

Regulador del Wireless LAN (WLC) FAQ

Contenido

[Introducción](#)

[Preguntas Frecuentes Generales](#)

[Preguntas Frecuentes sobre Troubleshooting](#)

[Información Relacionada](#)

Introducción

Este documento proporciona la información sobre lo más frecuentemente las preguntas hechas (FAQ) sobre el controlador LAN de la tecnología inalámbrica de Cisco (WLC).

Consulte [Convenciones de Consejos Técnicos Cisco](#) para obtener más información sobre las convenciones del documento.

Preguntas Frecuentes Generales

Q. ¿Cuál es regulador del Wireless LAN (WLC)?

A. Las redes inalámbricas se han convertido en una necesidad en la actualidad. Muchos entornos corporativos requieren el uso de redes inalámbricas a gran escala. Cisco ha propuesto el concepto de Red Inalámbrica Unificada de Cisco (CUWN), lo que facilita el manejo de tales implementaciones a gran escala. El WLC es un dispositivo que asume una función central en el CUWN. Las funciones tradicionales de los puntos de acceso, tales como asociación o autenticación de los clientes de red inalámbrica, son realizadas por el WLC. Los puntos de acceso, llamados Lightweight Access Point (LAPs) en el entorno unificado, se registran con un WLC y hacen un túnel de los paquetes de datos y administración a WLCs, que luego conmutan los paquetes entre los clientes de red inalámbricos y la porción cableada de la red. Todas las configuraciones se hacen en el WLC. Los LAP descargan la configuración completa de los WLC y actúan como la interfaz inalámbrica a los clientes. Para obtener más información sobre cómo un LAP se registra con un WLC, consulte el documento [Lightweight AP \(LAP\) Registration a un Wireless LAN Controller](#).

Q. ¿Qué es CAPWAP?

A. En el controller software release 5.2 o posterior, los puntos de acceso de Cisco lightweight utilizan el Control de IETF estándar y el Aprovisionamiento del protocolo Wireless Access Points (CAPWAP) para establecer la comunicación entre el controlador y otros Lightweight Access Point en la red. Controller software releases anteriores a 5.2, use el Lightweight Access Point Protocol (LWAPP) para estas comunicaciones.

CAPWAP, que se basa en el LWAPP, es un protocolo estándar, interoperable que habilita un controlador para manejar un grupo de puntos de acceso inalámbrico. CAPWAP se está

implementando en la versión de software 5.2 del controlador por estas razones:

- Para proporcionar una trayectoria de actualización de los productos de Cisco que utilizan LWAPP a los productos de Cisco de la siguiente generación que utilizan CAPWAP
- Para manejar los lectores RFID y los dispositivos similares
- Para habilitar los controladores e interoperar con los puntos de acceso de terceros en el futuro

Los puntos de acceso habilitados por LWAPP pueden descubrir y unirse a un controlador CAPWAP, y la conversión a un controlador CAPWAP es homogénea. Por ejemplo, el proceso de detección del controlador y el proceso de descarga de firmware cuando utiliza CAPWAP son iguales que cuando utiliza el LWAPP. La única excepción está para las implementaciones de la capa 2, que no son soportadas por CAPWAP.

Puede implementar los controladores CAPWAP y los controladores LWAPP en la misma red. El software habilitado por CAPWAP permite que los puntos de acceso se unan a cualquier controlador que ejecute CAPWAP o LWAPP. La única excepción es el Cisco Aironet 1140 Series Access Point, que soporta solamente CAPWAP y, por lo tanto, se une a solamente los controladores que ejecutan CAPWAP. Por ejemplo, un punto de acceso de las series 1130 Series puede unirse a un controlador que ejecute CAPWAP o LWAPP mientras que un punto de acceso de las series 1140 Series puede unirse solamente a un controlador que ejecute CAPWAP.

Para más información, consulte la sección [Access Point Communication Protocols](#) de la guía de configuración.

Q. ¿Hay guías de consulta para usar CAPWAP?

A. Siga estas guías de consulta cuando utiliza CAPWAP:

- Si su firewall se configura actualmente para permitir el tráfico solamente de los puntos de acceso que utilizan el LWAPP, debe cambiar las reglas de firewall para permitir el tráfico de los puntos de acceso que utilizan CAPWAP.
- Asegúrese de que los puertos 5246 y 5247 CAPWAP UDP (similares a los puertos 12222 y 12223 del LWAPP UDP) estén habilitados y no bloqueados por un dispositivo intermedio que podría evitar que un punto de acceso se una a el controlador.
- Si las listas de control de acceso (ACL) están en la trayectoria de control entre el controlador y sus puntos de acceso, debe abrir los nuevos puertos del protocolo para evitar que los puntos de acceso sean trenzados.

Los puntos de acceso utilizan un puerto de origen al azar UDP para alcanzar estos puertos destino en el controlador. En la versión de software 5.2 del controlador, el LWAPP fue quitado y substituido por CAPWAP, pero si tiene un nuevo punto de acceso que nunca se unió a un controlador, podría intentar utilizar el LWAPP para se conecte con el controlador antes de que descargue la imagen CAPWAP del controlador. Una vez que el punto de acceso descarga la imagen CAPWAP del controlador, utiliza solamente CAPWAP para comunicarse con el controlador.

Note: Después de 60 segundos de intentar unirse a un controlador con CAPWAP, el punto de acceso recurre al LWAPP. Si no puede encontrar un controlador que usa el LWAPP en el plazo de 60 segundos, intente otra vez unirse a un controlador que use CAPWAP. El punto de acceso repite este ciclo de switching de CAPWAP al LWAPP y nuevamente cada 60 segundos hasta que se une a un controlador.

Un punto de acceso con la imagen de recuperación del LWAPP (un punto de acceso convertido de modo autónomo o un punto de acceso nuevo) utiliza solamente el LWAPP para intentar unirse a un controlador antes de que descargue la imagen CAPWAP del controlador.

Q. ¿Cómo configuro mi WLC para la operación básica?

A. Para configurar el WLC para la operación básica, refiera al [ejemplo de la configuración básica del regulador del Wireless LAN y del Lightweight Access Point](#).

Q. ¿Cuáles son las opciones disponibles para acceder a WLC?

A. Ésta es la lista de opciones disponibles para acceder a WLC:

- Acceso a GUI con HTTP o HTTPS
- Acceso CLI con Telnet, el SSH, o acceso a la consola
- Acceso a través del puerto de servicio

Para obtener más información sobre cómo habilitar estos modos, consulte la sección [Cómo Utilizar el Buscador de Red e Interfaces de CLI](#) del documento [Guía de Configuración del Cisco Wireless LAN Controller, Release 5.1](#). Generalmente, la dirección IP de la interfaz de administración se utiliza para el acceso GUI y CLI. Los clientes de red inalámbrica pueden acceder a WLC solamente cuando está verificada la opción **Habilitar Administración del Controlador** para que se pueda acceder desde **Clientes de Red Inalámbrica**. Para habilitar esta opción, haga clic el menú **Administración** de WLC, y haga clic en **Admin. a través de la Red Inalámbrica** en el lado izquierdo. También se puede acceder a WLC con una de sus direcciones IP de la interfaz dinámica. Use el comando **config network mgmt-via-dynamic-interface** para habilitar esta función. Los equipos con cable sólo pueden tener acceso CLI con la interfaz dinámica de WLC. Los clientes de red inalámbrica tienen acceso CLI y GUI con la interfaz dinámica.

Q. ¿Cómo utilizo el puerto de la consola USB en el regulador del Wireless LAN de las Cisco 5500 Series?

A. El puerto de la consola USB en los reguladores de las 5500 Series conecta directamente con el conector USB de un PC usando cable USB de un tipo A a 5-pin mini B del tipo.

Note: 4-pin el mini conector del tipo B se confunde fácilmente con 5-pin el mini conector del tipo B. No son compatibles. Solamente 5-pin el mini conector del tipo B puede ser utilizado.

Para la operación con Microsoft Windows, el driver de la consola de Cisco Windows USB se debe instalar en cualquier PC conectado con el puerto de la consola. Con este driver, usted puede conectar y desenchufar el cable USB en y del puerto de la consola sin afectar a las operaciones del HyperTerminal de Windows. Solamente un puerto de la consola puede ser en un momento activo. Cuando un cable está conectado en el puerto de la consola USB, el puerto RJ-45 llega a estar inactivo. Inversamente, cuando el cable USB se quita del puerto USB, el puerto RJ-45 llega a ser activo

Para la información detallada, refiérase [usando el puerto de la consola del regulador USB de las Cisco 5500 Series](#).

Q. ¿Cómo accedo al Asistente de la Configuración del GUI en un regulador 4400?

A. Para configurar las configuraciones básicas en un regulador 4400 que usa al Asistente de la Configuración del GUI, usted debe conectar con el puerto del servicio del regulador. Después, configure su PC para utilizar la misma subred como el puerto del servicio del regulador; la dirección IP en el puerto del servicio cuando configurar el WLC es por primera vez 192.168.1.1. Comience al Internet Explorer 6.0 SP1 (o más adelante) o Firefox 2.0.0.11 (o más adelante) en su PC, y hojee a <http://192.168.1.1>. El Asistente de la Configuración del GUI aparece.

Para información detallada sobre este tema, refiera a la [guía de configuración del controlador LAN de la tecnología inalámbrica de Cisco, la versión 6.0](#).

Q. ¿Cómo accedo el WLC de un lugar remoto?

A. Usted puede utilizar Telnet y SSH para acceder el WLC de un lugar remoto. Telnet es un protocolo usado para el Acceso Remoto; SSH es también un protocolo usado para el Acceso Remoto, pero incluye la Seguridad agregada. Para más información, refiera a [SSH y a la sección de las sesiones telnets que configuran de la guía de configuración del controlador LAN de la tecnología inalámbrica de Cisco, la versión 6.0](#).

Q. ¿Puedo configurar una conexión del RETRASO esa los palmos a través de los switches múltiples?

A. Yes. RETRÁSESE con el VSS, o un interruptor de apilado (3750/2960) puso, trabajará mientras los fragmentos de un paquete del IP se envíen al mismo puerto. La idea es que si usted va a los switches múltiples, los puertos deben pertenecer al mismo L2 "entidad" en lo que respecta a las decisiones del Equilibrio de carga.

Q. ¿Cómo conmuta paquetes un WLC?

A. Todos los paquetes (802.11) del cliente son encapsulados en un paquete LWAPP por el LAP y enviados al WLC. WLC decapsula el paquete LWAPP y los actos basados en la dirección IP de destino en el paquete 802.11. Si el destino es uno de los clientes de red inalámbrica asociados al WLC, encapsula el paquete otra vez con el LWAPP y lo envía al LAP del cliente, donde se decapsula y es enviado al cliente de red inalámbrica. Si el destino está en el lado cableado de la red, quite el encabezado 802.11, agregue el encabezado Ethernet, y envíe el paquete al switch conectado, desde el cual se envía al cliente cableado. Cuando un paquete viene del lado cableado, el WLC quita el encabezado Ethernet, agrega el encabezado 802.11, los encapsula con el LWAPP, y los envía al LAP, donde es decapsulado, y el paquete 802.11 se entrega al cliente de red inalámbrica. Para obtener más información sobre esto, consulte la sección [Aspectos básicos de LWAPP del documento Deploying Cisco 440X Series Cisco 440X Series Wireless LAN Controllers](#).

Q. ¿Cuándo debo utilizar el modo del regulador principal en un WLC?

A. Cuando hay regulador principal habilitado, todos los Puntos de acceso nuevamente agregados sin primario, secundario, o los controladores terciarios asignados se asocian al regulador principal en la misma subred. Esto permite que el operador verifique la Configuración de punto de acceso y asigne primario, secundario, y los controladores terciarios al Punto de acceso usando el **todo el** página **AP > de los detalles**.

El regulador principal se utiliza normalmente solamente al agregar los nuevos Puntos de acceso a la solución de LAN de la tecnología inalámbrica de Cisco. Cuando no más de Puntos de acceso

se están agregando a la red, la solución de Cisco WLAN recomienda que usted inhabilita el regulador principal.

Q. ¿El 4400 rutea paquetes de WLC entre las VLAN?

A. Los 4400 WLC son una aplicación que se conecta a su red pero no funciona como un router. Debe haber un dispositivo de capa 3 en los paquetes ruteados entre las VLAN. El WLC asocia el SSID de los clientes a la subred VLAN y los coloca nuevamente fuera de la interfaz de administración para los routers ascendentes para rutear paquetes.

Q. ¿Cómo configuro el WLAN en un WLC?

A. WLAN es similar a SSID en los puntos de acceso. Se requiere para que a un cliente se asocie a su red inalámbrica. Para configurar un WLAN en un WLC, consulte el ejemplo de configuración del [documento WLAN Invitado y WLAN Interno usando el Ejemplo de Configuración de los WLC](#).

Q. ¿Cómo funciona DHCP con el WLC?

A. El WLC se diseña para actuar como agente de retransmisión DHCP al servidor DHCP externo y actúa como un servidor DHCP al cliente. Ésta es la Secuencia de eventos que ocurre:

1. Generalmente, el WLAN se une a una interfaz que se configura con un servidor DHCP.
2. Cuando el WLC recibe una solicitud de DHCP del cliente en un WLAN, retransmite la solicitud al servidor DHCP con su dirección IP de administración.
3. El WLC muestra su dirección IP virtual, que debe ser una dirección no enrutable, configurado generalmente como 1.1.1.1, como el servidor DHCP al cliente.
4. El WLC remite la respuesta DHCP del servidor DHCP al cliente de red inalámbrica con su dirección IP virtual. **Note:** También puede configurar el WLC para actuar como servidor DHCP. Para más información sobre cómo configurar un WLC como servidor DHCP, consulte la sección [Configuración de Escapes DHCP](#) del documento [Guía de Configuración de Cisco Wireless](#)

Q. ¿Cómo cambio la potencia y los canales para un LAP?

A. Una vez que el LAP se registra a un WLC, toda la configuración para un LAP se hace en el WLC. Hay una característica incorporada en el WLC llamado RRM, en donde el WLC funciona en el interior con un algoritmo y se ajusta automáticamente el canal y las configuraciones de potencia según la implementación de los LAP. RRM se enciende de forma predeterminada en el WLC. No necesita cambiar el canal y las configuraciones de potencia para un LAP, sino que puede reemplazar la función RRM y asignar estáticamente las configuraciones de potencia y del canal para un LAP. Para más información sobre cómo configurar manualmente las configuraciones de potencia y del canal, consulte [Asignación Estadística del Canal y Configuraciones de Transmisión de Potencia](#) para Radios de Punto de acceso del documento [Guía de Configuración de Controlador de LAN de la Red Inalámbrica Cisco, Versión 5.1](#).

Q. Tengo varios WLC en mi red. ¿Hay un dispositivo o software disponible para administrar varios WLC en mi red?

A. Sí, el Sistema de Control Inalámbrico (WCS) es un software del servidor que puede administrar

varios WLC en la red. Administra el WLC, sus puntos de acceso asociados, y los clientes. Para más información sobre el WCS, consulte [Guía de Configuración de Cisco Wireless Control System, Release 5.0](#).

Q. ¿Cómo edito el archivo de configuración del WLC?

A. Cuando usted salva la configuración del WLC, el regulador la salva en el formato XML en memoria flash. Para permitirle para leer y para modificar fácilmente el archivo de configuración, el software del regulador (versión 5.2 o más adelante) lo convierte a un formato CLI.

Cuando usted carga el archivo de configuración a un TFTP o a un servidor FTP, el regulador inicia la conversión del XML al CLI. Usted puede después leer o editar el archivo de configuración en el formato CLI en el servidor. Cuando le acaban, usted descarga el archivo de nuevo al regulador, donde se convierte a un formato XML y se guarda.

Para las instrucciones paso a paso en cómo editar el archivo de configuración, refiera a la sección de [archivos de configuración que edita de la guía de configuración 6.0 del WLC](#).

Q. ¿Puedo transferir las configuraciones de un WLC directamente a otros WLC?

A. No. No puede transferir las configuraciones de un WLC directamente a otros WLC. Para transferir el archivo a otros WLC, debe cargar el archivo de configuración de un WLC al servidor TFTP, y después descargar el archivo del servidor TFTP al WLC deseado.

Para cargar y descargar un archivo de WLC al servidor TFTP, consulte la sección [Administración del Controller Software y Configuraciones](#) de la [Guía de Configuración Cisco Wireless LAN Controller, Release 5.0](#).

Note: Antes de transferir el archivo de WLC al servidor TFTP, asegúrese de que ambos WLC funcionen con la misma versión de software.

Q. ¿Cómo encuentro la versión del código que se ejecuta en el WLC?

A. Del regulador GUI del Wireless LAN, **monitor > resumen del teclado**. En la página de resumen, el campo de la **versión de software** muestra la versión de firmware que se ejecuta en el regulador del Wireless LAN.

Para encontrar la versión de firmware que se ejecuta en el WLC con el WLC CLI, use el comando **show run-config**.

```
(Cisco Controller) >show run-config
```

```
Press Enter to continue...
```

```
System Inventory
```

```
Burned-in MAC Address..... 00:0B:85:33:52:80
```

```
Press Enter to continue Or <Ctl Z> to abort
```

```
System Information
```

```
Manufacturer's Name..... Cisco Systems Inc.
```

```
Product Name..... Cisco Controller
```

```
Product Version..... 4.0.217.0
```



```
RTOS Version..... 4.0.217.0
Bootloader Version..... 4.0.217.0
Build Type..... DATA + WPS
Compact Flash Size..... 256 MB
```

Para ver la imagen de boot activo, use el comando **show boot**

```
(Cisco Controller) >show boot
Primary Boot Image..... 4.0.217.0 (active)
Backup Boot Image..... 4.0.155.5
```

**Q. ¿Qué sucede a la red inalámbrica cuando realizo una actualización de software?
¿Todos los puntos de acceso (AP) registrados en WLC caen hasta que son actualizados, o son actualizados uno por vez por lo que la red inalámbrica puede permanecer activa (excepto por los AP específicos que son actualizados)?**

A. Una vez que se actualiza el WLC, debe ser reiniciados para que los cambios surtan efecto. Dentro de este tiempo, la conectividad al WLC se pierde. Los LAP registrados en un WLC pierden su asociación al WLC, por lo que el servicio a los clientes de red inalámbrica se interrumpe. Cuando actualiza el software del controlador, el software en los puntos de acceso asociados del controlador se actualiza también automáticamente.

Cuando un punto de acceso carga el software, cada uno de sus LED parpadea en la sucesión. Hasta 10 puntos de acceso se pueden actualizar de forma simultánea en el controlador. No desactive el controlador ni cualquier punto de acceso durante este proceso; si no, puede dañar la imagen del software. Actualizar un controlador con una gran cantidad de puntos de acceso puede tardar 30 minutos, según el tamaño de su red. Sin embargo, con la cantidad mayor de actualizaciones de punto de acceso simultáneas soportadas en el software release 4.0.206.0 y posterior, el tiempo de la actualización debe ser reducido perceptiblemente. Los puntos de acceso deben seguir accionados, y el controlador no se debe reajustar durante este tiempo.

Q. ¿Cuáles son las guías de consulta que deben seguirse antes de realizar una actualización del controlador Wireless LAN?

A. Cisco recomienda que la actualización esté realizada sobre el LAN u otro link de alta velocidad y latencia baja. Una conexión de red muy lenta pudo hacer que el TFTP entre en período de espera, y la actualización no será satisfactoria.

Cisco recomienda que el controlador se actualice solamente de un demonio del tftp en el mismo segmento que el controlador del Wireless LAN cuando utilizas el TFTP como el modo de transferencia.

Cuando intenta actualizar el controlador que usa un cliente de red inalámbrica asociado como el TFTP o el servidor FTP, la actualización falla. El controlador inalámbrico LAN no permite una (T) transferencia FTP de un demonio que esté situado en un cliente asociado a un AP unido al WLC. (Consulte [CSCsi73129](#) para más información.)

Además, sigue las guías de consulta documentadas en la sección [Guías de consulta para actualizar el software del controlador de la](#) guía de configuración.

Q. ¿Qué funciones del controlador requieren una reinicialización?

A. Después de que usted realice estas funciones en el regulador, usted debe reiniciar el regulador

para que los cambios tomen el efecto:

- Agregación del link del permiso o de la neutralización (RETRASO)
- Habilite una característica que sea dependiente en los Certificados (tales como https y autenticación Web)
- Agregue nuevo o modifique a los usuarios existentes del v3 SNMP
- Instale una licencia, cambie al conjunto de características de la licencia, o cambie la prioridad de una licencia de evaluación de la AP-cuenta en un regulador

Q. ¿Puede un punto de acceso (AP) basado en el software Cisco IOS que se ha convertido al modo ligero registrarse con Cisco 4100 Series WLC?

A. No, el AP basado en el Software de Cisco IOS que se convierte al modo ligero no puede registrarse con Cisco 40xx, 41xx, o 3500 WLC. Estos AP ligeros (LAP) pueden registrarse solamente con Cisco 4400 y el WLC de las Series 2000. Para la información sobre las restricciones de los AP que se convierten al modo ligero, consulte la sección de [Restricciones de Actualizar los puntos de acceso autónomos de Cisco Aironet al modo ligero](#).

Q. ¿Cuál es el número máximo de AP soportados en los 4402 y 4404 reguladores del Wireless LAN (WLCs)?

A. La limitación en el número de puntos de acceso soportados se basa en el hardware que posee. Los 4402 WLC con dos puertos Gigabit Ethernet vienen en configuraciones que soporten 12, 25, y 50 Puntos de acceso ligeros (revestimientos). Los 4404 WLC con cuatro soportes de los puertos Gigabit Ethernet 100 revestimientos.

Note: Los Puntos de acceso de la malla están también disponibles en las implementaciones interiores y al aire libre. Para más información sobre los números de punto de acceso (malla including AP) soportados en cada modelo del regulador, refiera a los *Puntos de acceso de la malla del cuadro 8-3 soportados por el modelo del regulador* en la sección del [Punto de acceso de la malla que controla de la guía de configuración de controlador del Wireless LAN 6.0](#).

Q. Realicé un downgrade de la imagen de 7.0.98.0 a 6.0.200.22 en mi 5508 WLC. Sin embargo, después de que el downgrade, el número máximo de AP soportados en el WLC cambiara a partir del 500 a 250 AP. ¿por qué?

A. Esto es una conducta esperada. Con la versión 6.0 del WLC, los 5508 soportes del regulador solamente hasta 250 Puntos de acceso ligeros. Con la versión 7.0.98.0, un regulador inalámbrico de las solas Cisco 5500 Series puede soportar hasta 500 Cisco Aironet AP.

Q. ¿Cómo se produce el roaming en un entorno WLC?

A. Roaming es un proceso en el que el cliente puede retener sesiones de aplicación ininterrumpidas en su traslado. Cuando un cliente de red inalámbrica se asocia y autentica a un WLC, pone una entrada para ese cliente en su base de datos del cliente. Esta entrada incluye el MAC y las direcciones IP del cliente, los contextos de seguridad y las asociaciones, los contextos de calidad de servicio, el WLAN, y el LAP asociado. Cuando un cliente se traslada a otro LAP asociado al mismo WLC, simplemente actualiza la base de datos del cliente con la nueva información LAP por lo que los datos pueden enviarse de forma adecuada al cliente. Cuando un cliente se traslada por a un LAP asociado a un diverso WLC, en las mismas subredes o en

diferentes subredes, envía la información en la base de datos del cliente al nuevo WLC. Esto ayuda al cliente a conservar su dirección IP a través de los traslados y mantiene a las sesiones TCP ininterrumpidas. Para más información sobre roaming en el entorno del WLC, consulte la sección [Configuración de Grupos de Movilidad de la Guía de Configuración del Cisco Wireless LAN Controller, Release 5.1](#).

Q. ¿Cómo el WLC administra a los usuarios invitados?

A. Los usuarios invitados son usuarios de la red de terceros, que necesitan el acceso limitado a los recursos de red y conectividad a Internet. El WLC proporciona el acceso inalámbrico y cableado del invitado usando la infraestructura de red inalámbrica existente. Un SSID separado se proporciona generalmente para los Usuarios invitados inalámbricos. A los usuarios invitados en las redes inalámbricas y cableadas se les asigna VLAN diferentes, que proporciona aislamiento del tráfico del invitado del resto del tráfico de datos. Esto proporciona un mejor control sobre el tráfico del invitado y mayor seguridad de la red. Los Usuarios invitados generalmente se autentican con la [autenticación Web](#). Para más información sobre el acceso del invitado, consulte el documento [Preguntas Frecuentes de Invitado Inalámbrico](#).

Para obtener los registros de usuario invitado, habilite Contabilidad de Radius para los usuarios, y use este comando: **debug aaa all enable**

Q. ¿Cómo configuro una base de datos local en el regulador del Wireless LAN (WLC)? ¿Cuáles son los caracteres especiales que se pueden utilizar para el nombre de usuario y contraseña del usuario de red local?

A. Las bases de datos de usuarios locales almacenan las credenciales (nombre de usuario y contraseña) de todos los usuarios de la red local. Estas credenciales se utilizan para autenticar a los usuarios. Puede configurar los usuarios locales de la red local con la GUI o el CLI. Puede ingresar hasta 24 caracteres alfanuméricos. Todos los caracteres especiales pueden ser utilizados cuando configura el nombre de usuario y contraseña a través de CLI, pero el carácter comillas simples no puede ser utilizado cuando configura el nombre de usuario y contraseña con la GUI.

Desde la CLI, use estos comandos para crear un usuario de red local:

- **config netuser add <nombre de usuario> <contraseña> wlan <id de wlan> userType permanent description <descripción>** — Agrega un usuario permanente a la base de datos de usuario local en la WLC.
- **config netuser add <username> <password> {wlan | guestlan} {wlan_id | guest_lan_id} userType guest lifetime seconds description <descripción>** — Agrega un usuario invitado en una WLAN o LAN de invitado cableado a la base de datos de usuario local en WLC.

Del GUI, puede configurar a los usuarios de red locales desde la página **Security >AAA > Usuarios de Red Locales**.

Q. ¿Es posible borrar automáticamente al usuario de red local en el WLC?

A. Los usuarios de la Red Local no se borran automáticamente. Tienes que borrarlos manualmente. Para borrar al usuario, diríjase a la página **Security >AAA >** de los **usuarios de red locales**. Para quitar a un usuario, colocar el mouse sobre el icono y el tecleo **quita**. Si configuran a un usuario de red local como Usuario invitado, debe especificar el tiempo de la vida, después de

lo cual borran al usuario automáticamente. El rango configurable es entre 60 segundos y 2592000 segundos.

Q. ¿Qué es un Grupo de Movilidad?

A. El grupo de movilidad es un grupo de WLCs configurado con el mismo nombre del grupo de movilidad. El cliente puede trasladarse sin dificultades por los WLC en el mismo grupo de movilidad. El WLCs en un grupo de la movilidad provee la redundancia entre ellos mismos. Para más información sobre grupos de movilidad, consulte [grupos FAQ de la movilidad del controlador del Wireless LAN del documento \(WLC\)](#).

Q. ¿Cuánto WLCs puedo tener en el mismo grupo de la movilidad?

A. Usted puede colocar hasta 24 WLCs regulares (Cisco 2000, 4100, y las 4400 Series) en un solo grupo de la movilidad. Usted puede configurar hasta 12 cuchillas del módulo de servicios de red inalámbrica (WiSM) en un grupo de la movilidad. Por lo tanto, hasta un máximo de 3600 (APS) de los puntos de acceso se soportan en un solo grupo de la movilidad.

Note: Con la versión 5.1 del WLC, puede haber hasta 72 WLCs en un dominio de la movilidad.

Q. ¿El WLC de las Cisco 4400 Series soporta el protocolo del Intercambio de paquetes entre redes (IPX)? ¿Algún producto Airespace soporta el protocolo IPX?

A. No, el protocolo IPX no es soportado en ninguna plataforma de WLC de Cisco.

Q. ¿Cuál es el acceso de los requisitos previos el Interfaz gráfica del usuario (GUI) del regulador del Wireless LAN (WLC)?

A. El regulador GUI del Wireless LAN es totalmente compatible con la Versión de Microsoft Internet Explorer 6.0 SP1 (o más adelante) y el Mozilla Firefox 2.0.0.11 (o más adelante).

Note: Opera y Netscape no se admiten.

Note: El Internet Explorer 6.0 SP1 (o más adelante) y el Mozilla Firefox 2.0.0.11 (o más adelante) son los únicos buscadores soportados para acceder al controlador GUI y para usar la autenticación Web.

Q. ¿Cómo extraigo el MIB del controlador LAN de la tecnología inalámbrica de Cisco (WLC) en la red?

A. Puede descargar el WLC MIB de Cisco de la página [Wireless Downloads \(clientes registrados solamente\)](#).

Complete estos pasos para descargar el WLC MIB:

1. De las descargas inalámbricas pague, haga clic el **regulador del Wireless LAN**, y elija la plataforma del WLC para la cual usted necesita el MIB.
2. Aparece la página páginas de descarga del software para WLC. Esta página contiene todos los archivos para el WLC incluidos los MIB.

3. Elija una versión de software y descargue los MIB estándar y Cisco MIB específicos. Estos dos archivos deben ser descargados y contener los MIB. Los nombres de archivo parecen similares a este ejemplo:

`standard-MIBS-Cisco-WLC4400-2000-XXXXXX.zip`

`Cisco-WLC-MIBS-XXXX.zip`

Q. ¿En la tunelización de invitado , cuántos túneles Ethernet sobre el IP (EoIP) se pueden formar entre un solo WLC del ancla a diverso WLCs interno?

A. Un solo WLC de anclaje soporta hasta 71 túneles de EoIP con un túnel por el WLC interno. Estos WLC pueden estar de diversos grupos de movilidad.

Q. ¿Cuáles son las diferencias funcionales entre los WLC de las 2100 Series y los 4400 WLC?

A. Las diferencias principales entre el WLCs de las 2100 y 4400 Series están en las características que soportan.

Estas características de hardware no se soportan en el WLCs de las 2100 Series

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

Estas funciones del software no se soportan en el WLC de las 2100 Series:

- Terminación VPN (tal como IPSec y L2TP)
- Opción del passthrough VPN
- 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 Protocol
- Reflejo de Puerto
- AppleTalk
- De QoS contratos del ancho de banda por usuario
- Traspaso IPv6
- Agregación del link (RETRASO)
- modo del Multicast-unicast

Un WLC de las 4400 Series soporta todas las características de hardware y de software anteriormente mencionadas.

Q. ¿Qué puntos de acceso ligeros (LAP) soportan los 4100 Series WLC ?

A. Sólo Airespace 1200, 1250, the Cisco 1000 Series, y Cisco 1500 Series LAP funcionan con 4100 Series WLCs.

Q. ¿Puedo utilizar esto ASA/PIX como un servidor DHCP en vez del servidor DHCP

de las ventanas para asignar las direcciones IP a mis clientes de red inalámbrica?

A. Sí, puede utilizar ASA/PIX como servidor DHCP para los clientes de red inalámbrica. Asegúrese de que la interfaz del WLAN a el cual el cliente pertenece, esté en la misma subred como ASA/PIX la interfaz en la cual se habilita el servidor. Sin embargo no puede asignar el gateway predeterminado a los clientes. El PIX/ASA se declara como el gateway predeterminado a los clientes. Para más información sobre cómo configurar el ASA como [PIX/ASA del servidor DHCP como ejemplo del servidor DHCP y de la configuración del cliente](#).

Q. ¿Es posible volver y hacer las correcciones en el asistente de configuración del controlador del Wireless LAN (WLC) a la hora de la configuración inicial?

A. Sí, esto puede hacerse con la tecla - (guión). Use esta tecla para ingresar nuevamente el valor de parámetro previo.

Por ejemplo, utilice al asistente de configuración del WLC para configurar el WLC desde el principio.

En vez de ingresar el nombre de usuario como **admin**, lo ingresa como **adminn**. Para corregir esto, ingrese - (tecla de guión) en la indicación siguiente, luego haga clic en **Enter**. El sistema devuelve el parámetro anterior.

`standard-MIBS-Cisco-WLC4400-2000-XXXXXX.zip`

`Cisco-WLC-MIBS-XXXX.zip`

Q. Del acuerdo al RFC1907 para el Protocolo de administración de red simple (SNMP), el campo de la ubicación SNMP debe soportar los tamaños a partir de la 1-255. Sin embargo, no puedo ingresar más de 31 caracteres en el campo de la ubicación SNMP. ¿por qué?

A. Esto es debido al Id. de bug Cisco [CSCsh58468](#) ([clientes registrados solamente](#)). Un usuario puede ingresar solamente 31 caracteres. No hay actualmente solución alternativa para esto.

Q. Con la gestión vía la característica sin hilos habilitada en los controladores del Wireless LAN (WLCs) en un grupo de la movilidad, puedo acceder solamente un WLC de ese grupo de la movilidad, pero no de todo. ¿por qué?

A. Esto es una conducta esperada. Cuando está habilitada, la gestión vía la característica sin hilos permite que un cliente de red inalámbrica alcance o maneje solamente el WLC a las cuales se registra su punto de acceso asociado. El cliente no puede manejar los otros WLC, aunque estos WLC están en los mismos grupos de movilidad. Esto se implementa por seguridad, y recientemente se modificó para apenas un WLC para limitar la exposición.

La gestión de la solución de Cisco WLAN sobre la característica sin hilos permite que los operadores de la solución de Cisco WLAN monitoreen y configuren el WLCs local usando un cliente de red inalámbrica. Esta característica se soporta para todas las tareas de administración, a menos que las cargas a y las descargas (las transferencias de origen y destino) del WLC.

Esto puede habilitarse a través de WLC CLI con el comando **config network mgmt-via-wireless enable**.

En el GUI, haga clic en **Management**; desde la parte izquierda haga clic en **Mgmt Via Wireless**, y marque la casilla de verificación **Enable Controller Management** para que sea accesible a los Clientes Inalámbricos.

Note: Cuando habilita esta opción, puede exponer los datos. Asegúrese de haber habilitado una autenticación adecuada y un esquema de cifrado.

Q. ¿Es posible asignar un regulador integrado en un 3750 Switch y un regulador del Wireless LAN 4400 dentro del mismo grupo de la movilidad?

A. Sí, es posible crear a un grupo de la movilidad entre un Catalyst 3750 Switch con un controlador integrado y los 4400 WLC.

Q. ¿Hay requisitos básicos a mantener cuando utilizo la característica del ancla de la movilidad para configurar los controladores del Wireless LAN (WLCs) para el acceso del invitado?

A. Éstos son los 2 requisitos básicos que necesitan ser mantenidos cuando utilizas el ancla de la movilidad para configurar el WLCs para el acceso del invitado.

- El anclaje de la movilidad del WLC local debe señalar al WLC del ancla, y el ancla de la movilidad del WLC del ancla debe señalar solamente a sí mismo.**Note:** Puede configurar WLC.de anclaje redundantes. Los WLC los usa para configurarWLC.
- Asegúrese de configurar la misma política de seguridad para el identificador de conjunto de servicios (SSID) en losWLC locales y de anclaje. Por ejemplo, si el SSID es “huésped” y usted activa la autenticación Web en el WLC local, asegúrese de que el mismo SSID y política de seguridad también se configuren en el WLC de anclaje.
- Para que la función de movilidad de anclaje funcione bien, asegúrese de que el WLC de anclaje y el WLC local usen la misma versión de IOS.

Q. ¿Cuáles son algunas de las opciones que se pueden configurar en un controlador LAN de la tecnología inalámbrica de Cisco (WLC) para mejorar su Interoperabilidad con los dispositivos del no Cisco?

A. La interoperabilidad de un WLC se puede mejorar con estas opciones:

- Las funciones de propietario reducen la posibilidad de interoperabilidad entre los dispositivos de tercero. Éstas son las funciones de propietario de Cisco:Aironet IE - El Aironet IE contiene la información, tal como el nombre del punto de acceso, la carga, número de clientes asociados, etc. enviada por el punto de acceso en las respuestas beacon y sondeo del WLAN. Los clientes CCX utilizan esta información para elegir el mejor punto de acceso con el cual asociarse.MFP: Protección de Trama de Administración es una característica introducida para proteger las tramas de la administración, tales como anulación de autenticación, disociación, beacons, y sondeos en donde el punto de acceso agrega un elemento de información del Message Integrity Check (MIC IE) a cada una de las tramas de

administración. Cualquier discrepancia en el MIC IE genera una alerta. Estas características se habilitan de forma predeterminada para cualquier WLAN que se cree en el WLC. Para inhabilitar estas características, haga clic en el menú WLAN en el WLC. Se muestra una lista de WLAN configuradas en WLC. Haga clic en WLAN a la que el cliente desea asociarse. En la pestaña Advanced de WLAN > Edit page, desmarque las casillas que corresponden a Aironet IE y MFP.

- Preámbulo corto - Un preámbulo corto mejora el desempeño del rendimiento de procesamiento y se habilita de forma predeterminada. Ciertos dispositivos, tales como teléfonos de SpectraLink pueden funcionar solamente con los preámbulos largos. En estos casos, se recomienda desmarcar los preámbulos cortos en la asociación. Para inhabilitar el preámbulo corto, haga clic en el menú **Wireless** de WLC GUI. Haga clic en **802.11b/g** > menú de la red en el lado izquierdo. Desmarque la casilla **Short Preamble**.
- Habilite el identificador de conjunto de servicios del broadcast (SSID) en el WLAN - con el broadcast SSID habilitado, la información del WLAN/SSID se envía en los beacons. Esto también ayuda a los clientes que realizan las exploraciones pasivas (que no transmiten la solicitud del sondeo), así como a los clientes configurados sin un SSID para asociarse al WLC con este WLAN. **Note:** Asegúrese de tener los mecanismos de autenticación sólidos puesto que los clientes involuntarios pueden asociarse a tu red inalámbrica.
- Inhabilite balanceo de carga agresivo global en el WLC.

Q. ¿Puede un regulador del Wireless LAN (WLC) ser manejado por los CiscoWorks (que se utiliza para manejar el Routers y el Switches)?

A. Yes. Los modelos del WLC de las 4400 Series (tales como 4402 y 4404) se pueden manejar por los CiscoWorks.

Q. ¿Qué es un AP Rogue? ¿Puede el AP Rogue en mi red inalámbrica ser bloqueado automáticamente?

A. Los AP que no son parte de su implementación inalámbrica se denominan AP rogue. Puede ser un AP autónomo o el AP ligero que se encuentra en el rango de los AP autorizados. Los AP rogue no pueden ser bloqueados automáticamente. Esto se debe hacer manualmente. La razón de esto es que, cuando encuentran a un AP rogue, el AP anula la asociación de los clientes de AP rogue, lo que causa la denegación de servicio a los clientes. Esto puede causar las cuestiones legales si el AP del vecino se detecta como rogue, y se deniega servicio a sus clientes. Para más información sobre cómo los AP rogue son detectados por el WLC, consulte la [detección del rogue del documento bajo redes inalámbricas unificadas](#).

Q. ¿Cuál es el número máximo de puntos de acceso rogue (AP) soportados por el WLC?

A. El regulador del Wireless LAN de las 4400 Series apoya a hasta 625 granujas, que incluye a los granujas reconocidos, mientras que las 2100 Series apoyan a 125 granujas.

Q. ¿Puede el regulador del Wireless LAN (WLC) enviar las notificaciones por correo electrónico al administrador cuando ocurre un evento crítico?

A. El WLC no envía el correo electrónico, sino que puede enviar los desvíos a las estaciones del

sistema de administración de la red (NMS), tales como HP OpenView (HPOV). El HPOV puede hacer escrituras habituales para enviar el correo electrónico en el recibo de los desvíos determinados.

El HPOV es un rango de productos del Hewlett Packard que consiste en una carpeta extensiva de los productos de administración de la red y de los sistemas. El HPOV se describe comúnmente como un conjunto de aplicaciones de software que permiten el sistema a gran escala y la administración de red de los activos de TI de la organización. El HPOV incluye los centenares de módulos opcionales del HP así como a los millares de otros proveedores que conecten dentro del marco bien definido y se comuniquen el uno con el otro.

Q. ¿Si los WLC en el mismo grupo de la movilidad es separado por los límites de la Traducción de Dirección de Red (NAT), pueden comunicarse los mensajes de movilidad?

A. En las versiones de software del controlador anteriores a 4.2, la movilidad entre los controladores en el mismo grupo de la movilidad no funciona si uno de los controladores está detrás de un dispositivo de la Traducción de Dirección de Red (NAT). Este comportamiento crea un problema para la característica del anclaje de invitado donde se espera que un controlador esté fuera del firewall.

Las cargas útiles del mensaje de la movilidad llevan la información de la dirección IP sobre el controlador de origen. Esta dirección IP se valida con la dirección IP de origen del encabezado IP. Este comportamiento plantea un problema cuando un dispositivo NAT se introduce en la red porque cambia la dirección IP de origen en el encabezado IP. Por lo tanto, en la característica de invitado WLAN, cualquier paquete de la movilidad que se rutee a través de un dispositivo NAT se cae debido a la discordancia de la dirección IP.

En el software del controlador versión 4.2 y posterior, la búsqueda del Grupo de Movilidad se modifica para usar la dirección MAC del controlador seguro. Como la dirección IP de origen es cambiada debido a mapping en el dispositivo NAT, se busca la base de datos del grupo de movilidad antes de que una contestación se envíe para obtener la dirección IP del controlador que hace la solicitud. Esto se hace con la dirección MAC del controlador que hace la solicitud.

Consulte [Uso de Grupos de Movilidad dispositivos NAT](#) para más información.

Q. Los puertos físicos en el WLC se fijan actualmente para actuar a la velocidad del 1000 mbps. ¿Es posible cambiar esta velocidad de puerto al 100 mbps?

A. No, la velocidad de puerto en el WLC no puede ser cambiado. Éstos se fijan en el 1000 mbps, por completo - velocidad de dúplex solamente.

Q. He fijado la administración de recursos de radio (RRM) a las configuraciones predeterminadas en mi WLC. Sin embargo, no puedo encontrar mi RRM para ajustar automáticamente el canal y los niveles de potencia. ¿por qué?

A. RRM posiblemente no funciona por ninguno de estos motivos

- RRM trabaja solamente si un AP oye las señales RF por lo menos de 3 AP próximos, con un tercer vecino que transmita una potencia de la señal mayor que -65dbm. Si cualquiera de

estas condiciones falla, el RRM no funciona.

- La característica del auto RRM incluye el ajuste del canal, el ajuste de energía, y la detección de agujeros de la cobertura. Estas características no funcionan si o están invalidadas o el método de asignación se elige como manual.

Mientras que un AP nuevo arranca, guarda inicialmente la potencia en el valor predeterminado de 1 (lo mayor posible). Cuando ve 3 o más AP con niveles de potencia mayores que 65 dBm (en el mismo Dominio RF-Movilidad y el mismo canal), intenta RRM primero (los canales del cambio). Si no tuvo éxito porque los canales están manualmente establecidos o hay más AP que canales disponibles, el AP cae su nivel de potencia.

Consulte [Administración de Recursos de Radio: Conceptos](#) para más información sobre cómo RRM trabaja.

Q. ¿Hace el regulador del Wireless LAN (WLC) localmente soporta la autenticación EAP-PEAP?

A. A través de la versión 4.1, el PEAP no se soporta localmente en el WLC. Necesita un servidor RADIUS externo. Con las versiones de la versión 4.2 y posterior del WLC, el EAP local ahora soporta la autenticación PEAPv0/MSCHAPv2 y PEAPv1/GTC.

Q. ¿Podemos poner el Lightweight Access Point (LAP) bajo la Conversión de Dirección de Red (NAT)? ¿El protocolo del Lightweight Access Point (LWAPP) del Access Point (AP) al WLC funciona con los límites NAT?

A. Sí, puede poner el LAP bajo el NAT. En el lado AP, usted puede tener cualquier tipo de NAT configurado, pero, en el lado del WLC, usted puede hacer solamente 1:1 (NAT estático) configurar. La PAT no se puede configurar en el lado del WLC porque los LAP no pueden responder al WLCs si los puertos son traducidos a los puertos con excepción de 12222 o de 12223, que están destinados a los datos y los mensajes del control.

Q. ¿Puedo poner el Lightweight Access Point (REVESTIMIENTO) bajo el Network Address Translation (NAT)? ¿El control de la norma de IETF y el aprovisionamiento del protocolo de los puntos de acceso de red inalámbrica (CAPWAP) del punto de acceso al WLC trabaja con los límites NAT?

A. Sí, puede poner el LAP bajo el NAT. En el lado AP, usted puede tener cualquier tipo de NAT configurado.

Pero en el lado del WLC, usted puede tener solamente 1:1 (NAT estático) configurado y la dirección IP del externo NAT configurada en la interfaz de administración dinámica AP (solamente para los reguladores de las Cisco 5500 Series). La PALMADITA no se puede configurar en el lado del WLC porque los revestimientos no pueden responder al WLCs si los puertos se traducen a los puertos con excepción de 5246 o de 5247, que se significan para el control y los mensajes de datos.

Note: Seleccione el rectángulo de **revisión de dirección del habilitar NAT** y ingrese el IP Address externo NAT si usted quiere poder desplegar su regulador de las Cisco 5500 Series detrás del router o del otro dispositivo de gateway que está utilizando el Network Address Translation (NAT) del mapeo uno a uno. El NAT permite que un dispositivo, tal como un router, actúe como agente entre Internet (público) y una red local (soldado). En este caso, asocia los IP Addresses del

intranet del regulador a una dirección externa correspondiente. La interfaz dinámica del AP manager del regulador se debe configurar con la dirección IP del externo NAT de modo que el regulador pueda enviar la dirección IP correcta en la respuesta de la detección.

Note: Con CAPWAP, el WLC detrás del NAT no se soporta con las 4400 Series, los reguladores del Wireless LAN de las 2100 Series y el WiSM.

Q. ¿Cómo configuro el WLC para permitir solamente a los clientes 802.11g?

A. Use el comando del comando **config 802.11b disable** command para inhabilitar o habilitar las transmisiones 802.11b/g para la red completa o para una radio individual de Cisco

Note: Debe utilizar este comando de inhabilitar la red antes de que utilices otros comandos de los config 802.11b. Este comando puede ser utilizado cualquier momento la interfaz CLI es activa.

Aquí está la sintaxis.

```
config 802.11b disable {network | Cisco_AP}
```

Aquí está un ejemplo en cómo inhabilitar las transmisiones AP01 802.11b/g:

```
config 802.11b disable network
```

Para inhabilitar las transmisiones **AP01** 802.11b/g, use este comando:

```
config 802.11b disable AP01
```

Alternativamente, puede utilizar este comando para inhabilitar las velocidades de datos 802.11b:

```
config 802.11b rate {disabled | mandatory | supported} rate
```

Q. ¿Cuál es el procedimiento para actualizar el software de sistema operativo (OS) en un WLC de Cisco?

A. Consulte el documento Actualización de [Wireless LAN Controller \(WLC\) Software](#) para proporcionar el procedimiento para una actualización de software en su WLC.

Q. ¿Puedo actualizar el WLC a partir de una versión importante a otra directamente?

A. Puede actualizar o instalar una versión anterior de software WLC solamente entre dos versiones. Para instalar más de dos versiones anteriores o posteriores, primero debe instalar una versión intermedia. Por ejemplo, si su WLC ejecuta la versión 4.2 o 5.0 , puede actualizar el WLC directamente al Software Release 5.1.151.0. Si su WLC ejecuta la versión 3.2, 4.0, o 4.1 , debe

actualizar el WLC a una versión intermedia antes de la actualización a 5.1.151.0. Para conocer la trayectoria de actualización para cualquier versión del WLC, consulte Release Notes de la versión correspondiente.

Q. ¿Cuál es Beamforming?

A. Beamforming (también llamado ClientLink) es un mecanismo de espacial-filtración usado en un transmisor para mejorar el poder de la señal recibida o la relación de transformación de relación señal/ruido (del SNR) en un receptor previsto (cliente). Beamforming utiliza el múltiplo transmite las Antenas para enfocar las transmisiones en dirección de un 802.11a o el cliente 802.11g, que aumenta el SNR del link descendente y la velocidad de datos al cliente, reduce los agujeros de la cobertura, y aumenta el funcionamiento general del sistema. Beamforming se soporta en los Puntos de acceso de las 1140 y 1250 Series del Cisco Aironet y trabaja con todo el 802.11a y clientes existentes 802.11g. Se inhabilita por abandono.

Para la información sobre configurar Beamforming, refiera a la sección de [Beamforming que configura de la guía de configuración de controlador del Wireless LAN](#).

Q. ¿Puedo descargar un anuncio de inicio de sesión para el regulador del Wireless LAN?

A. Usted puede descargar un archivo del anuncio de inicio de sesión usando el regulador GUI o el CLI. El anuncio de inicio de sesión es el texto que aparece en la pantalla antes de la autenticación de usuario cuando usted accede el regulador GUI o CLI usando Telnet, SSH, o una conexión del puerto de la consola.

Preguntas Frecuentes sobre Troubleshooting

Q. Hemos finalizado nuestra implementación inicial de Lightweight Access Point (LAPs). Cuando nuestros clientes se trasladan de una punta del edificio a la otra, permanecen asociados con el AP más cercano a ellos. Los clientes no son transferidos al AP más cercano siguiente hasta que la potencia de la señal del AP inicial se agote totalmente. ¿por qué?

A. El área de cobertura de un AP es controlada totalmente por el WLC. El WLC habla entre sus AP y maneja su potencia de la señal en base de cómo cada AP detecta otros AP. Sin embargo el movimiento del cliente a partir de un AP a otro es controlado totalmente por el cliente. La radio dentro del cliente determina cuando el cliente quiere trasladarse a partir de un AP al otro. Ninguna configuración en el WLC, el AP, o el resto de tu red puede influenciar la decisión del cliente para vagar por a un diverso AP.

Q. Conecté mi WLC con los switches Cat6500 configurados para rutear, y configuré el HSRP entre estos switches. Sin embargo, no puedo ahora alcanzar otras subredes con el WLC. ¿Cómo resuelvo este problema?

A. Cuando el HSRP existe, un dirección IP virtual y una dirección MAC se configura generalmente para el grupo del HSRP, que se utiliza para rutear. Los hosts continúan remitiendo los paquetes del IP a este IP y dirección MAC consistente incluso cuando uno de los switches se desactiva y se produce el cambio en un dispositivo en espera. Complete estos pasos para resolver el problema

de ruteo:

1. Asegúrese de que la dirección IP virtual se configura como el gateway predeterminado en el WLC. **Note:** Ciertas versiones anteriores del WLC no remiten los paquetes a la dirección MAC del HSRP, que da lugar en un error al rutear los paquetes. Actualiza el WLC para resolver este problema.
2. Asegúrese de que la interfaz virtual en el WLC se configura correctamente. Para más información sobre interfaces, consulte la sección [puertos que configura y de las interfaces de la guía de configuración del WLC](#).

Q. ¿Cómo prevengo los loops en el WLC?

A. Usted puede habilitar el STP en el WLC para prevenir los loops. **Del regulador del teclado** del WLC GUI, entonces navegue al submenú **avanzado** situado en el lado izquierdo de la aplicación. Haga clic en la opción de **Spanning Tree** y elija **Enable** para el **Spanning Tree Algorithm** situado a la derecha de la aplicación.

de forma predeterminada, el STP no necesita ser habilitado para prevenir los loops. Porque cada interfaz que se asocia a un WLAN en el WLC se asocia a primario y a los puertos de respaldo. Solamente un puerto se utiliza en una punta del tiempo determinada. El tráfico del WLAN se remite solamente a través del puerto primario. El WLC nunca utiliza el puerto secundario cuando el puerto primario es activo. El WLC utiliza el puerto secundario solamente cuando el puerto primario está abajo, así que los loops no ocurrirán de forma predeterminada.

Q. ¿Hay opción para proporcionar la seguridad complementaria a la red?

A. Usted puede utilizar la opción 82 para proporcionar la seguridad complementaria. La opción 82 bloquea los IP Addresses a los clientes desautorizados que acceden la red. Para más información, refiera a la sección de la [opción DHCP que configura 82 de la guía de configuración del controlador LAN de la tecnología inalámbrica de Cisco, la versión 6.0](#).

Q. ¿Hay manera de recuperar mi contraseña para el WLC?

A. Si olvidas la su contraseña en la versión 5.1 y posterior del WLC, puede utilizar el CLI de la consola en serie del controlador para configurar un nombre y una contraseña de usuario nuevo. Termina estos pasos para configurar un nombre y una contraseña de usuario nuevo.

1. Después de que el controlador arranque, ingresa la **Restore-Contraseña** en el prompt del usuario. **Note:** Por las razones de seguridad, el texto que ingresas no aparece en la consola del controlador.
2. En el prompt del Nombre de usuario del ingresar, ingresa un nombre de usuario nuevo.
3. En el prompt de contraseña del ingresar, ingresa una nueva contraseña.
4. En el prompt de contraseña del entrar de nuevo, entra la nueva contraseña de nuevo. El controlador valida y salva tus entradas en la base de datos.
5. Cuando reaparece el prompt del usuario, ingresa tu nuevo nombre de usuario.
6. Cuando aparece el prompt de contraseña, ingresa tu nueva contraseña. El controlador te abre una sesión con tu nuevo nombre de usuario y contraseña.

Note: Para el WLCs que funcionan con las versiones anteriores del firmware (antes de 5.1), no hay manera de recuperar la contraseña. Si usted utiliza el Cisco Wireless Control System (WCS)

para manejar el WLC, el módulo del regulador del Wireless LAN (WLCM) o el módulo de Servicios inalámbricos (WiSM), usted debe poder acceder el WLC del WCS y crear a un nuevo usuario administrador sin la registración en el WLC sí mismo. O, si no guardó la configuración en el WLC después de borrar al usuario, luego de la reinicialización (ciclo de alimentación) del WLC, debería volvero a traer con el usuario eliminado aún en el sistema. Si no tiene la cuenta de administración predeterminada u otra cuenta de usuario con las cuales acceder, su única opción es restaurar las configuraciones de fábrica del WLC y configurarlo nuevamente.

Q. Cambié el modo del Lightweight Access Point (LAP) de mi 1030 Access Point (AP) de Local a modo Bridge y el WLC 2006 no lo detecta más. ¿Cómo puedo restablecer los 1030 AP de nuevo a su Local modo AP?

A. Para configurar el Bridge en el modo local, complete estos pasos:

1. Diríjase al WLC GUI y elige la **red inalámbrica**. Visualiza la lista de AP registrada actualmente en la WLC. Haga clic en el AP para el cual necesita cambiar el modo. **Note:** Verifique si el AP soporta el modo REAP. Éste debe ser **YES** para los AP de bridging internos.
2. Marque la opción modo AP. Si dice Bridge, cámbielo de nuevo a **Local**. Esto cambia el Bridge AP al AP normal.

Para más información sobre cómo configurar el Bridging Mode, consulte [Ethernet Bridging en el ejemplo de configuración inalámbrico de la red de interconexión de la Punta-Punta](#).

Q. He configurado un Wireless LAN del invitado y el WLC se separa físicamente de mi LAN interno. Decidía utilizar la característica interna del DHCP de este WLC pero mis clientes de red inalámbrica no consiguen los dirección IP del WLC. ¿Cómo los Usuarios invitados inalámbricos consiguen los dirección IP del WLC cuando están conectados en físicamente una red separada?

- Marca si el alcance de DHCP se habilita en el WLC. Para marcar esto, haga clic en el menú del **controlador** y haga clic en el **servidor DHCP interno** del lado izquierdo.
- Generalmente, el servidor DHCP se especifica en la interfaz, que asocia al WLAN. Asegúrese de que el direccionamiento de la interfaz de administración del WLC está especificado como el servidor DHCP en la interfaz esa las correspondencias al Usuario invitado WLAN. Alternativamente, puede habilitar la opción de la invalidación del servidor DHCP en paginación **WLAN > del Edit** y especificar el direccionamiento de la interfaz de administración del WLC en el **campo del Addr del IP del servidor DHCP**.

Q. Hago un regulador del Wireless LAN de las 4400 Series (WLC) y los Puntos de acceso ligeros (revestimientos) registrar al WLC. He configurado los WLAN para que los clientes conecten en el WLC. El problema es que el WLC no transmite los identificadores del conjunto de servicio (SSID) esos yo configuré para los WLAN. ¿por qué?

A. El estado del administrador y los parámetros del broadcast SSID están invalidados de forma predeterminada. Termina estos pasos para habilitar el estado del administrador y transmitir el SSID:

1. Diríjase a WLC GUI y elija el **Controller > WLANs**. La paginación WLAN aparece. Esta paginación enumera los WLAN se configuran que.
2. Selecciona el WLAN para el cual quieres habilitar la difusión del SSID y del **Edit del teclado**.
3. En la página WLAN > Edit, marque **Admin Status** para habilitar el WLAN. También, el control **transmite el SSID** para asegurarse de que el SSID está transmitido en los mensajes del beacon enviados por el AP.

Q. ¿La solución del Cisco Unified Wireless soporta el WLCs redundante en el DMZ para la tunelización de invitado?

A. Sí, WLCs en el WLC redundante del soporte DMZ en el DMZ para la tunelización de invitado. Para obtener más información sobre cómo configurar WLC redundantes, consulte la sección [Configuración de Movilidad de Anclaje Automático](#) del documento Guía de Configuración de [Cisco Wireless LAN Controller , Release 5.1](#).

Q. Los clientes del Wireless LAN asociados a los Lightweight Access Point no pueden obtener las direcciones IP del servidor DHCP. . ¿Qué debo hacer?

A. El servidor DHCP para un cliente es generalmente marcado en la interfaz, que asocia al WLAN a el cual el cliente. Verifique si la interfaz está configurada correctamente. Para más información sobre cómo resolver problemas relacionados a DHCP, consulte la sección de los [problemas de dirección IP de los problemas de cliente del troubleshooting del documento en la red del Cisco Unified Wireless](#).

Q. ¿Hay documentos que expliquen los problemas de la conectividad del cliente del troubleshooting en una red del Cisco Unified Wireless?

A. Para información detallada sobre resolver problemas del cliente, refiera a estos documentos.

- [Unified Wireless Network: Resolución de Problemas de Clientes](#)
- [Comprensión del cliente del debug en los reguladores del Wireless LAN \(WLCs\)](#)

Q. Mi 1131 Lightweight Access Point (REVESTIMIENTO) no se registran con mi regulador del Wireless LAN 4402 (WLC). ¿Cuál puede ser la razón posible de esto?

A. Una razones comunes son que el modo de transporte del protocolo del Lightweight Access Point (LWAPP) está configurado en el WLC. Los 4402 WLC pueden actuar en el modo LWAPP de la capa 2 y de la capa 3. Considerando que, los 1131 LAPS pueden actuar solamente en el modo de la capa 3. El modo de la capa 2 no se soporta en los 1131 LAPS. Así pues, si el WLC se configura con el modo de transporte LWAPP de la capa 2, después tu LAP no se une a el WLC. Para resolver este problema, cambie al modo de transporte LWAPP de WLC de la capa 2 a la 3.

Para cambiar al modo de transporte LWAPP que usa el GUI, diríjase a la paginación del WLC y localiza la segunda selección en el campo principal que es modo de transporte LWAPP. Cambie esto a la capa 3 y reinicie el WLC. Ahora, tu LAP puede registrarse con el WLC. Para más información sobre problemas relacionados al registro de LAP, consulte [Troubleshooting del documento al Lightweight Access Point que no se une a un controlador del Wireless LAN](#).

Q. LaWLC no genera capturas para los rogues ad hoc y los debugs SNMP en el

WLC no muestran desvíos del WLC para ad hoc aunque el WLC GUI informó los rogues ad hoc. El WLC funciona con la versión de firmware 3.2.116.21. ¿Por qué ocurre esto?

A. Esto es debido al Id. de bug Cisco [CSCse14889](#) ([clientes registrados solamente](#)). El WLC envía constantemente los desvíos para el (APS) rogue detectado de los puntos de acceso pero no para los rogues ad hoc detectados. Este bug es fijo en las versiones de firmware 3.2.171.5 del WLC y posterior.

Q. Tenemos una infraestructura WLAN del Airespace de Cisco de la empresa. Los clientes WLAN no pueden hojear un dominio del Microsoft Active Directory (AD). Este problema se considera dentro de uno de nuestros edificios. Otros edificios no tienen el problema. No utilizamos ningún Access Control List (ACL) internamente. También, cuando un cliente fallado es duro-conexiones, pueden hojear inmediatamente el dominio de Microsoft AD. ¿Cuál podría ser el problema?

A. Una de las razones puede ser que el modo del multicast está invalidado en el WLC. Habilita el modo del multicast en el WLC y marca si puede acceder el dominio de Microsoft AD.

Q. ¿La movilidad de la capa 3 trabaja con una configuración de VLAN del grupo del Access Point (AP)?

A. Sí, la movilidad de capa 3 funciona con la configuración de VLAN del grupo AP. Actualmente, las fuentes del tráfico de un cliente de red inalámbrica vagado por de la capa 3 se ponen en la interfaz dinámica asignada en el WLAN o la interfaz del grupo VLAN AP.

Q. ¿Por qué nuestro (APS) de los puntos de acceso que se registran al otro WLCs que son en el mismo grupo RF se muestran que los rogues?

A. Esto puede ser debido al Id. de bug Cisco [CSCse87066](#) ([clientes registrados solamente](#)). El LWAPP AP en el mismo grupo RF es visto como rogue AP por otro WLC para una de estas razones:

- El AP ve a más de 24 vecinos. Los tamaños vecinos de la lista son 24, así que el 25to AP está señalado como rogue.
- El AP1 puede oír al cliente que comunica al AP2, pero el AP2 no puede ser oído. Por lo tanto, no puede ser validado como vecino.

La solución alternativa es fijar manualmente los AP a interno sabida en el WLC y/o el WCS. Termina estos pasos en el WLC para fijar manualmente los AP a interno sabida:

1. Diríjase al WLC GUI y elige la **red inalámbrica**.
2. Haga clic en **Rogue Aps** en el menú del lado izquierdo.
3. De la lista del rogue-AP, elige el punto de acceso y el clickEdit específicos.
4. Del menú del estado de la actualización, elige **interno sabida**.
5. Haga clic en Apply (Aplicar). Este bug es fijo en la versión 4.0.179.11.

Q. Tengo los 1200 Lightweight Access Point (REVESTIMIENTO) que se registrarán con mi regulador del Wireless LAN (WLC). He configurado mi servidor DHCP con la

opción 43. ¿Cómo puedo verificar si esté funcionando la opción DHCP 43 correctamente?

A. Con la opción DHCP 43, el servidor DHCP proporciona el dirección IP del WLCs junto con el dirección IP proporcionado con el DHCP. Esto se puede verificar del LAP si el AP es un protocolo basado Cisco IOS del Lightweight Access Point (LWAPP) AP, tal como los 1242 o el LAP 1131AG. En estos casos, publica el comando del **detalle DHCP del debug** en el lado AP para ver si el AP recibe con éxito la información de la opción 43 y qué recibe.

Q. Mi WLC 2006 muestra que diversos canales se han asignado al (APS) de las puntas de acceso registrado. Sin embargo, cuando exploro con utilidad Aironet Desktop (ADU) o Netstumbler, todos los AP están en el mismo canal (1). ¿Cuál es la razón?

A. Este problema ocurre cuando estos AP registrados están en el muy cerca con uno a. Probablemente ejecuta el Cisco bug ID [CSCsg03420](#) ([sólo clientes registrados](#)) .

Q. Cuando ejecuto el comando ipconfig/all en el command prompt de mi equipo, se muestra una dirección diferente del servidor DHCP. Muestra 1.1.1.1 como el dirección IP del servidor DHCP. Éste es el dirección IP de la interfaz virtual del WLC y no del direccionamiento del servidor DHCP. ¿Por qué es esto mostrada como el servidor DHCP?

A. Esto es porque el direccionamiento de la interfaz virtual de 1.1.1.1 actúa como proxy del DHCP para el servidor DHCP original. Si quieres ver el direccionamiento original del servidor DHCP en la salida del **ipconfig/de todo** el comando, después invalida la característica del proxy del DHCP en el WLC a las cuales el cliente es asociado. Esto se puede inhabilitar con el comando de la **neutralización del proxy DHCP de los config**.

Este comando substituirá el direccionamiento de la interfaz virtual de 1.1.1.1, que aparece sí mismo como el servidor DHCP, con el dirección IP del servidor DHCP real que definiste en la interfaz o en la opción de la invalidación del WLAN.

Q. Tenemos un par de servidores de control de acceso (ACS) que autentican a los clientes de red inalámbrica asociados a los controladores del Wireless LAN (WLCs). Un ACS actúa como un servidor de autenticidad primario y el otro como servidor de fallas. Si el servidor primario falla, el WLC recurre a secundario para autenticar a los clientes de red inalámbrica. Una vez que viene el servidor primario salvaguardia, el WLC no hace retraso al servidor primario. ¿por qué?

A. Esto es una conducta esperada. Estos pasos ocurren cuando autentican a un cliente con el WLC en las implementaciones múltiples ACS:

1. Sobre el arrancar, el WLC determina el ACS activo.
2. Cuando este ACS activo no responde al pedido de RADIUS del WLC, el WLC busca y hace un failover al ACS secundario.
3. Incluso cuando viene el ACS primario salvaguardia, el WLC no recurre a ella hasta que el ACS a el cual el WLC está autenticando actualmente falle.

En estos casos, reanuda el WLC para que el WLC identifique el ACS primario otra vez y el retraso a él. Este retraso no ocurre inmediatamente después de la reinicialización. Posiblemente tarde unos minutos.

Q. No puedo al Secure Shell (SSH) en el controlador del Wireless LAN (WLC) cuando utilizo el software de cliente SH del v2 de SecureCRT SSH. Mi WLC funciona con la versión 4.0.179.8.

A. SecureCRT trabaja solamente con el WLCs esa versión 4.0.206.0 o posterior del funcionamiento. Actualiza tu WLC a esta versión. Entonces, puede utilizar al cliente SH para SSH de SecureCRT en el WLC.

Q. ¿Cómo cifro los archivos de configuración en el WLC?

A. El cifrado de los archivos de configuración está ya disponible en los WLC. Si elige de WLC GUI, **Commands > Upload File**, podrá ver la casilla de verificación **Cifrado de Configuración de Archivo** .

Usted puede forzar el archivo para ser cifrado con el WCS de esta manera.

- Del WCS GUI, elige el **controlador de la configuración**. Visualiza la lista de WLCs configurada en el WCS. Haga clic en un WLC.
- En el lado izquierdo, haga clic en la opción de los **comandos**. Recibes una lista de comandos del controlador.
- En **Cargar/Descargar Comandos** , elija **descargar config**. del menú desplegable. Ahora, podrá ver este mensaje: **Note: La clave de cifrado del archivo de configuración no está establecida. Descargar el archivo de configuración fallará si la clave de cifrado es necesaria. Haga clic aquí para establecer la cifrado.**

Básicamente, puede forzar el WCS para fijar siempre una clave de cifrado para las configuraciones del WLC. La cifrado no se habilita de forma predeterminada, sino que puede ser habilitada en el WLC y el WCS, según lo necesario.

Q. ¿Cómo el WLCs soporta los Puntos de acceso de gran tamaño?

A. El Software Release 5.0 o Posterior del regulador permite que usted actualice a una imagen del punto de acceso de gran tamaño automáticamente borrando la imagen de recuperación para crear el espacio suficiente. Esta característica afecta solamente a los Puntos de acceso con el 8 MB del flash (los 1100, de 1200, y de los Puntos de acceso de las 1310 Series). Todos los más nuevos Puntos de acceso tienen un tamaño de Flash más grande que el 8 MB. En agosto 2007, no hay imágenes del punto de acceso de gran tamaño, pero como se agregan las nuevas funciones, el tamaño de la imagen del punto de acceso continuará creciendo. Para más información, refiera a la sección [de gran tamaño de las imágenes del punto de acceso que soporta de la guía de configuración del controlador LAN de la tecnología inalámbrica de Cisco, la versión 6.0](#).

Información Relacionada

- [Módulos controlador de LAN de la tecnología inalámbrica de Cisco](#)
- [Preguntas y Respuestas de los Cisco Wireless Cisco Wireless](#)

- [Contadores de MAC del 802.11 en el WLC](#)
- [Guía de configuración del controlador LAN de la tecnología inalámbrica de Cisco, versión 7.0](#)
- [Página de Soporte de Red Inalámbrica](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)