Guía de Diseño e Implementación de H-Reap

Contenido

Introducción

El Punto de acceso remoto híbrido del borde (H COSECHA) es una solución de red inalámbrica para las implementaciones de la sucursal y de la oficina remota. Permite a los clientes configurar y controlar los puntos de acceso en un sucursal u oficina remota desde la sede principal a través de un link de la red de área ancha (WAN) sin necesidad de implementar un controlador en cada oficina. El H COSECHA los Puntos de acceso puede conmutar el tráfico de datos del cliente

localmente y realizar la autenticación de cliente localmente cuando la conexión al regulador se pierde. Cuando está conectado con el regulador, H REAPs puede también tráfico de túnel de nuevo al regulador.

prerrequisitos

Requisitos

REAP híbrida se soporta solamente en los 1040, los 1130, los 1140, los 1240, los 1250, los 3500, los 1260, el AP801, los Puntos de acceso AP802 y en Cisco WiSM, Cisco 5500, 4400, 2100, 2500, y los reguladores de las 7500 Series de la flexión, el Switch integrado 3750G del regulador del Wireless LAN del Catalyst, el módulo de red del regulador para el Routers de los Servicios integrados.

Componentes Utilizados

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

- Cisco unificó la versión 7.0 de los reguladores
- Control y aprovisionamiento de los Puntos de acceso (CAPWAP) 1040 basados en protocolos, 1130, 1140, 1240,1250, 1260, AP801, AP802 y revestimientos de las 3500 Series

Convenciones

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

Fondo de las operaciones CAPWAP

El CAPWAP, en el cual se basa la arquitectura de la red inalámbrica unificada de Cisco, especifica dos diversos modos primarios de operación del unto de acceso de red inalámbrica:

- **MAC dividido**: en el modo MAC dividido, el sistema comparte las funciones clave de la especificación 802.11 entre el punto de acceso y el controlador. En este tipo de configuración, el controlador no tan sólo se responsabiliza de la mayor parte del proceso de las autentificaciones y asociaciones de 802.11, sino que también actúa como el único punto de ingreso y salida de todo el tráfico de usuarios. Túnel de los Puntos de acceso Fractura-MAC que todo el tráfico del cliente al regulador vía los datos CAPWAP hace un túnel (el control CAPWAP también sigue la misma trayectoria.).
- **MAC local** : MAC local, puesto que implementa toda la funcionalidad de 802.11 en el punto de acceso, permite el desacoplamiento del plano de los datos del trayecto de control mediante la finalización de todo el tráfico del cliente en el puerto cableado del punto de acceso. Esto permite no sólo el acceso de red inalámbrica directo a los recursos locales al Punto de acceso, pero proporciona la elasticidad del link permitiendo que el trayecto de control CAPWAP (el link entre el AP y el regulador) esté abajo mientras que persiste el servicio de red inalámbrica. Esta funcionalidad es especialmente útil en pequeñas sucursales remotas entre los links de WAN donde solamente se necesitan unos cuantos puntos de acceso y

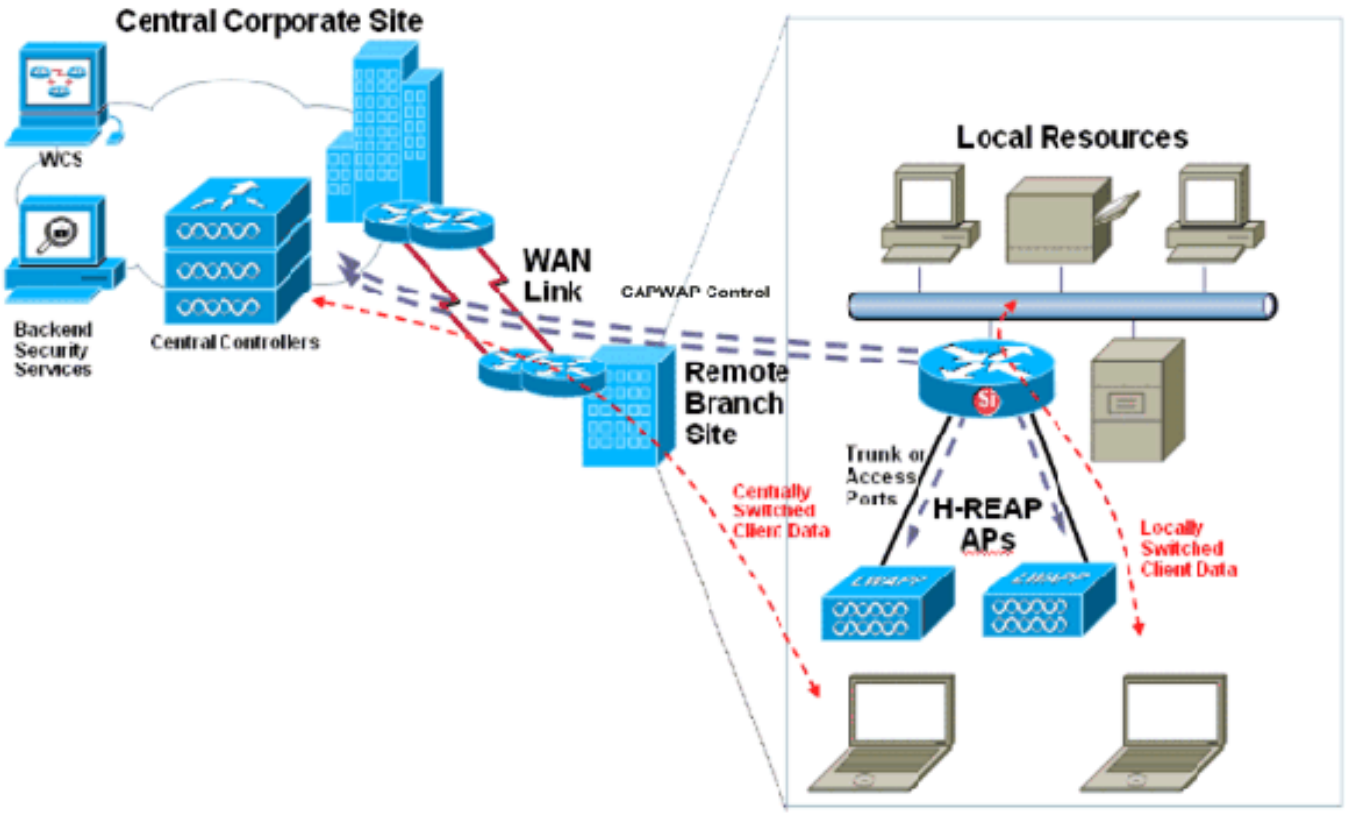
donde el costo de un controlador no está justificado.

Nota: Antes de que la versión 5.2 del regulador, la arquitectura inalámbrica unificada de Cisco fuera basada en el protocolo del LWAPP.

Hybrid Remote-Edge Access Point

Reguladores del borde de las 7500 Series remotas híbridas del Punto de acceso, o H COSECHA, es una característica soportada por 1040, 1130, 1140, 1240, 1250, 3500, 1260, AP801, los Puntos de acceso AP802 y en Cisco WiSM, Cisco 5500, 4400, 2100, 2500, y de la flexión, el Switch integrado 3750G del regulador del Wireless LAN del Catalyst, el módulo de red del regulador para el Routers de los Servicios integrados. El H COSECHA la característica se soporta solamente en la versión 4.0 del controlador de red del Cisco Unified Wireless o más adelante, la característica a elección de este software permite para la combinación de ambos las operaciones de la fractura y del MAC local CAPWAP para la flexibilidad de despliegue máxima. El tráfico del cliente en H REAPs se puede o conmutar localmente en el Punto de acceso o tunneled de nuevo a un regulador, que depende de cada configuración WLAN. Además, localmente el tráfico conmutado del cliente en el H REAP puede ser 802.1Q marcado con etiqueta para prever la separación de la cara tela. Durante una interrupción de la WAN, el servicio en todas las WLAN autenticadas y conmutadas localmente se mantiene.

Éste es un diagrama de un H común COSECHA la implementación:



Mientras que este diagrama indica, H REAP se ha diseñado y se piensa específicamente para las implementaciones del telecontrol y de la sucursal.

Este documento delinea el H COSECHA la teoría de operación, regulador y Configuración de punto de acceso, y las consideraciones de diseño de red.

H COSECHA la teoría de operación

H COSECHA los conceptos fundamentales

Hay algunos diversos modos por los cuales H COSECHA las funciones actúa para prever transferencia local y central, así como la supervivencia PÁLIDA del link. La mezcla de estos dos conjuntos de modos proporciona una gran variedad de funciones, pero también está sujeta a varias limitaciones dependiendo de la asociación.

Existen dos conjuntos de modos:

- **Conmutación central frente a conmutación local**Los WLAN (habitaciones de la Seguridad, de QoS, y de otros parámetros de la configuración atadas a los SSID) en H REAPs se pueden o fijar para requerir todo el tráfico de datos sean tunneled de nuevo al regulador (llamado transferencia central) o los WLAN se pueden configurar para caer todos los datos del cliente localmente en la interfaz atada con alambre H el REAP (conocida como Local Switching). Las WLANs conmutadas localmente pueden llevar opcionalmente etiquetas de 802.1Q para permitir que este tipo de WLANs se segmenten sobre la red con cable en el puerto Ethernet del punto de acceso.
- **Conectado frente a autónomo**UNA HÍBRIDO-COSECHA reputa en el modo conectado cuando su avión del control CAPWAP de nuevo al regulador es ascendente y operativo, significando que el link PÁLIDO no está abajo. Especifican al modo autónomo mientras que el estado operacional que el H COSECHA ingresa cuando tiene no más Conectividad de nuevo a su regulador.

Nota: Todo el H COSECHA la autenticación de la Seguridad que procesa (por ejemplo la derivación backend del [PMK] de la autenticación de RADIUS y en parejas de la clave principal) sucede en el regulador mientras que el Punto de acceso está en el estado conectado. Toda la autenticación del 802.11 y proceso de la asociación sucede en el H COSECHAN, ninguna materia en la cual el modo el Punto de acceso esté. Cuando en el modo conectado, H COSECHA los proxys estas asociaciones/autenticaciones al regulador. En el modo autónomo, el punto de acceso no puede informar al controlador de tales eventos.

H COSECHA las funciones varía dependiendo de su modo de operación (si un H REAP está en haber conectado o el modo autónomo), cómo cada red inalámbrica (WLAN) se configura para la transferencia de los datos (central o local) y la seguridad de red inalámbrica.

Cuando un cliente conecta con un H COSECHA el Punto de acceso, el Punto de acceso adelante todos los mensajes de autenticación al regulador y, sobre la autenticación satisfactoria, sus paquetes de datos entonces o se conmutan localmente o tunneled de nuevo al regulador, según la configuración del WLAN con el cual está conectado. En cuanto al mecanismo de autenticación de cliente y a la operación de Switching de los datos, los WLAN en H REAP pueden estar en de los estados siguientes dependiendo de la configuración de la red inalámbrica (WLAN) y del estado de la Conectividad del Punto de acceso/regulador:

- **autentificación central, conmutación central** : en este estado, para la WLAN especificada, el punto de acceso reenvía todas las solicitudes de autentificación de cliente al controlador y también tuneliza todos los datos del cliente de nuevo hacia el controlador. Este estado es válido solamente cuando el trayecto de control CAPWAP del Punto de acceso está para arriba. Esto significa que el H REAP está en el modo conectado. Cualquier WLAN que se

tunelice de nuevo al controlador se pierde durante una interrupción de la WAN, independientemente del método de autentificación.

- **autenticación central, Local Switching** — En este estado, para la red inalámbrica (WLAN) dada, el regulador maneja toda la autenticación de cliente, y el H COSECHA los paquetes de datos del Switches del Punto de acceso localmente. Después de que el cliente autentique con éxito, el regulador envía un comando de control CAPWAP al H REAP que da instrucciones el Punto de acceso para conmutar que los paquetes de datos del cliente dado localmente. Este mensaje se envía por cliente al realizarse satisfactoriamente la autentificación. Este estado es aplicable solamente en el modo conectado.
- **autenticación local, Local Switching** — En este estado, el H COSECHA las autenticaciones de cliente de las manijas del Punto de acceso y conmuta los paquetes de datos del cliente localmente. Este estado es válido solamente en el modo autónomo y sólo para los tipos de autentificación que se pueden gestionar localmente en el punto de acceso. Cuando un Punto de acceso de la híbrido-COSECHA ingresa el modo autónomo, los WLAN que se configuran para abierto, compartido, el WPA-PSK, o WPA2-PSK la autenticación ingresan la `autenticación local,` estado del `Local Switching` y continúan las nuevas autenticaciones de cliente.**Nota:** La encripción de los datos inalámbricos de Capa 2 siempre se gestionan en el punto de acceso. Todos los procesos de autentificación del cliente tienen lugar en el controlador (o en flujo ascendente desde el controlador, dependiendo de la configuración de la WLAN y del controlador) mientras el AP se encuentra en el estado conectado.
- **autenticación abajo, Local Switching** — En este estado, para la red inalámbrica (WLAN) dada, el H COSECHA los rechazos cualquier nuevo cliente que intente autenticar, pero continúa enviando los faros y las respuestas de la sonda para mantener a los clientes existentes conectados correctamente. Este estado es válido solamente en el modo autónomo.Si una WLAN conmutada localmente se configura para cualquier tipo de autentificación necesaria para procesarse en (o al norte de) el controlador (como pueda ser la autentificación EAP [WEP/WPA/WPA2/802.11i dinámico], WebAuth o NAC), tras un error de la WAN, ingresará en el modo de autentificación desactivada, conmutación local. En el pasado habría entrado en el estado de autentificación central, conmutación local. La conectividad inalámbrica existente se mantiene y el acceso a los recursos con cable locales continúa, pero no se permiten asociaciones nuevas. Si la sesión web de un usuario se desconecta cuando se utiliza WebAuth, o si el intervalo de validez de la clave EAP de un usuario expira cuando se usa 802.1X, y requiere volver a ingresar la clave, los clientes existentes pierden la conectividad y se les deniega la conectividad (esta duración depende del servidor RADIUS y, por lo tanto, no es estándar). También, el 802.11 que vaga por los eventos (entre H cosecha) acciona las reautentificaciones completas del 802.1x y así, representará la punta en la cual no prohiben los clientes existentes no más la Conectividad.Cuando la cuenta del cliente de tal red inalámbrica (WLAN) iguala cero, el H COSECHA cesa todas las funciones asociadas del 802.11 y baliza no más para el SSID dado, así moviendo la red inalámbrica (WLAN) al H siguiente COSECHE el estado: autentificación desactivada, conmutación desactivada.**Nota:** En el Software Release 4.2 o Posterior del regulador, los WLAN que se configuran para el 802.1x, el 802.1x WPA, el 802.1x WPA2, o el CCKM, pueden también trabajar en el modo autónomo. Pero estos tipos de autentificación requieren que un servidor RADIUS externo esté configurado. En las siguientes secciones se describen más detalles acerca de este tema. Pero, del Software Release 5.1 del regulador, el H SE COSECHA se puede configurar como servidor de RADIUS.
- **autenticación abajo, conmutando abajo** — En este estado, la red inalámbrica (WLAN) en un H dado COSECHA desasocia a los clientes existentes y para el enviar de los faros y de las

respuestas de la sonda. Este estado es válido solamente en el modo autónomo.Cuando un H COSECHA el Punto de acceso ingresa al modo autónomo, él desasocia a todos los clientes que estén en los WLAN centralmente conmutados. Para la autenticación Web WLAN, no desasocian a los clientes existentes, pero el H COSECHA el Punto de acceso envía no más los faros cuando el número de clientes asociados alcanza cero (0). También envía los mensajes de desasociación a los nuevos clientes que se asocian a las WLANs de autentificación web. Las actividades dependientes del controlador, como Control de acceso a la red (NAC) y autentificación web (acceso guest) se inhabilitan y el punto de acceso no envía ningún informe del sistema de detección de intrusiones (IDS) al controlador.**Nota:** Si su controlador está configurado para NAC, los clientes pueden asociarse solamente cuando el punto de acceso está en el modo conectado. Cuando se habilita NAC, es preciso crear una VLAN en mal estado (o en cuarentena) para que el tráfico de datos de todos los clientes asignados a esta VLAN pasen a través del controlador, incluso si la WLAN está configurada para la conmutación local. Después de asignar un cliente a una VLAN en cuarentena, todos sus paquetes de datos se conmutan centralmente.El punto de acceso de hybrid-REAP mantiene la conectividad del cliente incluso después de ingresar en el modo autónomo. Sin embargo, cuando el punto de acceso restablece una conexión con el controlador, desasocia todos los clientes, aplica la nueva información de la configuración del controlador y vuelve a permitir la conectividad del cliente.

H COSECHA el diseño y las limitaciones funcionales

H COSECHA las consideraciones PÁLIDAS

Porque el H REAP se ha diseñado específicamente para actuar a través de los links PÁLIDOS, se ha optimizado para tales instalaciones. Aunque H REAP es flexible cuando se trata de estos escenarios del diseño de red remota, todavía hay algunas guías de consulta que necesitan ser honradas al architecting una red con H COSECHAN las funciones.

- Un H COSECHA el Punto de acceso se puede desplegar con un IP Address estático o un DHCP Address. En el caso de DHCP, un servidor DHCP debe estar disponible localmente y debe poder proporcionar la dirección IP para el punto de acceso al iniciar.
- H COSECHA los soportes hasta cuatro paquetes fragmentados o un link PÁLIDO de la Unidad máxima de transmisión (MTU) del 500-byte del mínimo (MTU).
- El tiempo de espera del viaje de ida y vuelta no debe exceder 300 milisegundos (ms) para los datos y al ms 100 para la Voz y los datos entre el Punto de acceso y el regulador, y los paquetes de control CAPWAP se deben dar prioridad sobre el resto del tráfico.
- El controlador puede enviar paquetes multicast en formato de paquetes unicast o multicast al punto de acceso. En H COSECHE el modo, el Punto de acceso puede recibir los paquetes de multidifusión solamente en la forma del unicast.
- Para utilizar la itinerancia rápida del CCKM con H COSECHE los Puntos de acceso, usted necesitan configurar H COSECHAN a los grupos.
- H COSECHA el soporte SSID múltiples de los Puntos de acceso.
- La integración fuera de banda del NAC se soporta solamente en los WLAN configurados para H COSECHA la transferencia central. No se soporta para el uso en los WLAN configurados para H COSECHA el Local Switching.

Nota: Durante una actualización, cada AP necesita extraer una actualización de código de 4 MB a

través del link de la WAN. Planifique las actualizaciones y cambie Windows en concordancia.

Para asegurarse de que el soporte para esta limitación expuesta del tiempo de espera exista, se recomienda fuertemente que entre el Punto de acceso y el regulador, la prioridad esté configurada en la infraestructura intermediaria para elevar CAPWAP (puerto 5246 UDP) a la cola más prioritaria disponible. Sin la prioridad puesta en el control CAPWAP, los puntos en el otro tráfico de la red pueden mismo la causa probable H COSECHAR los Puntos de acceso para desplazar con frecuencia de conectado con los modos autónomos mientras que la congestión de link PÁLIDA evita que los mensajes del Punto de acceso/regulador (y las señales de mantenimiento) sean entregados. Se recomienda altamente a los diseñadores de red, que planean desplegar H COSECHAN EL AP sobre los links PÁLIDOS, para probar todas sus aplicaciones.

H frecuente COSECHA los problemas de conectividad serios de las causas del cambio. Sin el priorización de la red adecuada en el lugar, es prudente colocar los reguladores en los sitios remotos para asegurar el acceso de red inalámbrica constante y estable.

Nota: Si H REAP está configurado para hacer un túnel el tráfico del cliente de nuevo al regulador o no, el trayecto de datos CAPWAP se utiliza para remitir todas las sondas del cliente del 802.11 y peticiones de la autenticación/de la asociación, los mensajes RRM vecinos, y las peticiones EAP y de la autenticación Web de nuevo al regulador. Como tal, asegúrese de que los datos CAPWAP (puerto 5247 UDP) no estén bloqueados dondequiera entre el Punto de acceso y el regulador.

El híbrido COSECHA a los grupos

Para ordenar y manejar mejor su H COSECHE los Puntos de acceso, usted puede crear H COSECHA a los grupos y asigna los Puntos de acceso específicos a ellos. Todo el H COSECHA los Puntos de acceso en un grupo comparte el mismo CCKM, red inalámbrica (WLAN), e información de configuración de servidor de RADIUS de reserva. Esta característica es útil si usted hace que H múltiple COSECHE los Puntos de acceso en una oficina remota o en el suelo de un edificio y usted quiere configurarlos de una vez. Por ejemplo, usted puede configurar a un servidor de RADIUS de reserva para un H COSECHA al grupo bastante que teniendo que configurar el mismo servidor en cada Punto de acceso.

Scalability	Flex 7500	WLC 5500/Wism-2/Wism-1
Total Access Points	2,000	500
Total Clients	20,000	7,000
Max HREAP Groups	500	100
Max APs per HREAP Group	50	25
Max AP Groups	500	500

Las versiones de software 5.0.148.0 del regulador y posterior contienen dos que nuevo H

COSECHA las características del grupo:

- **Servidor de RADIUS de reserva** — Usted puede configurar el regulador para permitir un H COSECHA el Punto de acceso en el modo autónomo para realizar la autenticación completa del 802.1x a un servidor de RADIUS de reserva. Puede configurar un servidor RADIUS primario o un servidor RADIUS primario y secundario.
- **Autenticación local** — Usted puede configurar el regulador para permitir un H COSECHA el Punto de acceso en el modo autónomo para realizar la autenticación RÁPIDA del SALTO o EAP hasta 20 usuarios estáticamente configurados. Con el Software Release 5.0 del regulador hacia adelante, esto se ha aumentado a 100 usuarios estáticamente configurados. El regulador envía la lista estática de nombres de usuario y contraseña a cada H COSECHA el Punto de acceso cuando se une al regulador. Cada punto de acceso del grupo autentifica solamente a sus propios clientes asociados. Esta característica es ideal para clientes que emigra de una red autónoma del Punto de acceso a un CAPWAP H COSECHA la red del Punto de acceso y no necesita mantener una base de datos de usuarios grande ni agregar otro dispositivo de hardware para substituir las funciones del servidor de RADIUS disponibles en el Punto de acceso autónomo.

Las versiones de software del regulador que 7.0.116.0 y posterior contiene estos nuevo H COSECHAN las características del grupo:

- **Autenticación local** — Esta característica ahora se soporta incluso cuando H COSECHA los Puntos de acceso está en el modo conectado.
- **OKC ayunan vagando por** — H COSECHA a los grupos se requiere para CCKM/OKC rápidamente que vagan por para trabajar con H COSECHA los Puntos de acceso. La itinerancia rápida es alcanzada ocultando un derivado de la clave principal de una autenticación EAP completa de modo que un intercambio de claves simple y seguro pueda ocurrir cuando un cliente de red inalámbrica vaga por a un diverso Punto de acceso. Esta característica previene la necesidad de realizar una autenticación EAP completa RADIUS mientras que el cliente vaga por a partir de un Punto de acceso a otro. El H COSECHA los Puntos de acceso necesita obtener la información de la memoria caché CCKM/OKC para todos los clientes que pudieron asociarse así que pueden procesarla rápidamente en vez de enviarla de nuevo al regulador. Si, por ejemplo, usted tiene un regulador con 300 Puntos de acceso y 100 clientes que pudieron asociarse, enviando el caché CCKM/OKC para los 100 clientes no son prácticos. Si usted crea un H COSECHE al grupo que comprende un número limitado de los Puntos de acceso (por ejemplo, usted crea a un grupo para cuatro Puntos de acceso en una oficina remota), los clientes vagan por solamente entre esos cuatro Puntos de acceso, y el caché CCKM/OKC se distribuye entre esos cuatro Puntos de acceso solamente cuando los clientes se asocian a uno de ellos. Esta característica, junto con el radio y la autenticación local de reserva (Local-EAP), no asegura ningún tiempo muerto operativo para sus sitios secundarios.

Nota: La itinerancia rápida del CCKM entre H COSECHA y el NON-h COSECHA los Puntos de acceso no se soporta.

Refiera a configurar Híbrido-COSECHAN la sección de los grupos de la guía de configuración del controlador LAN de la tecnología inalámbrica de Cisco, liberan 7.0 para más información sobre cómo configurar H COSECHAN a los grupos.

Con trunk o sin trunk

H COSECHA los Puntos de acceso se puede conectar con los links del tronco 802.1q o los vínculos de acceso untagged. Cuando está conectado con un link de troncal, H COSECHA los Puntos de acceso envía su control y el tráfico de datos CAPWAP de nuevo al regulador vía el VLAN nativo. A continuación, las WLANs conmutadas localmente pueden descartar su tráfico en cualquier VLAN disponible (nativa o cualquier otra). Cuando el conjunto para actuar encendido un vínculo de acceso (sin la visibilidad del 802.1Q), H cosecha adelante todos los mensajes CAPWAP y datos del usuario localmente hacia fuera conmutados a la subred sola, untagged con la cual está conectado.

Las Pautas generales para la selección del modo del switchport para H REAPs son como sigue:

- Utilice un link de trunk si se configura más de una WLAN para la conmutación local y si el tráfico en estos SSIDs debe descartarse en varias subredes. El punto de acceso y el switchport de flujo ascendente deben configurarse para el trunking de 802.1Q. La configuración de H cosecha para el enlace del 802.1Q es la mayoría de la configuración común y proporciona la mayoría de la flexibilidad. El VLAN nativo también necesita ser configurado en el switchport que el H REAP está conectado con como toda la comunicación CAPWAP entre el AP y el WLC está en el VLAN nativo.
- Utilice un vínculo de acceso cuando H cosecha no tiene más que una sola red inalámbrica (WLAN) localmente conmutada ni tuvo múltiplo WLAN localmente conmutados que no requieran la separación del atar con alambre-lado. Sea consciente que un link de troncal puede todavía ser deseable bajo estas condiciones si la separación entre la Mensajería CAPWAP y los datos del usuario se desea. Pero, esto es ni requisitos para la configuración, ni un riesgo de seguridad.

Nota: H COSECHA los Puntos de acceso omite para actuar encendido untagged, las interfaces del vínculo de acceso.

H COSECHA la detección del regulador

H COSECHA los soportes cada mecanismo de detección del regulador característico de los Puntos de acceso en la arquitectura de la red inalámbrica unificada de Cisco. Cuando el punto de acceso tiene una dirección IP (proporcionada dinámicamente vía DHCP o a través de la asignación de direcciones estáticas), intenta detectar los controladores en el sistema mediante el broadcast IP, opción DHCP 43, DNS y OTAP (provisión por el aire). Finalmente, H REAPs recuerda los IP Addresses del regulador con el cual fueron conectados previamente. Refiera a Registro de Lightweight AP (LAP) en un Controlador LAN Inalámbrico (WLC) para obtener información sobre los distintos métodos que LAP puede usar para registrarse con un WLC.

Hay algunas advertencias a tener presente con respecto a la detección del regulador. Estas consideraciones se aplican a todos los puntos de acceso Aironet y no apenas H cosecha.

- La opción DHCP 43 es solamente un mecanismo de detección viable para H COSECHA si el Punto de acceso recibe su IP Addressing con el DHCP.
- OTAP solamente funciona para los puntos de acceso Aironet que ya se han conectado a un controlador y han descargado código. Se suministran sin el firmware de radio, por lo que OTAP no está preparada para funcionar inmediatamente. OTAP también requiere que se hayan encontrado otros puntos de acceso próximos y se hayan conectado a un controlador habilitado para OTAP. Esta característica es Obsoleta de la versión del WLC 6.0 hacia adelante.
- Se soporta un Punto de acceso en el cual H COSECHA las funciones no soporta el modo de

la capa 2 del LWAPP CAPWAP. Los reguladores se deben fijar para actuar con el LWAPP CAPWAP de la capa 3.
- Refiera a los reguladores del Wireless LAN de las Cisco 440X Series que despliegan para más información sobre la detección del Punto de acceso/regulador. operaciones

Más allá de estos mecanismos de detección tradicionales del regulador, el Software Release 4.0 y Posterior permite que los puntos de acceso Aironet con los puertos de la consola ahora soporten el aprovisionamiento manual a través de la consola CLI. Los puntos de acceso se pueden ahora configurar manualmente para las direcciones IP estáticas, la asignación de nombre de host y las direcciones IP de los controladores con los que se deben conectar los puntos de acceso. Esto significa que en los sitios donde no están disponibles otros mecanismos de detección, los Puntos de acceso se pueden configurar con toda la configuración de la conectividad necesaria manualmente a través del puerto de la consola.

Aunque esta característica se soporte en cada punto de acceso Aironet con un puerto de la consola, no apenas ésas configuradas para H COSECHAN, estas funciones son determinado útiles para H cosechan porque son más probables encontrarse instalados en los sitios que no se equipan de los servidores DHCP y de los mecanismos de detección del regulador, tales como adentro una sucursal. Como tal, este nuevo acceso a la consola evita la necesidad de enviar H cosecha dos veces: una primera vez a un sitio central para la provisión y una segunda vez al sitio remoto para la instalación.

H COSECHA las características admitidas

Porque H COSECHA los Puntos de acceso se diseñan para ser puestos a través de los links PÁLIDOS de los reguladores, no sólo están allí los aspectos del diseño que necesitan ser tenidos presente al architecting una red inalámbrica con H cosecha, pero hay también algunas características que están totalmente o en-parte sin apoyo.

No hay restricción del despliegue en el número de H COSECHA los Puntos de acceso para cada ubicación.

H COSECHA la Matriz de la función

Refiera a H COSECHAN la Matriz de la función para más información sobre las características soportadas con H COSECHAN.

Funciones de seguridad soportadas

El soporte de la Seguridad en el H COSECHA varía, que depende de los modos y estado mencionado previamente. Cualquier tipo de seguridad que requiera el control sobre el trayecto de datos, como VPN, no funciona con el tráfico en las WLANs conmutadas localmente porque el controlador no puede controlar los datos que no se tunelizan de nuevo hacia él. Cualquier otro trabajo del tipo de la Seguridad sobre los WLAN centralmente o localmente conmutados, con tal que la trayectoria entre el H COSECHE y el regulador está para arriba. Cuando este conducto está desactivado, sólo un subconjunto de estas opciones de seguridad permite que los nuevos clientes se conecten a las WLANs conmutadas localmente.

Como se mencionó anteriormente, para soportar la autenticación EAP del 802.1x, H COSECHA los Puntos de acceso en la necesidad del modo autónomo de tener sus propios servidores de RADIUS para autenticar a los clientes. Este servidor RADIUS de respaldo puede ser el que esté

usando el controlador. Usted puede configurar a un servidor de RADIUS de reserva para H individual COSECHA los Puntos de acceso a través del regulador CLI o para H COSECHA a los grupos con el GUI o el CLI. Un servidor de backup configurado para un punto de acceso individual reemplaza la configuración de servidor de RADIUS para un H COSECHA al grupo.

WLC Versión 4.2.61.0 y posterior soportan la itinerancia segura y rápida con Cisco Centralized Key Management (CCKM). H COSECHA la itinerancia segura de la capa 2 de los soportes del modo rápidamente con el CCKM. Con esta función no es necesaria la autentificación EPA de RADIUS completa, ya que el cliente realiza la itinerancia de un punto de acceso a otro. Para utilizar la itinerancia rápida del CCKM con H COSECHE los Puntos de acceso, usted necesitan configurar H COSECHAN a los grupos. El CCKM trabaja en el modo autónomo para ya los clientes conectados pero no para los nuevos clientes.

Refiera a configurar Híbrido-COSECHAN la sección de los grupos de la guía de configuración del controlador LAN de la tecnología inalámbrica de Cisco, liberan 7.0 para más información sobre cómo configurar H COSECHAN a los grupos.

Con H COSECHE en el modo conectado, el regulador está libre de imponer la exclusión del cliente/poner para evitar que algunos clientes se asocien a sus Puntos de acceso. Esta función puede utilizarse tanto en el modo manual como automatizado. Según las configuraciones globales y de la por-red inalámbrica (WLAN), los clientes pueden ser excluidos para un host de las razones, que se extiende de las tentativas relanzadas de la autenticación fallida al hurto IP, y para cualquier cantidad de tiempo determinada. Los clientes también pueden incluirse en esta lista de exclusión manualmente. La puesta en práctica de esta función solamente es posible mientras el punto de acceso se encuentra en el modo conectado. Pero, los clientes que se han colocado en esta lista de la exclusión siguen siendo incapaces de conectar con el Punto de acceso, incluso mientras que está en el modo autónomo.

Nota: Los WLAN que utilizan la autenticación de MAC (local o por aguas arriba) son permiten no más las autenticaciones de cliente adicionales cuando el Punto de acceso está en el modo autónomo, idénticas a la manera una red inalámbrica (WLAN) semejantemente configurada con el 802.1x o WebAuth actuaría en el mismo modo.

Soporte de la autenticación Web

La autenticación del Web interna, recibida en el regulador del Wireless LAN, se soporta para los WLAN que centralmente o localmente se conmutan. Sin embargo, la autenticación del Web externa se soporta solamente en una red inalámbrica (WLAN) centralmente conmutada.

Nota: Se soporta ninguno de los dos métodos de autenticación Web mientras que un H REAP está en el modo autónomo.

Características de la infraestructura soportadas

RRM

Debido al hecho de que muchas implementaciones remotas tengan solamente un pequeño puñado de H cosecha, las funciones completas del Administración de recursos de radio (RRM) no se pudo soportar en cada H COSECHA el sitio. RRM el código completo está presente en H COSECHA, pero los algoritmos del control de potencia de transmisión (TPC) adentro RRM no se accionan hasta cuatro o más Puntos de acceso esté dentro del rango de uno a. Así pues, un cierto H COSECHA las instalaciones pudo nunca accionar sus radios abajo. Como tal, sin nunca

poder accionar abajo sus radios en el primer lugar, H REAPs no ajusta la potencia de transmisión hacia arriba de compensar en caso de detección del agujero de la cobertura.

En el modo autónomo, RRM funciona en H cosecha que requiere el regulador que el proceso no se soporta.

Refiera a la administración de recursos de radio bajo redes inalámbricas unificadas para más información y detalles operativos de RRM.

DF

DFS (Dynamic Frequency Selection) está soportado tanto en los modos conectado como autónomo.

Seguimiento de la ubicación

La capacidad de prever la determinación exacta de la ubicación del dispositivo varía grandemente de la ubicación a la ubicación, basada grandemente en el número, densidad, y la colocación de H cosecha. La exactitud de la ubicación se articula pesadamente en la riqueza de la recopilación de información de la señal del dispositivo, que correlaciona directamente con los números de punto de acceso que pueden oír un dispositivo dado. Porque H COSECHA las implementaciones varía en el alcance, esta información sobre la ubicación puede ser reducida grandemente y la exactitud de la ubicación pudo sufrir así por consiguiente. Mientras que H COSECHA las implementaciones intentan indicar la ubicación de los dispositivos con la confianza más alta posible, las demandas expuestas de la exactitud de la ubicación de Cisco no se soportan en tales entornos.

Nota: H REAP no fue diseñado para proporcionar los servicios de ubicación. Por lo tanto, Cisco no puede soportar las demandas expuestas de la exactitud de la ubicación en H COSECHA las implementaciones.

Movilidad L2 y L3

La itinerancia de Capa 2 regular se soporta para las WLANs conmutadas localmente. Para prever tal itinerancia, asegúrese que los VLA N asignados a los WLAN localmente conmutados son constantes a través de todo el H cosechan en medio, que la itinerancia se requiere. Esto significa que no es necesario que los clientes vuelvan a realizar DHCP sobre los eventos de itinerancia. Esto ayuda a disminuir las latencias asociadas a las itinerancias.

La itinerancia de los eventos entre H cosecha en los WLAN localmente conmutados puede tomar entre el ms 50 el ms y 1500, que dependen del tiempo de espera PÁLIDO, de los diseños RF y de las características ambientales, así como la Seguridad teclea y las implementaciones de itinerancia cliente-específicas.

La capa 3 que vaga por no se soporta para los WLAN localmente conmutados, sino se soporta para los WLAN centralmente conmutados.

NAT/PAT

El NAT y la PALMADITA no se soportan para H COSECHAN los Puntos de acceso.

El otro H COSECHA las limitaciones

- H REAPs no soporta el WGB.

- Si usted ha configurado una red inalámbrica (WLAN) localmente conmutada, después el Listas de control de acceso (ACL) no trabaja y no se soporta. En una red inalámbrica (WLAN) centralmente conmutada, se soportan los ACL.
- Cualquier cambio a una configuración localmente conmutada de la red inalámbrica (WLAN) en la causa del regulador una pérdida temporaria en la Conectividad como la nueva configuración se aplica al H COSECHA. Como tal, cualquier cliente en éstos red inalámbrica (WLAN) localmente conmutada consigue temporalmente disconnected. La red inalámbrica (WLAN) se habilita inmediatamente y los clientes reasocian detrás.
- El controlador puede enviar paquetes multicast en formato de paquetes unicast o multicast al punto de acceso. En el modo hybrid-REAP, el punto de acceso puede recibir los paquetes multicast solamente en formato unicast.

Nota: Si el H REAP está conectado con el link del tronco 802.1q y hay localmente los WLAN conmutados configurados para el VLA N, después la orden de la configuración de la red inalámbrica (WLAN) vence importante a una limitación en el diseño. Si usted cambia la orden de la red inalámbrica (WLAN) por ejemplo la red inalámbrica (WLAN) 1 se configura para el ssid `WLAN-uno` y la red inalámbrica (WLAN) 2 se configura para el ssid `WLAN-B` y su orden se cambia con la red inalámbrica (WLAN) 1 de la configuración se convierte en ssid `WLAN-B` y la red inalámbrica (WLAN) 2 se convierte en ssid `WLAN-uno`, después ambos los WLAN pierden su asignación del VLA N que se configure del WLC.

Nota: El mismo problema se aplica de un H COSECHA que se una a un diverso regulador que tenga diversa orden de los mismos WLAN. Los controladores primarios y secundarios para un híbrido COSECHAN el Punto de acceso deben tener la misma configuración. Si no, el Punto de acceso puede perder su configuración, y ciertas características, tales como invalidación de la red inalámbrica (WLAN), los VLA N del grupo AP, número de canal estático, y así sucesivamente, no pueden potencialmente actuar correctamente. Además, aseegurese duplicar el SSID del H COSECHAN el Punto de acceso y su número del índice en ambos reguladores.

Tolerancia de fallas

H COSECHA la tolerancia de fallas permite que el acceso de red inalámbrica y los servicios ramifiquen los clientes cuando:

- H COSECHA la bifurcación AP pierde la Conectividad con el controlador primario.
- H COSECHA la bifurcación AP está conmutando al controlador secundario.
- H COSECHA la bifurcación AP está restableciendo la conexión al controlador primario.

H COSECHA la tolerancia de fallas, junto con el EAP local como delineado arriba, junto proporcione el tiempo muerto cero de la ramificación durante una interrupción de la red. Esta característica se habilita por abandono y no puede ser inhabilitada. No requiere ninguna configuración en el regulador o el AP. Sin embargo, asegurar los trabajos de la tolerancia de fallas suavemente y es aplicable, este los criterios debe ser mantenido:

- El ordenar y las configuraciones de la red inalámbrica (WLAN) tienen que ser idénticos a través de los controladores primarios y de backup.
- La asignación del VLA N tiene que ser idéntica a través de los controladores primarios y de backup.
- El Domain Name de la movilidad tiene que ser idéntico a través de los controladores primarios y de backup.
- Se recomienda para utilizar la plataforma del regulador como ambos controladores primarios y de backup.

Resumen

- H REAP no desconectará a los clientes cuando el AP está conectando de nuevo al mismo regulador proporcionado allí no es ningún cambio en configuración en el regulador.
- H REAP no desconectará a los clientes cuando la conexión con el controlador de backup proporcionado allí no es ningún cambio en configuración y el controlador de backup es idéntico al controlador primario.
- H REAP no reajustará sus radios en la conexión de nuevo al controlador primario proporcionado allí no es ningún cambio en configuración en el regulador.

Limitaciones

- Soportado solamente para H COSECHE con la central/la autenticación local con el Local Switching.
- Los clientes centralmente autenticados requieren la reautentificación completa si expira el temporizador de la sesión de cliente antes de que el H COSECHE el Switches AP de independiente al modo conectado.
- Los controladores primarios y de backup deben estar en el mismo dominio de la movilidad.

H COSECHA la configuración

Preparación de una red con cables

El primer paso a desplegar un H COSECHA la red es configurar el Switch con el cual el H REAP conectará. Esta configuración del switch del ejemplo incluye una configuración de VLAN nativa (la subred en la cual H REAPs comunique con el regulador con CAPWAP) y dos subredes en las cuales los datos de los clientes de dos WLAN localmente conmutados terminarán. Si el direccionamiento IP no se proporciona a los puntos de acceso ni a los clientes de las WLANs conmutadas localmente a través del switch de flujo ascendente (como se muestra más abajo), significa que los servicios de DHCP se deben proporcionar por otro medio o que el direccionamiento se debe proporcionar estáticamente. Aunque se recomienda DHCP, algunos clientes optarán por el direccionamiento de puntos de acceso estáticos y por proporcionar las direcciones de usuarios inalámbricos a través de DHCP. Las configuraciones del switch superfluas no se han incluido con el fin de simplificar este ejemplo.

```
ip dhcp excluded-address 10.10.10.2 10.10.10.99

ip dhcp pool NATIVE
network 10.10.10.0 255.255.255.0
default-router 10.10.10.1
!
ip dhcp pool VLAN11
network 10.10.11.0 255.255.255.0
default-router 10.10.11.1
!
ip dhcp pool VLAN12
network 10.10.12.0 255.255.255.0
default-router 10.10.12.1
!
interface FastEthernet1/0/1
description H REAP Example Config
switchport trunk encapsulation dot1q
switchport trunk native vlan 10
```

```
switchport trunk allowed vlan 10,11,12
switchport mode trunk
!
interface Vlan10
ip address 10.10.10.1 255.255.255.0
!
interface Vlan11
ip address 10.10.11.1 255.255.255.0
!
interface Vlan12
ip address 10.10.12.1 255.255.255.0
end
```

Nota: El direccionamiento de IP real en este ejemplo y todas las configuraciones posteriores se muestra únicamente con fines ilustrativos. Como tal, el direccionamiento IP se debe planificar teniendo en cuenta cada red y necesidad de forma individual.

En este ejemplo de configuración, el H REAP está conectado con la primera interfaz FastEthernet y recibe el IP Addressing vía el DHCP del Switch en el VLAN nativo (VLA N 10). Los vlanes innecesaria se podan del link de troncal conectado con el H COSECHAN para limitar el proceso de los paquetes extraños. Las VLANs 11 y 12 se han preparado para proporcionar el direccionamiento IP a los clientes de las dos WLANs vinculadas a ellos.

Nota: El Switch con el cual H REAPs conecta la Conectividad por aguas arriba de las necesidades con la infraestructura de ruteo. H COSECHA la orden de las mejores prácticas que la infraestructura de ruteo remote-site/WAN da prioridad al control CAPWAP (puerto 5246 UDP).

Aquí está una configuración de muestra de un router ascendente donde el H COSECHA EL AP fue conectado para dar prioridad al tráfico CAPWAP.

```
ip cef
!
frame-relay switching
!
class-map match-all 1
  match access-group 199
!
policy-map mypolicy
  class 1
   bandwidth 256
!
interface Serial0/0
ip address 10.1.0.2 255.255.255.0
encapsulation frame-relay
frame-relay interface-dlci 101
frame-relay intf-type dce
service-policy output mypolicy
!
access list 199 permit udp any any eq 5246
```

Detección del controlador de H-REAP mediante comandos de la CLI

H REAPs descubrirá lo más comúnmente posible los reguladores por aguas arriba vía la opción DHCP 43 o la resolución de DNS. Sin cualquiera de estos métodos disponibles, puede ser deseable proporcionar las Instrucciones detalladas a los administradores en los sitios remotos para poder configurar cada H REAP con la dirección IP de los reguladores con los cuales deben conectar. Opcionalmente, H COSECHA el IP Addressing se puede fijar manualmente también (si el DHCP es no disponible o no deseado).

Detalles de este ejemplo cómo la dirección IP H un REAP, el nombre de host, y la dirección IP del regulador se pueden fijar a través del puerto de la consola del Punto de acceso.

```
AP_CLI#capwap ap hostname ap1130
ap1130#capwap ap ip address 10.10.10.51 255.255.255.0
ap1130#capwap ap ip default-gateway 10.10.10.1
ap1130#capwap ap controller ip address 172.17.2.172
```

Nota: Los Puntos de acceso deben funcionar con el Cisco IOS Software Release 12.3(11)JX1 o Posterior Lwapp-habilitado de la imagen de recuperación IOS® para soportar el cuadro de los de estos comandos CLI. Los puntos de acceso con el prefijo SKU de LAP (por ejemplo, AIR-LAP-1131AG-A-K9) suministrado con posterioridad al 13 de junio de 2006, ejecutan Cisco IOS Software Release 12.3(11)JX1 o posterior. Estos comandos están disponibles para cualquier Punto de acceso que envíe del fabricante que funciona con este nivel de código, tenga el código actualizado manualmente a este nivel, o sea actualizado automáticamente conectando con una versión 6.0 o posterior corriente del regulador.

Estos comandos de configuración solamente se aceptan cuando el punto de acceso está en el modo autónomo.

Cuando un punto de acceso nunca se ha conectado a un controlador, los puntos de acceso tienen la contraseña CLI predeterminada de Cisco. Una vez conectados los puntos de acceso a un controlador, ninguna configuración de CLI se pueden realizar a través de la consola del punto de acceso hasta que se cambie la contraseña. Este comando exclusivo de la CLI se ingresa en el controlador con esta sintaxis:

```
(WLC_CLI)>config ap username <user-id> password <passwd> {all | <AP name>}
```

Para el punto de acceso anterior, se puede utilizar este comando:

```
(WLC_CLI)>config ap username admin password pass ap1130
```

Nota: Aunque este comando requiera la creación de un nombre de usuario, este campo no se implementa en este momento y se reserva para un uso futuro.

Nota: Todos los comandos **show** y debug funcionarán correctamente sin necesidad de cambiar las contraseñas predeterminadas de los puntos de acceso.

Configuración del controlador de H-REAP

Una vez que el H REAP ha descubierto y se ha unido al regulador, todo el H COSECHA las configuraciones se hace a través de la red o de las interfaces de la línea de comandos del regulador (alternativamente, la configuración se puede hacer centralmente con el [WCS] inalámbrico del sistema de control). El H COSECHA las configuraciones en esta sección se realiza a través de la interfaz gráfica del regulador.

Comience creando y configurando las WLANs que desee. Para esta configuración de ejemplo, las WLANs son como siguen (*las configuraciones personalizadas son necesarias*):

SSID de WLAN	Security	El conmutar

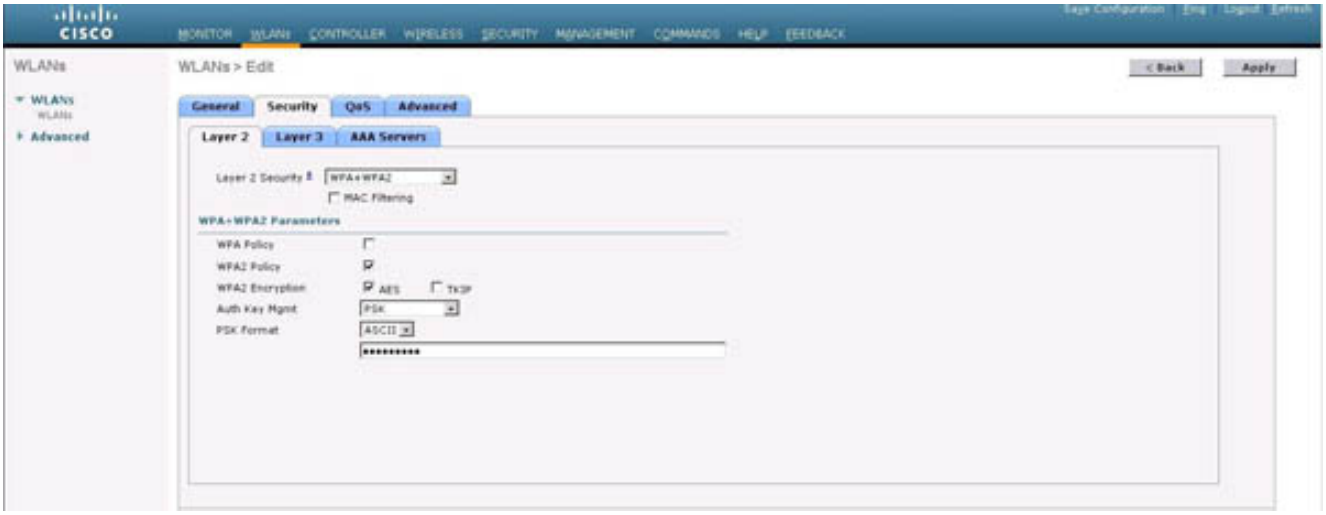
Corporativo	WPA2 (802.1X)	Local
RemoteSite	WPA2 - PSK	Local
Guest	WebAuth	Central

Para que un H COSECHE el Punto de acceso para actuar como un H COSECHA, el regulador con el cual está conectado debe tener por lo menos una red inalámbrica (WLAN) localmente conmutada (sin esto, las funciones de gran disponibilidad H REAP no será observado).

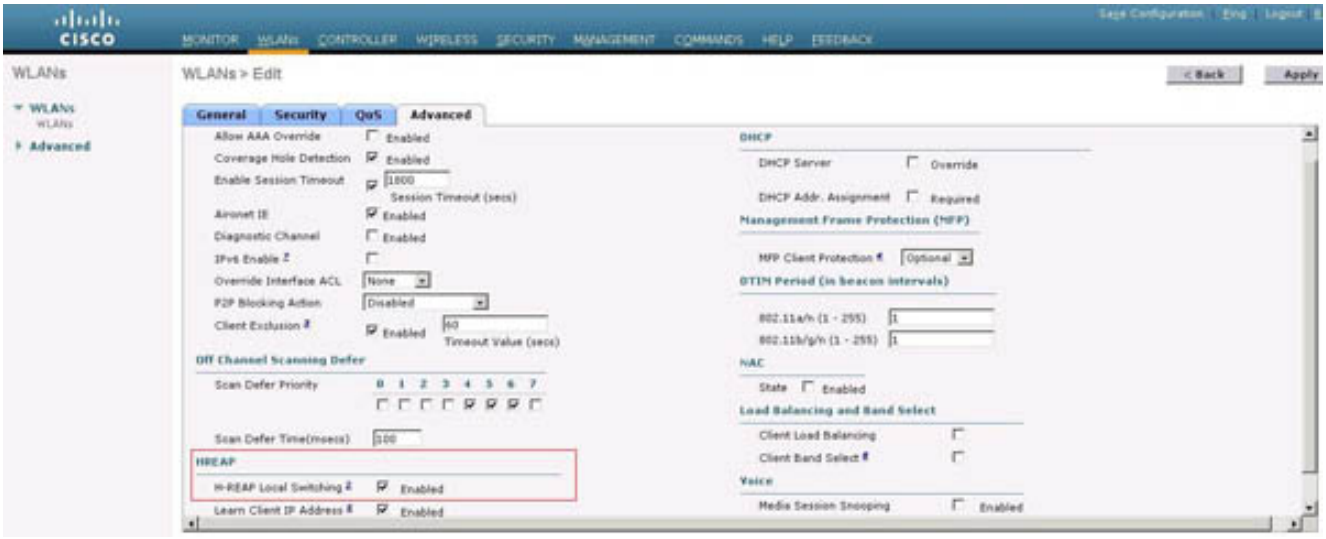
Complete estos pasos para configurar una WLAN localmente conmutada:

1. Vaya a la página principal del controlador, elija **WLANs** y haga clic en New.
2. Asigne a red inalámbrica (WLAN) un nombre, que también se utiliza como el SSID, y el tecleo **se aplica**.

3. En la red inalámbrica (WLAN) > edite la página, hacen clic la **ficha de seguridad**. En Layer 2 Security, seleccione el tipo de seguridad.En este ejemplo se utiliza WPA2-PSK. Elija **WPA+WPA2**.

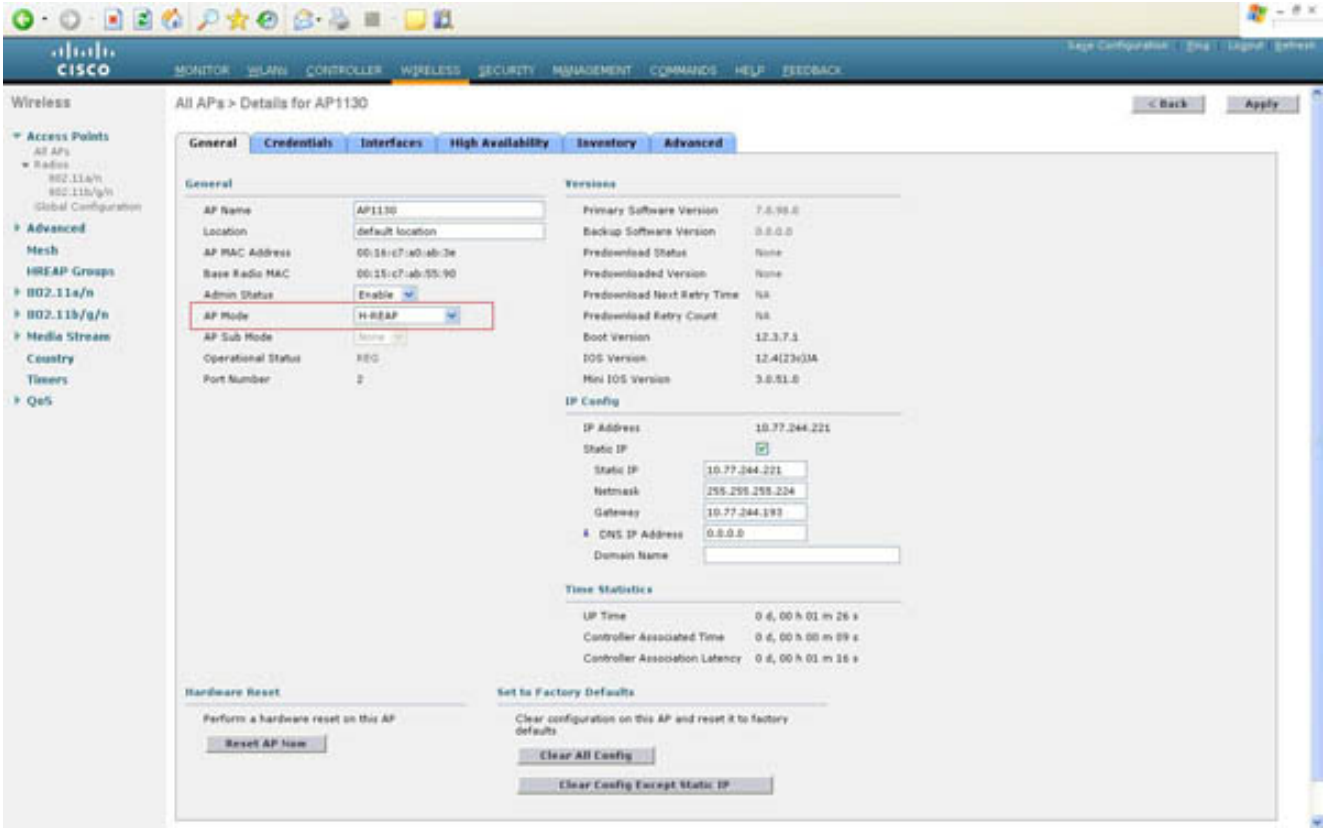


4. Marque **WPA2 Policy** para especificar las operaciones WPA de la WLAN.
5. Marque **AES** para establecer el método de encripción.
6. En Auth Key Mgmt, elija **PSK** en el menú desplegable.Dependiendo del formato de clave deseado, la opción elegida aquí depende del uso y el soporte de cliente. Seleccione **ascii** o hex. Ascii es normalmente más fácil porque acepta caracteres alfanuméricos. Elija el **ASCII** y ingrese la clave previamente compartida deseada.
7. Haga clic en la ficha Advanced (Opciones avanzadas). El control **H COSECHA el Local Switching** y se asegura que la red inalámbrica (WLAN) está habilitada para la operación.



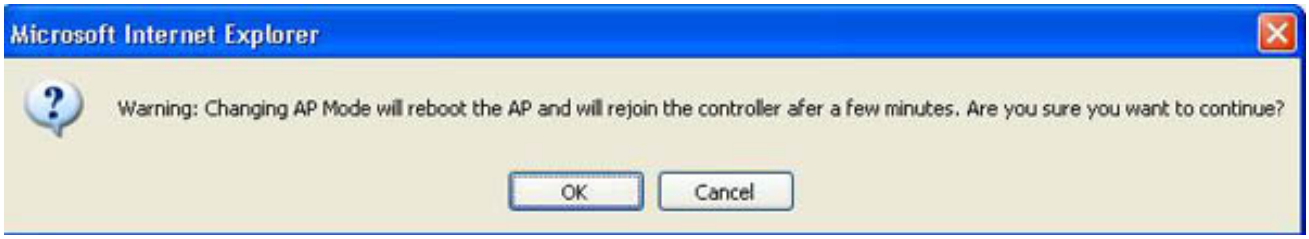
Sin este paso, la red inalámbrica (WLAN) no permite que los datos sean terminados localmente en H COSECHA los Puntos de acceso o no se ofrece en absoluto cuando el Punto de acceso está en el modo autónomo.**Nota:** Los Puntos de acceso no configurados para actuar en H COSECHAN el modo ignoran el H COSECHAN el Local Switching que fija y todo el tráfico del cliente es tunneled de nuevo al regulador.Con el H COSECHE la configuración de la red inalámbrica (WLAN) completa, el Punto de acceso puede entonces ser configurado para actuar en H COSECHAN el modo.

8. Después de que el punto de acceso haya detectado y se haya unido al controlador, vaya a la GUI web del controlador baja el encabezado Wireless y haga clic en **Detail** junto al punto de acceso elegido.
9. Por modo AP la dirección, elija **H COSECHAN del** menú desplegable para cambiar el Punto de acceso de su operación predeterminada del modo local para funcionar en H COSECHAN el
modo.



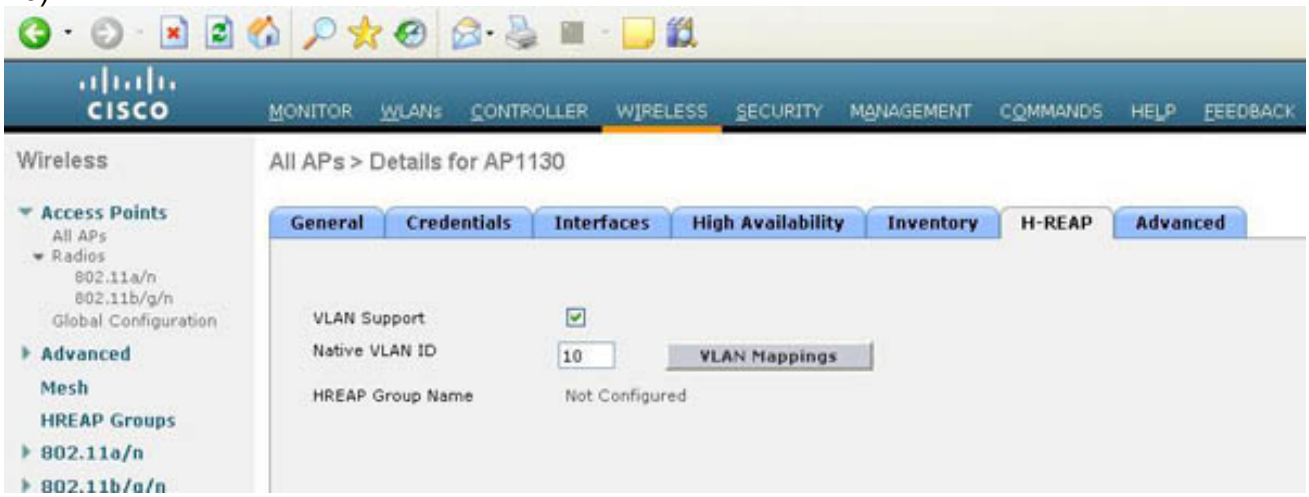
10. Haga clic en Apply (Aplicar). El punto de acceso debe reiniciarse para que la configuración de modo tenga

efecto.

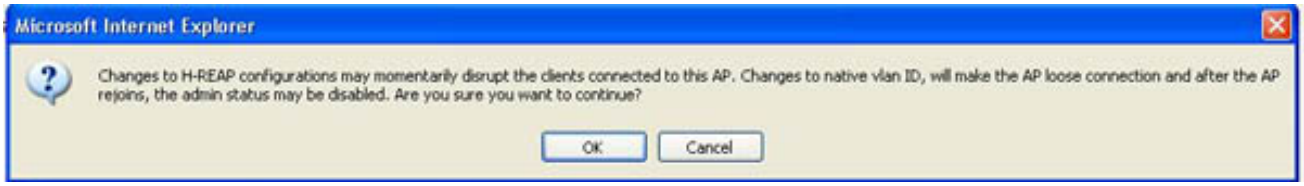


El punto de acceso se reinicia, vuelve a detectar el controlador y se une de nuevo al controlador.

11. Vuelva al encabezado **Wireless** de la GUI del controlador y seleccione el mismo link Detail del punto de acceso que antes.Por abandono, el H REAP no se configura para actuar encendido un link de troncal. Aunque el switchport al que está conectado se puede establecer en un link de trunk, el punto de acceso se sigue comunicando con el controlador a través de la VLAN nativa. Si el switchport es un link de troncal y se desea para hacer que el H REAP actúe en este modo, el soporte a VLAN debe ser habilitado.
12. Haga clic el **H COSECHAN la** lengueta. Marque **VLAN Support**.
13. De acuerdo con la configuración del switchport con el cual el H REAP está conectado, entre el número de ID del VLAN nativo del Punto de acceso al lado del título con el mismo nombre (en este ejemplo, el VLA N
10).



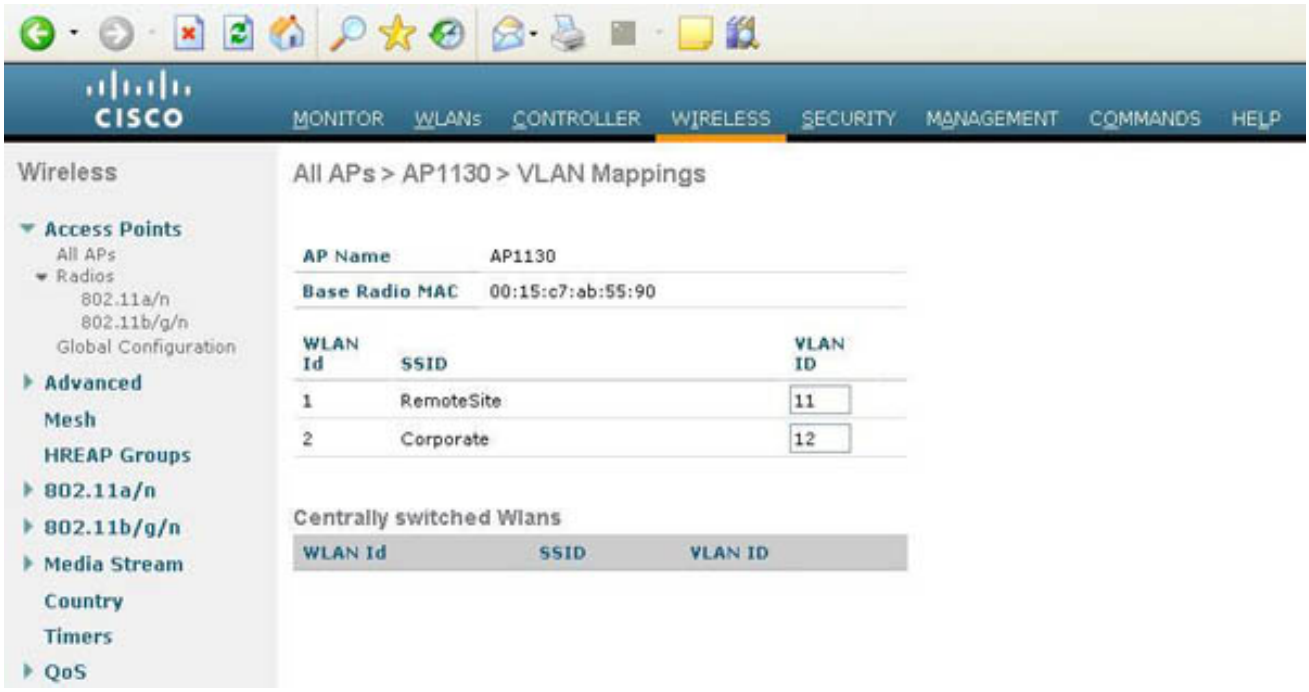
14. Haga clic en **Apply** para validar los cambios.Porque el H COSECHA las restauraciones la configuración de su acceso de Ethernet basado en los parámetros de la configuración dados, el Punto de acceso puede perder abreviadamente la Conectividad con el regulador. Una ventana emergente advierte de esta posibilidad. Click
OK.



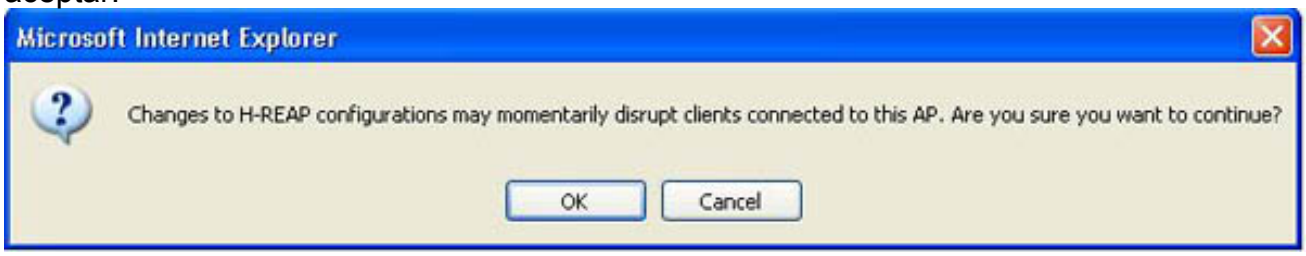
Nota: Tal y como indica la advertencia emergente, existe una remota posibilidad de que el punto de acceso se vuelva a conectar con el controlador en estado inhabilitado. Vuelva a seleccionar el link **Details** del punto de acceso desde el encabezado Wireless del controlador. A continuación, seleccione **Enable** junto a Admin Status. Aplique las opciones y continúe con la configuración.

15. Ingrese la página del detalle del Punto de acceso deseado, seleccione el H COSECHAN la etiqueta otra vez, y hacen clic el **VLA N que asocia** para configurar el 802.1Q que marca

con etiqueta por el WLAN localmente conmutado.



16. Establezca la VLAN por WLAN conmutada localmente en la que debe terminar el tráfico del cliente.**Nota:** Los WLAN no configurados para soportar H COSECHAN el Local Switching no permiten que la etiqueta del 802.1Q sea configurada aquí. La configuración de la VLAN para estas WLANs se establece en la configuración global del controlador porque los datos del cliente se tunelizan de nuevo hacia el controlador para su terminación.**Nota:** Las WLANs conmutadas localmente pueden compartir el mismo ID de VLAN o pueden tener asignaciones discretas. No hay limitaciones aquí, con tal que el VLAN asignado esté presente en el switchport del H COSECHE.
17. Haga clic en **Aply** para guardar los cambios.El servicio de la WLAN se interrumpe momentáneamente mientras se cambia el mapping de VLAN/WLAN. Haga clic en OK para aceptar.



Se crean los WLAN necesarios y configurado, los Puntos de acceso fijados para actuar en H COSECHAN el modo, el soporte a VLAN habilitado, y los VLA N configurados por la red inalámbrica (WLAN) localmente conmutada. Si los servicios de DHCP están disponibles en cada VLAN, los clientes deben poder conectarse a cada WLAN, recibir las direcciones en sus respectivas VLANs y pasar el tráfico. El H COSECHA la configuración es completo ahora.

Troubleshooting H-REAP

Hay algunos escenarios frecuentes y las situaciones que se presentan y previenen H liso COSECHAN la configuración y la conectividad del cliente. En esta sección se describen algunas de estas situaciones junto con sugerencias para solucionarlas.

H-REAP no se está uniendo al controlador

Esto puede ocurrir por varias razones. Empiece comprobando lo siguiente:

- **Cada H COSECHA las necesidades para ser correctamente IP dirigido.**Si DHCP se utiliza a través de la consola del punto de acceso, verifique que el punto de acceso obtenga una dirección.
  AP_CLI#**show dhcp lease**

  Si en la consola del punto de acceso se utiliza el direccionamiento estático, compruebe que se aplique el direccionamiento IP correcto.
  AP_CLI#**show capwap ip config**

- **Asegúrese de que el punto de acceso tenga conectividad de IP y que pueda hacer un ping de la interfaz de administración del controlador.**Una vez verificado el direccionamiento de IP, asegúrese de que el punto de acceso pueda comunicarse con el controlador haciendo ping en la dirección del controlador. Utilice el comando **ping** a través de la consola del punto de acceso con esta sintaxis:
  AP_CLI#**ping <WLC management IP address>**

  Si no es satisfactorio, asegúrese de que la red de flujo ascendente esté configurada correctamente y que el acceso WAN a la red corporativa está disponible. Verifique que el controlador esté operativo y que no esté situado detrás de un límite NAT/PAT. Asegúrese de que los puertos 5246 y 5247 UDP estén abiertos en cualquier Firewall intermediario. Haga ping del controlador en el punto de acceso con la misma sintaxis.
- **Verifique allí es Conectividad CAPWAP entre el Punto de acceso y el regulador.**La conectividad del IP entre el H COSECHA una vez y el regulador se verifica, realiza los debugs CAPWAP en el regulador para confirmar los mensajes CAPWAP se comunica a través de WAN y para identificar los problemas relacionados. En el controlador, cree en primer lugar un filtro MAC para limitar el alcance de la salida de los debugs. Utilice este comando para limitar la salida del comando subsiguiente a un único punto de acceso.
  AP_CLI#**debug mac addr <AP's wired MAC address>**

  Fije una vez para limitar la salida de los debugs, giran el debugging CAPWAP.
  AP_CLI#**debug capwap events enable**

  Si no se considera ningunos mensajes del debug CAPWAP, asegúrese que el H REAP tenga por lo menos un método por el cual un regulador pueda ser descubierto. Si tales métodos están disponibles (como la opción DHCP 43 o DNS), verifique si están correctamente configurados. Si no hay otro método de detección, asegúrese de que la dirección IP del controlador se ingrese en el punto de acceso a través de la CLI de la consola.
  AP_CLI#**capwap ap controller ip address <WLC management IP address>**

- **Marque las operaciones CAPWAP en el regulador y el H COSECHA.**Si por lo menos un solo método de detección del regulador está disponible para el H COSECHE, verifique los mensajes CAPWAP se envían del Punto de acceso al regulador. Este comando ya está habilitado de forma predeterminada.
  AP_CLI#**debug capwap client errors**

  Las direcciones IP del mensaje UDP que se envía pueden ver información adicional acerca de los controladores con los que se comunica el punto de acceso. Vea a las direcciones de origen y de destino de cada paquete que cruza la pila IP del punto de acceso.

```
AP_CLI#debug ip udp
```

Si aparece desde la consola del punto de acceso que se comunica con un controlador, es posible que se haya unido a otro controlador en el clúster. Para verificar si el H REAP está conectado con un regulador, utilice este comando.

```
AP_CLI#show capwap reap status
```

- **Verifique que el punto de acceso se haya unido al controlador correcto.**Si otros IP Addresses del regulador se dan al Punto de acceso durante la fase de la detección, el H REAP puede haberse unido a otro regulador. Verifique que la dirección IP del controlador que está disponible gracias al mecanismo de detección sea correcto. Identifique el controlador al que se ha unido el punto de acceso.

  ```
  AP_CLI#show capwap reap status
  ```

  Inicie sesión en la GUI web del controlador. Asegúrese de que todas las direcciones IP y MAC de los controladores se incluyan en la lista de movilidad del controlador y que todas compartan el mismo nombre de grupo de movilidad. A continuación, establezca los controladores primarios, secundarios y terciarios del punto de acceso para dictar a qué controlador se une el punto de acceso. Esto se lleva a cabo a través del link Details del punto de acceso. Si el problema descansa con el H REAP que se une a otro regulador, esto se puede facilitar grandemente usando las capacidades de administración sistema-anchas del Punto de acceso WCS.
- **Solucione los problemas de certificado si el punto de acceso está intentando unirse sin éxito al controlador.**Si los mensajes CAPWAP se consideran en el regulador, pero el Punto de acceso no puede unirse a, este probable es un problema del certificado.

Los comandos de la consola H-REAP no están operativos y devuelven un error

¡Cualquier comando configuration (configuración o claro de la configuración) se realizó con el H COSECHA la vuelta CLI el `ERROR!!!` El comando está inhabilitado. Esto puede ser debido a una de estas dos razones:

- H COSECHA los Puntos de acceso que están en el modo conectado no permitirán la configuración o el claro de cualquier configuración vía la consola. Cuando el punto de acceso se encuentra en este estado, las configuraciones deben realizarse a través de la interfaz del controlador. Si se necesita acceder a los comandos de configuración en el punto de acceso, asegúrese de que el punto de acceso esté en el modo autónomo antes de intentar ingresar algún comando de configuración.
- Una vez que el Punto de acceso ha conectado con un regulador en cualquier momento (incluso si el H REAP se ha movido de nuevo al modo autónomo), la consola del Punto de acceso no permitirá los comandos configuration hasta que se fije una nueva contraseña. Cada la contraseña H REAP necesita ser cambiada. Solamente es posible hacerlo desde la CLI del controlador al que está conectado el punto de acceso. Esta sintaxis de comando se puede utilizar en el controlador para establecer una contraseña de consola de punto de acceso individual o la contraseña de todos los puntos de acceso de todos los controladores:

  ```
  (WLC_CLI)>config ap username <user-id> password <passwd> {all | <AP name>}
  ```

  Nota: Para un punto de acceso cuyas contraseñas de consola no se han establecido, tenga en cuenta que esta configuración solamente se envía al punto de acceso donde el comando

se ingresa en el controlador. Para cualquier punto de acceso que se una posteriormente será preciso volver a ingresar el comando.Incluso cuando se ha asignado al punto de acceso una contraseña que no es la predeterminada y el punto de acceso se encuentra en el modo autónomo, el punto de acceso seguirá impidiendo el acceso a estos comandos. Para realizar los cambios a la configuración H el REAP, el retiro IP estático de la dirección preexistente y las configuraciones de IP Address del regulador se requiere. Esta configuración se llama la configuración privada CAPWAP y necesitará ser quitada antes de que cualquier nuevo comando CLI del Punto de acceso pueda ser entrado. A tal efecto, ingrese este comando:

```
AP_CLI#clear capwap private-config
```

Nota: Alternativamente, el AP se puede recuperar los valores predeterminados de fábrica mientras permanezca unido a un controlador. Haga clic en el botón **Clear Config** en la página de detalles de AP en el encabezado Wireless de la GUI de WLC. La configuración de AP se anula y se reinicia.**Nota:** Todos los comandos **show** y debug continuarán funcionando incluso sin tener especificada una contraseña distinta de la predeterminada y con el AP en el modo conectado.En este momento puede cualquier configuración CAPWAP ser hecha solamente.

Los clientes no pueden conectarse a H-REAP

Complete estos pasos:

1. Verifique que el Punto de acceso se ha unido a correctamente el regulador, el regulador tiene por lo menos una (y habilitado) red inalámbrica (WLAN) correctamente configurada, y se asegura que el H REAP está en el estado habilitado.
2. En el extremo del cliente, verifique que el SSID de la WLAN esté disponible (en el controlador, la configuración de la WLAN para que transmita su SSID puede ser de ayuda en este proceso de troubleshooting). Duplique la configuración de seguridad de la WLAN en el cliente. En las configuraciones de seguridad del lado del cliente residen la gran mayoría de problemas de conectividad.
3. Asegúrese de que los clientes en las WLANs localmente conmutadas cuenten con una dirección IP adecuada. Si se utiliza DHCP, asegúrese de que un servidor DHCP de flujo ascendente esté correctamente configurado y que proporcione direcciones a los clientes. Si se utiliza el direccionamiento estático, asegúrese de que los clientes estén configurados correctamente para la subred adecuada.
4. Para resolver problemas más lejos los problemas de la conectividad del cliente en el puerto de la consola H el REAP, ingrese este comando.

   ```
   AP_CLI#show capwap reap association
   ```

5. 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 <client's MAC address>
   ```

6. Para ejecutar un debug de los problemas de conectividad de 802.11 del cliente, utilice este comando.

   ```
   AP_CLI#debug dot11 state enable
   ```

7. Ejecute un debug del proceso de autentificación y las fallas de 802.1X del cliente con este comando.

   ```
   AP_CLI#debug dot1x events enable
   ```

8. Los mensajes backend controller/RADIUS se pueden hacer el debug de usando este comando.
   ```
   AP_CLI#debug aaa events enable
   ```

9. Alternativamente, para habilitar un juego completo de comandos del debug del cliente, utilice este comando.
   ```
   AP_CLI#debug client <client's MAC address>
   ```

H-REAP QA

Q. ¿Si configuro los revestimientos en un lugar remoto mientras que H cosecha, puedo dar a esos revestimientos un controlador primario y secundario?

Ejemplo: Un controlador primario está ubicado en el sitio A y un controlador secundario en el sitio B.

Si el controlador en el sitio A falla, el LAP conmuta por error al controlador en el sitio B. ¿Si ambos reguladores son inasequibles hacen la caída del REVESTIMIENTO en H COSECHAN el modo local?

A. Yes. Primero, el LAP conmuta por error al controlador secundario. Todas las WLAN que se conmutan localmente no tienen ningún cambio y todas las que se conmutan centralmente desvían el tráfico hacia el nuevo controlador. Y, si el controlador secundario falla, todas las WLANs marcadas para la conmutación local (y la autentificación de clave previamente compartida/abierta y el autenticador de AP) permanecen activadas.

Q. ¿Cómo los Puntos de acceso configurados en el trato del **modo local** con los WLAN configurados con H COSECHAN el Local Switching?

A. Las puntas de acceso de modo locales tratan estos WLAN como WLAN normales. La autentificación y el tráfico de datos se tunelizan de nuevo hacia WLC. Durante una falla del link de la WAN, esta WLAN está totalmente inactiva y no hay ningún cliente activo en ella hasta que se restaura la conexión al WLC.

Q. ¿Es posible realizar la autentificación web con conmutación local?

Sí, puede tener un SSID con la autentificación web habilitada y descartar el tráfico localmente después de la autentificación web. La autentificación web con conmutación local funciona correctamente.

Q. ¿Puedo utilizar mi Invitado-porta en el regulador para un SSID, que es dirigido localmente por el H COSECHA? En caso afirmativo, ¿qué sucede si pierdo la conectividad con el controlador? ¿Los clientes actuales se descartan inmediatamente?

Yes. Puesto que esta WLAN está localmente conmutada, la WLAN está disponible pero no se pueden autentificar clientes nuevos ya que la página web no está disponible. Sin embargo, no caen a los clientes existentes apagado.

Información Relacionada

- Guía de configuración del Controlador de LAN de la Red Inalámbrica Cisco, versión 4.0
- Actualización del Software del Controlador de la LAN Inalámbrica (WLC)
- Preguntas Frecuentes sobre el Troubleshooting de los Controladores de WAN Inalámbricos (WLC)
- Soporte de la Tecnología de la WLAN
- H COSECHA el ejemplo de configuración de los modos de operación
- Troubleshooting básico remoto híbrido del Punto de acceso del borde (H COSECHA)
- Ejemplos y Notas Técnicas de la Configuración del Controlador de la LAN inalámbrica
- Preguntas Más Frecuentes sobre Mensajes de Error y de Sistema del Controlador de la LAN inalámbrica (WLC)
- Mensajes de Error y de Sistema del Sistema de Control Inalámbrico (WCS)
- Soporte Técnico y Documentación - Cisco Systems