# Diseño y características FAQ del regulador del Wireless LAN (WLC)

ID del Documento: 118833

Actualizado: De marcha el 02 de 2015



### Productos Relacionados

- Controladores LAN inalámbricos Cisco de la serie 4400
- Cisco Wireless Controllers de la serie 5500
- Cisco Wireless Services Module 2 (WiSM2)
- Cisco Wireless Controllers de la serie 2500
- Cisco 2100 Series Wireless LAN Controllers
- Cisco Catalyst 3750 Series Integrated Wireless LAN Controllers
- Cisco Catalyst 6500 Series/7600 Series Wireless Services Module (WiSM)
- Controladores LAN inalámbricos Cisco de la serie 2000
- Cisco Wireless LAN Controller Module
- Controladores LAN inalámbricos Cisco de la serie 4100
- + demostración más

## Contenido



## Introducción

Este documento proporciona información sobre las preguntas más frecuentes (FAQ) sobre el diseño y las funciones disponibles con un Controlador de LAN inalámbrica (WLC).

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

## Preguntas frecuentes de diseño

## Q. ¿Cómo configuro el Switch para conectar con el WLC?

A. Configure el puerto del switch, con el cual el WLC está conectado, como puerto troncal del IEEE 802.1Q. Aseegurese que solamente los VLA N necesarios están permitidos en el Switch. Generalmente, la Administración y la interfaz del AP manager del WLC se dejan untagged. Esto significa que asumen el VLAN nativo del switch conectado. Esto no es necesario. Usted puede asignar un VLAN distinto a estas interfaces. Para más información, refiera a la *configuración el Switch para la* sección del *WLC del* ejemplo de la configuración básica del regulador y del Lightweight Access Point del Wireless LAN.

## Q. ¿Todo el tráfico de la red y a un cliente WLAN hace un túnel a través de un regulador del Wireless LAN (WLC) una vez que el punto de acceso consigue registrado con el regulador?

A. Cuando el AP se une a un WLC, un control y un aprovisionamiento del túnel del protocolo de los untos de acceso de red inalámbrica (CAPWAP) se forma entre los dos dispositivos. Todo el tráfico, que incluye todo el tráfico del cliente, se envía a través del túnel CAPWAP.

La única excepción a esto es cuando es un AP adentro híbrido-COSECHA el modo. Los Puntos de acceso de la híbrido-COSECHA pueden conmutar el tráfico de datos del cliente localmente y realizar la autenticación de cliente localmente cuando su conexión al regulador se pierde. Cuando están conectados con el regulador, pueden también enviar el tráfico de nuevo al regulador.

## Q. ¿Puedo instalar los Puntos de acceso ligeros (revestimientos) en una oficina remota y instalar un controlador LAN de la tecnología inalámbrica de Cisco (WLC) en mis jefaturas? ¿El LWAPP/CAPWAP trabaja sobre WAN?

A. Sí, usted puede tener el WLCs a través de WAN de los AP. LWAPP/CAPWAP trabaja sobre WAN cuando los revestimientos se configuran en el borde remoto AP (COSECHE) o el modo remoto híbrido del borde AP (H-REAP). Cualquiera de estos modos permite el control de un AP por un controlador remoto que esté conectado vía un link PÁLIDO. El tráfico se interliga sobre el link LAN localmente, que evita la necesidad de enviar innecesariamente el tráfico local sobre el link PÁLIDO. Éste es exacto uno de las ventajas más grandes del tener WLCs en su red inalámbrica.

**Nota:** No todos los AP ligeros soportan estos modos. Por ejemplo, el modo H-REAP se soporta solamente en 1131, 1140,1242, 1250, y los revestimientos AP801. COSECHE el modo se soporta solamente en los 1030 AP, pero los 1010 y 1020 AP no soportan COSECHAN. Antes de que usted planee implementar estos modos, marque para determinar si los revestimientos lo soportan. El software AP (AP autónomos) de Cisco IOS® que se ha convertido al LWAPP no soporta COSECHA.

## Q. ¿Cómo COSECHAN y los modos H-REAP trabajan?

A. En el modo de la **COSECHA**, todo el control y tráfico de administración, que incluye el tráfico de la autenticación, es tunneled de nuevo al WLC. Pero todo el tráfico de datos se conmuta localmente dentro de la oficina remota LAN. Cuando la conexión al WLC se pierde, todos los WLAN se terminan excepto la primera red inalámbrica (WLAN) (WLAN1). Conservan a todos los clientes que se asocian actualmente a esta red inalámbrica (WLAN). Para permitir que los nuevos clientes autentiquen y reciban con éxito el servicio en esta red inalámbrica (WLAN) dentro del

tiempo muerto, configure el método de autentificación para esta red inalámbrica (WLAN) como el WEP o WPA-PSK para hacer la autenticación localmente en la COSECHA. Para más información sobre COSECHE el despliegue, se refieren COSECHAN el Guía de despliegue en la sucursal.

En el modo **H-REAP**, un Punto de acceso hace un túnel el control y el tráfico de administración, que incluye el tráfico de la autenticación, de nuevo al WLC. El tráfico de datos de una red inalámbrica (WLAN) se interliga localmente en la oficina remota si la red inalámbrica (WLAN) se configura con el Local Switching H-REAP, o el tráfico de datos se devuelve al WLC. Cuando la conexión al WLC se pierde, todos los WLAN se terminan excepto los primeros ocho WLAN configurados con el Local Switching H-REAP. Conservan a todos los clientes que se asocian actualmente a estos WLAN. Para permitir que los nuevos clientes autentiquen y reciban con éxito el servicio en estos WLAN dentro del tiempo muerto, configure el método de autentificación para esta red inalámbrica (WLAN) como o WEP, PSK WPA, o WPA2PSK para hacer la autenticación localmente en H-REAP.

Para más información sobre H-REAP, refiera al diseño y al Guía de despliegue H-REAP.

## Q. ¿Cuál es la diferencia entre el Telecontrol-borde AP (COSECHE) y Híbrido-COSECHA (H-REAP)?

A. **REAP** no soporta marcar con etiqueta del VLA N del IEEE 802.1Q. Como tal, no soporta los VLAN múltiples. El tráfico de todos los identificadores del conjunto de servicio (SSID) termina en marcar con etiqueta del VLA N del IEEE 802.1Q de la misma subred, pero de los soportes H-REAP. El tráfico de cada SSID se puede dividir en segmentos a un VLA N único.

Cuando la Conectividad al WLC se pierde, es decir, en el modo autónomo, COSECHE los servicios solamente una red inalámbrica (WLAN), es decir, la primera red inalámbrica (WLAN). Se desactivan el resto de los WLAN. En H-REAP, hasta 8 WLAN se soportan dentro del tiempo muerto.

Otra diferencia principal es que, adentro COSECHE el modo, tráfico de datos se puede interligar solamente localmente. No puede ser conmutada de nuevo a la oficina central, pero, en el modo H-REAP, usted tiene la opción para volver el tráfico a la oficina central. El tráfico de los WLAN configurados con el Local Switching H-REAP se conmuta localmente. El tráfico de datos de otros WLAN se conmuta de nuevo a la oficina central.

Refiera al Telecontrol-borde AP (COSECHE) con los AP ligeros y al ejemplo de configuración de los reguladores del Wireless LAN (WLCs) para más información sobre REAP.

Refiera a configurar el híbrido COSECHAN para más información sobre H-REAP.

## Q. ¿Cuántos WLAN se soportan en el WLC?

A. Desde la versión de software 5.2.157.0, el WLC puede ahora controlar hasta 512 WLAN para los Puntos de acceso ligeros. Cada red inalámbrica (WLAN) tiene un ID DE WLAN separado (1 a 512), un nombre del perfil separado, y una red inalámbrica (WLAN) SSID, y se puede asignar las políticas de seguridad únicas. El regulador publica hasta 16 WLAN a cada Punto de acceso conectado, pero usted puede crear hasta 512 WLAN en el regulador y después publicar selectivamente estos WLAN (usando los grupos del Punto de acceso) a diversos Puntos de acceso para manejar mejor su red inalámbrica.

**Nota:** Los reguladores de Cisco 2106, 2112, y 2125 soportan solamente hasta 16 WLAN.

**Nota:** Para información detallada sobre las guías de consulta para configurar los WLAN en el WLCs, lea la sección WLAN que crea de la guía de configuración del controlador LAN de la tecnología inalámbrica de Cisco, versión 7.0.116.0.

## Q. ¿Cómo puedo configurar los VLA N en mi regulador del Wireless LAN (WLC)?

A. En el WLC, los VLA N se atan a una interfaz configurada en una subred de IP única. Esta interfaz se asocia sobre una red inalámbrica (WLAN). Entonces, los clientes que se asocian a esta red inalámbrica (WLAN) pertenecen al VLA N de la interfaz y se asignan una dirección IP de la subred a la cual la interfaz pertenece. Para configurar los VLA N en su WLC, complete el procedimiento en los VLA N en el ejemplo de configuración de los reguladores del Wireless LAN.

## Q. Tenemos aprovisionado dos WLAN con dos diversas interfaces dinámicas. Cada interfaz tiene su propio VLA N, que es diferente que el VLA N de la interfaz de administración. Esto parece trabajar, pero tenemos no aprovisionado los puertos troncales para permitir los VLA N que nuestros WLAN utilizan. ¿El punto de acceso marca los paquetes con etiqueta con el VLA N de la interfaz de administración?

A. El AP no marca los paquetes con etiqueta con el VLA N de la interfaz de administración. El AP encapsula los paquetes de los clientes en el protocolo ligero AP (LWAPP) /CAPWAP, y después pasa los paquetes encendido al WLC. El WLC entonces elimina la encabezado LWAPP/CAPWAP y adelante los paquetes al gateway con el VLA N apropiado marcan con etiqueta. La etiqueta del VLA N depende de la red inalámbrica (WLAN) a la cual el cliente pertenece. El WLC depende del gateway para rutear los paquetes a su destino. Para poder pasar el tráfico para los VLAN múltiples, usted debe configurar el Switch del uplink como puerto troncal. Este diagrama explica cómo los VLA N trabajan con los reguladores:

## Q. ¿Qué dirección IP del WLC se utiliza para la autenticación con el servidor de AAA?

A. El WLC utiliza la dirección IP de la interfaz de administración para cualquier mecanismo de autenticación (capa 2 o la capa 3) que implica a un servidor de AAA. Para más información sobre los puertos y las interfaces en el WLC, refiera a la sección de los *puertos que configura y de las interfaces de la* guía de configuración del controlador LAN de la tecnología inalámbrica de Cisco, versión 7.0.116.0.

## Q. Tengo diez Cisco 1000 Series Lightweight Access Point (revestimientos) y dos reguladores del Wireless LAN (WLCs) en el mismo VLA N. ¿Cómo pueden yo registrar seis revestimientos para asociarme a WLC1, y los otros cuatro revestimientos a asociarse al WLC2?

A. El LWAPP/CAPWAP permite la redundancia dinámica y el Equilibrio de carga. Por ejemplo, si usted especifica más de una dirección IP para la opción 43, un REVESTIMIENTO envía las peticiones de la detección LWAPP/CAPWAP a cada uno de los IP Addresses que el AP recibe. En la respuesta de la detección del WLC LWAPP/CAPWAP, el WLC integra esta información:

- Información sobre la carga actual del REVESTIMIENTO, que se define como el número de revestimientos que se unan a al WLC en ese entonces
- La capacidad del REVESTIMIENTO

- El número de clientes de red inalámbrica que están conectados con el WLC

El REVESTIMIENTO entonces intenta unirse al WLC menos-cargado, que es el WLC con la capacidad disponible más grande del REVESTIMIENTO. Además, después de que un REVESTIMIENTO se una a un WLC, el REVESTIMIENTO aprende los IP Addresses del otro WLCs en el grupo de la movilidad de su WLC unido.

Un REVESTIMIENTO se une a una vez un WLC, usted puede hacer que el REVESTIMIENTO se une a un WLC específico dentro de su reinicialización siguiente. Para hacer esto, asigne un WLC primario, secundario, y terciario para un REVESTIMIENTO. Cuando el REVESTIMIENTO reinicia, busca el WLC primario y se une a esa independiente del WLC de la carga en ese WLC. Si no responde el WLC primario, busca el secundario, y, si ninguna respuesta, el terciario. Para más información sobre cómo configurar el WLC primario para un REVESTIMIENTO, refiera a la *asignación primaria, secundaria, y a los controladores terciarios para la* sección *ligera AP de la* Conmutación por falla del controlador de WLAN para el ejemplo de configuración de los Puntos de acceso ligeros.

## Q. ¿Cuáles son las características que no se soportan en los reguladores del Wireless LAN de las 2100 Series (WLCs)?

A. Estas características de hardware no son 2100 reguladores soportados de la serie:

- Mantenga el puerto (la interfaz de Ethernet separada de la administración fuera de banda 10/100-Mb/s)

Estas funciones del software no son 2100 reguladores soportados de la serie:

- Terminación VPN (tal como IPSec y L2TP)
- Terminación de los túneles del regulador del invitado (la creación de los túneles del regulador del invitado se soporta)
- Lista del servidor Web de la autenticación del Web externa
- Layer 2 LWAPP
- Spanning-tree
- Reflejo de Puerto
- Cranite
- Fortaleza
- AppleTalk
- De QoS contratos del ancho de banda por usuario
- Traspaso IPv6
- Agregación del link (RETRASO)
- Modo unidifusión del Multicast
- Acceso de invitado atado con alambre

## Q. ¿Qué características no se soportan en los reguladores de las 5500 Series?

A. Estas funciones del software no se soportan en los reguladores de las 5500 Series:

- Interfaz estática del AP manager**Nota:** Para los reguladores de las 5500 Series, le no requieren configurar una interfaz del AP manager. La interfaz de administración actúa como interfaz del AP manager por abandono, y los Puntos de acceso pueden unirse a en esta interfaz.

- Tunelización asimétrico de la movilidad
- Spanning Tree Protocol (STP)
- Reflejo de Puerto
- Soporte del Access Control List de la capa 2 (ACL)
- Terminación VPN (tal como IPSec y L2TP)
- Opción del passthrough VPN
- Configuración de interligar, del APPLETALK, y del Point-to-Point Protocol over Ethernet (PPPoE) de 802.3

## Q. ¿Qué características no se soportan en las redes de interconexión?

A. Estas características del regulador no se soportan en las redes de interconexión:

- Soporte plurinacional
- CAC Carga-basado (soporte de las redes de interconexión solamente basado en el ancho de banda, o estático, CAC.)
- Alta disponibilidad (el latido del corazón rápido y la detección primaria se unen al temporizador)
- Autenticación EAP-FASTv1 y del 802.1x
- El Punto de acceso se une a la prioridad (los Puntos de acceso de la malla tienen una prioridad fija.)
- Localmente - certificado significativo
- Servicios location basados

## Q. ¿Cuál es el período de validez de los Certificados instalados fabricante (MIC) en un regulador del Wireless LAN y de los Certificados AP ligero?

A. El período de validez de un MIC en un WLC es 10 años. El mismo período de validez de 10 años se aplica a los Certificados AP ligero de la creación (si es un MIC o un certificado autofirmado (SSC)).

## Q. Tengo dos reguladores del Wireless LAN (WLCs) WLC1 nombrado y WLC2 configurados dentro del mismo grupo de la movilidad para la Conmutación por falla. Mi Lightweight Access Point (REVESTIMIENTO) se registra actualmente con WLC1. ¿Si WLC1 falla, el AP registrado a WLC1 reinicia durante su transición hacia el WLC de la supervivencia (WLC2)? ¿También, durante esta Conmutación por falla, el cliente WLAN pierde la Conectividad de la red inalámbrica (WLAN) con el REVESTIMIENTO?

A. Sí, el REVESTIMIENTO cancela de WLC1, reinicia, y después reregistra con WLC2, si WLC1 falla. Porque el REVESTIMIENTO reinicia, los clientes WLAN asociados pierden la Conectividad al REVESTIMIENTO que reinicia. Para la información relacionada, refiera al Equilibrio de carga AP y al retraso AP en las redes inalámbricas unificadas.

## Q. ¿Es vagando por dependiente en el modo del protocolo del Lightweight Access Point (LWAPP) que el regulador del Wireless LAN (WLC) se configura para utilizar? ¿Puede un WLC que actúa en el modo LWAPP de la capa 2 realizar la capa 3 que

## vaga por?

A. Mientras la movilidad que agrupa en los reguladores se configure correctamente, el cliente que vaga por debe trabajar muy bien. La itinerancia es inafectada por el modo LWAPP (la capa 2 o la capa 3). Sin embargo, se recomienda para utilizar el LWAPP de la capa 3 donde sea posible.

**Nota:** El modo de la capa 2 es soportado solamente por las Cisco y Series de WLCs y de los Puntos de acceso de las Cisco 1000 Series. El LWAPP de la capa 2 no es soportado por el otro regulador del Wireless LAN y Plataformas del Lightweight Access Point.

## Q. ¿Cuál es el proceso de itinerancia que ocurre cuando un cliente decide vagar por a un nuevo punto de acceso o regulador?

A. Ésta es la Secuencia de eventos que ocurre cuando un cliente vaga por a un nuevo AP:

1. El cliente envía una petición de la reasociación al WLC a través del REVESTIMIENTO.
2. El WLC envía el mensaje de la movilidad al otro WLCs en el grupo de la movilidad para descubrir con qué WLC era previamente asociado el cliente.
3. El WLC original responde con la información, tal como la dirección MAC, la dirección IP, el QoS, los contextos de seguridad, el etc. sobre el cliente a través del mensaje de la movilidad.
4. El WLC pone al día su base de datos con los detalles proporcionados del cliente; el cliente entonces pasa con el proceso del reauthentication, en caso necesario. El nuevo REVESTIMIENTO al cual asocian al cliente actualmente también se pone al día junto con otros detalles en la base de datos del WLC. Esta manera, el dirección IP del cliente se conserva a través vaga por entre el WLCs, que ayuda a proporcionar la itinerancia inconsútil.

Para más información sobre la itinerancia en un entorno unificado, refiera a la sección de los *Grupos de movilidad que configura de la* guía de configuración del controlador LAN de la tecnología inalámbrica de Cisco, versión 7.0.116.0.

**Nota:** El cliente de red inalámbrica no envía un pedido de autenticación (del 802.11) durante la reasociación. El cliente de red inalámbrica apenas envía la reasociación inmediatamente. Entonces, pasará con la autenticación del 802.1x.

## Q. ¿Qué puertos necesito permitir para la comunicación LWAPP/CAPWAP cuando hay un Firewall en la red?

A. Debe habilitar estos puertos:

- Habilite estos puertos UDP para el tráfico LWAPP:Datos - 12222Control - 12223
- Habilite estos puertos UDP para el tráfico CAPWAP:Datos - 5247Control - 5246
- Habilite estos puertos UDP para el tráfico de movilidad:16666 - Modo asegurado16667 - Modo sin garantía

La movilidad y los mensajes de datos se intercambian generalmente a través de los paquetes de EtherIP. **Protocolo IP 97** se deben permitir en el Firewall permitir los paquetes de EtherIP. Si usted utiliza el **ESP** para encapsular los paquetes de la movilidad, usted tiene que permitir el **ISAKMP** con el Firewall cuando usted abre el **puerto 500 UDP**. Usted también tiene que abrir **protocolo IP los 50** para permitir que los datos encriptados pasen con el Firewall.

Estos puertos son opcionales (dependiendo de sus requisitos):

- TCP 161 y 162 para SNMP (para el sistema de control inalámbrico [WCS])
- UDP 69 para TFTP
- TCP 80 y/o 443 para HTTP o HTTPS para acceso a GUI
- TCP 23 y/o 22 para Telnet o Secure Shell (SSH) para el acceso CLI

## Q. ¿Los reguladores del Wireless LAN soportan SSHv1 y SSHv2?

A. Los reguladores del Wireless LAN soportan solamente SSHv2.

## Q. ¿El ARP reverso (RARP) se soporta a través de los reguladores del Wireless LAN (WLCs)?

A. El Reverse Address Resolution Protocol (RARP) es un protocolo de la capa del link usado para obtener una dirección IP para un link-layer address dado tal como una dirección Ethernet. El RARP se soporta con el WLCs con versión de firmware 4.0.217.0 o más adelante. El RARP no se soporta en las versiones anteriores unas de los.

## Q. ¿Puedo utilizar al servidor DHCP interno en el regulador del Wireless LAN (WLC) para asignar los IP Addresses a los Puntos de acceso ligeros (revestimientos)?

A. Los reguladores contienen a un servidor DHCP interno. Este servidor se utiliza típicamente en las sucursales que no tienen ya un servidor DHCP. Para acceder el servicio del DHCP, haga clic el menú del **regulador del** WLC GUI; entonces haga clic al **servidor DHCP interno de la** opción en el lado izquierdo de la página. Para más información sobre cómo configurar el alcance de DHCP en el WLC, refiera a la sección del *DHCP que configura de la* guía de configuración del controlador LAN de la tecnología inalámbrica de Cisco, versión 7.0.116.0.

El servidor interno proporciona los DHCP Address a los clientes de red inalámbrica, los revestimientos, el dispositivo-MODE AP en la interfaz de administración, y los pedidos de DHCP que se retransmiten de los revestimientos. El WLCs nunca ofrece los direccionamientos a los dispositivos por aguas arriba en la red alámbrica. La opción DHCP 43 no se soporta en el servidor interno, así que el AP debe utilizar un método alternativo para localizar la dirección IP de la interfaz de administración del regulador, tal como broadcast de la subred local, DNS, oscurecimiento, o sobre - ventile la detección.

**Nota:** Versiones de firmware del WLC antes de que 4.0 no soporten el servicio del DHCP para los revestimientos a menos que los revestimientos estén conectados directamente con el WLC. La característica interna del servidor DHCP fue utilizada para proporcionar solamente los IP Addresses a los clientes que conectan con la red inalámbrica LAN.

## Q. ¿Qué el campo obligatorio del DHCP bajo una red inalámbrica (WLAN) significa?

A. El DHCP requerido es una opción que se puede habilitar para una red inalámbrica (WLAN). Necesita que todos los clientes que se asocian a esa red inalámbrica (WLAN) determinada obtienen los IP Addresses con el DHCP. No se permite a los clientes con los IP Address estáticos asociarse a la red inalámbrica (WLAN). Esta opción se encuentra bajo ficha Avanzadas de una

red inalámbrica (WLAN). El WLC permite el tráfico a/desde un cliente solamente si su dirección IP está presente en la tabla MSCB del WLC. El WLC registra la dirección IP de un cliente durante su pedido de DHCP o el DHCP renueva. Esto requiere que un cliente renueve su dirección IP que reasocia cada vez al WLC porque el cliente desasocia cada vez como una parte de su vaga por el proceso o el tiempo de espera de la sesión, su entrada se borra de la tabla MSCB. El cliente debe reautentificar y reasociar otra vez al WLC, que hace otra vez la entrada del cliente en la tabla.

## Q. ¿Cómo hace el trabajo centralizado Cisco de la administración de claves (CCKM) en un entorno LWAPP/CAPWAP?

A. Durante la asociación del cliente inicial, el AP o el WLC negocia en parejas una clave principal (PMK) después de que el cliente de red inalámbrica pase la autenticación del 802.1x. El WLC o el WDS AP oculta el PMK para cada cliente. Cuando un cliente de red inalámbrica reasocia o vaga por, salta la autenticación del 802.1x y valida el PMK inmediatamente.

La única implementación especial del WLC en el CCKM es que PMK del cliente del intercambio del WLCs vía los paquetes de la movilidad, tales como UDP 16666.

## Q. ¿Cómo fijo las configuraciones dúplex en el regulador del Wireless LAN (WLC) y los Puntos de acceso ligeros (revestimientos)?

A. Los Productos de tecnología inalámbrica de Cisco funcionan mejor cuando se autonegocia la velocidad y dúplex, pero usted tiene la opción para fijar las configuraciones dúplex en el WLC y los revestimientos. Para fijar las configuraciones dúplex/velocidades AP, usted puede configurar las configuraciones dúplex para los revestimientos en el regulador y después, a su vez, los avanza a los revestimientos.

**el name> de la velocidad <auto/10/100/1000> <all/Cisco AP del dúplex Ethernet <auto/half/full> ap de la configuración** es el comando de fijar las configuraciones dúplex con el CLI. Este comando se soporta con las versiones 4.1 y posterior solamente.

Para fijar las configuraciones dúplex para las interfaces físicas del WLC, utilice el **physicalmode del puerto de los config {todo | puerto} {100h | 100f | 10h |** comando **10f}**.

Este comandos estableces haber especificado o todos los accesos de Ethernet del panel de delante 10/100BASE-T para el 10 Mbps dedicado o 100 Mbps, semidúplex o operación en dúplex completo. Observe que usted debe inhabilitar el autonegotiation con el **comando disable del autoneg del puerto de los config** antes de que usted configure manualmente a cualquier modo físico en el puerto. También, observe que el **comando autoneg del puerto de los config** reemplaza las configuraciones hechas con el comando del **physicalmode del puerto de los config**. Por abandono, todos los puertos se fijan al auto negocian.

**Nota:** No hay manera de cambiar las configuraciones de la velocidad en los puertos de fibra.

## Q. ¿Hay una manera de seguir el nombre del Lightweight Access Point (REVESTIMIENTO) cuando no se registra al regulador?

A. Si su AP totalmente abajo y no se registra al regulador, no hay manera que usted puede seguir el REVESTIMIENTO a través del regulador. La única forma que sigue habiendo es que usted puede acceder el Switch en el cual estos AP están conectados, y usted puede encontrar el switchport en el cual están conectados usando este comando:

**show mac-address-table address** *<mac address>*

Esto le da el número del puerto en el Switch con el cual este AP está conectado. Entonces, publique este comando:

**show cdp nei** *<type/num>* **detail**

La salida de este comando también da el nombre del REVESTIMIENTO. Sin embargo, este método es solamente posible cuando su AP se acciona para arriba y está conectado con el Switch.

## Q. He configurado a 512 usuarios en mi regulador. ¿Hay manera de aumentar el número de usuarios en el regulador del Wireless LAN (WLC)?

A. La base de datos de usuarios locales se limita a un máximo de 2048 entradas en la **Seguridad >** página **general**. Esta base de datos es compartida por los usuarios de la administración local (que incluye a los embajadores del pasillo), los usuarios netos (que incluye a los Usuarios invitados), las entradas del filtro MAC, las entradas de la lista de la autorización del Punto de acceso, y las entradas de la lista de la exclusión. Junto, todos estos tipos de usuarios no pueden exceder el tamaño de la base de datos configurado.

Para aumentar la base de datos local, utilice este comando del CLI:

```
<Cisco Controller>config database size ?
<count>  Enter the maximum number of entries (512-2048)
```

**Nota:** Usted tiene que salvar la configuración y reajustar el sistema (usando el **comando reset system**) para que el cambio tome el efecto.

## Q. ¿Cómo aplico una política de contraseña fuerte en el WLCs?

A. El WLCs permite que usted defina una política de contraseña fuerte. Esto se puede hacer usando el CLI o el GUI.

En el GUI, van a la **Seguridad >**AAA **>** las **políticas de contraseña**. Esta página tiene una serie de opciones que se pueda seleccionar para aplicar una contraseña fuerte. Aquí tiene un ejemplo:

Para hacer esto del WLC CLI, utilice al fuerte-**pwd del switchconfig de los config** *{caso-control | consecutivo-control | valor por defecto-control | nombre de usuario-control | todo-control} {permiso |* comando de la *neutralización}*:

- **caso-control** - Marca el acontecimiento lo mismo carácter tres veces consecutivamente.
- **consecutivo-control** - Marca si los valores predeterminados o se están utilizando sus variantes.
- **valor por defecto-control** - Marca si o nombre de usuario o su se está utilizando el revés.
- **todo-controles** - Los permisos/inhabilitan todo el fuerte controles de la contraseña.

## P.. ¿Cómo la función de cliente pasiva se utiliza en los reguladores del Wireless LAN?

A. Los clientes pasivos son dispositivos de red inalámbrica, tales como escalas e impresoras eso

se configuran con un IP Address estático. Estos clientes no transmiten ningún IP información tal como dirección IP, máscara de subred, y información del gateway cuando ellos socio con un Punto de acceso. Como consecuencia, cuando utilizan a los clientes pasivos, el regulador nunca conoce la dirección IP a menos que utilicen el DHCP.

El WLCs actúa actualmente como proxy para los pedidos ARP. Sobre la recepción de un ARP la petición, el regulador responde con una respuesta ARP en vez del paso petición directamente al cliente. Este escenario tiene dos ventajas:

- El dispositivo ascendente que envía el pedido ARP al cliente lo va a hacer no saber dónde localizan al cliente.
- Poder para los dispositivos con pilas tales como teléfonos móviles e impresoras se preserva porque no tienen que responder a cada ARP peticiones.

Puesto que el regulador inalámbrico no tiene ninguna información relacionada IP sobre los clientes pasivos, no puede responder a ninguna pedidos ARP. La corriente el comportamiento no permite la transferencia de los pedidos ARP a los clientes pasivos. Ningunos la aplicación que intenta acceder a un cliente pasivo fallará.

La función de cliente pasiva habilita los pedidos ARP y las respuestas de ser intercambiado entre atado con alambre y clientes de red inalámbrica. Esta característica, cuando está habilitada, permite que el regulador pase los pedidos ARP de atado con alambre a los clientes de red inalámbrica hasta el cliente de red inalámbrica deseado consigue al estado de FUNCIONAMIENTO.

Para la información sobre cómo configurar la función de cliente pasiva, lea la sección encendido El usar el GUI para configurar al cliente pasivo adentro Cisco Guía de configuración de controlador del Wireless LAN, versión 7.0.116.0.

## P.. Cómo pueda I configura al cliente para reautentificar con el servidor de RADIUS ¿cada tres minutos o en periodo de tiempo especificado?

A. El parámetro de tiempo de espera de la sesión en el WLC se puede utilizar para lograr esto. Por abandono, el parámetro de tiempo de espera de la sesión se configura por 1800 segundos antes de un reauthentication ocurre.

Cambie este valor a 180 segundos para hacer al cliente reauthenticate después de tres minutos.

Para acceder el parámetro de tiempo de espera de la sesión, haga clic Menú **WLAN** en el GUI. Visualiza la lista de WLAN configurado en el WLC. Haga clic la red inalámbrica (WLAN) a la cual el cliente pertenece. Vaya a **la ficha Avanzadas** y usted encuentran la *sesión del permiso Parámetro de tiempo de espera*. Cambie el valor predeterminado a 180, y haga clic **Solicite los** cambios para tomar el efecto.

Cuando está enviado en un access-accept, junto con un valor de la Terminación-acción de El pedido de RADIUS, el atributo del Sesión-descanso especifica el número máximo de segundos del servicio proporcionados antes de la reautentificación. En este caso, El atributo del Sesión-descanso se utiliza para cargar el ReAuthPeriod constante dentro del Máquina de estado del temporizador del Reauthentication del 802.1x.

## P.. Tengo un Tunelización del invitado, los Ethernetes sobre el túnel IP (EoIP), configurado entre mi regulador del Wireless LAN 4400 (WLC), que actúa como el

## WLC del ancla, y vario WLCs remoto. Pueden los broadcastes de subred del WLC de esta ancla adelante a través el túnel de EoIP de la red alámbrica a los clientes de red inalámbrica asociados al ¿controladores remotos?

A. No, el WLC 4400 no remite los broadcasts de la subred IP del atado con alambre eche a un lado a los clientes de red inalámbrica a través del túnel de EoIP. Éste no es soportado característica. Cisco no soporta el Tunelización del broadcast de subred o del Multicast adentro topología del acceso de invitado. Puesto que la red inalámbrica (WLAN) del invitado fuerza el Point of Presence del cliente a una ubicación muy específica en la red, sobre todo fuera del Firewall, el Tunelización del broadcast de subred puede ser un problema de seguridad.

## P.. En un protocolo del regulador (WLC) y del Lightweight Access Point del Wireless LAN (LWAPP) puesto, qué Differentiated Services Code Point (DSCP) valora se pasan ¿para el tráfico de voz? ¿Cómo implementan a QoS en el WLC?

A. La solución WLAN de la red del Cisco Unified Wireless (UWN) soporta cuatro niveles de QoS:

- Platino/Voz
- Oro/vídeo
- De plata/mejor esfuerzo (valor por defecto)
- Bronce/fondo

Usted puede configurar la red inalámbrica (WLAN) del tráfico de voz para utilizar el platino QoS, asigna la red inalámbrica (WLAN) del ancho de banda baja para utilizar QoS de bronce, y para asignar el resto del tráfico en medio los otros niveles de QoS. Consulte Asignación un perfil de QoS a una red inalámbrica (WLAN) para más información.

## P.. Son puentes de Ethernet de Linksys soportados en una tecnología inalámbrica de Cisco unificada ¿Solución?

A. No, el WLC soporta solamente los Productos de Cisco WGB. Linksys WGB no es soportado. Aunque la única solución de la tecnología inalámbrica de Cisco no soporte Linksys WET54G y puentes de Ethernet WET11B, usted puede utilizar estos dispositivos en a Configuración inalámbrica de la única solución si usted utiliza estas guías de consulta:

- Conecte solamente un dispositivo con el WET54G o el WET11B.
- Permita a la característica de la reproducción MAC en el WET54G o el WET11B para reproducir dispositivo conectado.
- Instale los más nuevos drivers y firmware en los dispositivos conectados con WET54G o WET11B. Esta guía de consulta es especialmente importante para las impresoras de JetDirect porque versiones de firmware anteriores causan los problemas con el DHCP.

**Nota:** Otros Bridges de tercera persona no se soportan. Los pasos mencionados pueden también inténtese para otros Bridges de tercera persona.

## P.. Cómo lo hago salve los archivos de configuración en el regulador del Wireless LAN ¿(WLC)?

A. El WLC contiene a dos tipos de memoria:

- RAM volátil — Lleva a cabo la corriente, controlador activo configuración

- Memoria RAM no volátil (NVRAM) — Lleva a cabo la reinicialización configuración

Cuando usted configura el sistema operativo en el WLC, usted se está modificando el RAM volátil. Usted debe salvar la configuración del RAM volátil al NVRAM para aseegurarse que el WLC reinicia en la configuración actual.

Es importante saber qué memoria usted está modificando cuando usted se realiza estas tareas:

- Utilice al asistente de configuración.
- Borre la configuración de controlador.
- Salve las configuraciones.
- Reajuste el regulador.
- Logout del CLI.

# Características FAQ

### P.. Cómo fijo el tipo del Protocolo de Autenticación Extensible (EAP) en ¿Regulador del Wireless LAN (WLC)? Quiero autenticar contra un control de acceso El dispositivo del servidor (ACS), y yo conseguimos un “EAP sin apoyo” tecleamos adentro registros.

A. No hay configuración de tipo separada EAP en el WLC. Para la luz EAP (SALTO), Autenticación adaptable de EAP vía el Tunelización seguro (EAP-FAST), o Microsoft El EAP protegido (MS-PEAP), apenas el IEEE 802.1X de la configuración o el Wi-Fi protegieron el acceso (WPA) (si usted utiliza el 802.1x con el WPA). Cualquier tipo EAP que se soporte en El extremo posterior RADIUS y en el cliente se soporta vía la etiqueta del 802.1x. El EAP la determinación en el cliente y el servidor de RADIUS debe hacer juego.

Complete estos pasos para habilitar el EAP con el GUI en WLC:

1. Del WLC GUI, tecleo **WLAN**.
2. Una lista de WLAN configurados en el WLC aparece. Haga clic una red inalámbrica (WLAN).
3. En los **WLAN > editan**, hacen clic **Ficha de seguridad**.
4. Haga clic la **capa 2**, y elija la Seguridad de la capa 2 como 802.1x o WPA+WPA2. Usted puede también configurar los parámetros del 802.1x que están disponibles adentro la misma ventana. Entonces, del WLC los paquetes de la autenticación EAP adelante entre cliente de red inalámbrica y el servidor de autenticación.
5. Haga clic a los **servidores de AAA**, y elija servidor de autenticación del menú desplegable para esta red inalámbrica (WLAN). Asumimos que configuran al servidor de autenticación ya global. Para la información sobre cómo habilite la opción EAP en el WLCs a través del comando line interface(cli), refiérase al *El usar el CLI para configurar el RADIUS* sección del Cisco Guía de configuración de controlador del Wireless LAN, versión 7.0.116.0.

### P.. ¿Qué el SSID rápido está cambiando?

A. El cambio rápido SSID permite que los clientes se muevan entre los SSID. Cuando el cliente envía una nueva asociación para un diverso SSID, la entrada del cliente en se borra la tabla de conexiones del regulador antes de que agreguen al cliente al nuevo SSID. Cuando se inhabilita el cambio rápido SSID, el regulador aplica un retardo antes de que se permita a los clientes

trasladarse a un nuevo SSID. Para la información sobre cómo el permiso SSID rápido que cambia, refiere a *Configuración Cambio rápido SSID* sección del Cisco Guía de configuración de controlador del Wireless LAN, versión 7.0.116.0.

## P.. Puedo establecer un límite en el número de clientes que puedan conectar con una Tecnología inalámbrica ¿LAN?

A. Usted puede establecer un límite al número de clientes que puedan conectar con a red inalámbrica (WLAN), que es útil en los escenarios donde usted tiene un número limitado de clientes eso puede conectar con un regulador. El número de clientes que usted puede configurar por la red inalámbrica (WLAN) depende de la plataforma que usted está utilizando.

Lea la sección Configuración el número máximo de clientes por la red inalámbrica (WLAN) del Cisco Guía de configuración de controlador del Wireless LAN, versión 7.0.116.0 para información sobre los límites del cliente por la red inalámbrica (WLAN) para las diversas Plataformas de Reguladores del Wireless LAN.

## P.. Cuál es PKC y cómo él trabaja con el regulador del Wireless LAN ¿(WLC)?

A. Almacenamiento en memoria inmediata dominante dinámico de la significa PKC. Fue diseñado como extensión a la norma IEEE 802.11i.

PKC es una característica habilitada en los reguladores de las 2006/410x/440x Series de Cisco qué permisos equiparon correctamente a los clientes de red inalámbrica para vagar por fuera por completo reautentificación con un servidor de AAA. Para entender PKC, usted primero necesidad de entender el almacenamiento en memoria inmediata dominante.

El almacenamiento en memoria inmediata dominante es una característica que fue agregada al WPA2. Esto permite un móvil coloque para ocultar las claves principales (en parejas [PMK] de la clave principal) que gana con a la autenticación satisfactoria con un punto de acceso, y **lo reutiliza en a asociación futura con el mismo AP**. Esto significa que un móvil dado el dispositivo necesita autenticar una vez con un AP específico, y oculta la clave para Uso futuro. El almacenamiento en memoria inmediata dominante se maneja vía un mecanismo conocido como el identificador del PMK (PMKID), que es un hash del PMK, de una cadena, de la estación y del MAC direccionamientos del AP. El PMKID identifica únicamente el PMK.

Incluso con el almacenamiento en memoria inmediata dominante, una estación inalámbrica debe autenticar con cada uno AP que desea conseguir el servicio de. Esto introduce el tiempo de espera significativo y overheads, a que retrase el proceso de la mano-apagado y puede inhibir la capacidad soporte las aplicaciones en tiempo real. Para resolver este problema, PKC era introducido con el WPA2.

PKC permite que una estación reutilice un PMK que había ganado previamente con a proceso de autenticación satisfactoria. Esto elimina la necesidad de la estación a autentique contra los nuevos AP al vagar por.

Por lo tanto, en un intra-regulador que vaga por, cuando un dispositivo móvil se mueve a partir de un AP a otro en el mismo regulador, los re-cálculos del cliente un PMKID usando el PMK previamente usado y lo presenta durante el proceso de asociación. El WLC busca su caché del PMK para determinar si tiene tal entrada. Si él hace, desvía el proceso de autenticación e inmediatamente a los iniciados del 802.1x el intercambio de claves WPA2. Si no hace, pasa con el 802.1x estándar proceso de autenticación.

PKC se habilita por abandono con el WPA2. Por lo tanto, cuando usted habilita el WPA2 como La Seguridad de la capa 2 bajo configuración de la red inalámbrica (WLAN) del WLC, PKC se habilita en WLC. También, configure el servidor de AAA y al cliente de red inalámbrica para el EAP apropiado autenticación.

El supplicant usado en el lado del cliente debe también soportar el WPA2 adentro orden para que PKC trabaje. PKC se puede también implementar en un inter-regulador entorno de itinerancia.

**Nota:** PKC no trabaja con utilidad Aironet Desktop (ADU) como el cliente supplicant.

## P.. Cuáles son las explicaciones para estas configuraciones de tiempo de espera en el regulador: Descanso del Address Resolution Protocol (ARP), tiempo de inactividad del usuario, y sesión ¿Descanso?

A. **El tiempo de espera de ARP** se utiliza para borrar las entradas ARP en WLC para los dispositivos aprendidos de la red.

**El tiempo de inactividad del usuario:** Cuando un usuario está ocioso sin ningunos comunicación con el REVESTIMIENTO para la cantidad de tiempo fijada como tiempo de inactividad del usuario, el cliente deauthenticated por el WLC. El cliente tiene que reauthenticate y reasocie al WLC. Se utiliza en las situaciones donde un cliente puede salir de su REVESTIMIENTO asociado sin la notificación del REVESTIMIENTO. Esto puede ocurrir si la batería va absolutamente en el cliente o los socios del cliente separan.

**Nota:** Para acceder el ARP y el tiempo de inactividad del usuario en el WLC GUI, vaya a el menú del **regulador**. Elija al **general del** el lado izquierdo para encontrar el tiempo de inactividad ARP y del usuario coloca.

**El tiempo de espera de la sesión** es el tiempo máximo para un cliente sesión con el WLC. Después de este tiempo, el WLC de-autentica al cliente, y el cliente pasa con el proceso entero de la autenticación (reautentificación) otra vez. Esto es una parte de a la precaución de la Seguridad para girar las claves de encripción. Si usted utilice un método del Protocolo de Autenticación Extensible (EAP) con la administración de claves, la reintroducción ocurre en cada intervalo regular para derivar un nuevo cifrado clave. Sin la administración de claves, este valor de agotamiento del tiempo es el tiempo que Tecnología inalámbrica los clientes necesitan hacer un reauthentication completo. El tiempo de espera de la sesión es específico a la red inalámbrica (WLAN). Este parámetro se puede acceder del los **WLAN > Menú Edición**.

## P.. ¿Cuál es un sistema RFID? ¿Qué RFID marca con etiqueta es soportado actualmente por Cisco?

A. El Identificación de radiofrecuencia (RFID) es una tecnología que utiliza la radio comunicación de la frecuencia para una comunicación bastante de corto alcance. Un RFID básico el sistema se compone de las etiquetas RFID, de los lectores RFID, y del software de proceso.

Cisco soporta actualmente las etiquetas RFID de AeroScout y de Pango. Para más la información sobre cómo configurar las etiquetas de AeroScout, se refiere WLC Configuración para las etiquetas de AeroScout RFID.

## P.. ¿Puedo realizar la autenticación EAP localmente en el WLC? Hay ningunos ¿documente que explica esta característica local EAP?

A. Sí, la autenticación EAP se puede realizar localmente en el WLC. EAP local es un método de autentificación que permite que sean los usuarios y los clientes de red inalámbrica autenticado localmente en el WLC. Se diseña para el uso en las oficinas remotas eso quiera mantener la Conectividad a los clientes de red inalámbrica cuando el sistema backend se interrumpe, o el servidor de autenticación externa va abajo. Cuando usted habilite el EAP local, los servicios del WLC como el servidor de autenticación. Para más información sobre cómo la configuración un WLC para la autenticación EAP-rápida local, se refiere al Local Autenticación EAP en el regulador del Wireless LAN con el EAP-FAST y el servidor LDAP Ejemplo de configuración.

## P.. ¿Cuál es la característica de la invalidación de la red inalámbrica (WLAN)? ¿Cómo configuro esta característica? Lo vaya a hacer los revestimientos mantienen los valores de la invalidación de la red inalámbrica (WLAN) cuando fallan encima al respaldo ¿WLC?

A. La característica de la invalidación de la red inalámbrica (WLAN) nos permite para elegir los WLAN entre del WLAN configurados en un WLC que se puede utilizar activamente sobre una base individual del REVESTIMIENTO. Complete estos pasos para configurar una invalidación de la red inalámbrica (WLAN):

1. En el WLC GUI, haga clic la **Tecnología inalámbrica** menú.
2. Haga clic las **radios de la** opción en el lado izquierdo, y elija el **802.11 a/n** o el **802.11 b/g/n.**
3. Haga clic el link de la **configuración del** menú desplegable encontrado en el lado derecho que corresponde al nombre del AP en el cual usted quiera configurar la invalidación de la red inalámbrica (WLAN).
4. Elija el **permiso del** descenso-abajo de la invalidación de la red inalámbrica (WLAN) menú. El menú de anulación de WLAN es el elemento más reciente en el lado izquierdo de ventana.
5. La lista de todos los WLAN que se configuran en el WLC aparece.
6. De esta lista, marque los **WLAN a** los cuales usted quiere aparezca en el REVESTIMIENTO, y el tecleo **solicita los** cambios para tomar efecto.
7. Salve su configuración después de que usted haga éstos cambios.

Los AP conservan los valores de la invalidación de la red inalámbrica (WLAN) cuando consiguen registrados a el otro WLCs, a condición de que son los perfiles de la red inalámbrica (WLAN) y los SSID que usted quiere reemplazar configurado a través de todo el WLCs.

**Nota:** En la versión de software 5.2.157.0 del regulador, la característica de la invalidación de la red inalámbrica (WLAN) se ha quitado del regulador GUI y del CLI. Si es su regulador configurado para la invalidación y usted de la red inalámbrica (WLAN) actualice a la versión de software del regulador 5.2.157.0, el regulador borra la configuración de la red inalámbrica (WLAN) y transmite todos WLAN. Usted puede especificar que solamente ciertos WLAN estén transmitidos si usted configura grupos del Punto de acceso. Cada Punto de acceso hace publicidad solamente de los WLAN habilitados eso pertenezca a su grupo del Punto de acceso.

**Nota:** Los grupos del Punto de acceso no habilitan los WLAN que se transmitirán encendido por interfaz radio del AP.

## P.. Es el IPv6 soportado en los controladores LAN de la tecnología inalámbrica de Cisco (WLCs) y ¿Puntos de acceso ligeros (revestimientos)?

A. Actualmente, los reguladores de las 4400 y 4100 Series soportan solamente el IPv6

passthrough del cliente. El soporte nativo del IPv6 no se soporta.

Para habilitar el IPv6 en el WLC, marque el **IPv6 Habilite la** casilla de verificación en la configuración de la red inalámbrica (WLAN) SSID bajo la red inalámbrica (WLAN) > Edite la página.

También, requieren al modo de multidifusión de los Ethernetes (EMM) soportar el IPv6. Si usted inhabilite EMM, los dispositivos del cliente que utilizan el IPv6 pierden la Conectividad. Para habilitar EMM, van al regulador > página general y del Multicast de los Ethernetes El menú desplegable del modo, elige el **unicast** o **Multicast**. Esto habilita el Multicast o en el modo unidifusión o Modo de multidifusión. Cuando el Multicast se habilita como unicast del Multicast, los paquetes son replicado para cada AP. Éste puede ser hace un uso intensivo del procesador, así que utilícelo con precaución. El Multicast habilitado como Multicast del Multicast utiliza al usuario asignado dirección Multicast para hacer un Multicast más tradicional hacia fuera a los Puntos de acceso (APS).

**Nota:** El IPv6 no se soporta en los 2006 reguladores.

También, hay el Id. de bug Cisco CSCsg78176, que evita el usar del IPv6 passthrough cuando se utiliza la característica AAA Overrride.

## P.. Hace la red del soporte del regulador del Wireless LAN de las Cisco 2000 Series (WLC) ¿Autenticación para los Usuarios invitados?

A. La autenticación Web se soporta en todo el WLCs de Cisco. Autenticación Web es un método de autentificación de la capa 3 usado para autenticar a los usuarios con simple credenciales de autenticación. El no encryption está implicado. Complete estos pasos adentro orden para habilitar esta característica:

1. Del GUI, haga clic la **red inalámbrica (WLAN)** menú.
2. Haga clic una **red inalámbrica (WLAN)**.
3. Vaya a la **ficha de seguridad** y elija la **capa 3.**
4. Marque el cuadro de la **directiva de la red** y elija **Autenticación**.
5. Haga clic en **Aply** para guardar los cambios.
6. Para crear una base de datos en el WLC contra a las cuales autentique a los usuarios, vaya al **menú de seguridad** en el GUI, elija **El usuario de red local**, y completa estas acciones: Defina el nombre de usuario y contraseña del invitado para que el invitado utilice adentro orden a abrir una sesión. Estos valores son con diferenciación entre mayúsculas y minúsculas.Elija el ID DE WLAN que usted utiliza.**Nota:** Para una más configuración detallada, refiera a Tecnología inalámbrica Ejemplo de configuración de la autenticación Web del controlador LAN.

## P.. ¿Se puede el WLC manejar en el modo inalámbrico?

A. El WLC se puede manejar con el modo inalámbrico una vez que se habilita. Para más la información sobre cómo habilitar el modo inalámbrico refiere a *El habilitar Conexiones de red inalámbrica al GUI y al CLI* sección del Cisco Guía de configuración de controlador del Wireless LAN, versión 7.0.116.0.

## P.. ¿Cuál es agregación del link (RETRASO)? Cómo lo hago habilite el RETRASO

## en el Wireless LAN ¿Reguladores (WLCs)?

A. El RETRASO lía todos los puertos en el WLC en un solo EtherChannel interfaz. El sistema maneja dinámicamente el equilibrio y el puerto de la carga de tráfico Redundancia con el RETRASO.

Generalmente, la interfaz en el WLC tiene parámetros múltiples asociados a él, que incluye la dirección IP, gateway predeterminado (para la subred IP), primario puerto físico, puerto físico secundario, etiqueta del VLA N, y servidor DHCP. Cuando es el RETRASO no utilizada, cada interfaz se asocia generalmente a un puerto físico, pero al múltiplo las interfaces se pueden también asociar a un solo puerto del WLC. Cuando se utiliza el RETRASO, el sistema asocia dinámicamente las interfaces al Canal de puerto agregado. Esto ayudas en la redundancia del puerto y el Equilibrio de carga. Cuando un puerto falla, la interfaz se asocia dinámicamente al puerto físico disponible siguiente, y los revestimientos son equilibrado a través de los puertos.

Cuando el RETRASO se habilita en un WLC, del WLC los marcos de datos adelante en lo mismo puerto en el cual fueron recibidos. El WLC confía en el switch de vecino a tráfico del balance de la carga a través del EtherChannel. El WLC no realiza ningunos Balanceo de carga del EtherChannel en sus los propio.

## P.. Qué modela de la agregación del link de soporte de los reguladores del Wireless LAN (WLCs) ¿(RETRASO)?

A. RETRASO del soporte de los reguladores de las Cisco 5500 Series en el Software Release 6.0 o más adelante, RETRASO del soporte de los reguladores de las Cisco 4400 Series en el Software Release 3.2 o más adelante, y RETRASO se habilita automáticamente en los reguladores dentro de Cisco WiSM y el Catalyst 3750G integraron el Switch del regulador del Wireless LAN. Sin RETRASO, cada puerto del sistema de distribución en los soportes de un regulador de las Cisco 4400 Series hasta 48 Puntos de acceso. Con el RETRASO habilitado, un regulador de Cisco 4402 lógico el puerto soporta hasta 50 Puntos de acceso, el puerto lógico de un regulador de Cisco 4404 soportes hasta 100 Puntos de acceso, y el puerto lógico en el Catalyst 3750G Switch integrado del regulador del Wireless LAN y en cada regulador de Cisco WiSM soportes hasta 150 Puntos de acceso.

Cisco 2106 y el WLCs 2006 no soporta el RETRASO. Modelos anteriores, tales como el WLC de las Cisco 4000 Series, no soporte el RETRASO.

## P.. Cuál es la característica de la movilidad del auto-ancla en la Tecnología inalámbrica unificada ¿Redes?

A. la movilidad del Auto-ancla (o la movilidad de la red inalámbrica (WLAN) del invitado) se utiliza para mejorar la carga equilibrio y Seguridad para los clientes de itinerancia en su Tecnología inalámbrica LAN (WLAN). Bajo las condiciones de itinerancia normales, los dispositivos del cliente se unen a una red inalámbrica (WLAN) y se aseguran al primer regulador que entran en contacto. Si un cliente vaga por a una diversa subred, el regulador al cual el cliente vaga por configura una sesión no nativa para cliente con el regulador del ancla. Con el uso de la movilidad del auto-ancla característica, usted puede especificar un regulador o un conjunto de los reguladores como el ancla puntas para los clientes en una red inalámbrica (WLAN).

**Nota:** El ancla de la movilidad no se debe configurar para la movilidad de la capa 3. el ancla de la movilidad se utiliza solamente para el Tunelización del invitado.

## P.. Puede un regulador del Wireless LAN de Cisco 2006 (WLC) se configure como ancla ¿para una red inalámbrica (WLAN)?

A. Un WLC de las Cisco 2000 Series no se puede señalar como ancla para una red inalámbrica (WLAN). Sin embargo, una red inalámbrica (WLAN) creada en un WLC de las Cisco 2000 Series puede tener las Cisco 4100 Series WLC y WLC de las Cisco 4400 Series como su ancla.

## P.. ¿Qué tipo de Tunelización de la movilidad el regulador del Wireless LAN utiliza?

A. Software Release 4.1 del regulador a través 5.1 del soporte ambos asimétricos y Tunelización simétrico de la movilidad. Software Release 5.2 o Posterior del regulador soporte solamente el Tunelización simétrico de la movilidad, por el cual ahora es habilitado siempre valor por defecto.

En el Tunelización asimétrico, el tráfico del cliente a la red alámbrica se rutea directamente a través del regulador no nativo. Roturas asimétricas del Tunelización cuando el router ascendente hace la filtración del trayecto inverso (RPF) habilitar. En este caso, el tráfico del cliente se cae en el router porque revisión de "RPF" asegura eso la trayectoria de nuevo a la dirección de origen hace juego la trayectoria de la cual el paquete viene.

Cuando se habilita el Tunelización simétrico de la movilidad, todo el tráfico del cliente es enviado al regulador del ancla y puede entonces pasar con éxito revisión de "RPF". El Tunelización simétrico de la movilidad es también útil en estas situaciones:

- Si una instalación del Firewall en la trayectoria del paquete del cliente cae los paquetes porque la dirección IP de origen no hace juego la subred en la cual los paquetes se reciben, esto es útil.
- Si el VLA N del grupo de la acceso-punta en el regulador del ancla es diferente que el VLA N de la interfaz de la red inalámbrica (WLAN) en el regulador no nativo: en este caso, cliente el tráfico se puede enviar en un VLA N incorrecto durante la movilidad eventos.

## P.. Cómo lo haga accedemos el WLC cuando es la red ¿abajo?

A. Cuando la red está abajo, el WLC se puede acceder por el puerto del servicio. Este puerto se asigna una dirección IP en una subred totalmente diversa de otra los puertos del WLC y tan se llaman administración fuera de banda. Para más información, refiera *Configuración Puertos y interfaces* sección del Cisco Guía de configuración de controlador del Wireless LAN, versión 7.0.116.0.

## P.. Haga los controladores LAN de la tecnología inalámbrica de Cisco (WLCs) soportan la Conmutación por falla (o ¿característica de la Redundancia)?

A. Sí, si usted tiene dos o más WLCs en su red WLAN, usted puede configurelos para la Redundancia. Generalmente, un REVESTIMIENTO se une a al primario configurada WLC. Una vez que el WLC primario falla, el REVESTIMIENTO reinicia y se une a otro WLC en grupo de la movilidad. La Conmutación por falla es una característica en donde el REVESTIMIENTO sondea para el WLC primario y se une al WLC primario una vez que es funcional. Consulte la sección red inalámbrica (WLAN) Conmutación por falla del regulador para el ejemplo de configuración de los Puntos de acceso ligeros para más información.

## P.. Cuál es el uso del Listas de control de acceso (ACL) de la PRE-autenticación

## adentro ¿Reguladores del Wireless LAN (WLCs)?

A. Con la PRE-autenticación ACL, como el nombre implica, usted puede permitir al cliente el tráfico a y desde una dirección IP específica incluso antes del cliente autentica. Al usar a un servidor Web externo para la autenticación Web, algo del WLC las Plataformas necesitan una PRE-autenticación ACL para el servidor Web externo (Cisco Regulador de las 5500 Series, Cisco 2100 Series regulador, Cisco 2000 Series y el módulo de red del regulador). Para las otras Plataformas del WLC, la PRE-autenticación ACL no es obligatoria. Sin embargo, es una práctica adecuada a configure una PRE-autenticación ACL para el servidor Web externo al usar autenticación del Web externa.

## P.. Tengo una red inalámbrica (WLAN) MAC-filtrada y una red inalámbrica (WLAN) totalmente abierta en mi red. ¿El cliente elige la red inalámbrica (WLAN) abierta por abandono? O hace al cliente ¿asocíese automáticamente al ID DE WLAN que se fija en el filtro MAC? También, ¿por qué hay una opción de la “interfaz” en un filtro MAC?

A. El cliente puede asociarse a cualquier red inalámbrica (WLAN) a la cual configuren al cliente para conectar. La Opción de interfaz en el filtro MAC da la capacidad de aplicarse el filtro a una red inalámbrica (WLAN) o a una interfaz. Si es múltiple los WLAN se atan al lo mismo interconectan, usted pueden aplicar el filtro MAC a la interfaz sin la necesidad para crear un filtro para cada red inalámbrica (WLAN) individual.

## P.. Cómo puedo configure la autenticación de TACACS para los usuarios de administración en ¿Regulador del Wireless LAN (WLC)?

A. A partir de la versión 4.1 del WLC, el TACACS se soporta en el WLCs. Refiérase a Configuración TACACS+ para entender cómo configurar el TACACS+ para autenticar usuarios de administración del WLC.

## P.. Cuál es el uso de la configuración excesiva de la falla de autenticación en a ¿Regulador del Wireless LAN (WLC)?

A. Esta configuración es una de las directivas de la exclusión del cliente. El cliente la exclusión es una función de seguridad en el regulador. La directiva se utiliza a ponga a los clientes para prevenir el acceso ilegal a la red o a los ataques a la red inalámbrica.

Con esta directiva excesiva del error de la autenticación Web habilitada, cuando a el número de cliente de tentativas falladas de la autenticación Web excede de 5, el regulador considera que el cliente ha excedido las tentativas máximas de la red la autenticación y pone al cliente.

Complete estos pasos para habilitar o inhabilitar esto determinación:

1. Del WLC GUI, va a la **Seguridad > la protección inalámbrica Directivas > directivas de la exclusión del cliente**.
2. Marque o desmarque la **autenticación Web excesiva Errores**.

## P.. He convertido mi punto de acceso autónomo al modo ligero. En el modo ligero del protocolo AP (LWAPP) con RADIUS AAA el servidor para el cliente

## considerando, siguen normalmente al cliente con las estadísticas RADIUS basadas en Dirección IP del WLC. Es posible fijar las estadísticas RADIUS basadas en Dirección MAC del AP asociado a ese WLC y no a la dirección IP del ¿WLC?

A. Sí, esto se puede hacer con la configuración del lado del WLC. Complete éstos pasos:

1. Del regulador GUI, bajo la **Seguridad > radio El considerar**, hay una casilla desplegable para el tipo del ID de la estación de la llamada. Elija **Dirección MAC AP**.
2. Verifique esto a través del registro del LWAPP AP. Allí, usted puede ver estación que recibe la llamada el campo ID que visualiza Dirección MAC del AP al cual el cliente particular es asociado.

## P.. Cómo usted cambia el descanso del apretón de manos del Acceso protegido de Wi-Fi (WPA) ¿valore en un regulador del Wireless LAN (WLC) con el CLI? Sé que puedo hacer esto encendido (APS) de los Puntos de acceso de Cisco IOS® con el apretón de manos del wpa del dot11 valor de agotamiento del tiempo comando, pero cómo hágale ¿realice esto en un WLC?

A. La capacidad de configurar el descanso del WPA-apretón de manos con el WLCs era integrado en el Software Release 4.2 y Posterior. Usted no necesita esta opción adentro versiones anteriores del software WLC.

Estos comandos se pueden utilizar para cambiar el descanso del apretón de manos WPA:

**config advanced eap eapol-key-timeout** <value> **config advanced eap eapol-key-retries** <value>

Los valores predeterminados continúan reflejando la corriente del WLCs comportamiento.

```
   - the default value for eapol-key-timeout is 1 second.
   - the default value for eapol-key-retries is 2 retries
```

**Nota:** En IOS AP, esta configuración es configurable con el **dot11** comando del **apretón de manos del wpa**.

Usted puede también configurar los otros parámetros EAP con las opciones debajo el comando **avanzado del eap de los config**.

```
(Cisco Controller) >config advanced eap ?

eapol-key-timeout
   Configures EAPOL-Key Timeout in seconds.
eapol-key-retries
   Configures EAPOL-Key Max Retries.
identity-request-timeout
   Configures EAP-Identity-Request Timeout in seconds.
identity-request-retries
   Configures EAP-Identity-Request Max Retries.
key-index
   Configure the key index used for
   dynamic WEP(802.1x) unicast key (PTK).
max-login-ignore-identity-response
   Configure to ignore the same username count
   reaching max in the EAP identity response
request-timeout
   Configures EAP-Request Timeout in seconds.
request-retries
```

```
Configures EAP-Request Max Retries.
```

### P.. Cuál es el propósito de la característica de diagnóstico del canal en la red inalámbrica (WLAN) > ¿Edite > avanzó la página?

A. La característica de diagnóstico del canal le permite para resolver problemas los problemas adentro respeto a la Comunicación del cliente con una red inalámbrica (WLAN). El cliente y los Puntos de acceso pueden ser despache un conjunto definido de las pruebas para identificar la causa de la comunicación las dificultades a las cuales las experiencias del cliente y entonces permiten las medidas correctivas tómese para hacer al cliente operativo en la red. Usted puede utilizar el regulador GUI o CLI para habilitar el canal de diagnóstico, y le puede utilizar regulador CLI o WCS para funcionar con las pruebas de diagnóstico.

El canal de diagnóstico se puede utilizar para probar solamente. Si usted intenta a configure la autenticación o el cifrado para la red inalámbrica (WLAN) con el canal de diagnóstico habilitado, usted ve este error:

### P.. ¿Cuál es el número máximo de grupos AP que puedan ser configurados en un WLC?

A. Esta lista muestra al número máximo de grupos AP que usted puede configurar en un WLC:

- Un máximo de los grupos de 50 Puntos de acceso para las Cisco 2100 Series Regulador y módulos de red del regulador
- Un máximo de los grupos de 300 Puntos de acceso para las Cisco 4400 Series Regulador del Wireless LAN de los reguladores, de Cisco WiSM, y de Cisco 3750G Switch
- Un máximo de los grupos de 500 Puntos de acceso para las Cisco 5500 Series Reguladores

## Información Relacionada

- Tecnología inalámbrica Controlador LAN (WLC) FAQ
- Tecnología inalámbrica Mensajes de error y de sistema FAQ del controlador LAN (WLC)
- Ligero Punto de acceso FAQ
- Cisco Guía de configuración de controlador del Wireless LAN, versión 7.0.116.0
- Soporte del IPv6 en el regulador del Wireless LAN
- Tecnología inalámbrica Soporte de Producto
- Soporte Técnico y Documentación - Cisco Systems



## Discusiones relacionadas de la comunidad del soporte de Cisco

La comunidad del soporte de Cisco es un foro para que usted haga y conteste a las preguntas, las sugerencias de la parte, y colabore con sus pares.

Refiera a los convenios de los consejos técnicos de Cisco para la información sobre los convenios usados en este documento.

Actualizado: De marcha el 02 de 2015
ID del Documento: 118833