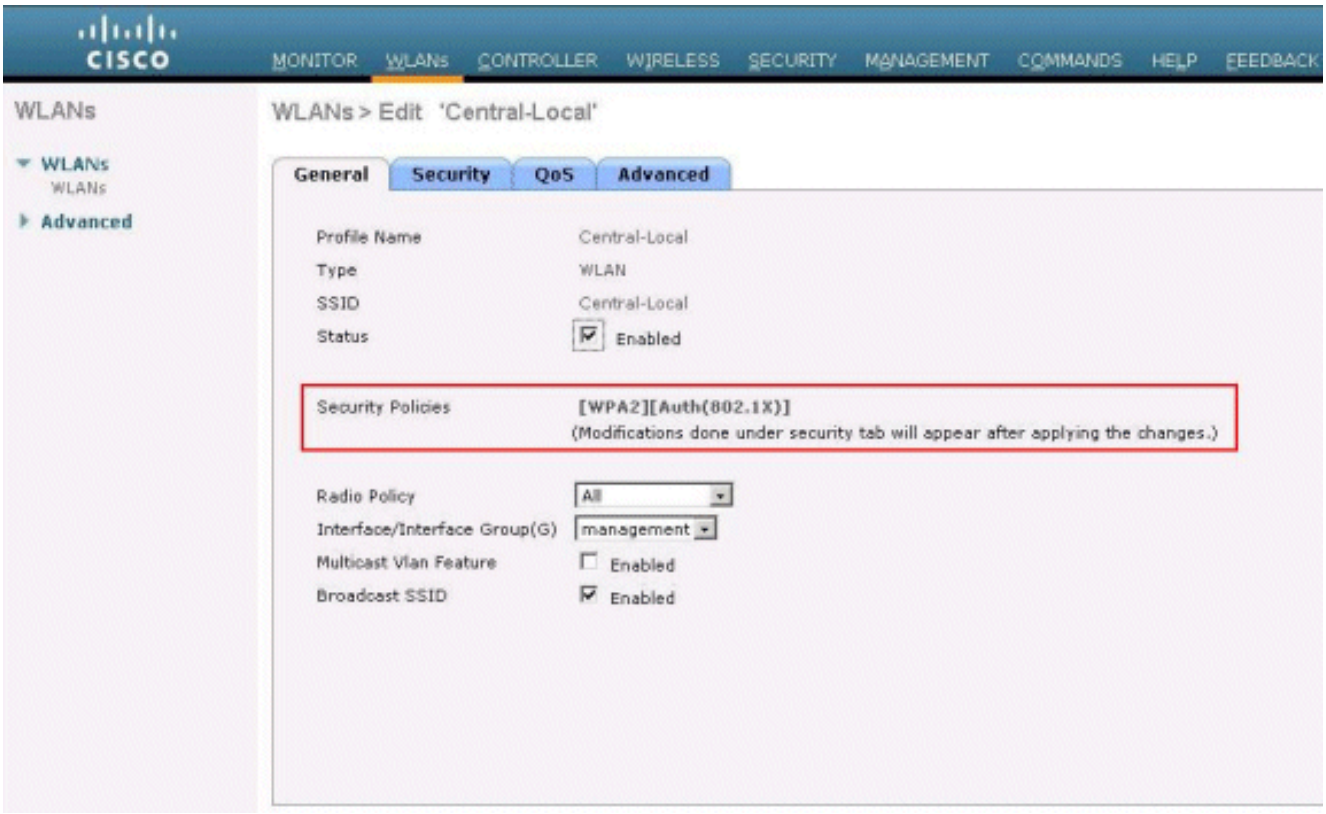
En este estado, para la WLAN dada, el WLC maneja toda la autenticación del cliente, y el LAP H-REAP conmuta los paquetes de datos localmente. Después de que el cliente se autentica exitosamente, el controlador envía comandos de control capwap al H-REAP e indica al LAP que conmute esos paquetes de datos del cliente de forma local. Este mensaje se envía por cliente al realizarse satisfactoriamente la autentificación. Este estado es aplicable solamente en el modo conectado.

Este ejemplo utiliza estos valores de configuración:

- Nombre de WLAN/SSID: **Central-Local**
- Seguridad de capa 2: **WPA2**.
- H-REAP Local Switching: **Habilitado**

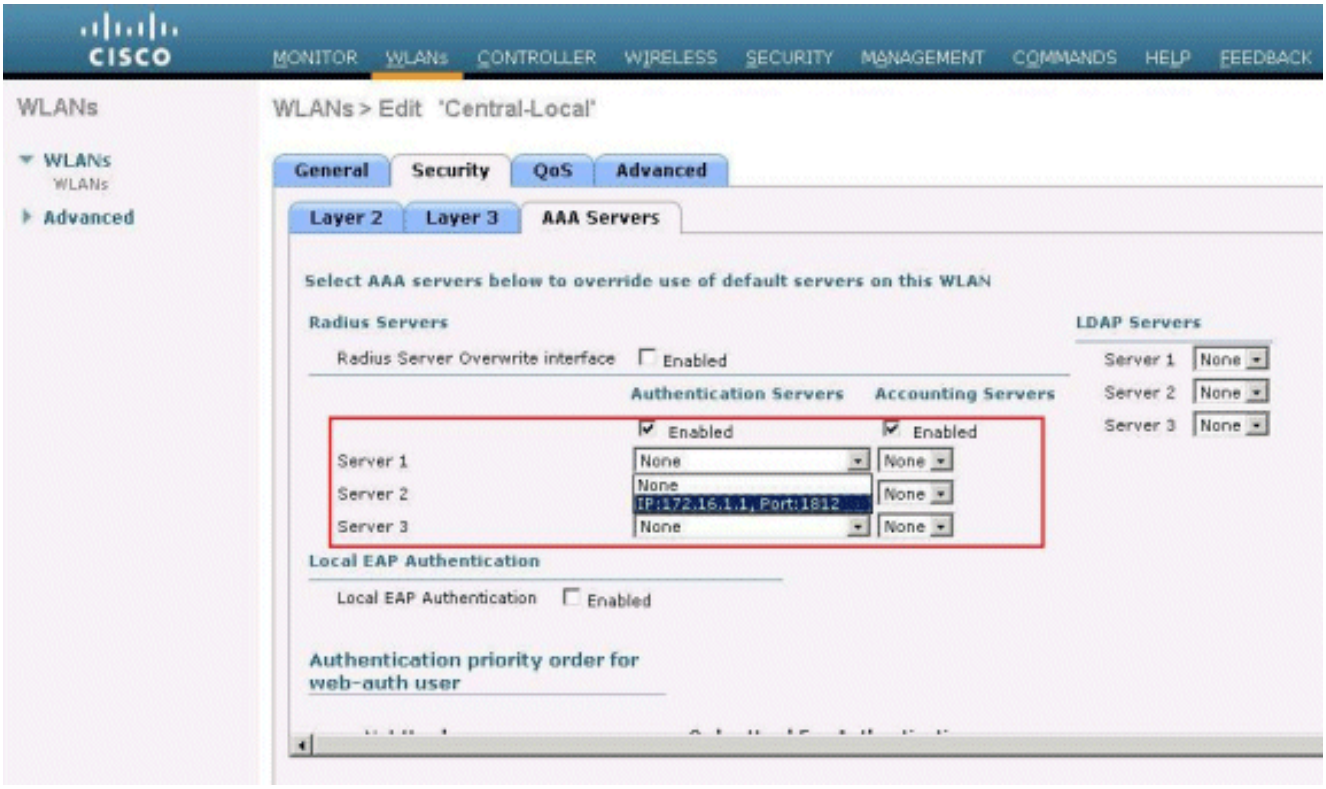
Desde la GUI del controlador, complete estos pasos:

1. Haga clic en **WLANs** para crear una nueva WLAN denominada Central-Local y luego haga clic en **Aplicar**.
2. Debido a que esta WLAN utiliza la autenticación central, elija la autenticación **WPA2** en el campo Layer 2 Security
   .

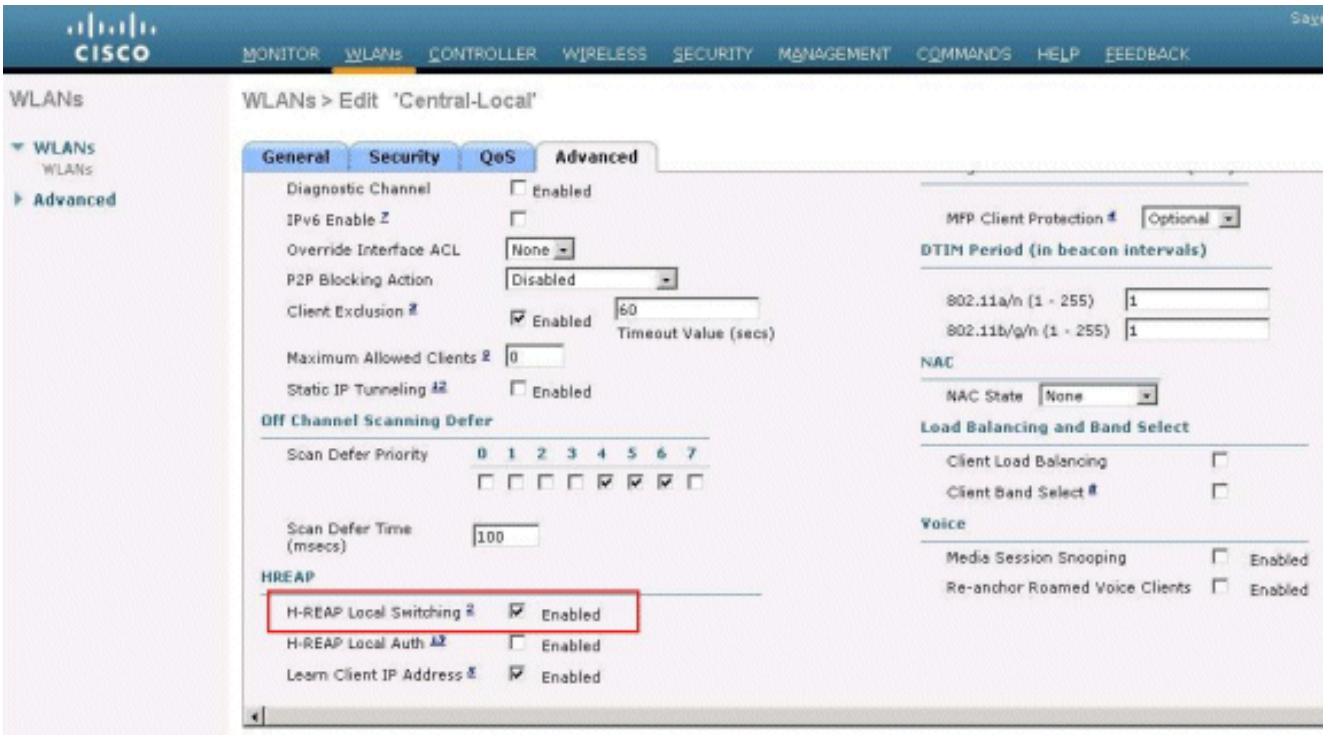


3. En la sección Servidores RADIUS, elija el servidor apropiado configurado para la

autenticación.



4. Marque la casilla de verificación **H-REAP Local Switching** para conmutar el tráfico del cliente que pertenece a esta WLAN localmente en el H-REAP.

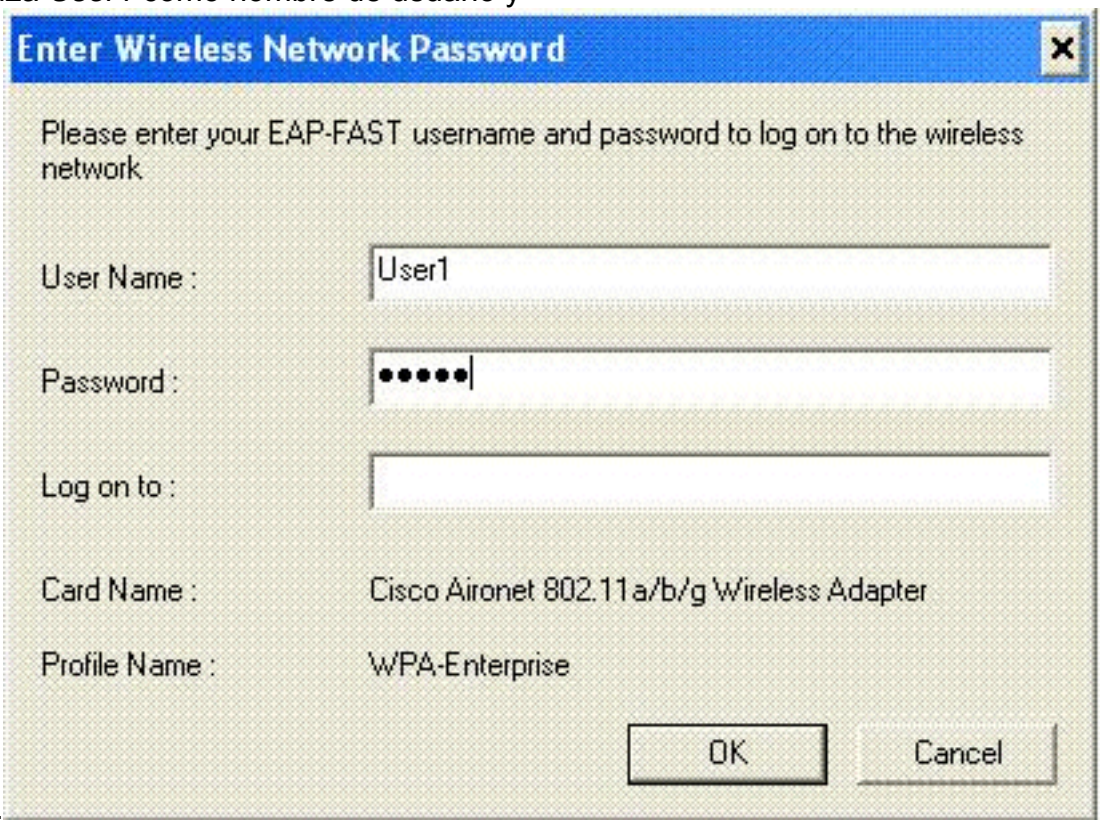


Verificar la autenticación central, conmutación local

Complete estos pasos:

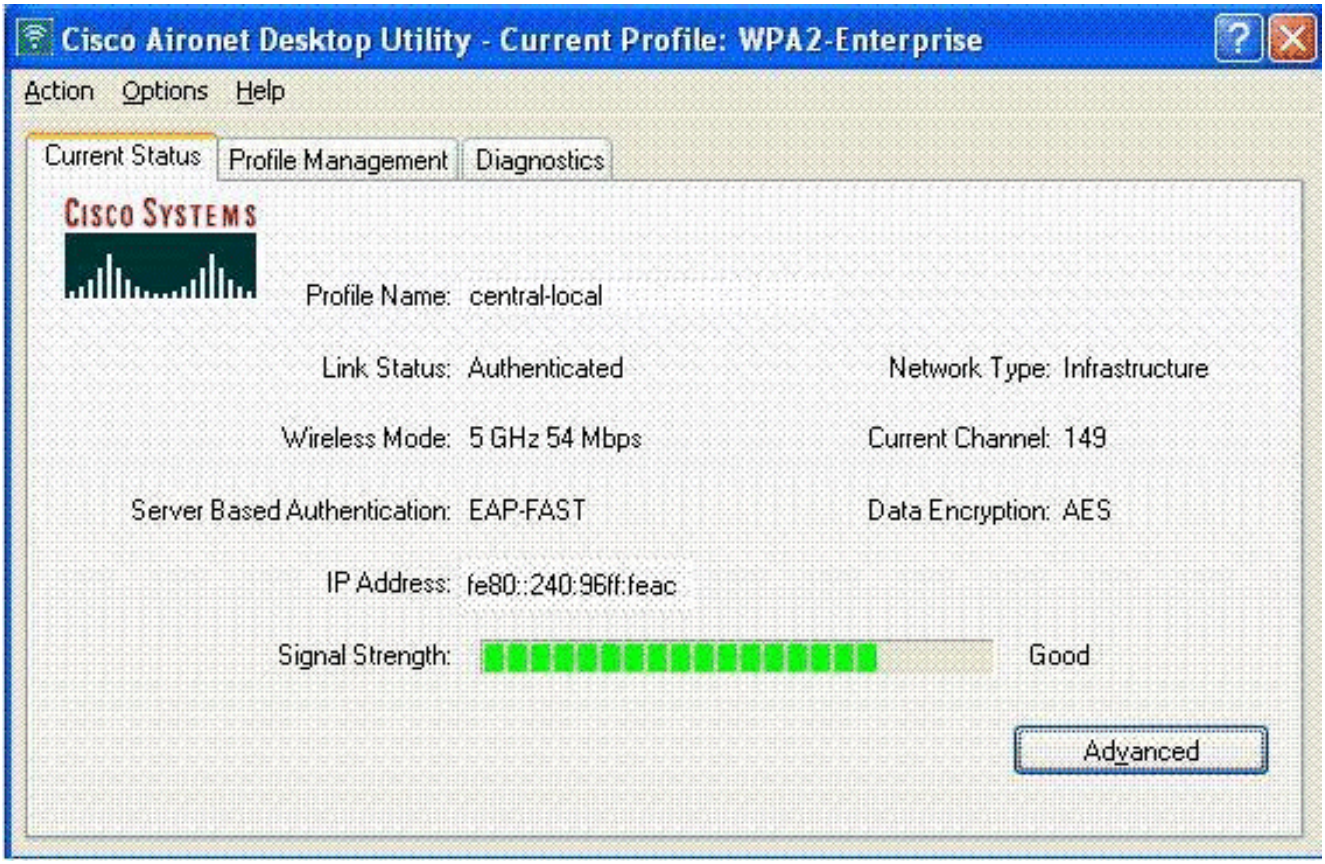
1. Configure el cliente inalámbrico con el mismo SSID y las mismas configuraciones de seguridad.En este ejemplo, el SSID es *Central-Local* y el método de seguridad es *WPA2*.
2. Ingrese el nombre de usuario y la contraseña tal como se configuraron en el servidor

RADIUS>Configuración de usuario para activar el SSID central-local en el cliente.Este ejemplo utiliza *User1* como nombre de usuario y



contraseña.

3. Click OK.El cliente es autenticado centralmente por el servidor RADIUS y se asocia con el AP H-REAP. El H-REAP se encuentra ahora en **autenticación central, conmutación local**.



Autenticación desactivada, conmutación local

Si se configura una WLAN conmutada localmente para cualquier tipo de autenticación que se requiere procesar en el WLC (como la autenticación EAP [WEP/WPA/WPA2/802.11i dinámica], WebAuth o NAC), tras una falla de la WAN, ingresa el estado **de autentificación desactivada, conmutación local**. En este estado, para la WLAN dada, el H-REAP rechaza cualquier cliente nuevo que intente autenticar. Sin embargo, continúa enviando señales y respuestas de sondeo para mantener a los clientes existentes conectados correctamente. Este estado es válido solamente en el modo autónomo.

Para verificar este estado, utilice la misma configuración explicada en la sección Autenticación central, conmutación local.

Si el link WAN que conecta el WLC está inactivo, el WLC pasa por el proceso de desregistro del H-REAP.

Una vez desregistrado, H-REAP pasa al modo autónomo.

El cliente asociado a través de esta WLAN aún mantiene su conectividad. Sin embargo, debido a que el controlador, el autenticador no está disponible, H-REAP no permite nuevas conexiones de esta WLAN.

Esto se puede verificar mediante la activación de otro cliente inalámbrico en la misma WLAN. Puede encontrar que la autenticación para este cliente falla y que ese cliente no puede asociarse.

Nota: Cuando un conteo de cliente de WLAN es igual a cero, el H-REAP deja de tener todas las funciones 802.11 asociadas y ya no hay balizas para el SSID dado. Esto mueve la WLAN al siguiente estado de H-REAP, **la autenticación inactiva, conmutación inactiva**.

Autenticación local, conmutación local

En este estado, el LAP de H-REAP maneja las autenticaciones del cliente y conmuta los paquetes de datos del cliente localmente. Este estado es válido solamente en el modo autónomo y solamente para los tipos de autenticación que pueden manejarse localmente en el AP y no implican el procesamiento del controlador

El H-REAP que anteriormente estaba en el estado **de autenticación central, conmutación local**, pasa a este estado, siempre que el tipo de autenticación configurado se pueda manejar localmente en el AP. Si la autenticación configurada no se puede manejar localmente, como la autenticación 802.1x, entonces en el modo autónomo, el H-REAP pasa a **la autenticación desactivada, el** modo **de conmutación local**.

Estos son algunos de los mecanismos de autenticación populares que se pueden manejar localmente en el AP en el modo autónomo:

- Abierto
- Compartido
- WPA-PSK
- WPA2-PSK

Nota: Todos los procesos de autenticación son manejados por el WLC cuando el AP está en el modo conectado. Mientras el H-REAP se encuentra en modo autónomo, las autenticaciones abiertas, compartidas y WPA/WPA2-PSK se transfieren a los LAPs donde ocurre toda la autenticación del cliente.

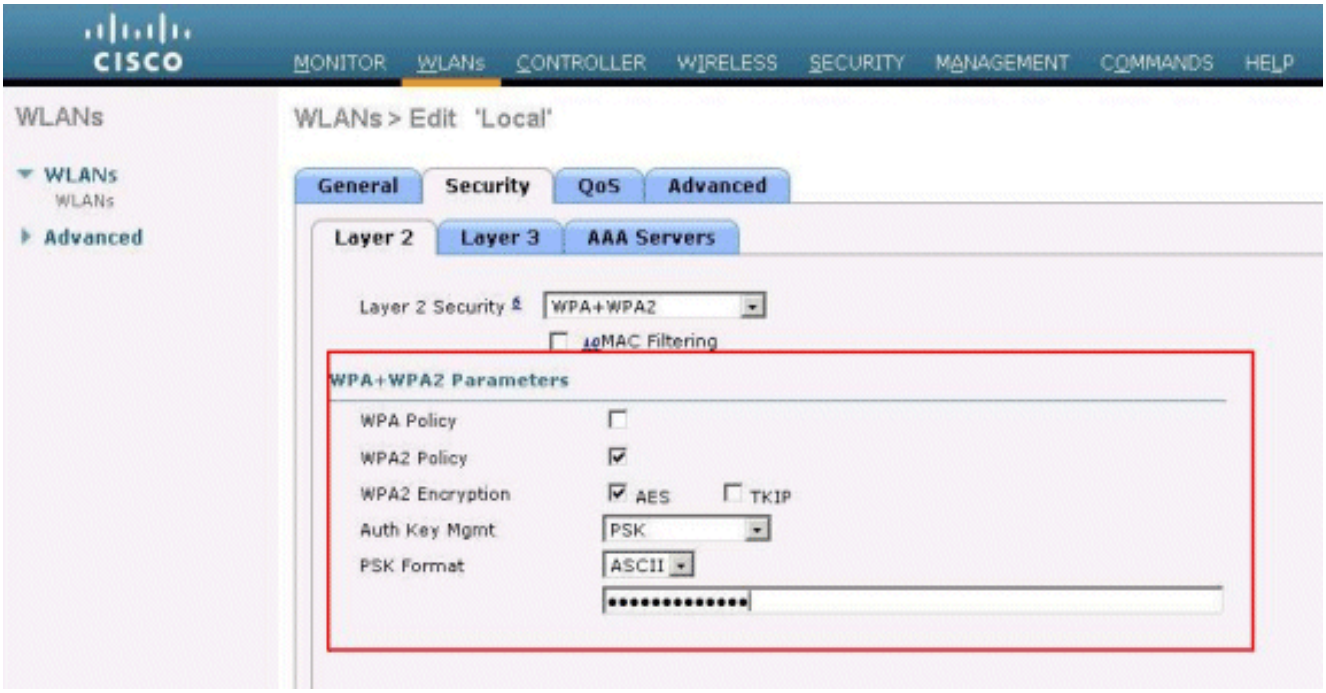
Nota: La autenticación Web externa no se soporta cuando se usa hybrid-REAP con conmutación local habilitada en la WLAN.

Este ejemplo utiliza estos valores de configuración:

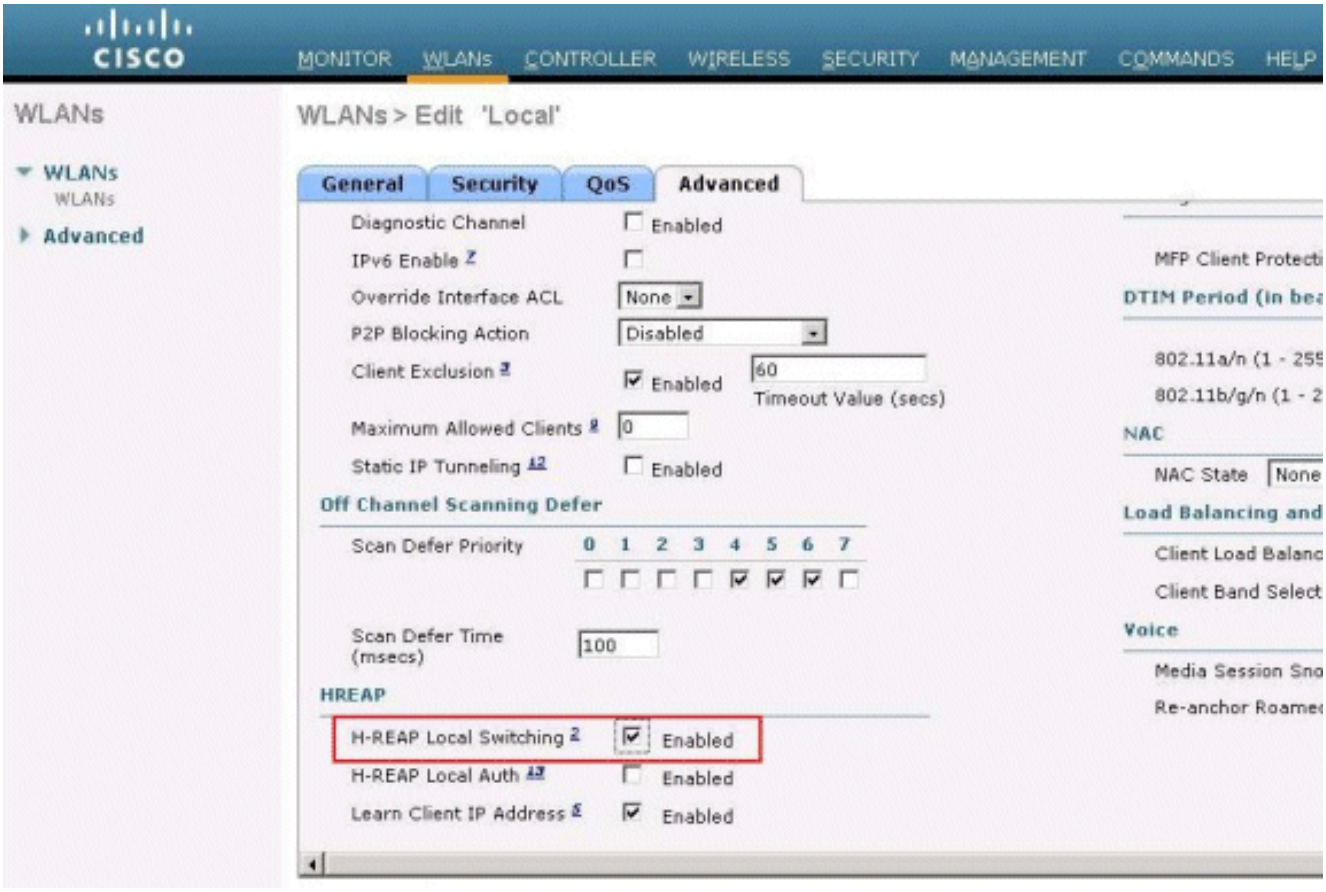
- Nombre de WLAN/SSID: **Local**
- Seguridad de capa 2: **WPA-PSK**
- H-REAP Local Switching: **habilitado**

Desde la GUI del controlador, complete estos pasos:

1. Haga clic en **WLANs** para crear una nueva WLAN denominada Local y luego haga clic en **Aplicar**.
2. Debido a que esta WLAN utiliza la autenticación local, elija **WPA-PSK** o cualquiera de los mecanismos de seguridad mencionados que se pueden manejar localmente en el campo Layer 2 Security .Este ejemplo utiliza **WPA-PSK**.



3. Una vez seleccionada, debe configurar la clave precompartida/frase de contraseña que se utilizará.Esto debe ser el mismo en el lado del cliente para que la autenticación sea exitosa.
4. Marque la casilla de verificación **H-REAP Local Switching** para conmutar el tráfico del cliente que pertenece a esta WLAN localmente en el H-REAP.



Verificación de la Autenticación Local, Switching Local

Complete estos pasos:

1. Configure el cliente con el mismo SSID y las mismas configuraciones de seguridad.Aquí, el SSID es *Local* y el método de seguridad es *WPA-PSK*.
2. Active el SSID local en el cliente.El cliente se autentica centralmente en el controlador y se asocia con el H-REAP. El tráfico del cliente se configura para conmutar localmente. Ahora, el H-REAP está en el estado Autenticación central, Conmutación local.
3. Desactive el enlace WAN que se conecta al controlador.El controlador como de costumbre pasa por el proceso de desregistro. H-REAP se desregistra del controlador.Una vez desregistrado, H-REAP pasa al modo autónomo.Sin embargo, el cliente que pertenece a esta WLAN aún mantiene la asociación con H-REAP.Además, debido a que el tipo de autenticación aquí puede ser manejado localmente en el AP sin el controlador, H-REAP permite asociaciones de cualquier nuevo cliente inalámbrico a través de esta WLAN.
4. Para verificar esto, active cualquier otro cliente inalámbrico en la misma WLAN.Puede ver que el cliente se autentica y se asocia correctamente.

Troubleshoot

- Para resolver problemas de conectividad del cliente en el puerto de la consola de H-REAP, ingrese este comando:
  ```
  AP_CLI#show capwap reap association
  ```

- Para resolver problemas de conectividad del cliente en el controlador y limitar la salida de debugging adicional, utilice este comando:

```
AP_CLI#debug mac addr
```

- Para ejecutar un debug de los problemas de conectividad de 802.11 del cliente, utilice este comando:
```
AP_CLI#debug dot11 state enable
```

- Ejecute un debug del proceso de autentificación y las fallas de 802.1X del cliente con este comando:
```
AP_CLI#debug dot1x events enable
```

- Puede ejecutar un debug de los mensajes del controlador/RADIUS backend mediante este comando:
```
AP_CLI#debug aaa events enable
```

- Alternativamente, para habilitar un juego completo de comandos del debug del cliente, utilice este comando:
```
AP_CLI#debug client
```

Información Relacionada

- Ejemplo de la configuración básica del controlador y del Lightweight Access Point del Wireless LAN
- Ejemplo de Configuración de VLANs en Controladores de LAN Inalámbrica
- Guía de configuración de controlador de LAN inalámbrica de Cisco, versión 7.0
- Guía de diseño e implementación de Hybrid REAP
- Troubleshooting Básico de Hybrid Remote Edge Access Point (H-REAP)
- Ejemplo de Configuración de Failover del Controlador WLAN para Puntos de Acceso Ligeros
- Soporte de Productos de Red Inalámbrica
- Soporte Técnico y Documentación - Cisco Systems