

Red inalámbrica unificada: Resuelva problemas del cliente

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Problemas de configuración](#)

[Discordancia SSID](#)

[Discordancia de la Seguridad](#)

[red inalámbrica \(WLAN\) discapacitada](#)

[Dato-tarifas sin apoyo](#)

[Clientes discapacitados](#)

[Preámbulos de radio](#)

[Características de Cisco Proprietary - Problemas con los clientes del otro vendedor](#)

[Problemas de la dirección IP](#)

[Problemas del cliente](#)

[Problemas RF](#)

[Mensajes de error](#)

[El resolver problemas del cliente con el WCS](#)

[Resolver problemas el WEP](#)

[Resolver problemas el WPA-PSK](#)

[Resolver problemas el 802.1x](#)

[Resolver problemas la red-Auth](#)

[Resolver problemas la dirección del DHCP y IP](#)

[Información Relacionada](#)

[Introducción](#)

El entorno del Radiofrecuencia (RF) es complejo y dinámico. Los diversos factores necesitan ser considerados para crear un buen entorno de red inalámbrica. Este documento explica los diversos problemas que puede encontrar cuando conecta un cliente inalámbrico en un entorno Cisco Unified Wireless, así como los pasos que debe seguir para identificar y resolver estos problemas.

[prerrequisitos](#)

[Requisitos](#)

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco unificó la solución de red inalámbrica
- Configuraciones básicas inalámbricas GUI de los reguladores LAN de Cisco (WLC)

Componentes Utilizados

Este documento es aplicable a todos los dispositivos que participen en el entorno unificado Cisco pero no se restringe a las versiones de software y hardware específicas.

Convenciones

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

Antecedentes

En Cisco el entorno unificado, el WLC asume una función central. Maneja la red inalámbrica entera. Los Puntos de acceso ligeros (revestimientos), que sirven a los clientes de red inalámbrica, se registran al WLC y descargan la configuración entera de WLC. El paso inicial es controlar si el REVESTIMIENTO se registra al WLC. Haga clic el menú inalámbrico del GUI WLC, y controle si el REVESTIMIENTO se enumera en la página.

Problemas de configuración

Para una conexión de red inalámbrica acertada, es esencial que la configuración en el WLC está hecha correctamente. Esta sección describe algunos lo más comúnmente posible - de los problemas considerados de la configuración.

Discordancia SSID

El cliente utiliza su SSID para identificar y para asociarse a la red inalámbrica, así que asegúrese de que el SSID esté configurado idénticamente en el WLC y el cliente. Para controlar el SSID configurado en el WLC, haga clic la página de las **redes inalámbricas (WLAN)**. Haga clic la *red inalámbrica (WLAN)* apropiada, y controle el *SSID* configurado conforme a la *ficha general*.

Nota: *El SSID* es con diferenciación entre mayúsculas y minúsculas. Puede ser que ayude al cliente de red inalámbrica a asociarse a la red inalámbrica (WLAN) si usted suprime y reconstruye la red inalámbrica (WLAN).

Discordancia de la Seguridad

Las configuraciones de Seguridad deben hacer juego entre el WLC y el cliente. Si el tipo de la autenticación es WEP estático, controle si el índice apropiado del clave de encriptación/dominante en el WLC hace juego el del cliente. Si el tipo de la autenticación es 802.1x o WPA, asegúrese de que el tamaño del tipo/de la clave de encriptación de la autenticación haga juego entre el cliente y el WLC. Para más información sobre cómo configurar el WLC y al cliente para las diversas soluciones de la Seguridad, refiera a la [autenticación en los ejemplos inalámbricos de la configuración de los reguladores LAN](#).

Nota: Acode 2 soluciones de la Seguridad, tales como WPA o 802.1x, no puede ser utilizado para una red inalámbrica (WLAN) configurada con las soluciones de la Seguridad de la capa 3, tales como autenticación Web o paso. Para más información sobre la Seguridad compatible las soluciones refieren a la [matriz de compatibilidad inalámbrica de la Seguridad de la capa 2 y de la capa 3 del regulador LAN](#).

[red inalámbrica \(WLAN\) discapacitada](#)

Para una conexión de red inalámbrica acertada, la red inalámbrica (WLAN) correspondiente debe ser activa en el WLC. Por abandono, el estatus de la red inalámbrica (WLAN) no se activa en el WLC. Para activar la red inalámbrica (WLAN), haga clic el menú de las **redes inalámbricas (WLAN)** en el WLC. Se muestra una lista de WLAN configuradas en WLC. Haga clic la red inalámbrica (WLAN) que se configura con el SSID al cual el cliente quiere asociarse. Conforme a la ficha general de las **redes inalámbricas (WLAN)** > **corrija la página**, controlan el cuadro del estatus.

[Dato-tarifas sin apoyo](#)

Para un estándar determinado, 802.11b/g o 802.11a, usted puede fijar opcionalmente ciertas tarifas de datos como obligatorio y otras tarifas de datos según lo utilizadas o inhabilitadas en el WLC. Para una asociación acertada, un cliente de red inalámbrica debe utilizar las tarifas de datos que se configuran como obligatorias en el WLC. Para controlar las tarifas de datos configuradas en el WLC, hacer clic el menú **inalámbrico** en el GUI WLC, y controlar las tarifas de datos configuradas bajo **802.11b/g/n > red o 802.11a/n > opción de red** que aparece en el lado izquierdo de la página. Controle la página de soporte del vendedor del cliente para determinar esto. Si usted actualiza el driver del cliente, puede ayudar al cliente a utilizar las tarifas de datos requeridos.

Nota: Para una mejor Conectividad, fije la tarifa de datos más baja a **obligatorio** en el WLC y otras tarifas de datos a **utilizado**.

[Clientes discapacitados](#)

En el WLC, hay una opción para inhabilitar manualmente a los clientes. Esta característica ayuda a evitar que los clientes no fiables intenten tener acceso a la red. Controle si la dirección MAC del cliente que no puede asociarse se encuentra en los clientes discapacitados enumera, y, si es así la quitan. Usted puede encontrar la lista de clientes discapacitados cuando usted hace clic la **opción de clientes discapacitada** bajo **menú de seguridad** en el GUI.

Nota: Los clientes pueden ser negados la asociación a la red si no siguen las directivas de la exclusión del cliente del valor por defecto configuradas en el WLC. Para más información sobre la directiva de la exclusión del cliente, refiera a la sección de las [directivas de la exclusión del cliente que configura de la guía de configuración inalámbrica del regulador LAN de Cisco, la versión 4.2](#).

[Radie los preámbulos](#)

El preámbulo de radio (a veces llamado una encabezado) es una sección de los datos en el jefe de un paquete, que contiene la información que los dispositivos de red inalámbrica necesitan cuando envían y reciben los paquetes.

Algunos clientes no utilizan el **preámbulo corto**, así que no pueden conectar con la red

inalámbrica (WLAN) que tiene **preámbulo corto** activado. Los preámbulos cortos mejoran el desempeño del rendimiento de procesamiento, así que se activan por abandono en el WLC. Para inhabilitar el preámbulo corto, haga clic en el menú **Wireless** de WLC GUI. Haga clic en **802.11b/g** > menú de la red en el lado izquierdo. *Uncheck el cuadro corto del preámbulo.*

Características de Cisco Proprietary - Problemas con los clientes del otro vendedor

Si los dispositivos cliente que no pueden conectar con la red son dispositivos de no-Cisco, inhabilitar algunas de las funciones propietarias de Cisco da lugar a una conexión satisfactoria. Para una lista de características que las ayudas del cliente, entran en contacto con al vendedor del dispositivo cliente de tercera persona.

Éstos son algunas de las funciones propietarias importantes:

- **Aironet IE** - El Aironet IE contiene la información, tal como el nombre del punto de acceso, la carga, número de clientes asociados, etc. enviada por el punto de acceso en las respuestas beacon y sondeo del WLAN. Los clientes CCX utilizan esta información para elegir el mejor punto de acceso con el cual asociarse.
- **MFP** — La protección del capítulo de la Administración es una característica introducida para asegurar la integridad de los bastidores de la Administración, tales como de-autenticación, desasociación, faros, y puntas de prueba en donde el Punto de acceso protege los marcos de la Administración que transmite cuando agrega un elemento de información del control de la Integridad del mensaje (IE MIC) a cada marco. Cualquier tentativa hecha por los intrusos para copiar, altera, o juega de nuevo el marco invalida el MIC, que causa cualquier Punto de acceso de recepción, que se configure para detectar los marcos MFP, para señalar la discrepancia. Estas características se habilitan de forma predeterminada para cualquier WLAN que se cree en el WLC. Para inhabilitar estas características, haga clic en el menú WLAN en el WLC. Se muestra una lista de WLAN configuradas en WLC. Haga clic en WLAN a la que el cliente desea asociarse. En la pestaña Advanced de WLAN > Edit page, desmarque las casillas que corresponden a Aironet IE y MFP.
- **Radie los preámbulos** — El preámbulo de radio (a veces llamado una encabezado) es una sección de los datos en el jefe de un paquete que contenga la información que el dispositivo de red inalámbrica y los dispositivos cliente necesitan para enviar y para recibir los paquetes. Usted puede fijar el preámbulo de radio a de largo o poner en cortocircuito dependiendo de qué configuración se utiliza en el cliente de red inalámbrica.
- **Transformación de la encapsulación de los Ethernetes** — Cuando el dispositivo de red inalámbrica recibe los paquetes de datos que no son 802.3 paquetes, el dispositivo de red inalámbrica debe utilizar un método de la transformación de la encapsulación para formatear los paquetes a 802.3. Aquí están los dos métodos de la transformación: 802.1H: Este método proporciona al rendimiento óptimo para los Productos de Aironet de red inalámbrica de Cisco. 802.1H es la configuración por defecto. RFC1042: Utilice esta configuración para asegurar la Interoperabilidad con el equipo del Aironet de red inalámbrica de no-Cisco. El RFC1042 no proporciona a las ventajas de la Interoperabilidad de 802.1H, sino es utilizado por otros fabricantes de equipo de red inalámbrica.
- **descanso del apretón de manos del wpa** — Algunos vendedores necesitan descansos más largos del apretón de manos del wpa. Usted puede utilizar el **comando timeout del apretón de manos del wpa dot11** para cambiar el descanso del apretón de manos del wpa.
- **ssid** — Algunos vendedores requieren el ssid ser difusión. Para difundir el ssid, *modo de*

invitado del permiso bajo configuración del ssid.

Problemas de la dirección IP

Los clientes de red inalámbrica necesitan los IP Addresses válidos comunicar con el resto de la red.

El regulador se comporta como un router con ayuda IP un direccionamiento. Es decir, completa la dirección IP y los unicasts del gateway él al servidor del DHCP vía el interfaz dinámico en el cual el cliente está instalado. Sea tan consciente que la vigilancia del tráfico del DHCP en el Switches, por abandono, bloqueará estos paquetes del DHCP en los puertos untrusted.

Cuando la oferta de DHCP vuelve al controlador, éste cambia la dirección IP del servidor DHCP a su dirección IP virtual. La razón que hace esto es porque cuando Windows vaga por entre los APs, la primera cosa lo hace es intento para entrar en contacto con el servidor del DHCP y para renovar su direccionamiento.

Con la dirección del servidor del DHCP de 1.1.1.1 (que es la dirección IP virtual típica en un regulador), el regulador puede interceptar ese paquete y falsificar hacia fuera Windows. Ése es también porque la dirección IP virtual es lo mismo en todos los reguladores. Si un equipo portátil de Windows se traslada a un AP en otro controlador, intentará entrar en contacto con la interfaz virtual en el controlador. Debido al evento de la movilidad y a la transferencia del contexto, el nuevo regulador a los cuales el cliente de Windows vagó por ya tiene toda la información para falsificar hacia fuera Windows otra vez.

Si usted quiere utilizar el servidor interno del DHCP, todo lo que usted tiene que hacer se pone la dirección IP de la Administración como el servidor del DHCP en el interfaz dinámico usted crea para la subred. Después asigne esa interfaz a la WLAN. La razón de que el controlador necesite una dirección IP en cada subred es para que pueda completar la dirección del gateway DHCP en la solicitud DHCP.

Vemos muchos problemas de la dirección IP DHCP. Aquí están las razones y los pasos para resolver estos problemas:

1. Si el tipo de autenticación configurado es una de las soluciones de la Seguridad de la capa 2, tales como 802.1x o WPA, el cliente debe autenticar con éxito para obtener una dirección IP válida. En primer lugar controle si autentican al cliente con éxito. **Nota:** Una excepción es si configuran al cliente para las soluciones de la Seguridad de la capa 3, tales como [autenticación Web](#), o asignan el cliente del [paso de la red una](#) dirección IP antes de la autenticación.
2. Cada red inalámbrica (WLAN) definida en el WLC se asocia a un interfaz dinámico del WLC, que se configura con un VLA N que pertenezca a una subred única. Asignan los clientes que se asocian a esta red inalámbrica (WLAN) los IP Addresses de la subred del interfaz del VLA N. Controle si la subred IP y el gateway de esta red inalámbrica (WLAN) se definen en el servidor del DHCP para que al cliente obtenga una dirección IP en esta subred. Refiera a la documentación del vendedor apropiado para configurar el servidor del DHCP. **Nota:** Como requisito previ6, se gira el control si el servidor del DHCP es accesible del WLC y si el servicio del DHCP.
3. Asegúrese de que la dirección IP del servidor del DHCP esté definida correctamente en el interfaz del WLC que se asocia a la red inalámbrica (WLAN). Para controlar esto, haga clic el

menú del **regulador** en el GUI. Haga clic el menú de los **interfaces** en el lado izquierdo, y controle el campo del servidor del **DHCP**. En la misma página, controle que el interfaz está asociado a un *puerto físico* que sea ascendente y activo. Para resolver problemas los temas relacionados del DHCP, utilizar los comandos `debug dhcp packet enable` y **poner a punto el permiso del mensaje DHCP** en el WLC. **Nota:** Usted puede también configurar WLC como servidor del DHCP. Para más información sobre cómo configurar el DHCP separe en el WLC, refieren a [usar el GUI para configurar la sección del DHCP de la guía de configuración inalámbrica del regulador LAN de Cisco del documento, la versión 5.0.](#)

4. El proxy del DHCP se activa por abandono en el WLC. Unicasts WLC el paquete al servidor del DHCP configurado en el interfaz o la red inalámbrica (WLAN) sí mismo de la red inalámbrica (WLAN). Si el servidor del DHCP no utiliza el comportamiento del proxy del DHCP de Cisco, inhabilite el proxy del DHCP en el WLC. Para más información sobre cómo inhabilitar el proxy del DHCP en el WLC, refiera a [configurar la sección del proxy del DHCP de la guía de configuración inalámbrica del regulador LAN de Cisco, la versión 5.2.](#)
5. WLC conecta generalmente con la red alámbrica a través de un conmutador. Controle si los puertos del switch que están conectados con el WLC y el servidor del DHCP se configuran como tronco y que no se prohíben los VLA N apropiados en esos puertos. Para más información sobre cómo configurar el Switches de Cisco, refiera al [configurar el puerto del 2 Switch de la capa que conecta con el WLC como sección del puerto troncal de la red inalámbrica \(WLAN\) del invitado del documento y de la red inalámbrica \(WLAN\) interna usando el ejemplo de la configuración de WLCs.](#)
6. No se permite a los clientes estáticos asociarse a la red inalámbrica (WLAN) si el **Addr del DHCP. El campo de la asignación** se activa para la red inalámbrica (WLAN). Esta opción necesita que todos los clientes que se asocian a esta red inalámbrica (WLAN) deben obtener los IP Addresses con el DHCP. Para controlar si se activa esta opción, haga clic el menú de las redes inalámbricas (WLAN) en el GUI WLC. Se muestra una lista de WLAN configuradas en WLC. Haga clic la red inalámbrica (WLAN) apropiada. Vaya a la **ficha Avanzadas** y localice el campo de la **asignación de dirección del DHCP**.
7. Algunos servidores del DHCP, tales como un Firewall de Cisco PIX, no utilizan los servicios de la retransmisión del DHCP. Validan solamente los paquetes del DHCP de la difusión, no ningunos paquetes de unidifusión de un Agente Relay del DHCP, así que asegúrese de que los clientes DHCP estén conectados directamente con el interfaz en el cual se activa el servidor. **Nota:** Controle el documento apropiado del vendedor para saber si hay soporte de relay del DHCP.

Problemas del cliente

Es igualmente importante que las cosas existen en el lado del cliente. Realice estos controles en el lado del cliente:

1. A veces, el indicador luminoso LED amarillo de la placa muestra gravedad menor del cliente no es reconocido por el ordenador. En ese caso, intente el indicador luminoso LED amarillo de la placa muestra gravedad menor en una diversa ranura. Si no trabaja, inténtela en un equipo diferente. Para más información sobre los problemas dentro de la instalación, refiera a la sección de [troubleshooting del documento Cisco Aironet 340, 350, y guía de instalación y configuración inalámbrica de los adaptadores del cliente LAN CB20A para Windows.](#) **Nota:** Asegúrese de que la placa de red inalámbrica sea compatible con el sistema

operativo que está instalado en la máquina. Esto se puede controlar de la hoja de datos del indicador luminoso LED amarillo de la placa muestra gravedad menor del cliente.

2. Controle si el cliente está instalado correctamente en la máquina. El estatus del indicador luminoso LED amarillo de la placa muestra gravedad menor del cliente se puede controlar de la pantalla del **administrador de dispositivos de Windows**. Busque el mensaje que lee, *“este dispositivo está trabajando correctamente.”* Si no es, indica que los drivers no están instalados correctamente. Intente desinstalar el driver y reinstalar los drivers en la máquina. Para desinstalar los drivers, hacer clic derecho el adaptador de red inalámbrica de la pantalla y del tecleo del administrador de dispositivos **desinstale**. Para más información sobre cómo reinstalar el adaptador del cliente, refiera a [instalar la sección del adaptador del cliente del documento Cisco Aironet 340, 350, y guía de instalación y configuración inalámbrica de los adaptadores del cliente LAN CB20A para Windows](#). **Nota:** Si usted utiliza el ACU para configurar el indicador luminoso LED amarillo de la placa muestra gravedad menor del cliente, asegúrese de que la radio no esté inhabilitada en el ACU. Además, controle si el estatus del indicador luminoso LED amarillo de la placa muestra gravedad menor se activa bajo **conexión de red** en el panel de control de Windows. **Nota:** Utilice solamente un software del suplicante para la placa de red inalámbrica. Se recomienda siempre para utilizar vendedor-proporcionó al suplicante para el indicador luminoso LED amarillo de la placa muestra gravedad menor. Como opción secundaria, usted puede utilizar el que está proporcionado por el vendedor de la PC o el WZC proporcionado por el Windows. **Nota:** Complete estos pasos para poner a punto WZC: Utilice el **seguimiento fijado los ras del netsh * comando enabled** para girar el depuración WZC. Utilice el **seguimiento fijado los ras del netsh * comando discapacitado** para apagar el depuración WZC. Los registros se escriben a *C:\Windows\tracing. eapol.log, rastls.log, y wzctrace.log* son los registros más importantes. **Nota:** Refiera a los [diagnósticos inalámbricos y al troubleshooting](#) para más información.
3. La configuración en el cliente debe hacer juego el de WLC. Esto refiere principalmente al SSID y a la configuración de Seguridad en el cliente. Si usted utiliza la utilidad de Cisco para configurar al cliente, refiera a [usar la sección del encargado del perfil del documento Cisco Aironet 340, 350, y guía de instalación y configuración inalámbrica de los adaptadores del cliente LAN CB20A para Windows](#).
4. Si usted no puede transferir los datos, incluso después una asociación de red inalámbrica acertada, intente inhabilitar el resto de los adaptadores así como los del VPN y de los adaptadores atados con alambre. Si hay más de un adaptador de red inalámbrica en la máquina, inhabilite otros adaptadores para evitar los conflictos entre ellos.
5. Si usted encuentra los problemas de la Conectividad solamente con un solo cliente, intente actualizar los drivers y los firmwares de ese cliente. Si usted encuentra los problemas de la Conectividad con una mayoría de los clientes y del usted para haber eliminado otros problemas, elija actualizar el WLC.
6. Asegúrese de que los dispositivos, es decir, cliente y el WLC, sean con certificación Wi-Fi para evitar cualquier problema de interoperabilidad relacionado con la Seguridad y operaciones.
7. Si usted utiliza una máquina de Windows, asegúrese de que usted haya instalado todas las últimas correcciones u hotfixes de la Seguridad disponibles de Microsoft. Si usted utiliza la utilidad del cliente de Windows, asegúrese de que usted haya instalado la última corrección disponible de Microsoft.
8. Algunos clientes responden lentamente a la autenticación EAP. Esto da lugar a los descansos en el WLC, y usted puede recibir este mensaje de error en el WLC:

```
Tue Jul 26 16:46:21 2005: 802.1x 'timeoutEvt' Timer expired for station
<Mac address of the client>
```

En respuesta a este mensaje, aumente los valores del time out EAP en el WLC para proporcionar al tiempo suficiente para que el cliente autentique. Utilice estos comandos de ajustar los temporizadores EAP en el WLC:

```
Tue Jul 26 16:46:21 2005: 802.1x 'timeoutEvt' Timer expired for station
<Mac address of the client>
```

```
Tue Jul 26 16:46:21 2005: 802.1x 'timeoutEvt' Timer expired for station
<Mac address of the client>
```

```
Tue Jul 26 16:46:21 2005: 802.1x 'timeoutEvt' Timer expired for station
<Mac address of the client>
```

Problemas RF

Interferencia RF es una de las causas principales para la mala conexión. Interferencia se puede causar por las redes adyacentes del 802.11 u otras fuentes, tales como hornos de microondas o teléfonos inalámbricos que actúen en la misma frecuencia. Interferencia causada por las redes adyacentes del 802.11 es de dos tipos:

- **Interferencia del cocanal:** Cuando los Puntos de acceso, cuya área de cobertura solapa, se configuran en el mismo canal o los canales con las frecuencias que solapan, él causan los problemas de la Conectividad para los clientes en la área de cobertura que solapa. Para evitar este problema, cambia el número de canal a un canal sin traslapo, o separa el Punto de acceso más lejos de modo que sus áreas de cobertura no solapen. Por ejemplo, en 802.11b/g, los canales 1, 6, y 11 de la red son canales sin traslapo.
- **Interferencia adyacente:** Cuando los Puntos de acceso se ponen demasiado cerca el uno al otro o utilizan los niveles de potencia de alto rendimiento, causa interferencia, incluso cuando los Puntos de acceso se configuran en los canales sin traslapo. Disminuya la potencia del Punto de acceso de fijar este problema. **Nota:** Los canales sin traslapo también se llaman los canales adyacentes, que explica la *interferencia adyacente del nombre*.

Utilice los analizadores de espectro para localizar las fuentes de interferencia, tales como hornos de microondas o los teléfonos inalámbricos que actúen en el rango 2.4 gigahertz, o los dispositivos que actúan en el rango 5 gigahertz. Quite las fuentes de interferencia una vez que se identifican. Alternativamente, usted puede cambiar el estándar en el cual su red inalámbrica actúa, por ejemplo, desde 802.11b/g al 802.11a para evitar interferencia.

Otro aspecto importante para la comunicación eficaz RF es potencia de la señal. La potencia de la señal pobre lleva a la conexión intermitente. Los obstáculos, tales como paredes, los metales, absorben y reflejan la energía RF, que reduce la potencia de la señal. Aumente la potencia al nivel requerido en el Punto de acceso de proporcionar a la cobertura adecuada. Usted puede también utilizar las antenas de alto alcance para ampliar el rango y la potencia de la señal, pero se asegura de que es FCC aprobada para actuar con el dispositivo.

Nota: La relación señal-ruido (SNR), que es la diferencia entre la potencia de la señal y el ruido RF (la señal o la energía RF de otras fuentes que actúan en la misma frecuencia como la red inalámbrica), es factor clave para medir la calidad del link. Un SNR más alto indica una buena calidad del link, que da lugar a una Transferencia de datos más rápida. Un valor inferior indica la baja calidad, que lleva a la Conectividad intermitente o al rendimiento pobre. Los analizadores de

paquete inalámbricos/el software del estudio sobre el sitio pueden mostrarle el SNR y la producción en una ubicación determinada.

En el entorno unificado Cisco, hay un concepto llamado Administración de recursos de radio (RRM) ejecutado en el WLCs. RRM es un software integrado en el regulador, que actúa como ingeniero RF del accesorio para proporcionar constantemente a la Administración en tiempo real RF de su red inalámbrica. Toma automáticamente el cuidado de todos los problemas mencionados RF. Para más información encendido RRM, refiera a la sección de [administración de recursos de radio que configura de la guía de configuración inalámbrica del regulador LAN de Cisco del documento, la versión 5.0.](#)

Mensajes de error

En medio del curso de la Conectividad del cliente, usted puede recibir los mensajes de error múltiple, en los lados WLC y del cliente.

- **El cliente no puede cualquier conseguir un retraso de la dirección IP o del encuentro en conseguir la dirección IP con el DHCP. El DHCP de la depuración en el regulador indica esto:**

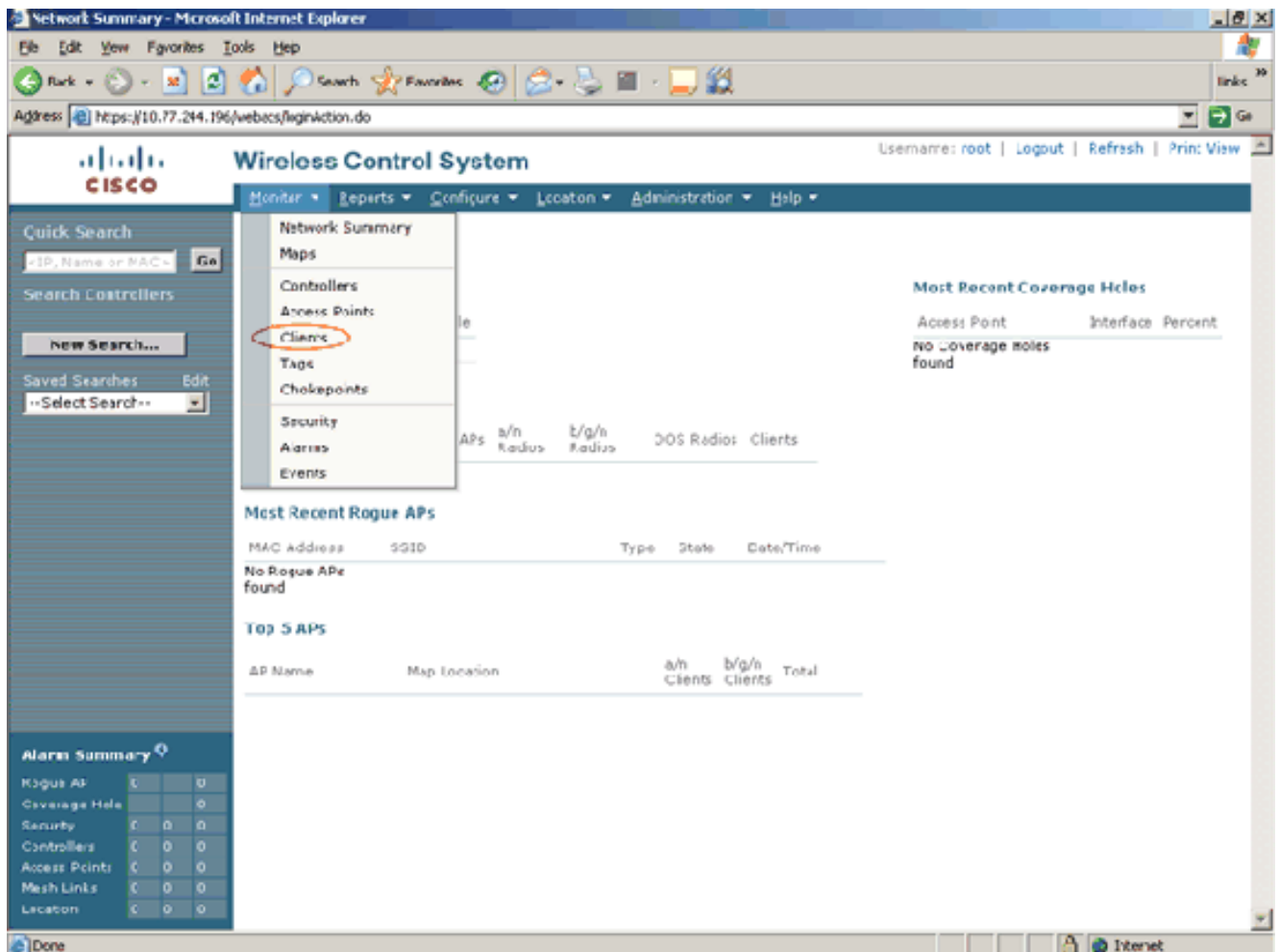
```
Sun Nov 9 22:09:05 2008: <mac address of the client> DHCP processing DHCP NAK
```

El NAK del DHCP es enviado generalmente por el servidor del DHCP para indicar una tentativa del cliente de obtener una dirección IP de la subred a la cual no pertenece. Esto ocurre generalmente cuando un cliente vaga por a partir de un WLC a otro, donde la misma red inalámbrica (WLAN) se asigna un diverso VLA N. Configure el proxy del DHCP en el WLC para proporcionar a un arreglo para esto.

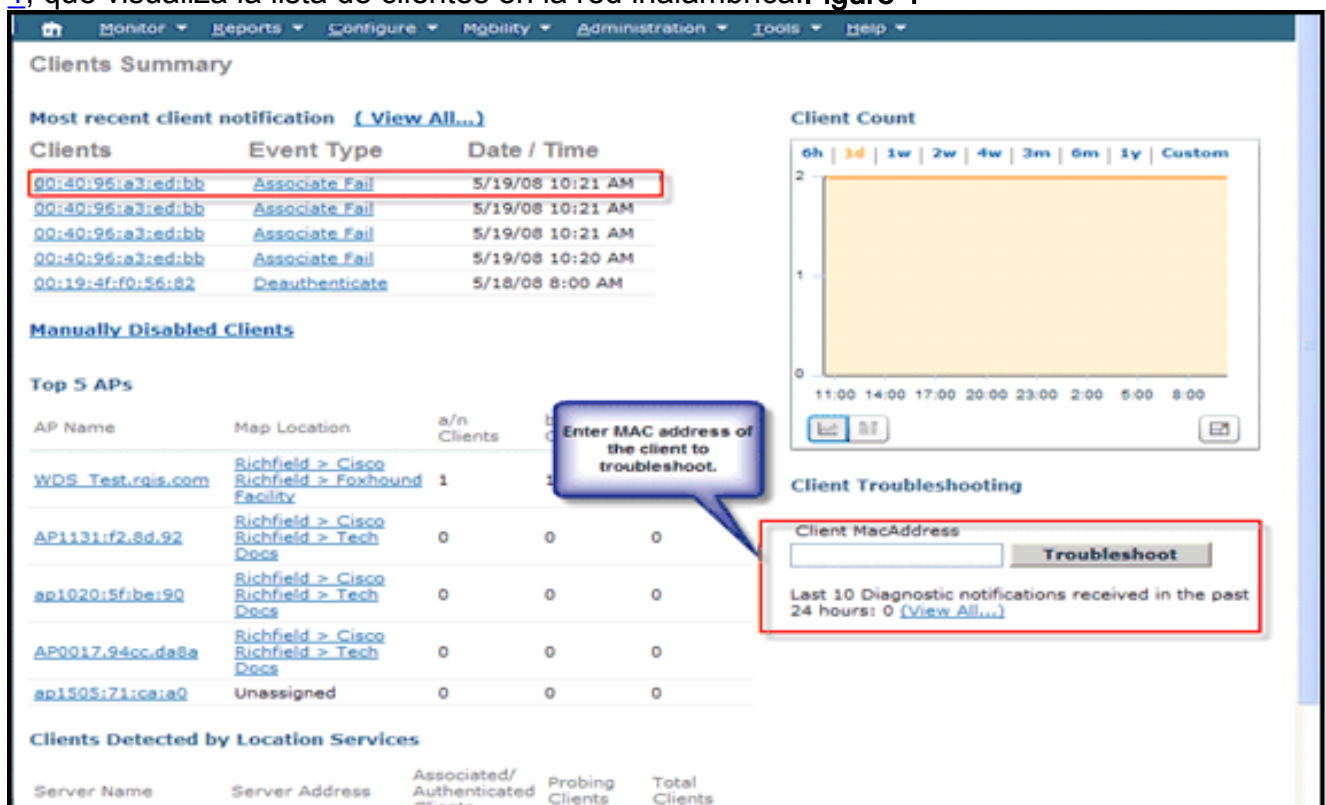
El resolver problemas del cliente con el WCS

El WCS se puede utilizar para resolver problemas los problemas cliente-relacionados en un entorno de red inalámbrica. Hace esto con la ayuda de la herramienta del troubleshooting incorporada al WCS. Para resolver problemas a un cliente con el WCS, necesidad de usuarios de realizar estos pasos

1. De la página del panel WCS, haga clic el menú del **monitor** y elija a los **clientes de la lista**.



2. Esto saca a colación la página de resumen del cliente tal y como se muestra en del [cuadro 1](#), que visualiza la lista de clientes en la red inalámbrica. **Figure 1**



3. Haga clic a un cliente para conseguir los detalles tales como el SSID o el método de autenticación de un cliente particular. [El cuadro 2](#) muestra un ejemplo de esto. El cuadro de diálogo del **Troubleshooting** en el Lado derecho inferior de la página de resumen del cliente

mostrada en el [cuadro 1](#) permite que los usuarios ingresen en el MAC address del dispositivo para resolver problemas. Esto le trae a la página de la herramienta del troubleshooting tal y como se muestra en del [cuadro 3](#). sobre la identificación y la selección del cliente a resolver problemas, los usuarios se presenta con la página de los detalles del cliente: **Figure 2**

The screenshot shows the Cisco WCS interface for a client named 'miadler'. The 'CCxV5' tab is selected and highlighted with a red box. The page is divided into two main sections: 'Client Properties' and 'RF Properties'. The 'Client MAC Address' is highlighted in yellow in the Client Properties table. The 'SSID' is highlighted in yellow in the RF Properties table.

Client Properties	
Client User Name	miadler
Client IP Address	10.50.10.233
Client MAC Address	00:40:96:a3:ed:bb
Client Vendor	Cisco
Controller	10.50.10.26
Port	1
Interface	management
VLAN ID	0
802.11 State	Associated
Mobility Role	Local
Policy Manager State	RUN
Anchor Address	0.0.0.0
Mirror Mode	Disable
CCX	V5
E2E	Not Supported
WGB Status	Regular Client

RF Properties	
AP Name	AP1240-ma-3fa4
AP Type	Cisco AP
AP Base Radio MAC	00:13:5f:0e:59:b0
Protocol	802.11a
AP Mode	local
Profile Name	sevt-pod1-ef
SSID	pod1-ef
Security Policy	
Association Id	1
Reason Code	None
802.11 Authentication	OPENSYSYEM

Security	
Authenticated	Yes
Policy Type	WPA2
Encryption Cipher	ccmpAes
EAP Type	EapFast
NAC State	Access

[Resolver problemas el WEP](#)

Los clientes de red inalámbrica de la herencia que todavía utilizan los mecanismos de seguridad WEP son a menudo duros de resolver problemas. Realice estos controles en el cliente y el AP:

- Longitud de clave WEP (y discrepancias de clave)
- Índice de clave WEP (y discordancias de la configuración)
- Método de autenticación configurado (ábrase contra la clave compartida)

[Discordancia de la autenticación](#)

Aunque la captura de los paquetes pueda ser un proceso aburrido, la herramienta del troubleshooting del cliente WCS puede ayudar fácilmente a señalar donde existe el problema. A menudo, este pequeño "TIP" es qué reduce el resolver problemas del tiempo. [El cuadro 2](#) muestra la **herramienta del troubleshooting WCS**. Según lo presentado en la figura, se identifica y se visualiza la etapa problemática, que fija la etapa para la análisis detallado.

Figure 3

CISCO Wireless Control System

Troubleshooting Client '00:40:96:a3:ed:bb'

Summary | Log Analysis | Event History | ACS View Server

802.11 Association | Open Authentication | IP Address Assignment | Successful Association

Problem

802.11 Association Failure

Suggested Action

- Potential mismatch of security type. Please check client supplicant configuration.

[Discordancia del índice de clave WEP](#)

Usted puede configurar generalmente hasta 4 claves WEP en el cliente y el AP. Una de las claves se elige como la clave de transmitir. Esto debe hacer juego entre el cliente y el AP. Por ejemplo, si la clave 2 se elige como la clave de transmitir en el cliente, esto debe hacer juego con la clave 2 en el AP, pero el AP puede tener una diversa clave que la clave de transmitir. El Otro problema es a menudo éste: los vendedores del cliente y de la infraestructura interpretan las especificaciones diferentemente, que causa diversas puestas en práctica en el producto. Un ejemplo común es el uso de los índices dominantes a partir la 0 a 3 contra los índices dominantes a partir la 1 a 4. Esto puede dar lugar a la configuración no coincidente y la falla de conexión intenta. En ese momento, la mucha atención de la paga a la “identificación de la clave” clasificada en el paquete decodifica, que dice si ésa es la causa raíz del problema.

[Resolver problemas el WPA-PSK](#)

El troubleshooting WPA-PSK es similar al WEP en gran medida. La mayoría de los intentos fallidos son debido a los misconfigurations en la clave. Con la herramienta del troubleshooting del cliente WCS, los administradores pueden recoger los registros de la transacción WPA. Los registros, según lo destacado abajo, visualización donde el problema potencial puede estar (*configuración incorrecta de la clave previamente compartida en el cliente en este ejemplo en particular*) y se deriva de la tabulación del **análisis del registro de la** herramienta del

troubleshooting del cliente del WCS. Ponga una red inalámbrica (WLAN) con el WPA-PSK como política de seguridad de la capa 2 y configure al suplicante del cliente con un PSK incorrecto. Éstos son registros de las claves misconfigured PSK en los eventos:

```
<TIMESTAMP> INFO 10.10.10.2
    Controller association request message received.
<TIMESTAMP> INFO 10.10.10.2
    Received reassociation request from client.
<TIMESTAMP> INFO 10.10.10.2
    The wlan to which client is connecting requires 802 1x authentication.
<TIMESTAMP> INFO 10.10.10.2
    Client moved to associated state successfully.
<TIMESTAMP> ERROR 10.10.10.2
    802.1x authentication message received, static dynamic wep supported.
<TIMESTAMP> ERROR 10.10.10.2
    Expecting EAPOL key from client but not received yet.
<TIMESTAMP> ERROR 10.10.10.2
    EAPOL-key is retransmitted.
<TIMESTAMP> ERROR 10.10.10.2
    Expecting EAPOL key from client but not received yet.
<TIMESTAMP> ERROR 10.10.10.2
    EAPOL-key is retransmitted.
<TIMESTAMP> ERROR 10.10.10.2
    Expecting EAPOL key from client but not received yet.
<TIMESTAMP> ERROR 10.10.10.2
    Excluding client as max EAPOL-key re-transmissions reached.
<TIMESTAMP> ERROR 10.10.10.2
    Excluding client as max EAPOL-key re-transmissions reached.
<TIMESTAMP> ERROR 10.10.10.2
    Client 802.1x authentication failure exceeded the limit.
<TIMESTAMP> ERROR 10.10.10.2
    EAPOL-key has possible incorrect psk configuration.
```

CISCO Wireless Control System

Troubleshooting Client '00:40:96:a3:ed:bb'

Summary | Log Analysis | Event History | ACS View Server

802.11 Association | Open Authentication | IP Address Assignment | Successful Association

Problem
802.11 Association Failure

Suggested Action

- Potential mismatch of security type. Please check client supplicant configuration.

[Resolver problemas el 802.1x](#)

Mientras que la adopción de la red inalámbrica (WLAN) llega a ser penetrante, los clientes de la herencia eliminan; el 802.1x es la dirección para la mayoría de las implementaciones futuras. Puede haber una variedad de problemas misconfiguration-relacionados en el encadenamiento (servidor AAA del <> de la red del <> L2/L3 del <> WLC del <> AP del cliente). Aquí se asume que las cosas existen entre el WLC y el servidor AAA. Los problemas que se presentan entre el suplicante (cliente) y el servidor AAA son generalmente éstos:

- Tipo incorrecto EAP
- Certificados vencidos incorrectos de las credenciales
- Método interno incorrecto EAP

En el lado del cliente, modifique las credenciales del usuario bajo ajustes de seguridad; por ejemplo, ingrese la contraseña incorrecta y vuelva a efectuar la misma prueba. La herramienta del troubleshooting señala exactamente donde miente el problema, así como la acción sugerida.

Troubleshooting Client '00:19:d2:64:63:0b'

Summary **Log Analysis** Event History

802.11 Association 802.1X Authentication IP Address Assignment Successful Association

Problem
802.1X Authentication Failure

Suggested Action

- Check whether Radius server(s) is reachable
- Check whether client's choice of EAP method is supported by radius server
- Check Clients username/password/cert is valid
- Check to see if the certificates used by the Authentication server are accepted by the client.

Haga clic la tabulación del **análisis del registro** en la figura mostrada arriba y controle los registros para saber si hay cualquier indicación de una autenticación fracasada del 802.1x.

```
<TIMESTAMP> INFO 10.10.10.2
    Received EAP Response from the client.
<TIMESTAMP> INFO 10.10.10.2
    EAP response from client to AP received.
<TIMESTAMP> INFO 10.10.10.2
    Radius packet received
<TIMESTAMP> INFO 10.10.10.2
    Received Access-Challenge from the RADIUS server for the client
<TIMESTAMP> INFO 10.10.10.2
    Sending EAP request to client from radius server.
<TIMESTAMP> INFO 10.10.10.2
    EAP response from client to AP received.
<TIMESTAMP> INFO 10.10.10.2
    Radius packet received
<TIMESTAMP> ERROR 10.10.10.2
    Received Access-Reject from the RADIUS server for the client.
<TIMESTAMP> ERROR 10.10.10.2
    Received eap failurefrom the client.
```

[Resolver problemas la red-Auth](#)

Bueno resolver problemas la práctica debe incluir generalmente un chequeo del “estado del Administrador de directivas” del cliente que tiene problemas. Mientras que se confirma en la captura de pantalla WCS abajo, pegan al cliente en la pregunta en el estado *WEBAUTH_REQD*. Esto significa que el proceso del 802.11 es completo sin ningunos errores, y estos posibles problemas pueden ocurrir:

- Nombre de usuario incorrecto/contraseña
 - Puesta en práctica incorrecta ACL (alcanzar el servidor externo de la red-auth, si ningunos)
 - DNS no configurado correctamente y más
- Nota:** Para más información sobre la autenticación Web del troubleshooting, refiera al [ejemplo de la configuración de la autenticación Web del](#)

[regulador del documento.](#)

Client 'unknown' - Intel:64:63:0b		
General	Statistics	Location
Client Properties		RF Properties
Client User Name		AP Name 00:14:1c:ed:46:b8
Client IP Address	10.10.10.15	AP Type Cisco AP
Client MAC Address	00:19:d2:64:63:0b	AP Base Radio MAC 00:14:1b:59:2d:80
Client Vendor	Intel	Protocol 802.11g
Controller	10.10.10.2	AP Mode local
Port	29	Profile Name web-auth
Interface	management	SSID sevt-webauth
VLAN ID	0	Security Policy
802.11 State	Associated	Association Id 2
Mobility Role	Unknown	Reason Code None
Policy Manager State	WEBAUTH_REQD	802.11 Authentication OPENSYSYSTEM
Anchor Address	0.0.0.0	
Mirror Mode	Disable	Security
CCX	V4	Authenticated No
E2E	V1	Policy Type Unknown
WGB Status	Regular Client	Encryption Cypher NONE
		EAP Type Unknown

Los registros recogieron de la visualización WCS que el proceso de la red-auth no ha sido acertado. Tal situación se puede simular en el laboratorio si usted fija la directiva de la capa 3 WLAN a la red-auth y no completa el proceso de la red-auth ni ingresa las credenciales incorrectas/inexistentes de la clave. Controle la sección de resumen de la herramienta del troubleshooting del cliente para saber dónde ocurrió el problema. Usted ve que éstos abren una sesión el WCS:

```
<TIMESTAMP> INFO 10.10.10.2
  Controller association request message received
<TIMESTAMP> INFO 10.10.10.2
  Received reassociation request from client
<TIMESTAMP> INFO 10.10.10.2
  The wlan to which client is connecting does not require 802 1x authentication
<TIMESTAMP> INFO 10.10.10.2
  Client web authentication is required
<TIMESTAMP> INFO 10.10.10.2
  Client moved to associated state successfully
<TIMESTAMP> INFO 10.10.10.2
  Controller association request message received
```


[Resolver problemas la dirección del DHCP y IP](#)

A menudo, los dispositivos cliente se utilizan en más de una red inalámbrica. Un ejemplo puede ser uso del empleado de un dispositivo corporativo en un hogar o una red pública. Un empleado puede hacer asignar una dirección IP estática en la red doméstica. Él conecta con la red corporativa con una dirección IP estática previamente asignada sin su conocimiento. Esto lleva a un problema de la Conectividad, que se puede señalar fácilmente con la ayuda de la habitación del troubleshooting del cliente WCS (según lo visualizado abajo). La mayoría de los problemas en este reino miente en el cliente de red inalámbrica, pero éste puede también señalar hacia un

problema potencial en la infraestructura cableada, tal como un alcance agotado, alcance incorrecto, tentativa etc. de crear este decorado cuando usted asigna una dirección IP estática incorrecta en el cliente o cambia los parámetros del alcance del DHCP en el conmutador.

Troubleshooting Client '00:19:d2:64:63:0b'

Summary | **Log Analysis** | **Event History**



802.11 Association 802.1X Authentication IP Address Assignment Successful Association

Problem

Client could not complete the dhcp interaction.

Suggested Action

- Check whether the DHCP server is reachable.
- Check whether dhcp server is configured to serve the wlan.
- Check whether dhcp scope is exhausted.
- Check whether multiple dhcp servers are configured with overlapping scopes.
- Check local dhcp server is present if dhcp bridging mode enabled (move it to second)
- Check if client is configured to get address from dhcp server
- Check if client has static ip configured and ensure client generates ip traffic * if ipsec wlan, ensure that client is configured to do dhcp exchanges in open (safenet/netscreen default config does not include it)

[Información Relacionada](#)

- [Guía de configuración inalámbrica del regulador LAN de Cisco, versión 5.1](#)
- [Administración de Recursos de Radio en Redes Inalámbricas Unificadas](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)