# Preguntas frecuentes sobre los puntos de acceso Cisco Aironet.

## Contenido



## Introducción

Este documento proporciona las respuestas a las preguntas frecuentes sobre los Puntos de Acceso (AP) Cisco Aironet.

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

## Preguntas frecuentes de diseño

### Q. ¿Cuál es el nombre de usuario predeterminado y cuál es la contraseña predeterminada para los AP basados en el Software Cisco IOS®?

A. Los AP basados en el Software Cisco IOS tienen una configuración predeterminada que incluye una combinación de nombre de usuario y contraseña, donde ambos son **Cisco** (con diferenciación entre mayúsculas y minúsculas). Después de restablecer los valores predeterminados de fábrica, prepárese para proporcionar Cisco como nombre de usuario y contraseña cuando la interfaz de línea de comandos (CLI) o la GUI se lo indiquen.

### Q. ¿Qué cable debo utilizar para una conexión de la consola?

A. Utilice un cable de conexión directa con un conector macho de nueve patillas y un conector hembra de nueve patillas para conectar el puerto COM1 o COM2 de su computadora con el puerto RS-232 en el AP. Utilice un programa de emulación de terminal de su computadora, por ejemplo:

- HyperTerminal de Microsoft Windows
- ProComm de Symantec
- Minicom

Utilice estas configuraciones de puerto:

| | |
|---|---|
| Velocidad: | 9600 bits por segundo (bps) |

| | |
|---|---|
| Bits de datos: | 8 |
| Bits de parada: | 1 |
| Paridad: | Ninguno |
| Control de Flujo: | Xon/Xoff |

**Nota:** Si el control de flujo Xon/Xoff no funciona, intente utilizar el control de flujo None.

## Q. Tengo un AP Aironet 1231. ¿Cisco tiene un cable de extensión 50 pies de modo que pueda tener el AP en un área y la antena en otra?

A. Sí, el numero de pieza del cable de 50 pies es AIR-CAB050LL-R. Usted puede utilizar este cable para conectar su AP con la antena.

## Q. ¿Cómo verifica el tipo de radio en un AP autónomo?

A. Usted puede utilizar el **comando show controllers** del modo EXEC privilegiado en el AP para obtener la información sobre el tipo de radio.

## Q. ¿Cómo configura una dirección IP en el AP?

A. De forma predeterminada, el AP solicita una dirección IP a través de DHCP.

Cisco IOS 12.3(2)JA y las versiones posteriors cambian el comportamiento predeterminado de los AP que solicitan una dirección IP de un servidor DHCP:

- Cuando usted conecta un AP serie 1200 o 1230 con una configuración predeterminada con su LAN, el AP solicita una dirección IP de su servidor DHCP. Si no recibe una dirección, continúa enviando las solicitudes indefinidamente.
- Cuando usted conecta los AP Serie 1100 con una configuración predeterminada con su LAN, los AP Serie 1100 hacen varios intentos para obtener una dirección IP del servidor DHCP. Si no recibe una dirección, se asigna a sí mismo la dirección IP 10.0.0.1 durante cinco minutos. Durante este período de cinco minutos, usted puede acceder a la dirección IP predeterminada y configurar una dirección estática. Si después de cinco minutos el AP no se configura de nuevo, desecha la dirección 10.0.0.1 y vuelve a pedir una dirección del servidor DHCP. Si no recibe una dirección, envía las solicitudes indefinidamente. Si durante el período de cinco minutos no puede acceder al AP en 10.0.0.1, puede reiniciar el AP para repetir el proceso.

Usted también puede establecer manualmente el dirección IP del AP. En una PC con Microsoft Windows conectada con el segmento Ethernet, desde la indicación DOS, ejecute este comando:

```
arp -s a.b.c.d 00-12-34-56-78-90
```

**Nota:** ***El a.b.c.d del*** término *representa la* dirección IP que debe ser fijada en el AP, y 00-12-34-56-78-90is la dirección MAC. Esta dirección aparece en el panel en la parte inferior del AP.

Ejecute este comando para verificar la dirección:

```
ping a.b.c.d
```

**Nota:** Este procedimiento no funciona si ya se ha asignado una dirección IP al AP mediante otro método.

## Q. ¿Cómo habilita el acceso HTTPS en el AP?

A. Para habilitar HTTPS, debe agregar este comando a su AP:

```
AP(config)#ip http secure-server
```

Cuando agrega el comando **ip http secure-server**, ve las claves RSA necesarias para lograr una comunicación segura regenerada en los AP.

## Q. ¿Cómo elige un cliente un punto de acceso (AP) para asociarse?

A. La opción Access Point (AP) se hace en la radio de la máquina del cliente. Según el fabricante, el driver, el tipo de tarjeta, etc., puede utilizar métricas diferentes para tomar la decisión. El mecanismo de afiliación AP más común utilizado en la mayoría de los clientes está basado en la intensidad de la señal recibida por el cliente desde los AP. El estándar 802.11 requiere solamente que la tarjeta de cliente inalámbrico informe la intensidad de la señal con una métrica simple denominada indicador de intensidad de señal recibida (RSSI). El cliente entonces se asocia al AP con la señal más fuerte. Es bien sabido que estos algoritmos pueden conllevar un rendimiento deficiente. El motivo principal se debe a la falta de conocimiento de la carga en diferentes AP.

## 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 de WAN Inalámbrico y los AP autónomos, el traslado no funciona.

## Q. ¿Cómo amplía la cobertura del AP?

A. Hay varias maneras de ampliar el área de cobertura para un AP. Estos son los métodos más importantes:

- Utilice los AP en el modo repeater.
- Utilice un AP secundario en el modo AP con los canales sin traslapo.
- Cambie el parámetro del nivel de intensidad del transmisor del AP existente para ampliar la cobertura.
- Coloque el AP de manera óptima.

Consulte los Métodos de Extensión del Área de Cobertura del Radio WLAN para obtener una descripción completa de cómo implementar estos métodos.

## Q. ¿Cuáles son las implicaciones si su AP está en el modo repeater?

A. El puerto Ethernet está inhabilitado en el modo repeater. El rendimiento efectivo se corta por la mitad una vez para cada salto alejado del AP primario.

Para configurar los repetidores, debe habilitar las extensiones Aironet en el punto de acceso primario (root) y los puntos de acceso del repetidor. Las extensiones Aironet, que están habilitadas de forma predeterminada, mejoran la capacidad del punto de acceso de comprender las capacidades de los dispositivos cliente Cisco Aironet asociados al punto de acceso. Si usted inhabilita las extensiones Aironet, a veces, puede mejorar la interoperabilidad entre el punto de acceso y los dispositivos cliente que no son de Cisco. Los dispositivos cliente que no son de Cisco pueden encontrar difícil la comunicación con los puntos de acceso del repetidor y la punta del acceso root a los cuales los repetidores están asociados.

La infraestructura SSID se debe asignar a la VLAN nativa. Si se crea más de una VLAN en un punto de acceso o en un puente inalámbrico, no se puede asignar una infraestructura SSID a una VLAN no nativa. Este mensaje aparece cuando la infraestructura SSID se configura en una VLAN no nativa:

```
AP(config)#ip http secure-server
```

Dado que los puntos de acceso crean una interfaz virtual para cada interfaz de radio, los puntos de acceso del repetidor se asocian con el punto de acceso root dos veces: una vez para la interfaz real y una vez para la interfaz virtual.

**Nota:** Usted no puede configurar varias VLAN en los puntos de acceso del repetidor. Los puntos de acceso del repetidor soportan solamente la VLAN nativa.

## Q. ¿Cuáles son las funciones soportadas por la opción de la Extensión Aironet?

A. La extensión Aironet es una función propietaria implementada por Cisco. Las extensiones Aironet contienen elementos de información que soportan estas funciones.

- **Equilibrio de carga** El punto de acceso utiliza las extensiones Aironet para dirigir los dispositivos cliente a un punto de acceso que proporcione la mejor conexión a la red basada en factores como el número de usuarios, las frecuencias de errores de bits, la carga y intensidad de la señal.El balanceo de carga es propietario entre los dispositivos que comprenden las extensiones Aironet. El balanceo de carga es implementado por extensiones en las respuestas de probe o en las señalizaciones AP, que proporcionan información sobre lo siguiente:Intensidad de la señal de la estación baseCarga de la estación base (% del transmisor ocupado)Número de saltos a la backboneNúmero de asociaciones del clienteEl cliente evalúa estos aspectos y se asocia al “mejor”. Los clientes que no son de Cisco no comprenden estas extensiones.
- **MIC:** Message Integrity Check (MIC) Propietaria de Cisco - MIC es una función de seguridad WEP adicional que previene los ataques contra los paquetes cifrados llamados ataques de manipulación de bits. MIC se implementa en el punto de acceso y en todos los dispositivos cliente asociados.
- **Temporal Key Integrity Protocol propietario de Cisco (CKIP)**, también conocido como hashing de clave WEP, es una función de seguridad WEP adicional que protege contra un ataque en WEP, en el cual el intruso utiliza un segmento descifrado llamado vector de inicialización (IV) en los paquetes cifrados para calcular la clave WEP.

- Además de estos, las extensiones Aironet transportan más información que incluye lo siguiente:Carga que los AP manejan actualmenteNúmero de saltos de la red cableadaTipo de dispositivo, que ayuda a identificar el producto conforme al sistema de Cisco para su administraciónNombre del dispositivoNúmero de clientes asociadosTipo de radio, una función usada para determinar ciertas funciones sobre la radio, como datarate, tipo de la radio (1310, 1200, 352 o 342), tipo de la seguridad (WEP/802.1x), etc.

Los dispositivos que son CCX compatible también pueden aprovecharse de algunas de las funciones de la extensión Aironet. Aquí está una lista de las funciones disponibles con las diferentes versiones de los Cisco Compatible Extension:

Extensión Compatible de Cisco - Versiones y Funciones

## Q. ¿Puede usted conectar dos computadoras juntos sin un AP a través de tarjetas de interfaz inalámbricas?

A. Yes. Desde Aironet Client Utility (ACU), usted puede configurar a los clientes para ejecutar en el modo ad hoc. Esta conexión es solamente una conexión peer a peer. Una PC se convierte en el elemento primario y controla la conexión. Las otras PC en el modo ad hoc son estaciones secundarias.

## Q. ¿Necesita un hardware especial para soportar el cifrado?

A. El modelo de hardware específico determina el nivel de cifrado para la unidad:

- Los modelos 341 y 351 soportan solamente el cifrado de 40 bits.
- Los modelos 342 y 352 soportan el cifrado de 40 y 128 bits.
- Todos los modelos de las series 1100, 1200 y 1300 soportan el cifrado de 40 y 128 bits.

## Q. ¿Es posible ver todos los AP y sus clientes asociados que pertenecen a esa red/infraestructura determinada desde un solo AP?

A. Esto es posible de un AP VxWorks. Un solo AP VxWorks puede mostrar todos los clientes y sus AP en una red. Esto se logra si hace clic en **Association > Entire Network > Apply**. En un AP basado en IOS, no muestra todos los clientes asociados en esa red sin la ayuda de un dispositivo de administración, como WLSE, con un AP como WDS o un controlador si la imagen en AP es una imagen LWAPP.

## Q. Utilizo CCKM en mi red, pero todo el proceso de autenticación sigue ocurriendo siempre que el dispositivo cliente se traslada. En pocas palabras, el traslado seguro rápido no funciona como se esperaba. ¿por qué?

A. Esto posiblemente se debe a bug CSCsg10128. Este bug está corregido en la Versión 3.1.03.

## Q. ¿Los Puntos de Acceso de Cisco soportan la función UniDirectional Link Detection (UDLD) para interrumpir la conexión de Ethernet a los switches si hay una falla de cable de la Capa 1/Capa 2?

A. No, los Puntos de Acceso de Cisco no soporta la función UDLD.

## Q. ¿Cómo suministra energía a un AP Aironet?

A. Las opciones de energía para su AP dependen del modelo AP que usted tenga. Consulte Opciones de Energía de los Productos Controlador de WLAN y Cisco Aironet para obtener más información.

## Q. Tengo un AP1010, AP1030 y un AIR-LAP-1232AG. ¿Pueden utilizar WS-PWR-PANEL para Power over Ethernet (PoE)?

A. WS-PWR-PANEL soporta solamente los puntos de acceso con una sola radio. Consulte la matriz de compatibilidad disponible en la sección *Administración de Energía Inteligente de Cisco y Cisco PoE* de Nota sobre la Aplicación Power Over Ethernet Cisco Aironet para obtener más información.

## Q. ¿Cómo guarda la configuración del AP?

A. Las modificaciones a la configuración se guardan inmediatamente. Usted puede volcar la configuración actual en un formato de texto desde el **menú Setup**. Luego, elija el **Cisco Services > Manage System Configuration** y descargue la configuración del sistema.

## Q. ¿Cómo determino la frecuencia o el canal específicos que mi AP o bridge utilizan?

A. Utilice el **comando show controllers dot11Radio0** para mostrar la frecuencia y el canal en el que están el AP o el bridge. Este resultado de ejemplo muestra dónde encontrar la información:

```
ap#show controllers dot11Radio0
!
interface Dot11Radio0
Radio AIR-AP1242GA, Base Address 0014.1b58.08f
Version 5.80.12
Serial number: GAM09200992
Number of supported simultaneous BSSID on Dot1
Carrier Set: Americas (US )
DFS Required: No
Current Frequency: 2412 MHzChannel 1
```

## Q. ¿Cómo hago para que mi AP funcione con otros dispositivos IEEE 802.11B?

A. Para habilitar el AP para que se comunique con otro dispositivo 802.11b, apague las extensiones Aironet. Marque la casilla de verificación **Non-Aironet 802.11** en la ventana Express Setup. Alternativamente, puede haga clic en el botón de opción **Use Aironet Extension** en la ventana Advanced AP Radio.

## Q. ¿Qué dispositivos pueden asociarse a un AP?

- AP a cliente
- AP a AP (en el modo repeater)
- AP (en el modo repeater) a estación base (en modo AP)
- AP a bridge del grupo de trabajo

## Q. ¿En qué frecuencia se comunica un AP?

A. En los Estados Unidos, los AP IEEE 802.11B transmiten y reciben en uno de 11 canales dentro de la frecuencia de 2.4 GHz. Los AP IEEE 802.11a transmiten y reciben en uno de ocho canales en la frecuencia de 5 GHz. Los AP IEEE 802.11g transmiten y reciben en uno de 11 canales dentro de la frecuencia de 2.4 GHz. Estos son rangos de frecuencia pública y no tienen licencia de FCC.

## Q. ¿Cómo asegura los datos a través de un link de radio AP?

A. Hay varios métodos para asegurar sus datos a través de un link de red inalámbrica AP. Para aprender más sobre los diferentes métodos de seguridad, consulte Preguntas Frecuentes sobre la Seguridad de Red Inalámbrica Cisco Aironet.

## Q. ¿Cuántos clientes pueden asociarse al AP?

A. El AP tiene la capacidad física de manejar 2048 direcciones MAC; sin embargo, dado que el AP es un medio compartido y actúa como hub de red inalámbrica, el rendimiento de cada usuario disminuye a medida que el número de usuarios aumenta en un AP individual. Idealmente, no más de 24 clientes pueden asociarse al AP, dado que el rendimiento del AP se reduce con cada cliente que se asocie al AP.

## Q. ¿Hay una limitación en el número de filtros de direcciones MAC que se pueden configurar en el AP?

A. Usted puede utilizar CLI para configurar hasta 2048 direcciones MAC para filtrar; sin embargo, con el uso de la interfaz del navegador web, usted puede configurar solamente hasta 43 direcciones MAC para filtrar.

## Q. ¿Cuál es el rango típico para un AP?

A. La respuesta a esta pregunta depende de muchos factores, que incluyen los sigiuentes:

- Velocidad de datos (ancho de banda) que usted desee
- Tipo de antena
- Longitud del cable de la antena
- Dispositivo que recibe la transmisión

En una instalación óptima, el rango puede ser hasta 91.5 metros.

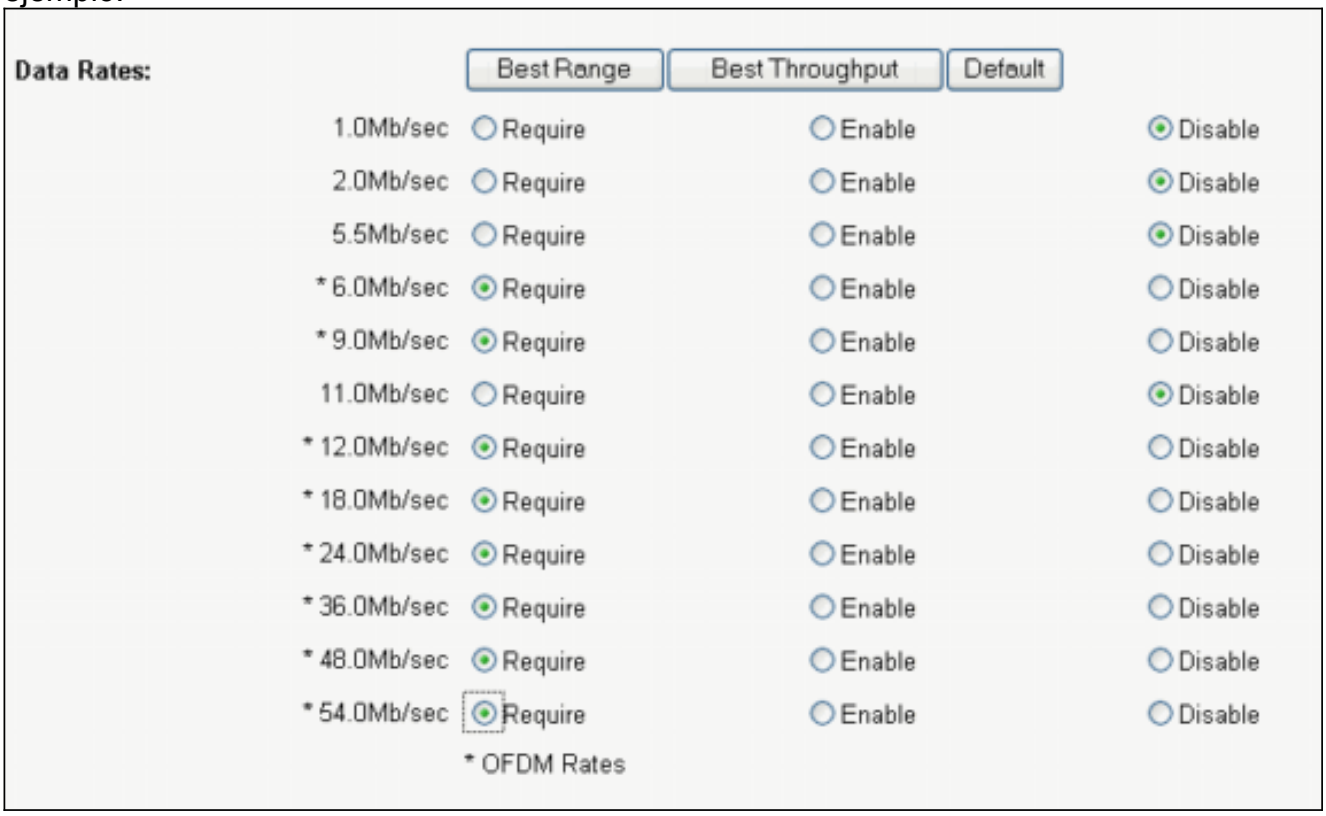
## Q. ¿Cuáles son las configuraciones disponibles del nivel de intensidad de transmisión para AP 1200?

A. Las configuraciones de intensidad de transmisión son diferentes y dependen de la radio que se utiliza. Consulte la Hoja de datos de Puntos de Acceso Cisco Aironet 1200 Series para conocer la lista completa de niveles de configuración de energía. Dado que las configuraciones de energía varían en función del canal, realice un sondeo del sitio. El sondeo del sitio es importante para obtener información precisa sobre la configuración para utilizar. Consulte Preguntas Frecuentes sobre el Sondeo del Sitio Inalámbrico para obtener detalles sobre los sondeos de sitio.

## Q. ¿Cómo puedo establcer el AP de modo que solamente los clientes IEEE 802.11g puedan conectarse? No deseo que los clientes IEEE 802.11B se conecten y ralenticen la red inalámbrica. Hay una segunda red paralela 802.11b para clientes no seguros.

A. Para que el AP reciba clientes 802.11g solamente, complete estos pasos en la GUI:

1. Vaya a la sección de las interfaces de red y haga clic en **Radio 0-802.11G**.
2. Haga clic en la pestaña **Settings** en la parte superior de la ventana Radio 0-802.11G.
3. Elija **Disable** para estas velocidades de datos: 1.02.05.511.0
4. Elija **Require** para el resto de las velocidades de datos. Estas son las otras velocidades de datos: 6.09.012.018.024.036.048.054.0
5. Haga clic en **Apply** en la parte inferior de la ventana. Esta ventana proporciona un ejemplo:




## Q. ¿Es verdad que si permito solamente los clientes IEEE 802.11g en una red inalámbrica, no pueden interferir con una red paralela IEEE 802.11B porque utilizan diferentes esquemas de modulación?

A. No, esto no es verdad. Estos clientes 802.11g pueden interferir si utilizan la misma frecuencia. Asegúrese de utilizar diferentes canales. Los tres canales sin traslapo son 1, 6, y 11.

## Q. ¿Cuál es la velocidad del puerto Ethernet AP?

A. El puerto Ethernet AP soporta 10 Mbps o 100 Mbps a través de un conector RJ-45, en dúplex completo o en medio dúplex. Configure la velocidad y el dúplex con las mismas configuraciones que su switch o hub.

## Q. ¿Hay un mecanismo para failover o redundancia para mi AP?

A. Sí, usted puede configurar standby activa para proporcionar redundancia en caso de que el AP primario falle. Refiera a los Release Note para los Puntos de acceso del Cisco Aironet para más información.

## Q. ¿Qué es una clave WEP?

A. WEP significa Wired Equivalent Privacy. Usted puede utilizar WEP para cifrar y descifrar las señales de datos que se transmiten entre los dispositivos LAN inalámbricos (WLAN). WEP es una función IEEE 802.11 opcional que previene la divulgación y la modificación de los paquetes en tránsito, y también proporciona control de acceso para el uso de la red. WEP hace a un link WLAN tan seguro como un link cableado. Como el estándar especifica, WEP utiliza el algoritmo RC4 con una clave de 40 bits o 10 bits. RC4 es un algoritmo simétrico porque RC4 utiliza la misma clave para el cifrado y el descifrado de datos. Cuando WEP está habilitado, cada estación de radio tiene una clave. La clave se utiliza para codificar los datos antes de la transmisión de estos a través de las ondas. Si una estación recibe un paquete que no se revuelva con la clave apropiado, la estación desecha el paquete y nunca entrega tal paquete al host. Consulte Ejemplos de Configuración de Wired Equivalent Privacy (WEP) en bridges y Puntos de Acceso Aironet para obtener información sobre cómo configurar WEP.

## Q. Cuando usted utiliza el protocolo Light Extensible Authentication Protocol (LEAP), ¿qué número de puerto especifica para comunicarse con su Cisco Secure Access Control Server (ACS)?

A. De forma predeterminada, ACS escucha una solicitud de autenticación en el puerto 1645 y contabilización en el puerto 1646, pero usted puede configurar el puerto 1812 para la autenticación y 1813 para contabilización. Confirme que estos puertos estén correctamente configurados en la página Configuración del Servidor de Autenticación en AP.

## Q. En los AP basados en el Cisco IOS Software, ¿puede usted ejecutar claves Wired Equivalent Privacy estáticas (WEP) y el protocolo Extensible Authentication Protocol (EAP) en forma conjunta en el mismo AP para la autenticación? Esto ha funcionado con los AP basados en Vxworks.

A. No, usted no puede ejecutar las claves WEP estáticos para el cifrado y EAP para la autenticación en el mismo identificador de conjunto de servicios (SSID). VxWorks ha permitido esta configuración debido a la vulnerabilidad del software, pero esta capacidad no es una función. Lo que puede hacer es crear dos SSID y dos VLAN (uno por SSID). Luego, configure la autenticación abierta con WEP para un SSID y la autenticación EAP para el otro SSID.

## Q. ¿Realmente necesita que se realice un sondeo de sitio?

A. Yes. Debido a la naturaleza sensible de las transmisiones de radiofrecuencia (RF), usted debe conocer los otros tipos de tráfico RF que pueden estar en su entorno, incluso si no tiene conocimiento de la presencia de tráfico. Un sondeo de sitio permite una mejor comprensión de esta amenaza invisible para el buen funcionamiento de sus dispositivos de red inalámbrica. El sondeo de sitio también ayuda a su instalador profesional a asegurar la cobertura RF deseada. Consulte las Preguntas Frecuentes sobre el Sondeo de Sitio de Red Inalámbrica.

## Q. Si usted intenta modificar el AP y le indican que proporcione un nombre de usuario y una contraseña, ¿qué ingresa?

A. Una indicación para proporcionar un nombre de usuario y una contraseña indica que el Administrador de Usuarios está habilitado. Consulte a su administrador AP para descubrir el nombre de usuario y la contraseña que debe utilizar. Si usted es el administrador AP y no conoce cuáles son estas cuentas de usuario, debe ejecutar una recuperación de contraseña. Consulte Procedimiento para la Recuperación de la Contraseña para el Equipo Cisco Aironet.

## Q. ¿Puede utilizar dos antenas externas para cubrir dos células de radio (por ejemplo, la antena 1 para la célula 1 y la antena 2 para la célula 2)?

A. Usted no puede utilizar dos antenas en un AP para cubrir dos células de radio. Los intentos de utilizar las antenas para cubrir dos células de radio pueden dar lugar a problemas de conectividad. El propósito de las dos antenas es aumentar la cobertura de una célula en un esfuerzo para superar los problemas que se presentan con la distorsión de múltiples trayectorias y valores de señal nulos. Consulte Trayectorias Múltiples y Diversidad para obtener más información sobre las distorsiones de trayectorias múltiples y diversidad.

## Q. ¿Cuál es el uso del comando mobility network-id en un AP?

A. Usted utiliza el **comando mobility network-id** para configurar la movilidad de Capa 3 en una red inalámbrica. Usted utiliza el **comando mobility network-id ssid** para asociar un identificador de conjunto de servicios (SSID) a un ID de red de movilidad de Capa 3. Con la movilidad de Capa 3, los clientes pueden trasladarse por diferentes AP que residen en diferentes subredes. Los clientes de traslado permanecen conectados con su red y no cambian las direcciones IP.

Usted debe utilizar un módulo de servicios (WLSM) de LAN inalámbrica (WLAN) como su dispositivo de servicios del dominio inalámbricos (WDS) para configurar correctamente la movilidad de Capa 3. La movilidad de Capa 3 no se soporta cuando usted utiliza un AP como su dispositivo WDS. Para obtener más información sobre la movilidad de Capa 3, consulte la sección *Comprensión de la Mobilidad de Capa 3* de Configuración de Administración de Radio, Traslado Rápido Seguro y WDS.

El comando debe ser utilizado cuando el AP participa en una infraestructura WDS con un módulo WLSM (que actúa como el dispositivo WDS) donde hay movilidad de Capa 3. Si usted utiliza este comando incorrectamente, surgen problemas de conectividad en la red WLAN, por ejemplo:

- Los clientes no obtienen la dirección IP de DHCP.
- En algunos casos, los clientes no pueden asociarse al AP.
- Los clientes de red inalámbrica no pueden asociarse al AP.
- La autenticación del protocolo Extensible Authentication Protocol (EAP) no sucede. Con el **comando mobility network-id** configurado, el AP intenta crear un túnel de encapsulación de ruteo genérico (GRE) para el reenvío de paquetes EAP. Si no se establece ningún túnel, los paquetes no pueden ir a ningún lado.
- El AP que se configura como un dispositivo WDS no funciona según lo esperado y la configuración WDS no funciona.

## Q. ¿Cuántos identificadores de conjunto de servicios (SSID) puede tener por VLAN?

A. Usted puede tener solamente un SSID por VLAN. El uso de múltiples SSID a través de una sola VLAN no se soporta con los AP Aironet.

## Q. ¿Cuál es el valor BSSID cuando hay múltiples ESSID asignados a los AP?

A. Si el AP se está ejecutando en el modo lightweight, entonces cada ESSID en un AP será manejado a través de un BSSID diferente (donde cada BSSID está basado en la MAC de base de radio y se diferencia solamente en el cuarteto de orden inferior.)

Si el AP está ejecutando un IOS, todos los ESSID en el AP serán manejados a través del mismo BSSID (a menos que se configure MBSSID, en cuyo caso serán manejados a través de BSSID diferentes).

## Q. ¿Es posible configurar mi radio A para bridge y la radio G para la funcionalidad AP? En caso afirmativo, ¿cómo puedo hacerlo?

A. Sí, es posible configurar cada radio en su AP para lograr una funcionalidad diferente. En su escenario, esto se puede hacer si usted configura diferentes identificadores de conjunto de servicio (SSID) para la radio A y G. Luego, configure la función en un parámetro de red de radio para la radio G al AP y para la radio A al root bridge.

## Q. Cuándo dos clientes se asocian a dos AP diferentes que estén conectados en la misma subred, ¿la comunicación sucede a través de la red cableada o en forma inalámbrica?

A. Para este escenario, si los dos AP se configuran en el modo root, la comunicación entre los dos AP es a través de la red cableada. Si uno de los AP se configura en el modo repeater y el otro AP se configura en el modo root, la comunicación entre los AP sucede en forma inalámbrica.

## Q. ¿Puede habilitar el ruteo o Network Address Translation (NAT) en los AP de Cisco?

A. No, las funciones de ruteo y NAT no se soportan en los AP.

## Q. ¿Hay alguna manera de programar una tiempo en que el AP basado en el Cisco IOS Software esté disponible? Quiero proporcionar acceso basado en el tiempo a los clientes que se conectan con el AP.

A. Usted puede configurar listas de control de acceso (ACL) basadas en el tiempo con uso de rangos de tiempo. Las ACL basadas en el tiempo lo ayudan a asegurarse de que los usuarios pueden acceder a la red inalámbrica en un período de tiempo determinado, por ejemplo, 9:00 a. m. a 5:00 p. m. (0900 a 1700). El uso de las ACL basadas en el tiempo no apaga el AP o la radio. Las ACL basadas en el tiempo detienen el paso del tráfico en el AP de modo que los usuarios no pueden acceder a la red. Para la información sobre cómo configurar esta característica, refiera al *time basado ACL usando la sección de rangos de tiempo de las* Listas de acceso de ConfiguringIP.

## Q. ¿Pueden los AP tener los múltiples conjuntos DHCP a través de diferentes subredes?

A. Cuando usted configura el AP como un servidor DHCP, las direcciones IP se asignan a los dispositivos que están en la misma subred como el servidor DHCP. Los dispositivos se

comunican con los otros dispositivos en la subred, pero no se comunican más allá de la subred. Si usted necesita pasar datos más allá de la subred, debe asignar un router predeterminado. El dirección IP del router predeterminado debe estar en la misma subred que el AP que usted configuró como el servidor DHCP.

## Q. ¿Cuál es la medida dBm? ¿Cómo determino los valores dBm equivalentes para la intensidad de la señal (en mW) detallada en mi punto de acceso (AP) Aironet?

A. La unidad dB mide la intensidad de una señal como una función de su relación con respecto a otro valor estandarizado. Esta abreviatura dB se combina a menudo con otras abreviaturas para representar los valores se comparan. Por lo tanto, dBm es el valor que surge de comparar dB con un valor de referencia estandarizado de 1 mW.

La fórmula para calcular este valor dBm de la intensidad de la señal dada en el mW es la siguiente:

```
ap#show controllers dot11Radio0
!
interface Dot11Radio0
Radio AIR-AP1242GA, Base Address 0014.1b58.08f
Version 5.80.12
Serial number: GAM09200992
Number of supported simultaneous BSSID on Dot1
Carrier Set: Americas (US )
DFS Required: No
Current Frequency: 2412 MHzChannel 1
```

Esta lista define los términos en la fórmula. log10 es el logaritmo base 10.

- Signal es la intensidad de la señal (por ejemplo, 50 mW).
- Reference es la intensidad de referencia (por ejemplo, 1 mW).

### Ejemplo:

Si usted quiere calcular la intensidad en dB de la intensidad de señal 50 mW, aplique esta fórmula:

```
ap#show controllers dot11Radio0
!
interface Dot11Radio0
Radio AIR-AP1242GA, Base Address 0014.1b58.08f
Version 5.80.12
Serial number: GAM09200992
Number of supported simultaneous BSSID on Dot1
Carrier Set: Americas (US )
DFS Required: No
Current Frequency: 2412 MHzChannel 1
```

Esta fórmula deriva en una regla común que establece lo siguiente:

- Por cada aumento de 3 dB (dBm aquí), la intensidad de la transmisión actual (mW) aumenta el doble. Por cada disminución de 3 dB, la intensidad de la transmisión se reduce a la mitad de su valor actual.
- Por cada aumento de 10 dB (dBm aquí), la intensidad de la transmisión actual (mW) aumenta diez veces. Por cada disminución de 10 dB, el valor actual de la intensidad de la transmisión

se reduce diez veces.

- Por cada aumento de 30 dB (dBm), la intensidad de la transmisión actual aumenta 1000 veces. Por cada disminución de 30 dB, el valor actual de la intensidad de la transmisión se reduce 1000 veces.

Esta tabla proporciona los valores dBm a mW aproximados:

| dBm | mW |
|---|---|
| 0 | 1 |
| 1 | 1.25 |
| 2 | 1.56 |
| 3 | 2 |
| 4 | 2.5 |
| 5 | 3.12 |
| 6 | 4 |
| 7 | 5 |
| 8 | 6.25 |
| 9 | 8 |
| 10 | 10 |
| 11 | 12.5 |
| 12 | 16 |
| 13 | 20 |
| 14 | 25 |
| 15 | 32 |
| 16 | 40 |
| 17 | 50 |
| 18 | 64 |
| 19 | 80 |
| 20 | 100 |
| 21 | 128 |
| 22 | 160 |
| 23 | 200 |
| 24 | 256 |
| 25 | 320 |
| 26 | 400 |
| 27 | 512 |
| 28 | 640 |
| 29 | 800 |
| 30 | 1000 or 1 W |

Consulte los Valores de Intensidad de RF para obtener más información.

## Q. ¿Cómo cambio la configuración de fecha y hora en Cisco 1231 AP?

A. Vaya a la interfaz web (GUI), elija **Services > SNTP**, selecione **Time Settings** y luego cambien la hora.

## Q. Si CCKM no está configurado en el cliente, pero está configurado en los AP, ¿el cliente estará asociado con el AP? ¿Pueden los clientes trasladarse normalmente?

A. El comportamiento depende de la configuración del AP. Si CCKM NO está configurado o NO se soporta en el cliente, el cliente no se asocia a un AP que esté configurado como CCKM "mandatory". Si la infraestructura (AP) está configurada como CCKM "optional", el cliente se asocia y hace su protocolo de enlace sin CCKM.

Según los clientes implementados, típicamente se recomienda configurar CCKM en "optional" en la infraestructura que permite la asociación de todos los dispositivos pero que SOLAMENTE soporta el traslado rápido de los dispositivos asociados con CCKM/capaces.

## Q. ¿Cuál es la diferencia en la capacidad de memoria entre AP 1240 y 1230?

A. Estas son las capacidades de memoria de AP 1240 y 1230:

- AP 1240 es un AP de plataforma de 32 MB.
- AP 1230 es un AP de plataforma de 16 MB.

## Q. Tengo dos AP 1240 que soportan flexibilidad de función de link. Me gustaría puentear entre ellos con 802.11a, con clientes unidos en las bandas 802.11b/g. ¿Hay restricciones para hacer esto?

A. La flexibilidad de función de link del punto de acceso proporciona soporte de funcionalidad de modo bridge para los puntos de acceso que tienen la capacidad de banda doble (series 1200, 1230 y 1240AG). En la configuración de destino, la radio 802.11a se ejecuta en el modo bridge, mientras que la radio 802.11g está en el modo de punto de acceso.

El requisito es que cuando usted configure un AP con flexibilidad de función de link, una de las radios del AP se debe configurar como AP root, y el segundo AP que se puentea hacia atrás debe estar en el modo WGB o repetidor al AP root.

## Q. ¿Cuántos auriculares de telefonía IP inalámbrica se recomiendan por AP?

A. El ajuste de tamaño de la red de telefonía IP es esencial para asegurarse de que estén disponibles el ancho de banda y los recursos adecuados para transportar el tráfico de voz esencial. Además de las directrices de diseño de telefonía IP habituales para ajustar el tamaño de los componentes, como puertos de gateway PSTN, transcoders, ancho de banda WAN, entre otros, considere también estas cuestiones 802.11b al ajustar el tamaño de su red de telefonía IP inalámbrica:

- Número de los dispositivos 802.11b por AP: Cisco recomienda que no tenga más de 15 a 25.
- Número de teléfonos 802.11b por AP

Antes de que pueda ocurrir cualquier discusión sobre los planes de red, ayuda a comprender los elementos básicos de la capacidad de la red total. Estas directrices de capacidad de la red se aplican para ajustar el tamaño de la red de Telefonía IP Inalámbrica:

- No más de siete llamadas G.711 simultáneas por AP
- No más de ocho llamadas G.729 simultáneas por AP

**Nota:** Estas recomendaciones de diseño suponen que la Detección de Actividad de Voz (VAD) se ha inhabilitado en los Teléfonos IP Inalámbricos Cisco 7920.

El uso de VAD en los teléfonos Cisco 7920 puede conservar el ancho de banda, pero Cisco recomienda que usted inhabilite VAD en todos los servidores Cisco Callmanager para proporcionar una mejor calidad de voz en general. Además de la determinación de cuánto ancho de banda es necesario para realizar una llamada VoIP 802.11b, usted también debe considerar la contención de radio general para un canal RF determinado. La regla general es que usted no implemente más de 20 a 25 extremos 802.11b por AP. Cuanto más extremos usted agregue a un AP, más reduce la cantidad de ancho de banda general y aumenta potencialmente las demoras de la transmisión. El número máximo de teléfonos por AP depende de los patrones de llamada de los usuarios individuales (basados en las proporciones Erlang). Cisco recomienda que no más de siete llamadas simultáneas utilicen G.711 u ocho llamadas simultáneas utilicen G.729. Más allá de ese número de llamadas, cuando la cantidad de datos de antecedente es excesiva, la calidad de voz de todas las llamadas pasa a ser inaceptable. Las velocidades de paquetización para estas recomendaciones están basadas en velocidades de muestra de 20 ms con VAD inhabilitado. Esta velicidad genera 50 paquetes por segundo (pps) en cada dirección. Un tamaño de muestra más grande (como 40 ms) puede dar lugar a un número más grande de llamadas simultáneas, pero también aumenta la demora de extremo a extremo de las llamadas VoIP.

El número de teléfonos 802.11b que puede implementar por subred de Capa 2 o VLAN depende de estos factores:

- No utilice más de siete llamadas activas G.711 u ocho llamadas activas G.729 por AP.
- La relación de llamadas se utiliza para determinar el número de llamadas activas e inactivas. Esta relación a menudo se determina con las calculadoras Erlang. De acuerdo con estos factores y proporciones Erlang normales de clase empresarial (entre 3:1 y 5:1), Cisco le recomienda que no implemente más de 450 a 600 teléfonos Cisco 7920 por VLAN o subred de Capa 2.

Consulte la sección *Ajuste de Tamaño de la Red* de Infraestructura de Redes Inalámbricas y también ¿Está su WLAN Preparada para Voz?, para obtener más información detallada.

## Q. ¿Cómo puedo detener a un AP1200 para que deje de procesar solicitudes de autenticación después de un determinado número de intentos?

A. Usted puede utilizar la opción de la cantidad máxima de reintentos en el servidor AAA para limitar la cantidad de veces que los clientes puedan intentar acceder a una red. El valor de la cantidad máxima de reintentos se puede configurar manualmente en el servidor AAA, o usted puede utilizar la cantidad predeterminada de reintentos, que depende del servidor AAA que se utilice.

## Q. ¿Dónde puedo encontrar información sobre las diferencias en las diversas plataformas de AP y LAP?

A. Consulte las Preguntas Frecuentes sobre el Hardware de Inalámbrico de Cisco. Este documento contiene información útil que compara los diferentes modelos AP y LAP.

## Q. ¿Los Puntos de Acceso Cisco Aironet soportan Point-to-Point-Protocol over

## Ethernet (PPPoE)?

A. No, PPPoE no se soporta en los Puntos de Acceso Cisco Aironet.

## Q. ¿Los Puntos de Acceso Cisco Aironet soportan VLAN Trunking Protocol (VTP)?

A. No, VTP no se soporta en los Puntos de Acceso Cisco Aironet.

## Q. ¿Los AP Cisco Aironet soportan el protocolo estándar Inter-Access Point Protocol (IAPP) basado en 802.11f?

A. No, los AP Cisco Aironet no soportan IAPP basado en 802.11f. Los Puntos de Acceso Cisco ofrecen su propio protocolo Inter-Access Point Protocol comprobado, sólido y con múltiples funciones.

## Q. ¿Cuál es el uso de los comandos bridge-group 1 block-unknown-source y bridge-group 1 source-learning en un AP?

A. Utilice el comando de interfaz de configuración **bridge-group block-unknown-source** para bloquear el tráfico de direcciones MAC desconocidas en una interfaz específica. Utilice la forma **no** del comando para inhabilitar el origen desconocido que bloquea en una interfaz específica.

Para que STP funcione correctamente, **block-unknown-source** se debe inhabilitar para las interfaces que participan en STP.

```
ap#show controllers dot11Radio0
!
interface Dot11Radio0
Radio AIR-AP1242GA, Base Address 0014.1b58.08f
Version 5.80.12
Serial number: GAM09200992
Number of supported simultaneous BSSID on Dot1
Carrier Set: Americas (US )
DFS Required: No
Current Frequency: 2412 MHzChannel 1
```

Cuando usted habilita STP en una interfaz, **block-unknown-source** se inhabilita de forma predeterminada.

El comando **bridge-group 1 source-learning** permite que el AP obtenga la dirección de origen del cliente. Utilice la forma **no** del comando para inhabilitar AP a fin de que no obtenga la dirección de origen del cliente.

## Q. ¿Hay alguna manera de dar prioridad al tráfico que atraviesa el AP de modo que el tráfico de un SSID determinado configurado en el AP utilice un ancho de banda mayor que los otros SSID en el mismo AP?

A. Esto se puede lograr mediante la implementación de Calidad de Servicio (QoS) en los AP.

- Cree políticas QoS y aplíquelas a las VLAN configuradas en su punto de acceso. Estos documentos explican QoS y cómo configurar las políticas QoS en AP.Calidad de Servicio de

Red InalámbricaConfiguración de QoS en los Puntos de Acceso Aironet

- Luego, mapee los SSID configurados en el AP a las VLAN individuales mencionadas. De esta manera, si usted da prioridad al tráfico basado en VLAN, puede, a su vez, dar prioridad al tráfico basado en SSID.

## Q. ¿Hay alguna manera de limitar el número máximo de dispositivos cliente que puedan conectarse con un solo punto de Acceso Autónomo?

A. El comportamiento predeterminado de un dispositivo cliente de Cisco es que se conecte con el AP que tenga la mejor intensidad de señal disponible. Sin embargo, usted puede limitar los clientes que puedan conectarse con un AP determinado mediante la autenticación MAC. Usted debe proporcionar la dirección MAC del cliente al AP de modo que el AP pueda permitir solamente esos clientes y evitar que el resto de los clientes que no son parte de la lista de direcciones MAC permitidas se conecten con ese AP determinado.

## Q. ¿De dónde puede usted descargar el último software?

A. El equipo de Cisco Aironet actúa mejor cuando usted carga todos los componentes con la versión de software más actualizada. Consulte el Centro de Software para Redes Inalámbricas Cisco (clientes registrados solamente) para descargar el software y los drivers más recientes.

## Q. ¿Es necesario apagar todas las laptops y demás dispositivos de red inalámbrica durante una actualización de AP?

A. No, no hay necesidad de apagar los dispositivos. Una actualización de AP es un proceso seguro, y todo puede permanecer encendido. Asegúrese de que no estar conectado a un servidor TFTP.

## Q. ¿Dónde puedo encontrar instrucciones sobre cómo actualizar Cisco IOS® en los AP Cisco Aironet?

A. Consulte Trabajo con las Imágenes de Software para conocer las instrucciones sobre cómo actualizar el Cisco IOS en el AP.

**Nota:** Utilice la opción **force-reload** con el **comando archive download-sw**.

**Nota:** Cuando usted actualiza el AP o puentea el software del sistema ingresando el **comando archive download-sw** en CLI, debe utilizar la opción de **force-reload**. Si el AP o bridge no recarga la memoria Flash después de la actualización, es posible que las páginas en la interfaz del navegador web no reflejen la actualización. Este ejemplo muestra cómo actualizar el software del sistema usando el **comando archive download-sw**:

```
AP#archive download-sw /force-reload /
overwrite tftp://10.0.0.1/image-name
```

## Q. Tengo 1100 AP. Quiero actualizar la radio AP de IEEE 802.11B a IEEE 802.11g. Si actualizo la radio en el AP, ¿puedo utilizar las tarjetas de PC existentes? ¿O debo actualizar las tarjetas de PC también? Actualmente, las tarjetas son tarjetas

### 802.11b.

A. Una actualización de la radio 802.11b a 802.11g no conlleva una mejora del rendimiento si usted utiliza solamente clientes 802.11b. Una ventaja de una actualización de radio a 802.11g es que usted pueda conectar clientes 802.11b y 802.11g con el AP. Con la actualización, los clientes 802.11b se conectan a 11 Mbps y los clientes 802.11g se conectan a 54 Mbps.

### Q. ¿Cómo configura el AP de nuevo según su configuración predeterminada de fábrica?

A. Consulte Procedimiento para la Recuperación de la Contraseña para el Equipo Cisco Aironet.

## Preguntas Frecuentes sobre Troubleshooting

### Q. He hecho algunos cambios de configuración en el AP. Cuando intento guardar los cambios, recibo este mensaje en el AP: **"Error writing new config file "flash: /config.txt.new" nv_done: unable to open "flash: /config.txt.new" nv_done: unable to open "flash: /private-multiple-fs.new" [OK]". ¿Qué significa el mensaje?**

A. Este mensaje de error indica que no hay espacio en la memoria Flash para guardar la nueva configuración. Intente eliminar los archivos crash viejos que existan. O, si hay más de una versión del Cisco IOS Software, elimine la que usted no utilice. Esto puede liberar algo de espacio en la memoria Flash. Ejecute el **comando dir flash** para determinar si hay algunos archivos crashinfo de excepción viejos que pueda eliminar o imágenes viejas que no se utilicen. Ejecute el **comando write memory** para liberar espacio de modo que usted pueda escribir la configuración en la memoria.

### Q. Utilizo Aironet Client Utility (ACU) 6.3 y los Puntos de Acceso (AP) Cisco 1200 que ejecutan Cisco IOS Software Release 12.3(8)JA. Cuando el cliente inalámbrico se asocia con el AP, el nombre AP no se visualiza en ACU. ¿por qué?

A. El **nombre AP** es el nombre de host para el AP. Si las extensiones Aironet están habilitadas en el AP, el nombre AP se visualiza en ACU.

Si usted no desea ver el nombre AP, puede inhabilitar las extensiones Cisco Aironet al estándar IEEE 802.11B (**no dot11 extensions aironet** en la interfaz de radio). Las extensiones Cisco Aironet están habilitadas de forma predeterminada en el AP.

Si previamente están inhabilitadas, puede habilitar las extensiones Cisco Aironet con este comando:

```
AP(config-if)#dot11 extension aironet
```

En una señalización, el AP incluye un elemento de información que es propiedad de Cisco y que contiene el nombre AP. Si usted apaga las extensiones Aironet en el AP, el AP no señaliza su nombre. Consulte Cómo Inhabilitar y Habilitar las Extensiones Aironet para obtener más información sobre las extensiones Aironet.

### Q. Mi punto de acceso (AP) acepta y se conecta solamente con un cliente en un

## momento. ¿Cuál puede ser el motivo?

A. Un motivo posible podría ser que el parámetro **max-associations** está configurado en **1** en la configuración del identificador de conjunto de servicios (SSID). Utilice el comando **max-associations** SSID configuration mode para configurar la cantidad máxima de asociaciones soportadas por la interfaz de radio (para el SSID especificado). Utilice la forma **no** del comando para restablecer el parámetro en el valor predeterminado. Este máximo predeterminado es 255.

## Q. ¿Cómo recuperar contraseñas olvidadas?

A. Consulte Procedimiento para la Recuperación de la Contraseña para el Equipo Cisco Aironet.

## Q. Los números de serie no aparecen en ninguno de los BR350 o los AP350 que tenemos por comandos. Estos son VxWorks y no se han convertido al IOS. ¿Cómo recupero esta información de los dispositivos?

A. Los AP y bridges Serie 350 que ejecutan VxWorks no muestran el número de serie en el software. La única manera de identificar el número de serie en estas unidades es examinar físicamente la etiqueta en el hardware mismo.

## Q. ¿Cuáles son las posibles fuentes de interferencia para el link de radiofrecuencia (RF) de AP?

A. La interferencia puede provenir de diversas fuentes, por ejemplo:

- Teléfonos inalámbricos de 2.4 GHz
- Hornos de microondas incorrectamente protegidos
- Equipos de red inalámbrica que fabrican otras compañías

Los motores eléctricos y las piezas de metal móviles de maquinaria también pueden causar interferencia. Si desea más información, consulte estos documentos:

- Troubleshooting de Problemas que Afectan la Comunicación de Radiofrecuencia
- Problemas de Conectividad Intermitente en los Bridges Inalámbricos

## Q. Veo el mensaje de error: %C4K_EBM-4-HOSTFLAPPING:Host [mac-addr] in vlan [num] is flapping between port [num] and port [num] connected to the Access Points. ¿Cómo se resuelve esto?

A. Este mensaje de error ocurre cuando el switch obtiene la misma dirección MAC a través de puertos múltiples. Esto puede deberse a estos motivos:

1. Cuando un cliente se traslada de un AP a otro AP, el nuevo AP informa al cliente la dirección MAC al switch. Si ambos AP están conectados con el mismo switch, la dirección MAC del cliente se asocia con ambos puertos del switch conectados con los AP. Esto crea una entrada duplicada para el cliente y genera este mensaje de error hasta el momento en que el switch sincroniza su tabla CAM. Este mensaje de error es muy normal en un entorno de red inalámbrica; sin embargo, si ocurre demasiado traslado, esto puede sobrecargar el CPU del switch. Verifique el firmware y el driver del cliente. Además, asegúrese de que la cobertura

sea buena de modo que el cliente no se traslada a menudo.
2. Cuando hay un loop, el switch puede obtener la misma dirección MAC a través de múltiples puertos conectados con otros switches. Asegúrese de que TP esté habilitado en el switch.

## Q. ¿Por qué la tarjeta del cliente no se asocia al AP más cercano?

A. Si hay AP múltiples en su topología de red inalámbrica, su cliente mantiene una asociación con el AP al cual el cliente se asoció originalmente, hasta que el cliente pierda las señalizaciones keepalive de ese AP. Si se pierde el contacto y si los intentos de recuperar el contacto con el AP original continúan fallando, el cliente busca otro AP. El cliente intenta asociarse a este nuevo AP si el cliente tiene autorizaciones y derechos suficientes en el nuevo AP.

## Q. Tengo un Cisco AP y Cisco Secure Access Control Server (ACS) 3.2. Tengo implementado el protocolo Extensible Authentication Protocol (EAP) en la red. Los usuarios no están autentidados por el servidor RADIUS. Cuando ejecuto los comandos debug en el AP, obtengo este resultado: **"Jun 2 15:58:13.553: %RADIUS-4-RADIUS_DEAD: RADIUS server 10.10.1.172:1645,1646 is not responding. Jun 2 15:58:13.553: %RADIUS-4-RADIUS_ALIVE: RADIUS server 10.10.1.172:1645,1646 has returned. Jun 2 15:58:23.664: %DOT11-7-AUTH_FAILED: Station 0040.96a0.3758 Authentication failed."** ¿Por qué veo estos mensajes de error en el AP?

A. Uno de los motivos por los que aparecen estos mensajes de error es que el secreto compartido no es lo mismo en el AP y ACS. Este error es común cuando usted configura EAP. Si hay una discordancia de secreto compartido entre el AP y ACS 3.2, EAP no funciona. El servidor RADIUS no acepta los paquetes que envía el AP. Asegúrese de que el secreto compartido en el AP coincida con el que está configurado en el servidor ACS. Para obtener información sobre cómo ejecutar un debug, consulte las Autenticaciones de Debug.

## Q. Cuando vi los logs en el AP, encontré este error: **"Mar 9 11:05:26.225 Information Group rad_acct: Radius server 10.10.1.172:1645,1646 is responding again (previously dead). Mar 9 11:03:09.361 Error Group rad_acct: No active radius servers found."** ¿Cuál es la causa de este error y cómo puedo resolver el problema?

A. El normal ver este log cuando en el AP está establecida la configuración **radius-server deadtime**. Es un log de información y no un problema principal. Utilice el **comando radius-server deadtime** para establecer un intervalo durante el cual el AP no intente utilizar servidores que no responden, lo que permite evitar la espera para que finalice una solicitud antes de intentar con el siguiente servidor configurado. Un servidor marcado como inactivo es omitido por las solicitudes adicionales durante los minutos que usted especifique, hasta 1440 (24 horas).

## Q. Tengo un AP1230 con Cisco IOS Software Release 12.3(4)JA. Cuando actualizo la lista de control de acceso (ACL), recibo este mensaje: **"% Warning: Saving this config to nvram may corrupt any network management or security files stored at the end of nvram. ¿Continúe? [no]: ″**

A. Esto es un mensaje de advertencia y no un error. Si usted selecciona [no], no se guarda en los puntos de acceso (AP). Las configuraciones no se guardan en la RAM no volátil (NVRAM); se guardan en la memoria Flash.

Aunque es una advertencia, usted tiene un problema de memoria en este AP. Usted tiene

numerosos archivos .rcore que ocupan mucho espacio en su memoria. Este resultado muestra un ejemplo:

```
AP(config-if)#dot11 extension aironet
```

Para limpiar la memoria, borre todos los archivos .rcore de la memoria Flash.

Este es un ejemplo del comando que debe ingresar en el modo enable:

```
ap#delete flash:r13_5705_9760_1EA7A81E.rcore
```

**Nota:** Ejecute este comando **delete flash:** para cada archivo .rcore en su memoria Flash.

## Q. Tengo un Módulo de Servicios de LAN Inalámbrica (WLSM) con el Cisco IOS Software Release 12.4(4)T1 instalado. Las conexiones a los clientes se están interrumpiendo. Después de mirar los logs, veo varios mensajes como "Previous authentication no longer valid"y "Disassociated because sending station is leaving (or has left) BSS". ¿Cuál es el problema?

A. Ambos mensajes señalan un problema de RF. Asigne diferentes canales en el AP para reparar este problema.

## Q. Los AP Cisco Aironet en mi red WLAN no transmiten los identificadores de conjunto de servicio (SSID). ¿Cuál puede ser el motivo? ¿Debo habilitar una función particular en el AP?

A. Mientras no habilite el modo Guest en el Administrador SSID, el AP no transmite el SSID en sus señalizaciones. Usted puede verificar con un cliente y realizar un escaneo en busca de SSID para asegurarse de que no se enumera.

Para habilitar al modo guest en un SSID, escriba este comando en el AP en el modo global configuration:

```
Ap<config>#dot11 ssid ssid-string
Ap<config-ssid>#guest-mode
```

## Q. Tengo mi AP AIR-AP1231G-A-K9. ¿Por qué no veo una opción para activar la radio A en este AP y solamente puedo vea la opción para las radios G? ¿No puedo asociar a los clientes 802.11b a él?

A. El AP AIR-AP1231G-A-K9 tiene una radio G. El numero de pieza AP1231G implica que este tiene solamente radio G. Las radios G son compatibles con las radios B de versiones anteriores, porque funcionan en la misma frecuencia. No hay radio A en esta unidad y por eso usted no puede activarla. Puede ser que necesite agregar el módulo de la radio A. La radio A funciona en una frecuencia diferente (en 5 GHz) de las radios G y B (en 2.4 GHz).

## Q. Tengo un Teléfono IP Inalámbrico Cisco 7920 que se conecta con un AP Cisco.

## Veo que el 7920 está asociado al AP, pero no hay una dirección IP asignada. Utilizo el protocolo Extensible Authentication Protocol (EAP). Veo el mensaje "Info Station [SEP001121ceb9a4]001121ceb9a4 Authenticated", que es seguido por "Info Station [SEP001121ceb9a4]001121ceb9a4 Reassociated" y "Warning EAP retry limit reached for Station [SEP001121ceb9a4]001121ceb9a4". Luego, veo "Info Deauthenticating [SEP001121ceb9a4]001121ceb9a4, reason 'Previous Authentication No Longer Valid' ". ¿Cuál es el problema?

A. El motivo por el que recibe estos mensajes es que el secreto compartido en el AP es diferente del secreto compartido desde el servidor RADIUS. Asegúrese de que las claves secretas compartidas para EAP sean idénticas en ambos. Usted debe escribir de nuevo la clave secreta compartida en el AP y en el servidor RADIUS.

## Q. Tengo un problema con mi AP. Continúa enviando demasiados mensajes RTS en explosiones que causan la desasociación inesperada de los clientes asociados. Estos clientes estaban asociados a este AP en un nivel de señal de entre -91 y -95 dBm. ¿Cuál es el motivo de esta desasociación inesperada? ¿Es esta una conducta esperada del AP?

A. Sí, es una conducta esperada. Su cliente está en el mismo edge de la célula del 1 Mbps. Puesto que usted lo ve en -91 a -95 dBm, se espera la conducta errática.

Instale más AP para abordar este problema. O, si su cobertura deseada está en un área enfocada en lugar de ser omnidireccional, utilice antenas direccionales.

RTS es causado por los mecanismos de reintentos que se ejecutan. El cliente debe responder a un RTS con un CTS, pero, si el cliente los ve en un sniffer como un grupo de aproximadamente ocho tramas RTS sin los CTS correspondientes, el cliente no oye el AP o el cliente está tan lejos que el AP no puede oírlo. Ambos dispositivos tienen que oírse, no solo su AP que oye al cliente. Por lo tanto, si la antena en el cliente no tiene un gran diseño (probable) o su transmisor no transmite en 100 mW (muy probable) o su receptor no está cerca de la sensibilidad de -90 a -95 dBm (casi garantizado si no es un cliente de Cisco), usted obtiene la operación que describe.

## Q. Utilizamos los AP Inalámbricos LWAPP Cisco. Aunque he visto muchas retransmisiones TCP y ACK duplicados en los clientes, no los veo nuestro entorno cableado. ¿Es eso normal para la red inalámbrica?

A. Los paquetes dañados y los paquetes retransmitidos son dos de las métricas fundamental de una WLAN 802.11. El análisis de los paquetes dañados y retransmitidos en 802.11 difiere del análisis en una LAN cableado por tres motivos:

- Primero, las WLAN 802.11 típicamente tienen muchos más paquetes dañados que las LAN cableadas, por lo que la importancia de las tramas dañadas en WLAN 802.11 se mejora.
- En segundo lugar, 802.11 define una capa de link de datos confiable, lo que significa que cada paquete dañado debe dar lugar a una retransmisión. Las LAN cableadas no definen típicamente una capa de link de datos confiable, por lo que una retransmisión ocurre solamente si un protocolo de capa superior confiable está en uso.
- Finalmente, la confiabilidad de la capa superior es típicamente de extremo a extremo, lo que significa que un paquete dañado en cualquier lugar entre el origen y el destino causa una

retransmisión. Una retransmisión 802.11, puesto que ocurre en la capa 2, se implementa entre interfaces inalámbricas, por lo que una retransmisión 802.11 se puede causar solamente por una corrupción en el “segmento” local. Esto hace mucho más fácil identificar la ubicación de la corrupción en una WLAN 802.11 que en una LAN cableado tradicional. Exploremos las implicaciones de estas diferencias.

Uno de los desafíos de un entorno de red inalámbrica es que es difícil determinar si el analizador ve las mismas cosas que los clientes. Las diferencias entre el analizador y el cliente —diferentes radios, antenas o ubicaciones físicas— pueden hacer que el analizador vea cosas diferentes que el cliente. Por ejemplo, si el analizador está lejos del AP, pero el cliente inalámbrico está cercano del AP, el analizador puede ver una trama dañada, mientras que la estación ve una trama sin daño. Puesto que sabemos que cada trama dañada da lugar a una retransmisión, podemos utilizar los números relativos de retransmisiones y de tramas dañadas para evaluar el grado hasta el cual el analizador ve lo que ve la estación en la red.

## Q. Vemos esta transmisión de mensaje syslog en nuestra red. ¿Por qué ocurre esto y cómo lo detenemos?

```
Ap<config>#dot11 ssid ssid-string
Ap<config-ssid>#guest-mode
```

A. Estos mensajes son mensajes de advertencia y se ven cuando se habilita WLAN Override y el ID de WLAN determinado no se selecciona ni se anuncia en una slot/radio.

## Q. Tengo problemas cuando actualizo mi AP usando el servidor TFTP. Cada vez que intento actualizar, agrega una extensión .tar al archivo c1200-k9w7-tar.default de la imagen de actualización, lo que hace que el AP no reconozca el archivo. No pude encontrar una manera de deshacerme de la extensión .tar adicional. (Descargué e intenté solarwind y tftpd32). ¿Qué debo hacer para eliminar este problema?

A. El problema podría ser que el Sistema Operativo esté ocultando el tipo de archivo conocido. Vaya a **My Computer**. Haga clic en **Tools > Folder Options > View**, deslícese hasta encontrar el parámetro **Hide extensions for known file types** y anule la selección de la casilla. Esto debe eliminar el problema.

## Q. Con frecuencia, mis Puntos de Acceso obtienen un mensaje de alarma "high CPU utilization". En estos casos, un reboot del hardware restaura el correcto funcionamiento del Punto de Acceso. ¿Cómo puedo superar este problema?

A. Hay varios motivos por los que los Puntos de Acceso pueden obtener "high CPU utilization."

- Si el Punto de Acceso de Cisco (AP) está conectado con la red a través de un switch, a veces se observa "high CPU utilization" en el AP. Esto se debe a que, de forma predeterminada, todas las VLAN se permiten en el AP del switch con el cual el AP está conectado. Esto puede crear un problema, especialmente cuando se aplica a una gran red. Si todas las VLAN se permiten en el AP, esto puede dar lugar a **high CPU utilization** y la conectividad puede ser afectada. Los clientes asociados al Punto de Acceso enfrentan problemas de rendimiento, y a veces high CPU utilization también puede desconectar la red Inalámbrica.Para evitar este problema, elimine las VLAN en el switch de modo que solamente el tráfico VLAN en el cual el

AP está interesado pase a través del AP.
- Si los Puntos de Acceso se configuran con las interfaces Loopback, a veces "high CPU utilization" se observa en el AP. Aunque las interfaces Loopback se puedan configurar en el AP Cisco, no se soportan en el AP, así que no deben ser configuradas. Se aconseja quitar las interfaces Loopback si se configuran en el AP.**Nota:** Los AP y los bridges no soportan el comando interface loopback.

Como primer paso en el troubleshooting de este problema, ejecute el comando **show process cpu** en el AP. Esto le da una idea de qué procesos utilizan el CPU.

Además, si el AP ejecuta una versión anterior a 12.3(2)JA2, actualice a la versión 12.3(2)JA2, porque hay un problema conocido en las versiones anteriores donde las solicitudes de servicio anularon el CPU.

### Q. El Router Wi-Fi 871W interrumpe las sesiones establecidas mediante wi-fi de modo que la sesión VPN del usuario debe ser restablecida en todo momento. ¿Cuál es la razón?

A. Hay varios motivos posibles que pueden causar este problema. Conecte ambas las antenas con el Router 871W. Cambie el canal a 1, a 6 o a 11 y verifique qué canal recibe el mejor funcionamiento. Además, puede ser que tenga otros AP cerca que puedan causar interferencia. Este es solo un motivo posible.

## Información Relacionada

- Descargas de Productos de Red Inalámbrica Cisco (clientes registrados solamente)
- Preguntas y Respuestas de Cisco Aironet 1240 AG Series
- Preguntas y Respuestas de Cisco Aironet 1230 AG Series
- Guía de Configuración del Cisco Aironet Access Point Software para VxWorks
- Guía de Configuración del Cisco IOS Software para los Puntos de Acceso Cisco Aironet, 12.2(13)JA
- Notas Técnicas de Troubleshooting de Cisco Aironet 350 Series
- Soporte de Productos de Red Inalámbrica
- Soporte Técnico y Documentación - Cisco Systems