Lightweight Access Point FAQ

Contenido

Introducción

Este documento proporciona información sobre las preguntas más frecuentes (FAQ) sobre los Puntos de Acceso Ligeros de Cisco (LAP)

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

LAP FAQ

Q. ¿Cuál es un Punto de acceso de las livianas de Cisco (REVESTIMIENTO)?

A. El LAP de Cisco es parte de la arquitectura Red Inalámbrica Unificada de Cisco. UN LAP es un AP que se diseña para ser conectado con un controlador del Wireless LAN (WLAN) (WLC). El LAP proporciona el soporte dual de la banda para IEEE 802.11a, 802.11b, y 802.11g y aire simultáneo que monitorea para la gestión dinámica, en tiempo real de la radiofrecuencia (RF). Además, los revestimientos de Cisco manejan las funciones sensibles al tiempo, tales como cifrado de la capa 2, que permiten a Cisco WLAN para soportar con seguridad la Voz, el vídeo, y las aplicaciones de datos.

Los AP son el “peso ligero,” que significa que él no puede actuar independientemente de un regulador del Wireless LAN (WLC). El WLC administra las configuraciones y el firmware AP. Los AP son “tacto cero” desplegado, y la configuración individual de los AP no es necesaria. Los AP son también ligeros en el sentido que manejan solamente las funciones en tiempo real MAC. Los AP salen de todas las funciones no en tiempo real MAC que se procesarán por el WLC. Esta arquitectura se denomina “parte la arquitectura MAC”.

Q. ¿Puedo configurar el REVESTIMIENTO para actuar a la independiente de un regulador del Wireless LAN (WLC)?

A. No, los LAPs no puede funcionar independiente del WLCs. Los LAPs funcionan conjuntamente con un WLC solamente. La razón es que el WLC proporciona todos los parámetros de la configuración y firmware que el LAP necesita en el proceso de inscripción.

Q. ¿Qué es un Protocolo Ligero AP (LWAPP)?

A. El LWAPP es un proyecto de protocolo de la Internet Engineering Task Force (IETF) que define la mensajería del control para las operaciones de la disposición y de la autenticación y operaciones en tiempo de ejecución. El LWAPP también define el mecanismo de tunelización para el tráfico de datos.

UN LAP descubre un controlador con el uso de los mecanismos de la detección de LWAPP. El LAP envía al controlador una solicitud de unión al LWAPP. El controlador envía al LAP una respuesta de incorporación al LWAPP, que permite que el AP se una a el controlador. Cuando el LAP se une a al controlador, el LAP descarga el software del controlador si las revisiones en el LAP y el controlador no coinciden. Posteriormente, el LAP estará totalmente bajo el control del controlador. El LWAPP asegura la comunicación de control entre el LAP y el controlador mediante una distribución de claves seguras. La distribución de claves seguras requiere certificados digitales X.509 ya suministrados en el LAP y el controlador. Los certificados instalados en fábrica se denominan con el término “MIC”, que son las siglas de Manufacturing Installed Certificate (Certificado de Instalación de Fábrica). El Cisco Aironet AP que envió antes de julio del 18 de 2005, no tiene un MIC. Estos AP crean un certificado autofirmado (SSC) cuando se actualizan para poder actuar en el modo ligero. Los controladores se programan para aceptar SSC para la autenticación de AP específicos.

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. ¿Cómo distingo entre un AP (autónomo) regular y un LAP?

A. La manera más fácil de distinguir entre un AP regular y un LAP es mirar el número de pieza del AP.

- LAP (Lightweight AP Protocol [LWAPP]) — Los números de pieza *siempre* comienzan con **AIR-LAPXXXX**.
- AP Autónomo (Cisco IOS® Software) — Los números de pieza *siempre* comienzan con **AIR-APXXXX**.

Los LAP del Cisco Aironet 1000 Series son una anomalía a este los criterios. Los números de pieza de los LAP de las 1000 Series son:

- AIR-AP1010-A-K9 para los LAP 1010
- AIR-AP1020-A-K9 para los LAP 1020
- AIR-AP1030-A-K9 para los LAP 1030

Nota: Los números de pieza pueden variar, que depende del país y del dominio controlador. Los números de parte que esta lista proporciona son sólo ejemplos.

Asegúrese de solicitar el AP apropiado para su Wireless LAN (WLAN).

Q. ¿Qué modelos de AP pueden ejecutar Lightweight AP Protocol (LWAPP)?

A. Estas plataformas del Cisco Aironet AP pueden ejecutar el LWAPP:

- Aironet 1500 Series
- Cisco Aironet 1250 Series
- Aironet 1240 AG Series
- Aironet 1230 AG Series
- Aironet 1200 Series
- Aironet 1130 AG Series
- Aironet 1000 Series
- 1140 Series AP del Aironet**Nota:** Las 1140 Series AP se soportan solamente con el WLC que versión de los funcionamientos 5.2 o más adelante.

Nota: Puede solicitar estos Aironet AP con el Cisco IOS Software para que funcionen como AP autónomos o con LWAPP. El número de pieza determina si un AP basado en Cisco IOS Software o un AP basado en LWAPP. Aquí están los ejemplos:

- AIR-AP1242AG-A-K9 es un AP basado en Cisco IOS Software .
- AIR-LAP1242AG-P-K9 es un AP basado en LWAPP .

Nota: Los 1000 Series AP y los 1500 Series AP son excepciones a este criterio. Todos las 1000 Series AP y las 1500 Series AP soportan solamente el LWAPP.

Q. ¿Cómo instalo y configuro un Punto de acceso Lwapp-habilitado?

A. El LWAPP-habilitar AP **A.** es parte de la solución de red inalámbrica integrada Cisco y no requiere ninguna configuración manual antes de que se monten. El AP es configurado por un Controlador de LAN LWAPP-capaz de la Red Inalámbrica Cisco (WLC). Refiera a los Puntos de acceso Lwapp-habilitados guía de inicio rápido del Cisco Aironet para la información sobre cómo instalar y configurar inicialmente un Punto de acceso Lwapp-habilitado.

Q. ¿Cómo configuro mi LAP y mi controlador del Wireless LAN (WLC) junto?

A. Los LAPs utilizan el protocolo ligero AP (LWAPP), y cuando se unen a un WLC, el WLC envía a los LAPs todos los parámetros de la configuración y firmware. Consulte Ejemplo de Configuración Básica del Wireless LAN Controller y del Lightweight Access Point para una configuración básica.

Q. ¿Puedo conectar un AP autónomo con un controlador del Wireless LAN (WLC) y esperar que el AP trabaje?

A. No, solamente los LAPs trabaja cuando están conectados con un WLC. Los AP autónomos no entienden el protocolo ligero AP (LWAPP) o el protocolo CAPWAP que el WLC utiliza. Para conectar un AP autónomo con un WLC, debe primero convertir el AP autónomo al modo ligero.

Q. Tengo un Punto de acceso basado en software del Cisco IOS autónomo. ¿Puedo convertirlo al modo ligero?

A. Sí, pero no todos los modelos basados en programas del Cisco IOS autónomo AP puede ser convertido. Éstos son los modelos que puede convertir al modo ligero del protocolo AP (LWAPP):

- Todos los Cisco Aironet 1130 AG AP
- Todos los Aironet 1240 AG AP
- Para todas las plataformas modulares de las 1200 Series basadas en programas AP (1200/1220 actualización del Cisco IOS Software, 1210, y 1230 AP) del Aironet del Cisco IOS, la capacidad de convertir el AP depende de la radio.Si la radio es IEEE 802.11g, MP21G y MP31G se soportan.Si la radio es IEEE 802.11a, RM21A y RM22A se soportan.Puede actualizar las 1200 Series AP con cualquier combinación de radios soportados:G solamenteA solamenteG y A

Nota: Un AP autónomo debe funcionar con el Cisco IOS Software Release 12.3(7)JA o Posterior antes de que puedas convertirlo al LWAPP.

Nota: Sólo los controladores Cisco 4400 y 2006 inalámbricos LAN (WLCs) soportan AP autónomos que se convirtieron a modo ligero. El WLCs de Cisco debe funcionar con una versión mínima de software de 3.1. El Cisco Wireless Control System (WCS) debe funcionar con una versión mínima de 3.1. El utilitario de la actualización se soporta en las plataformas del Microsoft Windows 2000 y de Windows XP.

Consulte actualizar los puntos de acceso autónomos del Cisco Aironet al modo ligero para los detalles en cómo realizar la conversión.

Q. ¿Qué restricciones se imponen ante un Punto de acceso basado en software del Cisco IOS después de la conversión al modo ligero?

A. Tenga estas guías de consulta presente cuando usted utiliza los Puntos de acceso autónomos que se han convertido al modo ligero:

- Los AP que se convierten al protocolo ligero AP (LWAPP) no soportan los servicios del dominio de red inalámbrica (WDS). los AP de los LWAPP-convertir comunican solamente con los controladores de la Red Inalámbrica Cisco LAN (WLAN) (WLCs) y no pueden comunicar

con los dispositivos WDS. Sin embargo, el WLC proporciona las funciones que son equivalentes al WDS cuando el AP se asocia al WLC.

- Los Puntos de acceso convertidos soportan 2006, 4400, y los reguladores de WiSM solamente. Cuando usted convierte un Punto de acceso autónomo al modo ligero, el Punto de acceso puede comunicar con los reguladores de las Cisco 2006 Series, los reguladores de las 4400 Series, o los reguladores en Cisco WiSM solamente.
- En el Software Release 4.2 o Posterior del regulador, todos los Puntos de acceso de las livianas de Cisco soportan 16 BSSIDs por la radio y un total de 16 LAN inalámbricos por el Punto de acceso. En las versiones anteriores, soportaron solamente 8 BSSIDs por la radio y un total de 8 LAN inalámbricos por el Punto de acceso. Cuando un Punto de acceso convertido se asocia a un regulador, sólo la Tecnología inalámbrica LAN con ID 1 a 16 se avanza al Punto de acceso.
- Los AP que se convierten al LWAPP deben obtener una dirección IP y detectar el WLC con el uso del DHCP, de un sistema de nombres del dominio (DN), o de un broadcast de la subred IP.
- Los AP que se convierten al LWAPP no soportan el LWAPP de la capa 2.
- Los AP que se convierten al LWAPP proporcionan un puerto de la consola solo lectura.
- La herramienta de la conversión de la actualización agrega el clave-hash del certificado autofirmado (SSC) a solamente uno de los reguladores en Cisco WiSM. Después de que se haya completado la conversión, agregue el clave-hash de SSC al segundo regulador en Cisco WiSM copiando el clave-hash de SSC del primer regulador al segundo regulador. Para copiar el clave-hash de SSC, abra la página de las directivas AP del regulador GUI (**Seguridad >AAA > las directivas AP**), y copie el clave-hash de SSC de la columna del hash de la clave SHA1 conforme a la lista de la autorización AP. Entonces, con el GUI del segundo regulador, abra la misma página y pegue el clave-hash en el campo del hash de la clave SHA1 debajo agregan el AP a la lista de la autorización. Si usted tiene más de un Cisco WiSM, utilice el WCS para avanzar el clave-hash de SSC al resto de reguladores.

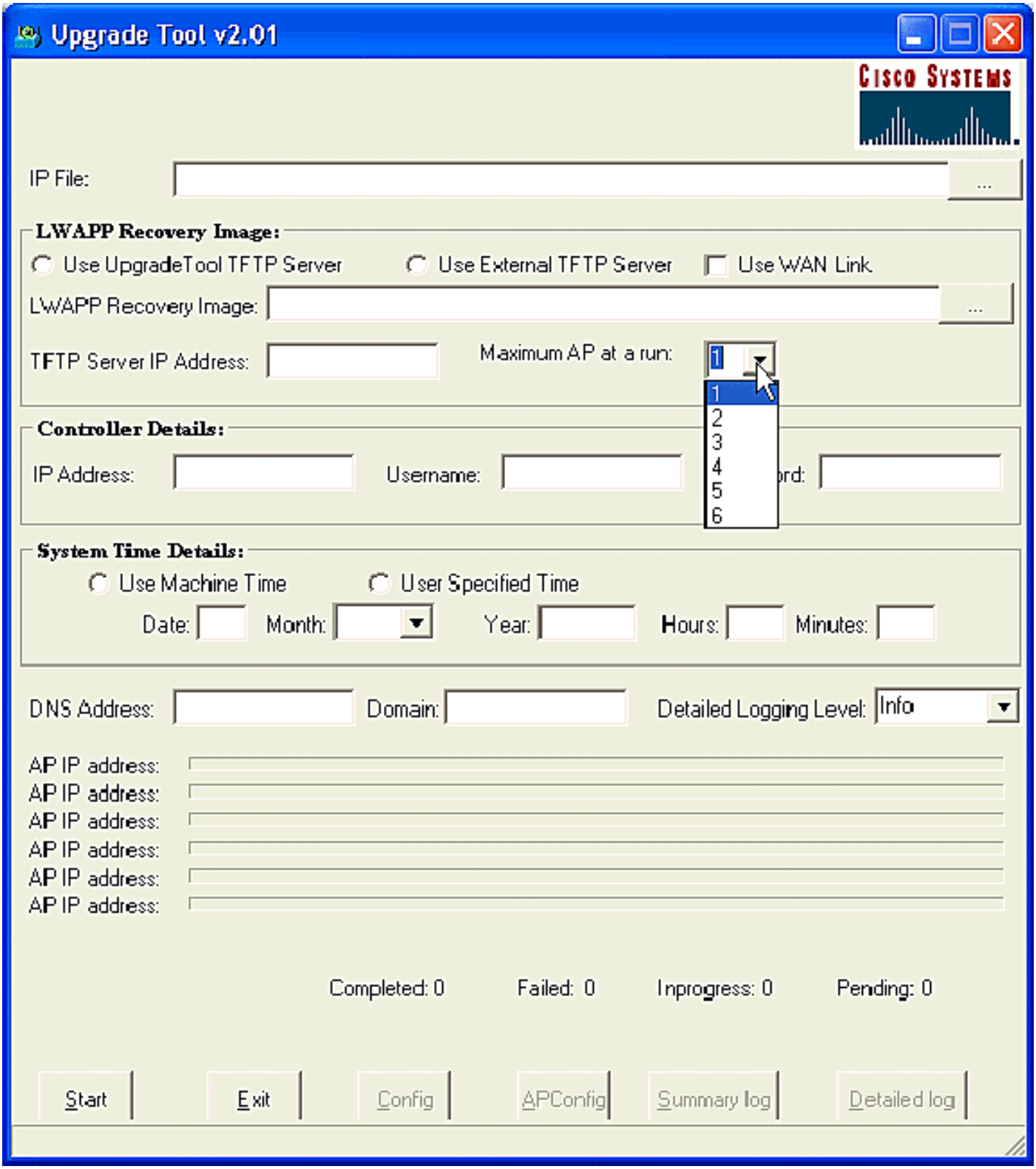
Consulte Release Note para el Cisco Aironet 1130AG, 1200, puntos de acceso de la serie 1230AG, y 1240AG para el Cisco IOS Release 12.3(7)JX para los detalles.

Q. He convertido mi Punto de acceso al modo ligero, pero necesito convertirlo de nuevo al modo autónomo. ¿Es posible?

A. Sí, puede convertir los AP autónomos que has convertido al modo ligero de nuevo al modo autónomo. Termina los pasos de progresión en *convertir un Lightweight Access Point de nuevo a la sección de modo autónoma de* actualizar los puntos de acceso autónomos del Cisco Aironet al modo ligero.

Q. ¿Cuántos Puntos de acceso se pueden convertir vía la herramienta de actualización al mismo tiempo?

A. Con la última versión 2.01 de la herramienta, puede actualizar un máximo de seis en un momento AP.



Q. He convertido mi AP al protocolo ligero AP (LWAPP), pero el AP no se registra con el controlador. Consigo el mensaje "Unir a-petición del LWAPP no incluyo el certificado válido en CERTIFICATE_PAYLOAD del AP." ¿Qué causa este problema?

A. Este error significa que los certificados digitales X.509 son inválidos. Puede ser que sea que usted está experimentando el Id. de bug Cisco CSCsd42296 (clientes registrados solamente). La solución alternativa para este problema es reajustar los AP a los valores predeterminados de fábrica.

Otra posibilidad es que el certificado autofirmado (SSC) no está registrado en el WLC. El

Agregado manual de SSC en el controlador puede ser necesario. Consulte Agregado manual del certificado autofirmado al controlador para los AP de los LWAPP-Convertir para el procedimiento.

Q. ¿Puedo configurar un Software basado AP del Cisco IOS como un Workgroup Bridge y socio con el protocolo ligero AP (LWAPP) - los AP basados?

A. Usted puede configurar un Punto de acceso para actuar como Workgroup Bridge de modo que pueda proporcionar la conectividad de red inalámbrica a un Lightweight Access Point en nombre de los clientes que son conectados por los Ethernetes con el Punto de acceso del Workgroup Bridge. Cuando usted configura el Punto de acceso para actuar como Workgroup Bridge y para conectar con una red unificada Cisco, puede proporcionar la conectividad de red inalámbrica a los clientes atados con alambre que son conectados por los Ethernetes con el Punto de acceso del Workgroup Bridge. Por ejemplo, si usted necesita proporcionar la conectividad de red inalámbrica para un grupo de dispositivos atados con alambre, usted puede conectarse los dispositivos a un concentrador o a un Switch, conecte el hub o switch con el puerto Ethernet del punto de acceso, y configure el Punto de acceso como Workgroup Bridge.

Los Bridges del documento en un ejemplo de la configuración de red del Cisco Unified Wireless proporcionan un ejemplo de configuración.

Q. ¿Puede un cliente inalámbrico trasladarse entre los AP LWAPP y los AP autónomos?

A. No, NO se soporta el traslado entre los AP autónomos y LAP. El motivo es que, cuando está conectado con los AP LWAPP, el tráfico pasa a través de un túnel LWAPP. Puesto que no hay túnel de movilidad entre el controlador del Wireless LAN y los AP autónomos, el roaming no funciona.

Q. ¿Qué opciones de la antena están disponibles con los diversos modelos de los LAPs del Cisco Aironet 1000 Series?

A. El recinto del LAP de las 1000 Series contiene:

- Un IEEE 802.11a o una antena de radio 802.11b/g
- Cuatro antenas internas de ganancia alta (dos 802.11a y dos 802.11b/g)

Usted puede habilitar o inhabilitar estas antenas independientemente para producir un 180-grado sectorizado o la área de cobertura omnidireccional 360 grados. Algunos de los LAPs de las 1000 Series pueden también utilizar las antenas externas. Los LAPs de las 1000 Series vienen en tres modelos:

- 1010 LAP
- 1020 LAP
- 1030 LAP

Éstas son las opciones disponibles de la antena:

- 1010 LAP:Cuatro antenas internas de alta gananciaNingún adaptador de antena externa
- 1020 LAP:Cuatro antenas internas de alta gananciaUn adaptador de la antena externa 5-GHzDos adaptadores de la antena externa 2.4-GHz
- 1030 LAP (LAP de borde remoto):Cuatro antenas internas de alta gananciaUn adaptador de

la antena externa 5-GHzDos adaptadores de la antena externa 2.4-GHz

A. External-Antenna Model B. Internal-Antenna Model

Nota: Los LAPs de las 1000 Series deben utilizar antenas externas o internas de fábrica por la para evitar una violación de los requisitos FCC y evitar un vacío de las autoridades del usuario para actuar el equipo.

Q. ¿Qué Opción de energía está disponible para los LAPs del Cisco Aironet 1000 Series?

A. El LAP de las 1000 Series del Aironet puede recibir el poder de una fuente de alimentación externa 110 a 220 VAC-to-48 VDC o del poder sobre el equipo de los Ethernet. La fuente de alimentación externa (AIR-PWR-1000) conecta adentro a 110 seguros a través de la salida eléctrica de 220 VAC. El convertidor produce los 48 requeridos VDC para hacer salir para las 1000 Series LAP. La salida del convertidor alimenta en el lado de las 1000 Series LAP a través de un conector de 48 VDC.

Nota: Puede suministrar el suministro de energía externo AIR-PWR-1000 con los cables de alimentación de salida eléctrica country-specific . Entra en contacto Cisco cuando ordenas para recibir el cable de alimentación eléctrica correcto.

Q. ¿Puede el Telnet/SSH I en un punto de acceso basado LWAPP?

A. En la versión 5.0 del Wireless LAN Controller y posterior, el controlador soporta el uso de los protocolos telnet o del Secure Shell (SSH) de resolver problemas los Lightweight Access Point. Usted puede utilizar estos protocolos para hacer hacer el debug de más fácil, especialmente cuando el punto de acceso no puede conectar con el controlador. Puede configurar Telnet y el

soporte SSH solamente a través del controlador CLI.

Para habilitar el telnet o la conectividad SSH en un punto de acceso, use el comando **config ap {telnet | ssh}** . El punto de acceso de las livianas de Cisco se asocia a este Controlador de LAN de la Red Inalámbrica Cisco para toda la operación de la red y en caso de reajuste de hardware.

```
config ap {telnet | ssh} {enable | disable} Cisco_AP
```

Ejemplos

```
> config ap telnet enable cisco_ap1
> config ap telnet disable cisco_ap1
> config ap ssh enable cisco_ap2
> config ap ssh disable cisco_ap2
```

Q. Cómo configurar las credenciales globales para los puntos de acceso. ¿Cuáles son el nombre de usuario predeterminado y la contraseña en la versión 5.0?

A. Los puntos de acceso del Cisco IOS se envían de la fábrica con la palabra Cisco como la contraseña de habilitación predeterminada. Esta contraseña permite que los usuarios registren en el modo sin privilegios y que ejecuten la demostración y que hagan el debug de los comandos, que plantea una amenaza de seguridad. El contraseña de habilitación predeterminado se debe cambiar para prevenir el acceso no autorizado y habilitar a los usuarios para ejecutar los comandos de configuración del puerto de la consola del punto de acceso.

En el software del controlador antes de la versión 5.0, puede establecer la contraseña de habilitación del punto de acceso solamente para los puntos de acceso que están conectados actualmente con el controlador. En el Software Release 5.0 del controlador, puede fijar un nombre de usuario global, una contraseña, y un contraseña de habilitación globales del uso que todos los puntos de acceso hereden mientras que se unen a el controlador. Esto incluye todos los puntos de acceso que se unan a actualmente al controlador y cualquiera que se une a en el futuro. Si lo desea, puede reemplazar las credenciales globales y asignar un nombre de usuario único, una contraseña, y una contraseña de habilitación para un punto de acceso específico.

Para la información sobre cómo configurar las credenciales globales del AP, consulte configurar las credenciales globales para los puntos de acceso.

Q. Tengo controlador del Wireless LAN (WLC) 2006 y el Access Point (AP) 1242 con la versión de firmware 3.2.78.0. Tengo problemas con los puntos de acceso que conectan con ella y recibo estos mensajes de error: “lwapp_clinet_error; not receive read response(3). Lwapp_image_broc; unable to open TAR file"

A. AP 1242s es protocolo convertido del Lightweight Access Point (LWAPP) AP. Una vez que los convierte e intenta utilizar, intentan buscar el controlador para unirse a él. Si los AP no encuentran el controlador, después este tipo de mensaje aparece en la consola. Pero en este caso el controlador tiene una versión de firmware de 3.2.78.0 que no sea compatible trabajar con los AP actualizados. Necesitas tener versión de firmware 3.2.116.21 para trabajar con los AP actualizados. Una vez que se actualiza el firmware del controlador, estos AP se unen a el controlador y comienzan a funcionar.

Q. Los clientes muestran un dirección MAC de 00:17:0f:37:65:c4 cuando está

asociado a un punto de acceso, pero el punto de acceso muestra que que es tiene un dirección MAC de radio bajo de 00:17:0f:37:65:c0. . ¿Por qué el cliente muestra un diverso MAC que el punto de acceso? ¿Hay una manera de determinar que el dirección MAC el dispositivo registre si tengo dos puntos de acceso con los dirección MACes muy cercanos?

A. Si miras un modo del punto de acceso detalladamente, puede ver que tiene un dirección MAC de radio bajo y un dirección MAC del FastEthernet. Además, ése es el dirección MAC de radio bajo que cambia con el WLAN. El cliente ve realmente el BSSID bajo la forma de dirección MAC.

Q. Tengo una red inalámbrica existente (AP autónomos) con un punto de acceso que se configure como repetidor. Esta red debe ser emigrada a una red inalámbrica del LWAPP. ¿Puedo utilizar el LWAPP AP como repetidores?

A. Los LWAPP AP deben unirse a un controlador, y no soportan a un modo repetidor puesto que todos tienen que tener cierta conectividad al controlador primero. Cisco AP autónomos se puede configurar como repetidores, pero debido a la reducción en el ancho de banda efectivo disponible para terminar a los clientes, los repetidores no son lo más altamente posible la configuración recomendada. Mientras que cualquier Cisco Aironet AP o el modelo del LAP se puede utilizar en el LWAPP o el modo autónomo, para realizar ese cambio, se requiere una nueva imagen del software. Esto es determinado complejo cuando va de autónomo al LWAPP, tan directamente, no, un AIR-LAP1232AG-A-K9 no soporta nativo al modo repetidor. Podría ser cargada con el software autónomo y ser hecha para soportar al modo repetidor, pero ése implicaría un Cambio de software y una configuración separada.

Q. ¿Cuántos AP puede el WLCs soportar?

A. El número de AP soportados por el WLC depende del número de modelo:

- **2106** — Un WLC independiente que soporta hasta 6 AP con 8 interfaces Fast Ethernet.
- **4402** — Un WLC independiente que soporta 12, 25, o 50 AP.
- **4404** — Un WLC independiente que soporta 100 AP.
- **5500** — Un WLC independiente que soporta 12, 25, 50,100, o 250 Puntos de acceso para los Servicios inalámbricos del negocio crítico en las ubicaciones de todos los tamaños.
- **WLCM** — Un módulo del WLC que se diseña específicamente para la serie del router del servicio integrado de Cisco (ISR). Está actualmente disponible en una versión de 6, de 8 o de 12 AP.
- **WS-C3750G** — UN WLC que soporta 25 o 50 AP que viene integrado con el Catalyst 3750 Switch. Las conexiones de backplane WLC aparecen como accesos de Ethernet 2-Gig que se puedan configurar por separado como trunks del dot1q para proporcionar la conexión en los 3750. O los puertos del carruaje pueden ser link agregado para proporcionar una sola conexión EtherChannel a los 3750. Porque el WLC se integra directamente, tiene acceso a todas las características avanzadas de los Ruteo y Switching disponibles en el switch para pila 3750. Este WLC es ideal para las oficinas o los edificios medianos. La versión `50 AP puede escalar hasta 200 AP cuando cuatro 3750s se empilan juntos como switch virtual.
- **WiSM** — Un módulo del WLC que se diseña específicamente para la serie del Catalyst 6500 Switch de Cisco. Soporta hasta 300 AP por el módulo. Dependiendo de la plataforma 6500, WISMs múltiple se puede instalar para ofrecer las capacidades significativas del

escalamiento. El WiSM aparece como sola interfaz del link agregada en los 6500 que se pueden configurar como trunk dot1 para proporcionar la conexión en los 6500 backplane. Este módulo es ideal para los edificios grandes o los campus.

Q. ¿Cuál es el número máximo de asociaciones del cliente que los Puntos de acceso puedan apoyar?

A. El número máximo de asociaciones del cliente que los Puntos de acceso puedan apoyar depende de estos factores:

- El número máximo de asociaciones del cliente diferencia para el peso ligero y los Puntos de acceso IOS de Autonmous.
- Pudo haber un límite por la radio y un límite total por el AP.
- Hardware AP (16-MB AP tienen un límite más bajo que el 32-MB y los AP más altos).

Para los detalles completos en los límites de la asociación del cliente, refiera a la sección de los *límites de la asociación del cliente de la* guía de configuración del controlador LAN de la tecnología inalámbrica de Cisco, la versión 7.0.

Q. ¿Los 1252 AP soporta el bridging?

A. Sí, el Bridging Mode se soporta en las 1252 Series AP.

Q. ¿La infraestructura ligera del protocolo AP (LWAPP) soporta el PPP a través de Ethernet (PPPoE) (PC cliente a un servidor PPPoE)?

A. No, la infraestructura del LWAPP no soporta el PPPoE. La razón es que el Ethertype del PPPoE está caído en el controlador.

Q. ¿Cómo puedo reajustar manualmente el LAP del Cisco Aironet 1000 Series?

A. Usted puede reajustar el AP a los valores predeterminados de fábrica a través del controlador del Wireless LAN (WLAN) (WLC). Para la restauración, el LAP se debe registrar al WLC.

Complete estos pasos:

1. Desde WLC GUI, haga clic en **Wireless**. La pestaña Wireless proporciona acceso a la configuración de red inalámbrica de Cisco WLAN Solution.
2. Elija **Access Points > Cisco APs**, y luego haga clic en **Detalles** para navegar a la ventana para los AP específicos.
3. Haga clic en **Eliminar Config.** en la parte inferior de esta ventana. Esto borra la configuración en el LAP y la reajusta a los valores predeterminados de fábrica.

Para reajustar los LAPs a los valores predeterminados de fábrica con el uso del command-line interface (CLI), publica el comando **claro del AP-nombre del AP-config del** WLC CLI.

Q. ¿Dónde puedo conseguir más información sobre los LAPs del Cisco Aironet 1000 Series?

A. Consulte los Cisco 1000 Series Lightweight Access Point - Q&A. El documento proporciona las

respuestas a muchas preguntas que se relacionen con los LAPs de las 1000 Series.

Q. ¿Qué dispositivos de Cisco soportan el modo ligero de la capa 2 del protocolo AP (LWAPP)?

A. El modo de la capa 2 del LWAPP se soporta solamente en estos dispositivos de Cisco:

- controlador del Wireless LAN de las Cisco 4100 Series (WLC)
- WLC de las Cisco 4400 Series
- LAP del Cisco Aironet 1000 Series

Q. Entiendo que los LAPs de Cisco utilizan una cadena del identificador de clase del vendedor (VCI) con la opción DHCP 43 para la detección del controlador. ¿Cuál es el valor de la cadena del VCI para los LAPs de Cisco?

A. El Cisco Aironet 1000 Series AP utiliza un formato de la cadena para la opción DHCP 43, mientras que el otro Aironet AP utiliza el tipo, longitud, formato del valor (TLV) para la opción DHCP 43. Debe programar los servidores DHCP para volver la opción en base de la cadena del VCI del DHCP AP (opción DHCP 60). Este vector proporciona los valores de la cadena del VCI para los diversos LAPs:

Access Point	Vendor Class Identifier (VCI)
Cisco Aironet 1000 series	Airespace.AP1200
Cisco Aironet 1100 series	Cisco AP c1100
Cisco Aironet 1130 series	Cisco AP c1130
Cisco Aironet 1200 series	Cisco AP c1200
Cisco Aironet 1240 series	Cisco AP c1240
Cisco Aironet 1300 series	Cisco AP c1300
Cisco Aironet 1500 series	Cisco AP c1500[1]
	Cisco AP.OAP1500[2]
	Cisco AP.LAP1505[3]
	Cisco AP.LAP1510[4]
	Airespace.AP1200[5]
Cisco 3201 Lightweight Access Point	Cisco AP C3201WMIC

Q. ¿Cuál es la significación de los valores del bloque del Type Length Value (TLV) en cuanto a la opción DHCP 43? ¿Cómo se calcula el valor TLV?

A. La opción DHCP 43 se puede habilitar en el servidor DHCP del router del Cisco IOS usando este comando:

Option 43 hex <*string*>

La cadena hexadecimal en este comando es ensamblada concatenando los valores TLV para el submarino option de la opción 43.

Tipo + longitud + valor

- **El tipo** es siempre el código de submarino option 0xf1.
- **La longitud** es el número de los tiempos 4 de los dirección IP de administración del controlador en el hexadecimal.
- **El valor** es el dirección IP del controlador enumerado secuencialmente en el hexadecimal.

Por ejemplo, asume que hay dos controladores con los dirección IPes 10.126.126.2 y 10.127.127.2 de la interfaz de administración:

- El tipo es 0xf1.
- La longitud es 2 * 4 = 8 = 0x08.
- Las direcciones IP traducen a 0a7e7e02 (10.126.126.2) y 0a7f7f02 (10.127.127.2).
- Ensamblar la cadena entonces rinde f1080a7e7e020a7f7f02. El comando IOS entonces agregado al alcance de DHCP es:
  `option 43 hex f1080a7e7e020a7f7f02`

Q. ¿Hace el balanceo de carga del soporte AP del controlador del Wireless LAN (WLC)?

A. Sí, puede hacer el balanceo de carga AP en un WLC. Consulte Troubleshooting FAQ del controlador del Wireless LAN (WLC) para más información.

Q. ¿Cómo configuro el failover del controlador del Wireless LAN (WLC) para los LAPs?

A. Consulte Failover del Controlador de WLAN para el ejemplo de configuración de los Lightweight Access Point para los detalles en cómo configurar el WLC Failover.

Q. ¿Cómo puedo inhabilitar el botón de reinicio en los AP después de la conversión del modo autónomo al modo ligero?

A. Usted puede invalidar el botón de reinicio en los AP que has convertido al modo ligero. El botón de reinicio se etiqueta “MODE” en el exterior del AP. Utilice este comando para inhabilitar o habilitar el botón de reinicio en uno o todos los AP convertidos asociados a un controlador:

`config ap reset-button {enable | disable}` {*`ap-name`* **`| all}`**

El botón de reinicio en los AP convertidos se habilita de forma predeterminada.

Q. ¿Puedo tener un AP apto para un Lightweight AP Protocol (LWAPP) conectado a través de un link de WAN desde el controlador inalámbrico de LAN (WLC)? Si es así, ¿cómo es que trabaja?

A. Sí, algunos LAP soportan la función llamada Remote-Edge AP (REAP). Con esta función, puede tener un LAP a través de un link de WAN desde el WLC con el que se conecta el LAP. El modo REAP habilita un LAP para residir a través de un link de WAN y aún poder comunicarse con el WLC y proporcionar las funciones de un LAP regular. Consulte Ejemplo de Configuración de Remote-Edge AP (REAP) con Lightweith APs y Wireless LAN Controllers (WLCs) para un ejemplo detallado de esta configuración.

Nota: El modo REAP se soporta solamente en el Cisco Aironet 1030 LAPs en este momento. Las funcionalidades de REAP serán incluidas en un rango más amplio de los LAPs en el futuro.

Q. ¿Sin embargo tenemos las mismas restricciones WAN en el modo monitor AP que hacemos con AP y H-REAP regulares AP? ¿Es decir, requerimos un 100ms o un mejor RTD entre el controlador y un modo monitor AP?

A. No, el modo monitor AP no tiene la restricción de 100 ms porque no hay asociación del cliente, que es la razón de la restricción. La limitación del tiempo de espera de 100 ms fue creada fuera de variado, y de a menudo riguroso, los requisitos de la autorización del cliente, que es porqué ambo el modo local y H-REAP AP tienen limitaciones idénticas del tiempo de espera. Obviamente, el modo monitor AP no tiene las mismas limitaciones del cliente.

Q. Mi versión del WLC es 3.2. Se configura para Layer 3 Lightweight Access Point Protocol (LWAPP). El MTU para la red entre este WLC y mi Lightweight Access Point (LAP) se configura como 900 bytes. Mi LWAPP AP no puede unirse a este WLC. ¿Cuál puede ser la razón de esto?

A. El MTU configurado en su escenario es 900 bytes. Pero una solicitud de unión al LWAPP es más grande que 1500 bytes. Así pues, aquí el LWAPP requiere un fragmento de la solicitud de unión al LWAPP. La lógica para todo el LWAPP AP es que los tamaños del primer fragmento son 1500 bytes (incluyen el IP y el encabezado UDP) y el segundo fragmento es 54 bytes (incluye el IP y el encabezado UDP). Si la red entre el LWAPP AP y el WLC tiene un tamaño de MTU menor de 1500 (tal como VPN, GRE, MPLS, y así sucesivamente) como en su caso, el WLC no puede manejar la solicitud de unión al LWAPP. Por lo tanto, el LWAPP no puede unirse a el controlador.

Actualice su controlador a la versión 4.0 para manejar esta situación. Esta versión puede manejar los fragmentos de la capa 3. Consulte Cisco bug ID CSCsd94967 (clientes registrados solamente) para más información sobre este problema.

Q. Tengo un WLC que conseguí de Singapur. Con este WLC, mi intención era hacer que una oficina remota se conectase (REAP) de forma inalámbrica. Tengo oficinas en otros países. Sin embargo, recibo los mensajes de error del dominio controlador del WLC de Singapur. ¿Hay una manera de forzar el WLC para validar el (APS) de los puntos de acceso con diversos dominios controladores? El mensaje de error que recibo es: El "AP "AP_NAME" no puede asociarse. **El dominio controlador configurado en él "- R" no corresponde con el código del país 'SG del controlador "A.B.C.D" - Singapur"**

A. El WLC soporta solamente un dominio controlador. Por lo tanto, un WLC que utiliza el dominio controlador - A se puede utilizar solamente con los AP que utilizan el dominio controlador - A (y así sucesivamente). En este caso, el WLC se fija a - el SG para Singapur, así que él soporta solamente los AP en el dominio controlador de Singapur.

Cuando compras los AP y el WLCs, asegúrese de que compartan el mismo dominio controlador. Solamente entonces los AP podrán registrarse con el WLC.

Soporte para códigos múltiples de país - Con la versión 4.1.171.0 y posteriores del WLC, se introduce el soporte para códigos múltiples de país. Con la versión 4.1.171.0 y posteriores, puede configurar hasta 20 códigos de país por controlador. El soporte para códigos múltiples de país lo

habilita para manejar los puntos de acceso en varios países desde un solo controlador. Esta función no se soporta para el uso con puntos de acceso de la malla del Cisco Aironet.

Q. ¿Cuáles son los diversos modos en los cuales un Lightweight Access Point (LAP) puede actuar?

A. Un LAP puede actuar en cualquiera de estos modos:

- **Modo local** - Éste es el modo de operación predeterminado. Cuando un REVESTIMIENTO se pone en el modo local, el AP transmitirá en el canal normalmente asignado. Sin embargo, el AP también monitorea el resto de los canales en la banda durante 180 segundos para analizar cada uno de los otros canales para 60ms durante el tiempo del NON-transmitir. Durante este tiempo, el AP realiza las medidas del suelo del ruido, interferencia de las medidas, y explora para los eventos IDS.
- **COSECHE el modo** — El modo remoto del Punto de acceso del borde (COSECHE) permite a un REVESTIMIENTO para residir a través de un link PÁLIDO y todavía para poder comunicar con el WLC y proporcionar las funciones de un REVESTIMIENTO regular. COSECHE el modo se soporta solamente en los 1030 revestimientos.
- **Modo H-REAP** — H-REAP es una solución de red inalámbrica para las implementaciones de la sucursal y de la oficina remota. Clientes de los permisos H-REAP para configurar y para controlar el (APS) de los Puntos de acceso en una bifurcación o una oficina remota de la oficina corporativa a través de un link PÁLIDO sin la necesidad de desplegar un regulador en cada oficina. H-Cosechar puede conmutar el tráfico de datos del cliente localmente y realizar la autenticación de cliente localmente cuando la conexión al regulador se pierde. Cuando están conectados con el controlador, los H-REAPs también pueden tunelizar de nuevo el tráfico hacia el controlador.
- **Modo monitor** - El modo monitor es una característica diseñada para permitir especificó el LWAPP-habilitar AP para excluirse de manejar el tráfico de datos entre los clientes y la infraestructura. En lugar de otro actúan como sensores dedicados para los servicios basados ubicación (LB), la detección rogue del punto de acceso, y la detección de intrusos (ID). Cuando los AP están en el modo monitor no pueden servir los clientes y continuamente el ciclo a través de todos los canales configurados que escuchan cada canal el ms aproximadamente 60.**Nota:** De la versión 5.0 del controlador, LWAPPs se puede también configurar en el modo monitor optimizado ubicación (LOMM), que optimiza el cálculo el monitorear y de la ubicación de los Tags RFID. Para más información sobre este modo, consulte la versión 5.0 del software de red del Cisco Unified Wireless.**Nota:** Con la versión 5.2 del regulador, la sección **optimizada ubicación del modo monitor (LOMM)** se ha retitulado **que seguía la optimización**, y el **LOMM habilitó la** casilla desplegable se ha retitulado **optimización de seguimiento del permiso**.**Nota:** Para más información sobre cómo configurar el seguimiento de la optimización, lea el RFID óptimo que sigue en la sección de los Puntos de acceso.
- **Elimina las plantas débiles el modo del detector** - LAP que actúa en el monitor rogue del modo del detector al rogue AP. No transmiten ni contienen los AP rogue. La idea es de que el detector rogue pueda ver todos los VLAN en la red puesto que los AP rogue se pueden conectar con las VLAN en la red (así la conectamos con un puerto troncal). El switch envía todas las listas del dirección MAC del rogue AP/Client al detector rogue (RD). El RD entonces remite ésos hasta el WLC para comparar con los MAC de los clientes que el WLC AP ha oído sobre el aire. Si los MAC corresponden con, después el WLC sabe que el rogue AP con quien

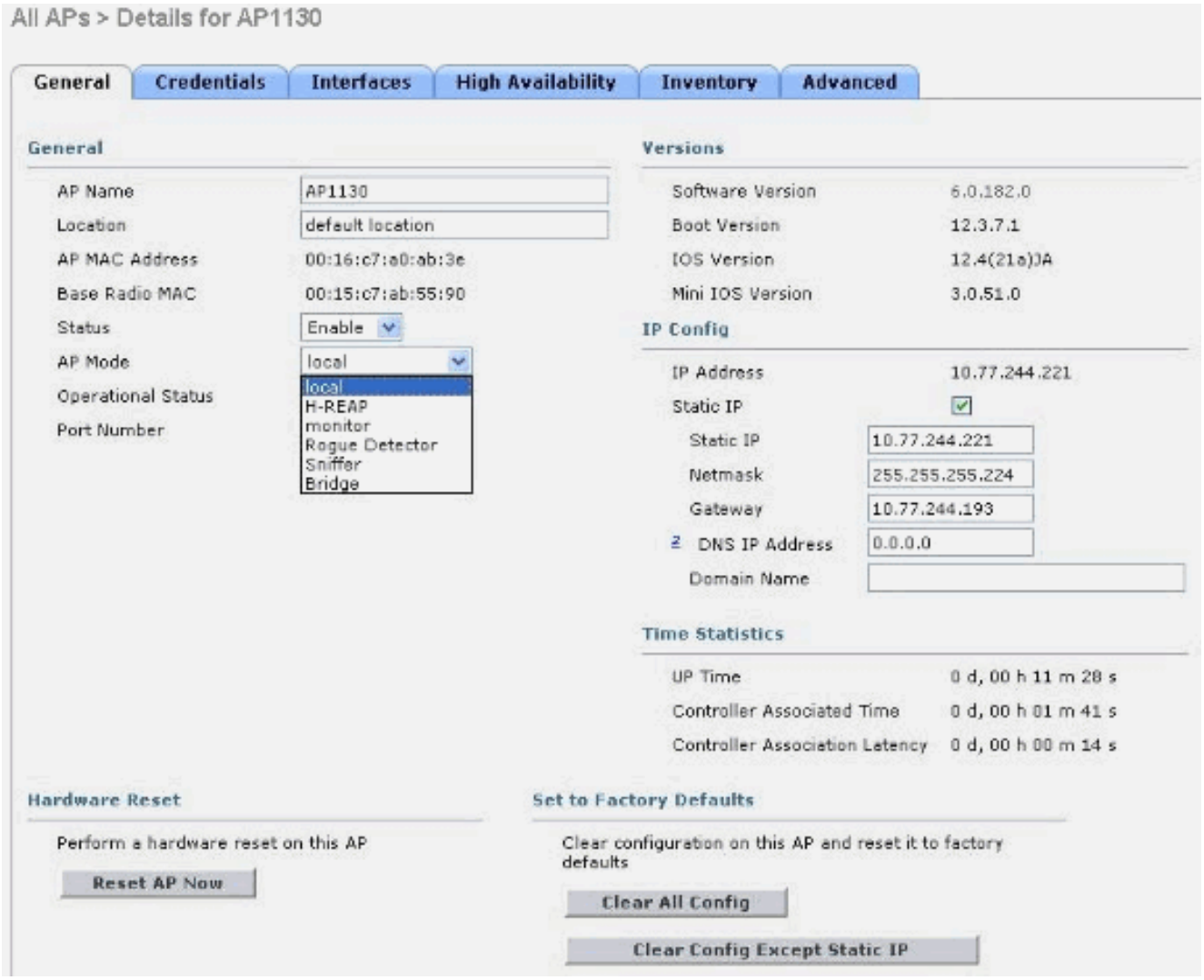
esos clientes están conectados está en la red alámbrica.

- **Modo del sabueso** - Un LWAPP que actúa en el modo del sniffer funciona como un sniffer y captura y remite todos los paquetes en un canal particular a una máquina remota que ejecute Airopeek. Estos paquetes contienen la información sobre el grupo fecha/hora, potencia de la señal, los tamaños de paquetes y así sucesivamente. La característica del sniffer puede ser habilitada solamente si ejecutas Airopeek, que es un software de tercera persona del analizador de red que soporta decodificar de los paquetes de datos.
- **Modo Bridge** — Utilizan al modo Bridge cuando los Puntos de acceso se ponen en un entorno de la malla y se utilizan para interligar entre uno a.

Q. ¿Cómo cambio el modo en un Lightweight Access Point?

A. Para cambiar el modo de un Lightweight Access Point, complete estos pasos.

1. Del WLC GUI, elija la **Tecnología inalámbrica > los Puntos de acceso > todos los AP**, y seleccione el AP para el cual el modo necesita ser cambiado de la lista de AP registradoes.
2. **El todo el los AP > los detalles para la** página **AP** aparece. En la **ficha general de** esta página, seleccione **modo AP del** menú desplegable, como se muestra:



Q. He instalado nuevamente los puntos de acceso LAP-1131AG que se han preparado a un controlador determinado. Mi versión del controlador es 4.0.155.5.

Cuando los arranco con el mismo controlador del Wireless LAN (WLC) a el cual se preparan, eventual dan vuelta verde claro. Según la documentación, esto verde claro en el LED de estado significa que están conectados con el WLC. Pero no podría encontrar este punto de acceso en la lista del punto de acceso del WLC. ¿Por qué ocurre esto? ¿Hizo el protocolo del Lightweight Access Point (LWAPP) llega a ser asociado?

A. Si el punto de acceso se prepara a un WLC en la capa 3 pero no puede conseguir un dirección IP durante el lanzamiento, después el LED de estado de las vueltas del WLC a verde claro y no entra la búsqueda y reanuda la secuencia hasta que consiga un dirección IP del DHCP.

Así pues, en tales escenarios, el verde de torneado del LED de estado no indica que el LWAPP está registrado con el controlador. Después de que los puntos de acceso puedan conseguir sus DHCP Address, buscan para el WLC y si no encontraron, pasan con un proceso de la reinicialización y proceden según lo esperado. Hay un bug asociado a esto.

Consulte ID de bug Cisco CSCsf10580 (clientes registrados solamente) para más información.

Q. ¿Qué los LED en el REVESTIMIENTO indican?

A. Esto es un link a un vídeo corto que explique cómo interpretar el LED en un 1130AG AP ligero:

Interpretando el REVESTIMIENTO LED - LAP1130

Q. ¿Cuál es la diferencia entre los puntos de acceso del tejado (RAPs) y los puntos de acceso del Poste-top (PAP) como modos de puntos de acceso ligeros de la malla (correspondencias)?

A. Éstos son los modos que las correspondencias al aire libre pueden actuar como parte de la red de interconexión. La solución de interconexión de redes de la malla, que es parte de la solución de red del Cisco Unified Wireless, habilita dos o más correspondencias ligeras del Cisco Aironet para comunicar con uno a sobre uno o más saltos sin hilos para unirse a los LAN múltiples o para ampliar la cobertura de red inalámbrica 802.11b.

Estos puntos de acceso se utilizan como parte de la red de interconexión y actúan en dos modos:

1. RAP
2. PAP

RAP — Los mapas de Cisco que actúan en el modo del RAP son el nodo primario a cualquier bridging o red de interconexión y conectan un Bridge o una red de interconexión con la red alámbrica. Por lo tanto, puede solamente haber un RAP para cualquier segmento interligado o de la red de interconexión. En una red de interconexión, las correspondencias de Cisco se configuran, se monitorean, y se actúan desde y a través de cualquier Controlador de WLAN de Cisco (WLC) desplegado. Cualquier MAP que tiene la conexión alámbrica al WLC asume el papel del RAP. Este RAP utiliza la interfaz inalámbrica del regreso para comunicar con los PAP vecinos.

PAP — Los mapas de Cisco que actúan en el modo PAP no tienen ninguna conexión alámbrica a un WLC de Cisco. Pueden ser los clientes totalmente sin hilos y soporte que comunican con otros PAP o RAPs, o pueden ser utilizadas para conectar con los dispositivos periféricos o una red alámbrica. El acceso de Ethernet está invalidado por abandono por las razones de seguridad,

pero debe habilitarlo para los PAP.

Consulte la sección Zero Touch Configuration de la Cisco Mesh Networking Solution Deployment Guide para más información sobre cómo un MAP asume el papel del RAP y del PAP.

Q. ¿Cómo interpretas el patrón de radiación de las antenas del Lightweight Access Point de las 1000 Series (LAP)?

A. Los diagramas del acimut están generalmente con el dispositivo/la antena en la orientación de funcionamiento normal (la vertical, vuelve a llenar, en el centro del diagrama para el omni; horizontal, soporte en el centro, dirección delantera hacia el "0" en el diagrama). El lado A es muy probablemente delantero y representado en las 0 marcas para el acimut, y la marca 90 para la elevación. Lado B se representa en 180 la marca para el acimut, y 270 para la elevación. El modelo no cambia en el libre-espacio si se invierte la unidad. Pero las superficies inmediatas pueden causar la reflexión/atenuación y pueden alterar el modelo. Los objetos metálicos cerca de los radiadores (dentro de ~2 longitudes de onda o tan) pueden también torcer el modelo perceptiblemente. Antena Aironet de Cisco la guía de referencia tiene más información. Las antenas de las 1000 Series se explican en la sección más más reciente del documento.

Q. ¿Podemos restringir qué AP se unen a un controlador? Veo la paginación de las políticas SECURITY/AAA/AP, donde puede autorizar los AP contra el AAA o el certificado. ¿Yo pueden agregar un AP a la lista de la autorización, pero estas cosas restringen solamente mi lista de la autorización de AP para unirse a el controlador?

A. No, la manija AP de los controladores en una primera viene, primero sirve la base. Usted puede jugar posiblemente con los campos primarios, secundarios, y terciarios para aumentar las probabilidades en las conexiones AP a tu preferencia.

Q. ¿Con el LWAPP, es posible determinar los SSID que un AP tiene sobre una base individual AP? ¿Qué se requiere poder tener AP específicos en una zona que utilicen un SSID único, y todo el resto que utilicen otro conjunto de los SSID?

A. Con la opción de la invalidación WLAN, puede elegir que los SSID un AP ofrecen. Los controladores soportan solamente hasta 16 SSID cada uno, así que puede elegir solamente entre de los 16 soportados. Esto se hace sobre una base del por-AP.

Q. Cuando habilito algún LWAPP ordena en mi LAP, yo consigue un error que diga que el comando está inhabilitado. ¿Por qué ocurre esto?

```
AccessPoint#clear lwapp ap controller ip address ERROR!!! Command is disabled.
```

A. Una vez que tu AP se ha unido a con éxito un controlador, los comandos del LWAPP están inhabilitados. Para habilitar los comandos del LWAPP otra vez, debe fijar el nombre de usuario/la contraseña del AP del controlador CLI con el comando del **<pwd> <cisco-ap>/all de la contraseña del <name> del nombre de usuario ap de los config**. Una vez que se hace eso, puede hacer un privado-**config claro del lwapp** en el AP CLI para permitir que reedites manualmente los comandos de configuración del LWAPP AP.

Nota: Si usted está funcionando con la versión 5.0 y posterior del WLC, utilice este comando de fijar el nombre de usuario y contraseña en el AP:

config ap mgmtuser add username *AP_username* **password** *AP_password* **secret** *secret* **{all | Cisco_AP}**

Q. ¿Cuándo dos AP son en el mismo canal y pueden verse, cuál son las implicaciones (para la producción de itinerancia, el etc.) sobre el uso de cuatro canales en vez de tres? ¿Cómo los AP reaccionan en tal situación y cómo un cliente reacciona?

A. Si los AP están en el mismo canal o no, no afecta determinado al cliente que vaga por. Qué importa es suficiente coincidencia de la célula tales que los clientes pueden hacer las transiciones fluidas de la área de cobertura de un AP al siguiente. El intento de un movimiento de un diseño del tres-canal a un diseño del cuatro-canal es aumentar la flexibilidad del diseño (debido a canal del suplemento del `'). Este acercamiento es miope porque, mientras que agregas un dígito binario de la flexibilidad de despliegue (puesto que tienes otro canal), aumentas realmente la cantidad de interferencia del cocanal. Lo que obtiene en la flexibilidad del diseño con el enfoque de cuatro canales, lo pierde en la interferencia agregada del cocanal. Lo importante: no utilices un diseño del cuatro-canal.

Q. ¿Podemos controlar cuando los clientes vagan por? ¿Puede nosotros deja al cliente vagar por basado solamente en la potencia de la señal sobre una base individual AP y para todos los adaptadores del cliente?

A. Hoy, la itinerancia es siempre una función del cliente, y la opción para vagar por o no se implementa diferentemente en los diversos clientes. La itinerancia dirigida es una parte de CCX, pero es una característica opcional y no se utiliza hoy.

Q. ¿Hay requisitos o recomendaciones específicos para una conexión WAN que se implemente entre REAP/HREAP AP en el sitio remoto y el WLC en el sitio principal?

A. Éstos son algunos de los factores principales que se considerarán para la conexión PÁLIDA:

- Asegúrese de que el ancho de banda de la conexión PÁLIDA sea por lo menos 128kbps.
- Asegúrese de que el tiempo de espera o el retardo de ida y vuelta entre los dos sitios a través del link WAN no sea más que 300ms porque más que un retardo 300ms pueden crear los problemas de autenticación al cliente, especialmente cuando se implementa la autenticación central.

Q. Tuve un apagón de red por algunas horas, lo que hizo que los LAPs perdieran la comunicación con los WLCs. Después que la red volvió a funcionar, los LAPs tomaron la dirección IP del servidor DHCP, por más que estos APs etuvieran configurados con un dirección IP estática. En el "show ap config general <ap-name>" aparece como "Fallback IP Address." ¿Por qué ocurre esto?

A. El LAP intenta hasta 20 veces asociarse al WLC con los mensajes de la detección de LWAPP. En caso de que no pueda conectarse, intenta obtener una nueva dirección IP con el DHCP. Si el LAP puede conseguir una dirección IP del servidor DHCP, esta dirección IP es la activa, y la dirección IP asignada se utiliza estáticamente para el retraso. La idea detrás de esto es que en caso de que los LAPs se muevan a un diverso VLAN (por ejemplo, a otro edificio), pueden extraer un dirección IP y unirse a un WLC. Este comportamiento se explica en el bug CSCse66714. Debe

actualizar el WLC a la versión de software 4.0.206.0.

Q. ¿Es obligatorio configurar un nombre de Grupo de Bridge para una red de interconexión?

A. Un nombre de Grupo de Bridge (BGN) se puede utilizar para agrupar lógicamente los AP en la malla. Aunque por abandono, los AP vengan con un valor nulo BGN permitir la asociación, recomendamos que fijas un BGN. Usted puede realizar esta configuración cambia con el CLI o el GUI con este comando:

```
config ap bridgegroupname set Bridge Group Name Cisco AP
```

Nota: Los BGN pueden ser máximo de diez los caracteres. Si usted ingresa más de 10 caracteres en el BGN colocan en la página de la Configuración de punto de acceso de la malla del regulador GUI, genera un mensaje de error. Un error también aparece cuando usted configura este parámetro con el comando CLI o el WCS **determinado** (CSCsk64812) de **Cisco_MAP del nombre de grupo del bridgegroupname ap de los config**.

Cuando configuras el BGN en una red en funcionamiento, asegúrese de que configures del MAP más lejano y trabaja tu manera de nuevo al RAP. Esto es muy importante porque puede trenzar un MAP del niño que no pueda asociarse a un padre, que puede tener un BGN actualizado. Utiliza diversos BGN para agrupar lógicamente diversas partes de tu red. Esto es útil en las situaciones donde haces que los rap dentro de la misma área y de ti RF quieran mantener los segmentos de tu malla separados.

Si quieres agregar un nuevo AP a una red en funcionamiento, debe preconfigurar el BGN en el nuevo AP. Si sacas a colación la red de interconexión del rasguño con nuevo, el hacia fuera-de--box AP, el BGN se preestablece en los AP a un valor nulo. Los AP se unen a en una nueva red con este valor predeterminado del BGN. Usted puede verificar el BGN de un AP con este comando:

```
show ap config general Cisco AP
```

Q. ¿Qué sucede si el BGN no se configura correctamente?

A. Si el AP se proporciona de forma incorrecta con un bridgegroupname diferente del deseado, dependiente sobre el diseño de red, este AP puede o no puede llegar hacia afuera y encontrar su sector o árbol correcto. Si no puede alcanzar un sector compatible, puede trenzarse. Para recuperar un AP tan trenzado, el concepto de bridgegroupname predeterminado se ha introducido. La idea básica es que un AP, que no puede conectar con cualquier otro AP con su bridgegroupname configurado, intenta conectar con el bridgegroupname del valor por defecto.

Éste es el algoritmo usado para detectar esta condición y recuperación del hilo:

1. Explora y encuentra pasivo todos los nodos vecinos, sin importar su bridgegroupname.
2. El AP intenta conectar con los vecinos que se oyen con su propio bridgegroupname con el protocolo inalámbrico adaptante del camino (AWPP).
3. Si el paso de progresión 2 falla, intenta conectar con el bridgegroupname predeterminado con AWPP.
4. Para cada intento fallido del paso de progresión 3, la exclusión-lista el vecino e intenta conectar al mejor vecino siguiente.
5. Si el AP no puede conectar con todos los vecinos en el paso de progresión 4, reanuda el AP.
6. Si está conectado con el bridgegroupname predeterminado por 30 minutos, pre-explora

todos los canales e intenta conectar con el bridgegroupname correcto.

Nota: Cuando un AP puede conectar con el bridgegroupname predeterminado, los informes del nodo del padre el AP como un niño/un nodo predeterminado/entrada vecina en el Controlador de WLAN de modo que un administrador de la red sea consciente del AP trenzado. Tal AP no puede validar ningún cliente u otros nodos de la malla como sus niños, ni puede pasar cualquier tráfico de datos a través.

Q. ¿Puede un Bridge del LAP 1030 a otros modelos del Bridge? ¿También puede un LAP 1020 soportar el bridging?

A. El modelo del LAP 1020 no soporta el bridging. El LAP 1030 soporta el bridging (un salto) a otro LAP 1030 pero no a un BR1310, BR1400, o LAP 1500 ahora.

Q. ¿Es posible configurar el bridging sin hilos entre el LAP AP? Como una radio en los LAPs de mis NON-conexiones realizaría el bridging de nuevo a los LAPs atados con alambre del Root Bridge (LAP conectado con un WLC). ¿Es posible?

A. No. Esto no se puede hacer en el LAP AP. La malla AP puede realizar el bridging de punto a punto básico en una red del Cisco Unified Wireless. El único otro el interligar posible está con IOS AP en el modo WGB (Workgroup Bridge). Este el IOS AP actúa como clientes (con los dispositivos atados con alambre detrás de ellos) a un LAP AP. Pero los clientes de red inalámbrica no pueden conectar con estos IOS AP.

Q. Tengo un LAP 1131, y este punto de acceso se registra con éxito a los controladores del Wireless LAN. Cuando conecto el Punto de acceso sin el alimentador de corriente, las radios están para arriba (el estado de LED es verde), pero cuando conecto el AP con el alimentador de corriente, las radios están abajo (el estado de LED es anaranjado). ¿Cómo yo puede la resolución esto publicar?

A. Este problema puede ser debido al poder incorrectamente configurado sobre los parámetros de los Ethernetes (POE); complete estos pasos para resolver este problema:

1. Haga clic la **Tecnología inalámbrica** para acceder estos parámetros.
2. Haga clic el link del **detalle del** Punto de acceso deseado. Los nuevos parámetros aparecen en el todo el página AP > de los detalles bajo configuraciones del POE.
3. En la página AP > de los detalles del Punto de acceso para las configuraciones del POE, **estado del alimentador de corriente del** tecleo, y elige **instalado**.
4. Marca la casilla de verificación para habilitar el estado del alimentador de corriente para el punto de acceso. Se requiere este parámetro si el switch conectado no soporta el IPM y se utiliza un alimentador de corriente. Este parámetro no se requiere si el switch conectado soporta el IPM.

Q. En los AP autónomos, el reenvío de paquete seguro público (PSPF) se utiliza para evitar los dispositivos del cliente asociados a este AP inadvertidamente de compartir los archivos con otros dispositivos del cliente en la red inalámbrica. ¿Hay característica equivalente en los AP ligeros?

A. La característica o el modo que realiza la función similar de PSPF en la arquitectura ligera se

llama modo de bloqueo entre iguales. El modo de bloqueo entre iguales está realmente disponible con los controladores que manejan el LAP.

Si este modo se inhabilita en el regulador (que es la configuración predeterminada), permite que los clientes de red inalámbrica comuniquen con uno a través del regulador. Si se habilita el modo, bloquea la comunicación entre los clientes a través del controlador.

Trabaja solamente entre los AP que se han unido a al mismo controlador. Cuando está habilitado, este modo no bloquea a los clientes de red inalámbrica terminado en un controlador de la capacidad de conseguir a los clientes de red inalámbrica terminado en un diverso controlador, incluso en el mismo grupo de la movilidad.

Q. ¿Puede los mensajes SNMP de una manija del LAP AP como un IOS AP?

A. El LAP AP no puede manejar los mensajes SNMP en sus los propios. Para manejar los mensajes SNMP, debe configurar a un snmp community en el WLC a las cuales se registra el LAP. Toda la información AP es manejada por el WLC.

Información Relacionada

- Preguntas Frecuentes sobre el Troubleshooting de los Controladores de WAN Inalámbricos (WLC)
- Módulos controlador de LAN de la tecnología inalámbrica de Cisco
- Controlador LAN de la tecnología inalámbrica de Cisco (WLC) FAQ
- Guía de Configuración de Cisco Wireless LAN Controller , Release 3.2
- Ejemplo de la configuración básica del controlador y del Lightweight Access Point del Wireless LAN
- Soporte Técnico y Documentación - Cisco Systems