Implementación de teléfonos IP de Vocera en la infraestructura UWN

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Convenciones
Resumen ejecutivo
Descripción general de la placa Vocera
Consideraciones sobre la capacidad de las llamadas de Vocera
Capacidad del servidor de comunicaciones de Vocera
La solución Vocera
Planificación de infraestructuras de Vocera
Descripción general de la arquitectura
Multidifusión en una implementación de LWAPP
Método de entrega de unidifusión-multidifusión
Método de Entrega Multicast-Multicast
Configuración de Multicast de Router y Switch
Habilitación del Ruteo IP Multicast
Activar PIM en una Interfaz
Desactivar Snooping de VLAN IGMP del Switch
Mejoras de Multicast en la Versión 4.0.206.0 y Posteriores
Escenarios de implementación
Implementación de controlador único
Implementación de nivel 2 de controlador múltiple
Implementación de varios controladores de capa 3
Implementaciones de VoWLAN: Recomendaciones de Cisco
Recomendaciones para edificios de varias plantas, hospitales y almacenes
Mecanismos de seguridad admitidos
Consideraciones sobre LEAP
Infraestructura de red inalámbrica
VLAN de voz, datos y vocera
Dimensionamiento de la red
Recomendaciones del switch
Implementaciones y configuración
Configuración de la placa
Ajuste de AutoRF para su entorno
Configuración de la infraestructura de red inalámbrica

Crear interfaces
Crear la interfaz de voz de Vocera
Configuración específica de la conexión inalámbrica
Configuración de WLAN
Configurar detalles del punto de acceso
Configuración de la radio 802.11b/g
Verificación de telefonía IP inalámbrica
Asociación, autenticación y registro
Problemas comunes de roaming
El distintivo pierde la conexión a la red o el servicio de voz se pierde al roaming
El distintivo pierde calidad de voz mientras se desplaza
Problemas de audio
Audio de un solo lado
Audio irregular
Problemas de registro y autenticación
Apéndice A
Colocación de antena y punto de acceso
Distorsión de interferencias y múltiples rutas
Atenuación de señal
Información Relacionada

Introducción

Este documento proporciona aspectos del diseño y pautas de instrumentación para la implementación de la tecnología Vocera® Badge Voice over WLAN (VoWLAN) en la infraestructura de red inalámbrica unificada de Cisco.

Nota: El soporte para los productos Vocera debe obtenerse directamente de los canales de soporte de Vocera. El Soporte Técnico de Cisco no está capacitado para admitir problemas relacionados con Vocera.

Esta guía es un suplemento de la Guía de implementación del controlador de LAN inalámbrica de Cisco y solo aborda los parámetros de configuración que son específicos de los dispositivos VoWLAN de Vocera en una arquitectura ligera. Consulte Implementación de Controladores LAN Inalámbricos Cisco 440X Series para obtener más información.

Prerequisites

Requirements

Se supone que los lectores están familiarizados con los términos y conceptos presentados en Cisco IP Telephony SRND y Cisco Wireless LAN SRND. .

Guía de diseño de Wireless UC - http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns818/landing_wireless_uc.html

Cisco Unified Communications SRND basado en Cisco Unified Communications Manager

7.x—http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns818/landing_uc_mgr.html

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

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

Resumen ejecutivo

En esta tabla se resumen las cuatro funciones clave y su comportamiento en una red Cisco Unified Wireless.

	Controlador único	Roaming de Capa 2 de Controlador a Controlador	Roaming de Capa 3 de Controlador a Controlador
Badge-to-Badge	Sin configuración especial	Sin configuración especial	Sin configuración especial
Badge-to-Phone	Sin configuración especial	Sin configuración especial	Sin configuración especial
Difusión	Activar multidifusión del controlador	Activar multidifusión de controlador Desactivar detección IGMP-VLAN de Vocera o ejecutar 4.0.206.0 o posterior	4.0.206.0 o posterior
Ubicación de la placa	Sin configuración especial	Sin configuración especial	Sin configuración especial

Descripción general de la placa Vocera

Las insignias de comunicación permiten a los usuarios comunicarse de forma instantánea con cualquier otro usuario de insignias, así como realizar un seguimiento de la ubicación de las insignias y la integración de la central de sucursales privada (PBX). La utilización de una red inalámbrica 802.11b/g requiere el uso de la entrega de paquetes unidifusión de multidifusión y UDP con requisitos limitados de calidad de servicio (QoS) a partir de la versión 3.1 (Compilación 1081) del software Vocera Server. Las funciones de cifrado son privacidad equivalente a conexión con cables (WEP) de 64/128 bits, protocolo de integridad de clave temporal (TKIP), comprobación

de integridad de mensaje (MIC) y protocolo de integridad de clave temporal (CKIP) de Cisco, combinadas con las funciones de autenticación de clave precompartida de acceso Wi-Fi protegido (WPA-PSK), protocolo de autenticación ampliable protegido por WPA (PEAP) y Protocolo de autenticación extensible (LEAP).

Con sólo pulsar un botón, el servidor Vocera responde con Vocera, que es un mensaje para ejecutar comandos como grabar, donde (am) /is..., llamar, reproducir, difundir, mensajes, etc. El servidor Vocera proporciona los servicios o la configuración de llamadas necesarios para completar la solicitud.

El sistema de comunicación con capacidad 802.11b de Vocera utiliza compresión de voz propia y el uso de un rango de puertos UDP. El software Vocera System se ejecuta en un servidor Windows que administra la configuración de llamadas, la conexión de llamadas y los perfiles de usuario. Se han asociado con el software Nuance 8.5 Speech Recognition y Voiceprint para habilitar las comunicaciones de voz de insignia. Vocera recomienda un servidor Windows independiente para ejecutar el software de soluciones de telefonía Vocera para habilitar la conectividad del servicio telefónico sencillo antiguo (POTS) con las placas.

Consideraciones sobre la capacidad de las llamadas de Vocera

Consulte la sección Dimensión de la Red de este documento para obtener más detalles.

Capacidad del servidor de comunicaciones de Vocera

Refiérase a las Especificaciones del Sistema de Comunicaciones de Vocera para obtener más información sobre la matriz de dimensionamiento del servidor Vocera.

La solución Vocera

Vocera Badge utiliza la entrega de paquetes unidifusión y multidifusión para proporcionar varias características clave que conforman esta solución completa. Estas son cuatro de las funciones esenciales que se basan en la entrega adecuada de paquetes. También se proporciona una comprensión básica de cómo cada función utiliza la red subyacente para la entrega y la funcionalidad.

- Badge to Badge Communications: cuando un usuario de Vocera llama a otro usuario, la insignia se pone en contacto primero con el servidor de Vocera, que busca la dirección IP de la insignia de la llamada y se pone en contacto con el usuario de la insignia para preguntarle al usuario si puede realizar una llamada. Si el destinatario de la llamada acepta la llamada, el servidor de Vocera notifica a la placa de llamada la dirección IP de la placa de llamada para configurar la comunicación directa entre las insignias sin intervención del servidor. Todas las comunicaciones con el servidor Vocera utilizan el códec G.711 y todas las comunicaciones de placa a placa utilizan un códec Vocera propietario.
- Comunicación de telefonía de distintivos: cuando se instala un servidor de telefonía de Vocera y se configura con una conexión a un PBX, un usuario puede llamar a extensiones internas fuera del PBX o de líneas telefónicas externas. Vocera permite a los usuarios realizar llamadas diciendo los números (cinco, seis, tres, dos) o creando una entrada de la libreta de direcciones en la base de datos de Vocera para la persona o función en ese número (por

ejemplo, farmacia, casa, pizza) el servidor de Vocera determina el número al que se llama, ya sea interceptando los números en la extensión o consultando el nombre en la base de datos y seleccionando el número. A continuación, el servidor Vocera pasa esa información al servidor de telefonía Vocera que se conecta al PBX y genera la señalización de telefonía adecuada (por ejemplo, DTMF). Todas las comunicaciones entre el servidor de placa y Vocera y el servidor de Vocera y el servidor de telefonía Vocera utilizan el códec G.711 sobre UDP de unidifusión.
- Difusión de Vocera: un usuario de la barra de Vocera puede llamar y comunicarse con un grupo de usuarios de insignias de Vocera al mismo tiempo mediante el comando Broadcast. Cuando un usuario transmite a un grupo, la insignia del usuario envía el comando al servidor Vocera que, a continuación, busca a los miembros de un grupo, determina qué miembros del grupo están activos, asigna una dirección multicast para utilizarla en esta sesión de difusión y envía un mensaje a la insignia de cada usuario activo ordenándole que se una al grupo multicast con la dirección multicast asignada.
- Función de ubicación de la placa: el servidor de Vocera realiza un seguimiento del punto de acceso al que se asocia cada insignia activa, ya que cada insignia envía una señal de mantenimiento activa de 30 segundos al servidor con el BSSID asociado. Esto permite al sistema Vocera calcular aproximadamente la ubicación de un usuario de placa. Esta función tiene un grado de precisión relativamente bajo porque una barra puede no estar asociada al punto de acceso al que está más cerca.

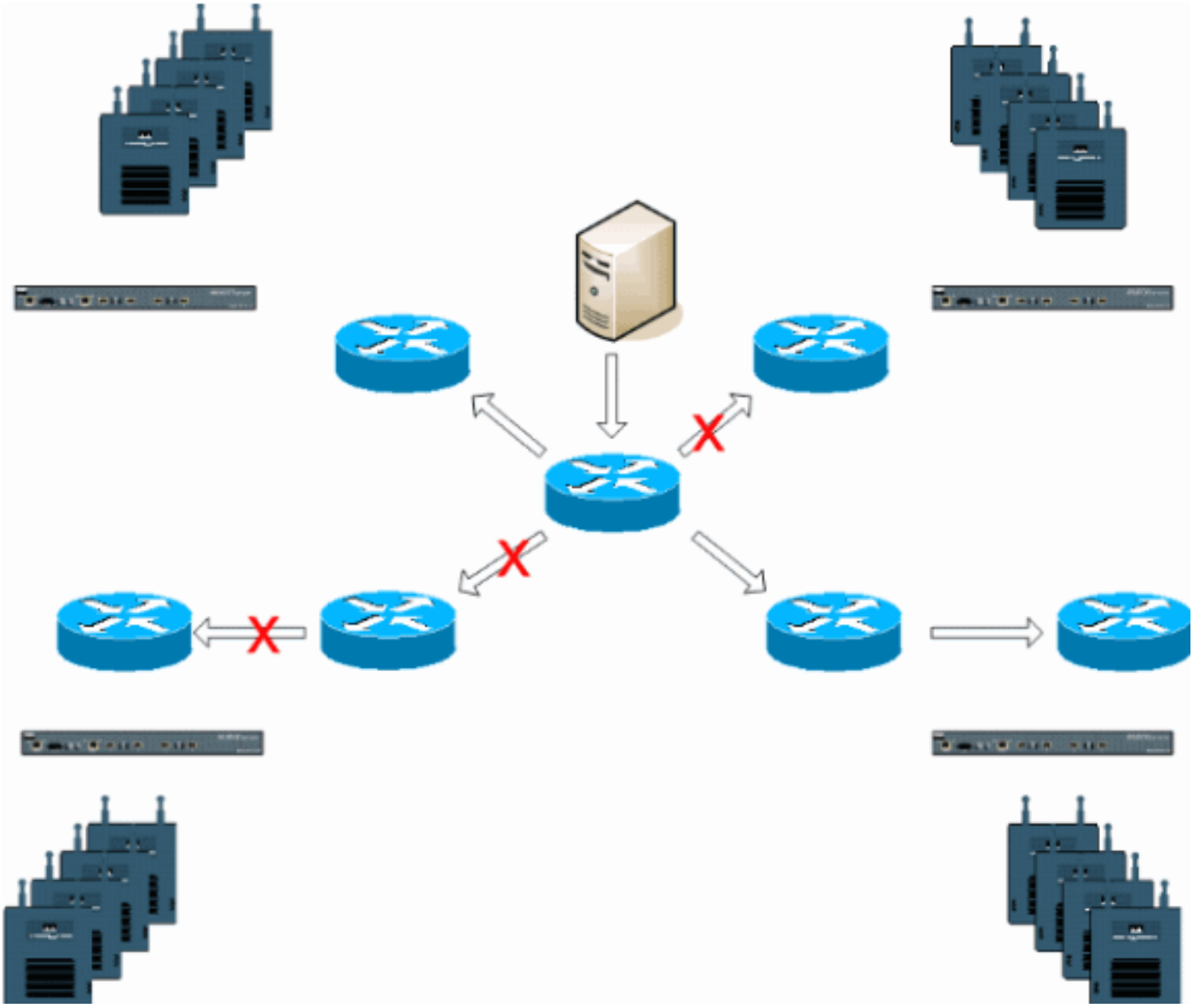
Planificación de infraestructuras de Vocera

El informe técnico de Vocera Vocera Infrastructure Planning Guide , describe los requisitos mínimos del sondeo del sitio que muestran que el distintivo debe tener una potencia de señal de recepción mínima de -65 dBm, una relación señal-ruido mayor que 25 dB y una correcta superposición del punto de acceso y separación del canal. Aunque las insignias utilizan una antena omnidireccional similar como un portátil que se utiliza para un sondeo del sitio, no imita muy bien el comportamiento de la insignia, dado que los usuarios afectan a la potencia de la señal. Dado este requisito único y este comportamiento del dispositivo transmisor, el uso de la arquitectura de Cisco y la administración de recursos de radio es ideal para asegurarse de que no haya características inusuales del sitio de radiofrecuencia (RF).

La placa Vocera es un dispositivo de baja potencia que se usa junto al cuerpo con capacidades limitadas de corrección de errores de señal. Los requisitos de Vocera en este documento pueden lograrse fácilmente. Sin embargo, puede saturarse si hay demasiados SSID para que procese y permita que la insignia funcione eficazmente.

Descripción general de la arquitectura

Figura 1: Reenvío y separación de multidifusión general con conexión inalámbrica de protocolo de punto de acceso ligero (LWAPP)



Multidifusión en una implementación de LWAPP

Para implementar la función de difusión de Vocera es necesario comprender la multidifusión dentro de una implementación de LWAPP. Este documento trata más adelante los pasos esenciales para habilitar el multicast dentro de la solución basada en controlador. Actualmente hay dos métodos de entrega que el controlador LWAPP utiliza para entregar multicast a los clientes:

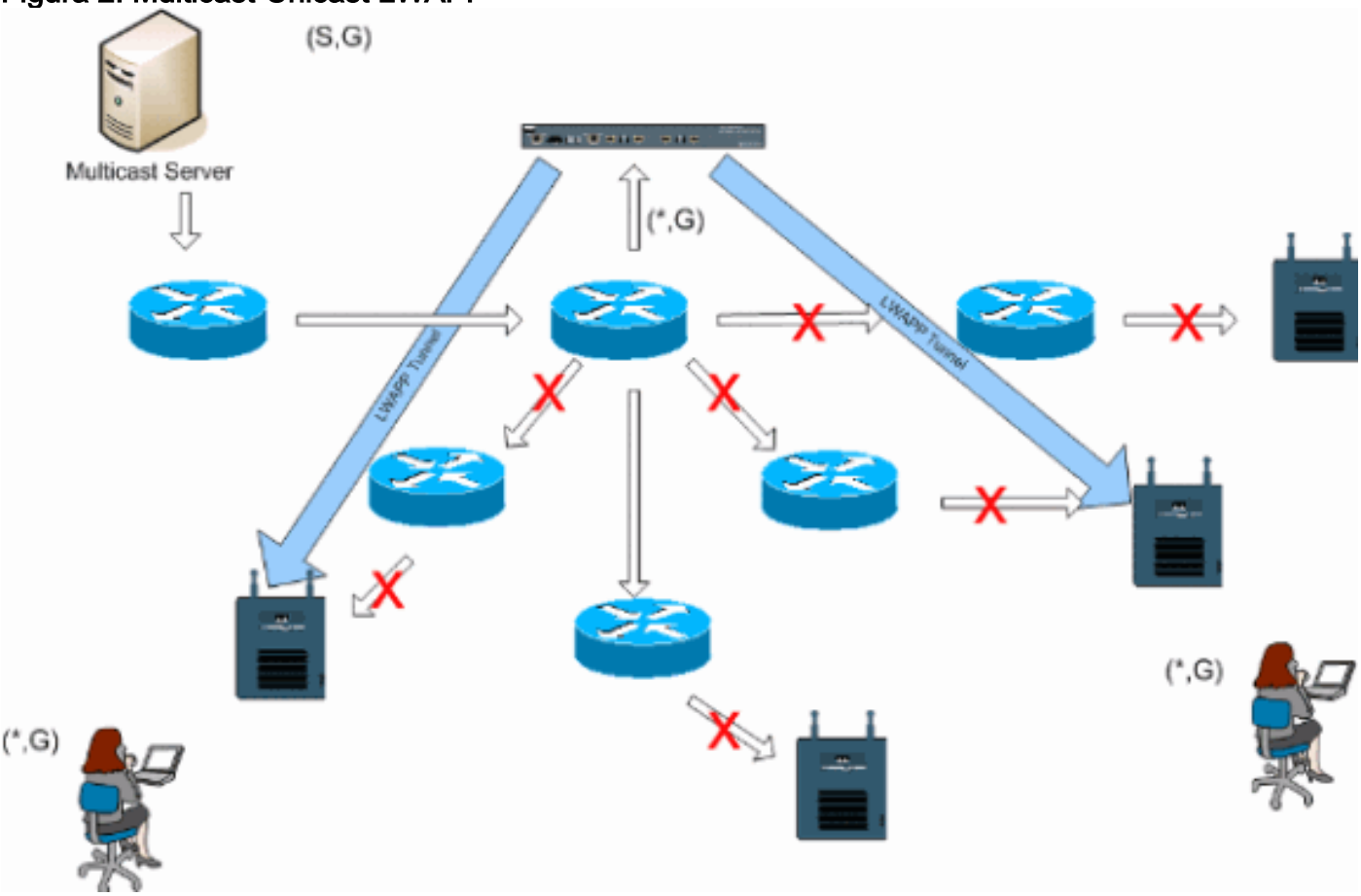
- Unicast-Multicast
- Multicast-Multicast

Método de entrega de unidifusión-multidifusión

El método de entrega unidifusión-multidifusión crea una copia de cada paquete multicast y lo reenvía a cada punto de acceso. Cuando un cliente envía una unión multicast a la LAN inalámbrica, el punto de acceso reenvía esta unión a través del túnel LWAPP al controlador. El controlador puentea esta unión multicast en su conexión de red de área local directamente conectada que es la VLAN predeterminada para la WLAN asociada del cliente. Cuando un paquete de multidifusión IP llega de la red al controlador, el controlador replica este paquete con un encabezado LWAPP para cada punto de acceso que tiene un cliente dentro del dominio

inalámbrico que se ha unido a este grupo específico. Cuando el origen de la multidifusión también es un receptor dentro del dominio inalámbrico, este paquete también se duplica y se reenvía al mismo cliente que envió este paquete. Para las insignias Vocera, este no es el método preferido de entrega multidifusión dentro de la solución del controlador LWAPP. El método de entrega de unidifusión funciona con implementaciones pequeñas. Sin embargo, debido a la considerable sobrecarga del controlador de LAN inalámbrica (WLC), este nunca es el método de entrega de multidifusión recomendado.

Figura 2: Multicast-Unicast LWAPP



Nota: Si se configuran VLAN de grupo AP y se envía una unión IGMP desde un cliente a través del controlador, se coloca en la VLAN predeterminada de la WLAN en la que está el cliente. Por lo tanto, es posible que el cliente no reciba este tráfico multicast a menos que el cliente sea miembro de este dominio de broadcast predeterminado.

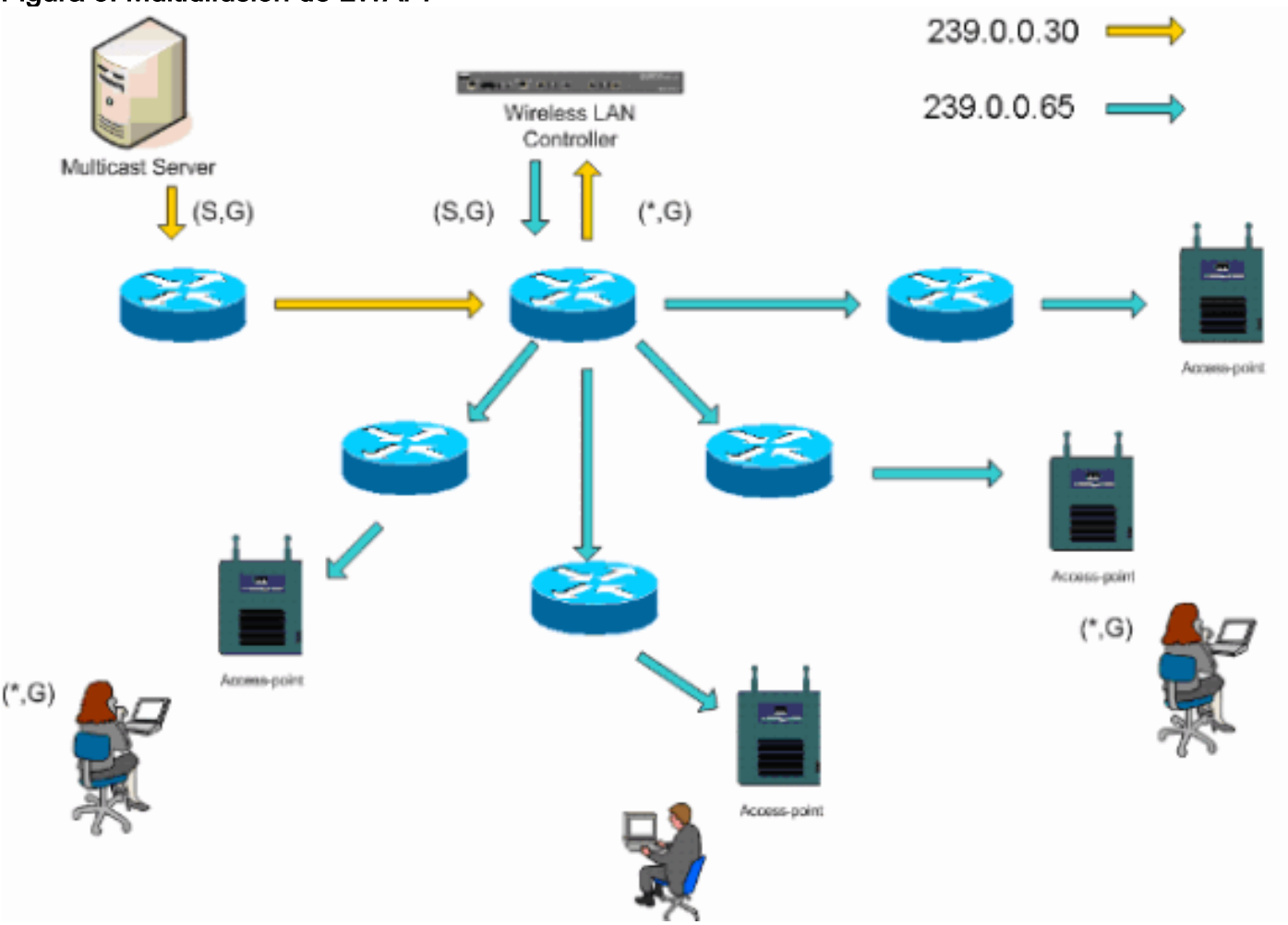
Método de Entrega Multicast-Multicast

El método de entrega multicast-multicast no requiere que el controlador replique cada paquete multicast recibido. El controlador se configura para una dirección de grupo multicast no utilizada de la que cada punto de acceso se convierte en miembro. Con la Figura 3, el grupo multicast definido desde el WLC al punto de acceso es 239.0.0.65. Cuando un cliente envía una unión multicast a la WLAN, el punto de acceso reenvía esta unión a través del túnel LWAPP al controlador. El controlador reenvía este protocolo de capa de link a su conexión de red de área local directamente conectada que es la VLAN predeterminada para la WLAN asociada del cliente. El router que es local al controlador luego agrega esta dirección de grupo multicast a esa interfaz para la entrada de reenvío (*,G). Con la Figura 3, el ejemplo de unión multicast se envió al grupo multicast 239.0.0.30. Cuando la red ahora reenvía el tráfico multicast, la dirección multicast de 239.0.0.30 se reenvía al controlador. El controlador luego encapsula el paquete multicast en un paquete multicast LWAPP dirigido a la dirección del grupo multicast (ejemplo aquí es 239.0.0.65)

que se configura en el controlador y se reenvía a la red. Cada punto de acceso en el controlador recibe este paquete como miembro del grupo multicast del controlador. A continuación, el punto de acceso reenvía el paquete de multidifusión de los clientes/servidores (por ejemplo, 239.0.0.30) como una transmisión a la WLAN/SSID identificada dentro del paquete de multidifusión LWAPP.

Nota: Si configura incorrectamente su red multicast, podría terminar recibiendo paquetes multicast de punto de acceso de otro controlador. Si el primer controlador tiene que fragmentar este paquete multicast, el fragmento se reenvía a la red y cada punto de acceso debe dedicar tiempo a descartar este fragmento. Si permite todo el tráfico, como cualquier cosa del rango de multidifusión 224.0.0.x, esto también se encapsula y posteriormente se reenvía por cada punto de acceso.

Figura 3: Multidifusión de LWAPP



Configuración de Multicast de Router y Switch

Este documento no es una guía de configuración de multidifusión de red. Consulte Configuración del Ruteo IP Multicast para obtener una historia de implementación completa. Este documento describe los aspectos básicos para habilitar la multidifusión en su entorno de red.

Habilitación del Ruteo IP Multicast

El routing de multidifusión IP permite que el software Cisco IOS® reenvíe paquetes de multidifusión. El comando de configuración global **ip multicast-routing** es necesario para permitir que multicast funcione en cualquier red habilitada para multicast. El comando **ip multicast-routing** debe estar habilitado en todos los routers dentro de su red entre los WLC y sus respectivos

puntos de acceso.

```
Router(config)#ip multicast-routing
```

Activar PIM en una Interfaz

Esto habilita la interfaz de routing para el funcionamiento del protocolo de administración de grupos de Internet (IGMP). El modo de multidifusión independiente del protocolo (PIM) determina cómo el router rellena su tabla de routing multidifusión. El ejemplo que se proporciona aquí no requiere que el punto de encuentro (RP) se conozca para el grupo de multidifusión y, por lo tanto, el modo disperso-denso es el más deseable dada la naturaleza desconocida de su entorno de multidifusión. Esta no es una recomendación de multidifusión que se debe configurar para funcionar, aunque la interfaz de Capa 3 conectada directamente a su controlador debe estar habilitada para PIM para que la multidifusión funcione. Todas las interfaces entre sus WLC y sus respectivos puntos de acceso deben estar habilitadas.

```
Router(config-if)#ip pim sparse-dense-mode
```

Desactivar Snooping de VLAN IGMP del Switch

El snooping de IGMP permite que una red conmutada con multidifusión habilitada limite el tráfico a aquellos puertos de switch que tienen usuarios que desean que se vea multicast mientras se recortan los paquetes multicast de los puertos de switch que no desean ver el flujo multicast. En una implementación de Vocera, puede no ser deseable habilitar la indagación de CGMP o IGMP en el switchport ascendente al controlador con versiones de software anteriores a 4.0.206.0.

La itinerancia y la multidifusión no se definen con un conjunto de requisitos para verificar que el tráfico multicast puede seguir a un usuario suscrito. Aunque la insignia de cliente es consciente de que ha itinerado, no reenvía otra unión IGMP para asegurarse de que la infraestructura de red continúe entregando el tráfico multicast (difusión Vocera) a la insignia. Al mismo tiempo, el punto de acceso LWAPP no envía una consulta de multidifusión general al cliente itinerante para solicitar esta unión IGMP. Con un diseño de red de Vocera de Capa 2, la inhabilitación de la indagación IGMP permite que el tráfico se reenvíe a todos los miembros de la red Vocera sin importar dónde se desplacen. Esto garantiza que la función de difusión de Vocera funcione independientemente de dónde se desplace el cliente. Inhabilitar la indagación de IGMP globalmente es una tarea muy poco deseable. Se recomienda que la indagación IGMP solamente se inhabilite en la VLAN Vocera que está conectada directamente a cada WLC.

Refiérase a Configuración de Snooping de IGMP para obtener más información.

```
Router(config)#interface vlan 150
Router(config-if)#no ip igmp snooping
```

Mejoras de Multicast en la Versión 4.0.206.0 y Posteriores

Con la versión 4.0.206.0, Cisco introduce una consulta IGMP para permitir que los usuarios deambulen en la Capa 2 enviando una consulta IGMP general cuando esto ocurra. El cliente luego responde con el grupo IGMP del que es miembro y esto se enlaza a la red cableada como se describió anteriormente en este documento. Cuando un cliente se traslada a un controlador

que no tiene conectividad de Capa 2, o a un itinerario de Capa 3, se agrega ruteo sincrónico para paquetes de origen multicast. Cuando un cliente, que ha completado un itinerario de Capa 3, origina un paquete de multidifusión desde la red inalámbrica, el controlador externo encapsula este paquete en Ethernet sobre IP (EoIP) en el túnel IP al controlador de anclaje. A continuación, el controlador de anclaje lo reenvía a los clientes inalámbricos asociados localmente, así como lo reenvía a la red con cables donde se enruta mediante métodos de ruteo multicast normales.

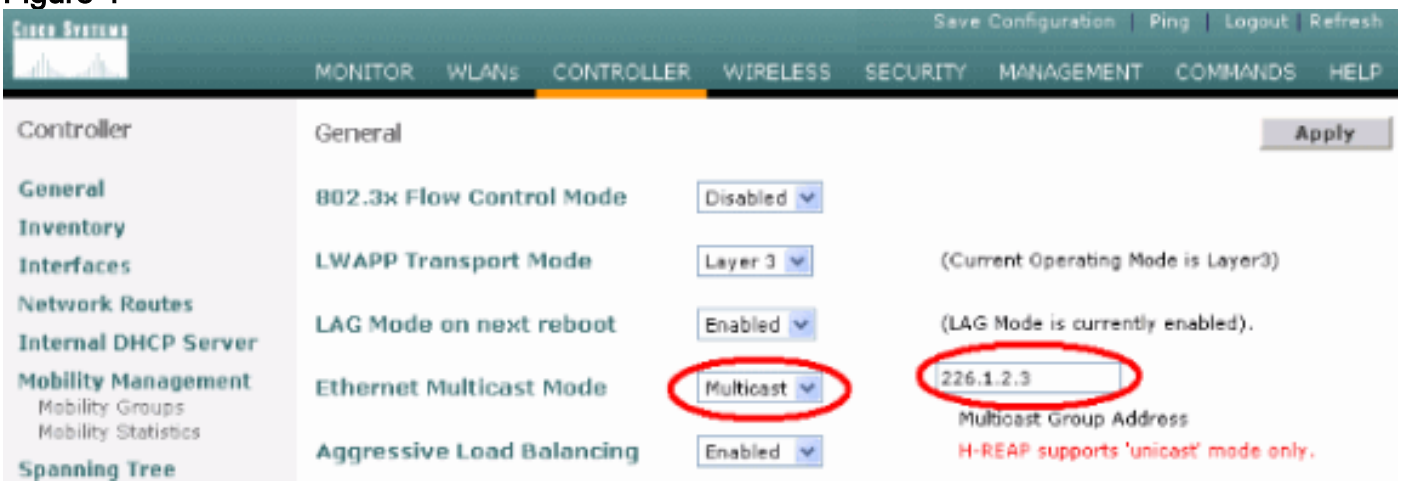
Escenarios de implementación

Estos tres escenarios de implementación abarcan las prácticas recomendadas y los parámetros de diseño para ayudar con una implementación correcta de la barra Vocera:

- Implementación de controlador único
- Implementación de nivel 2 de controlador múltiple
- Implementación de varios controladores de capa 3

Es esencial comprender cómo interactúan las funciones de la barra Vocera dentro de un entorno MAC dividido LWAPP. Con todos los escenarios de implementación, se debe habilitar la multidifusión y se debe inhabilitar el balanceo de carga agresivo. Todas las WLAN de placa deben estar contenidas en el mismo dominio de broadcast a través de toda la red.

Figure 4



Implementación de controlador único

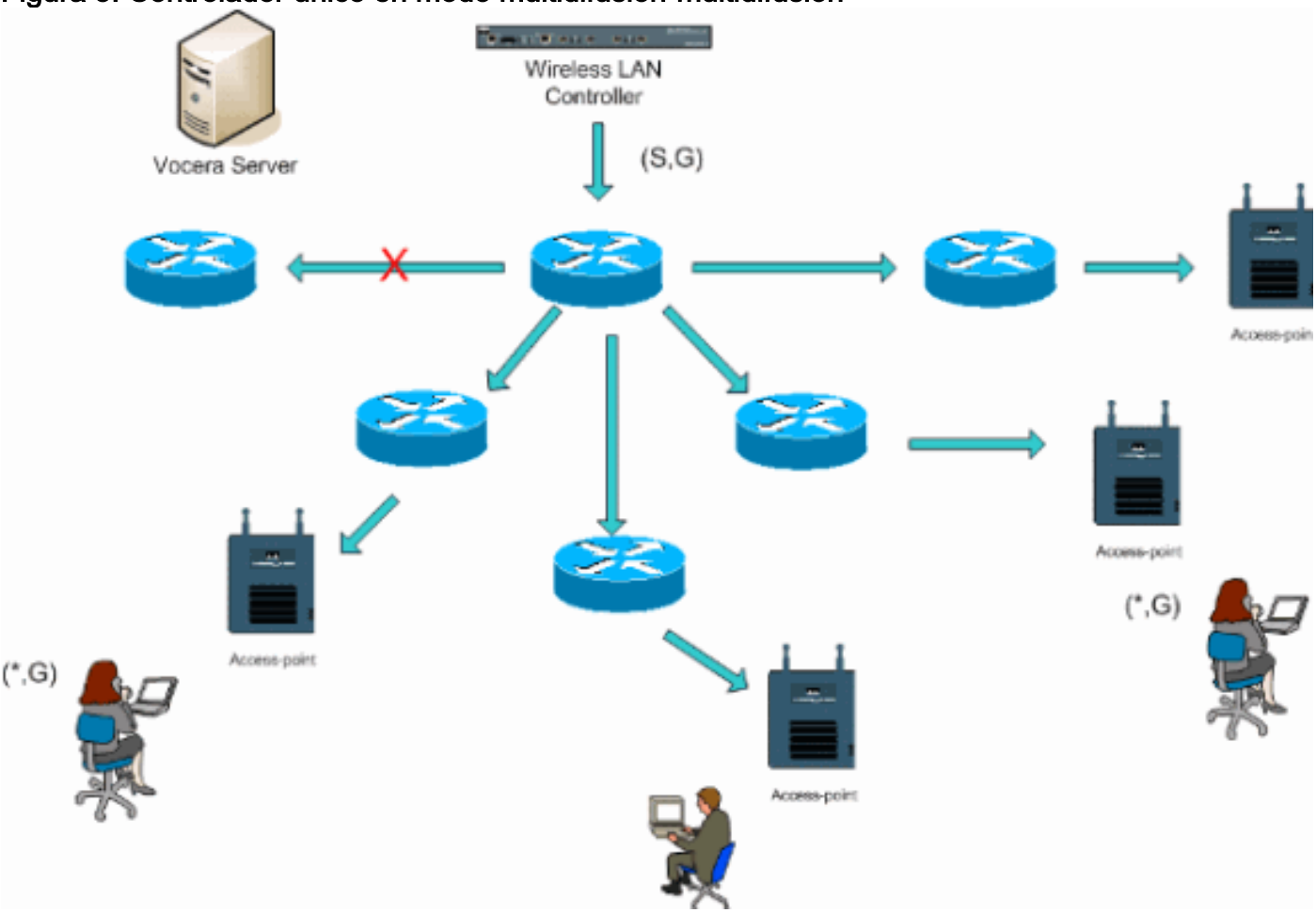
Este es el escenario de implementación más directo. Le permite implementar la solución Vocera Badge sin preocuparse demasiado por la implementación. Su red debe estar habilitada para el ruteo de multidifusión IP solamente para permitir que los puntos de acceso reciban los paquetes de multidifusión LWAPP. Si es necesario, puede limitar la complejidad de la multidifusión de la red configurando todos los routers y switches con el grupo multicast de los controladores.

Con la multidifusión configurada globalmente en el controlador, el SSID adecuado, la configuración de seguridad y todos los puntos de acceso registraron la solución Vocera Badge y todas sus funciones funcionan como se esperaba. Con la función Vocera Broadcast (Difusión de Vocera), un usuario se traslada y el tráfico multicast sigue como se esperaba. No es necesario configurar parámetros adicionales para permitir que esta solución funcione correctamente.

Cuando una barra Vocera envía un mensaje multicast, como lo hace con la difusión Vocera, se reenvía al controlador. El controlador luego encapsula este paquete multicast dentro de un paquete multicast LWAPP. La infraestructura de red reenvía este paquete a cada punto de

acceso conectado a este controlador. Cuando el punto de acceso recibe este paquete, entonces observa el encabezado multicast del LWAPP para determinar a qué WLAN/SSID transmite luego este paquete.

Figura 5: Controlador único en modo multidifusión-multidifusión



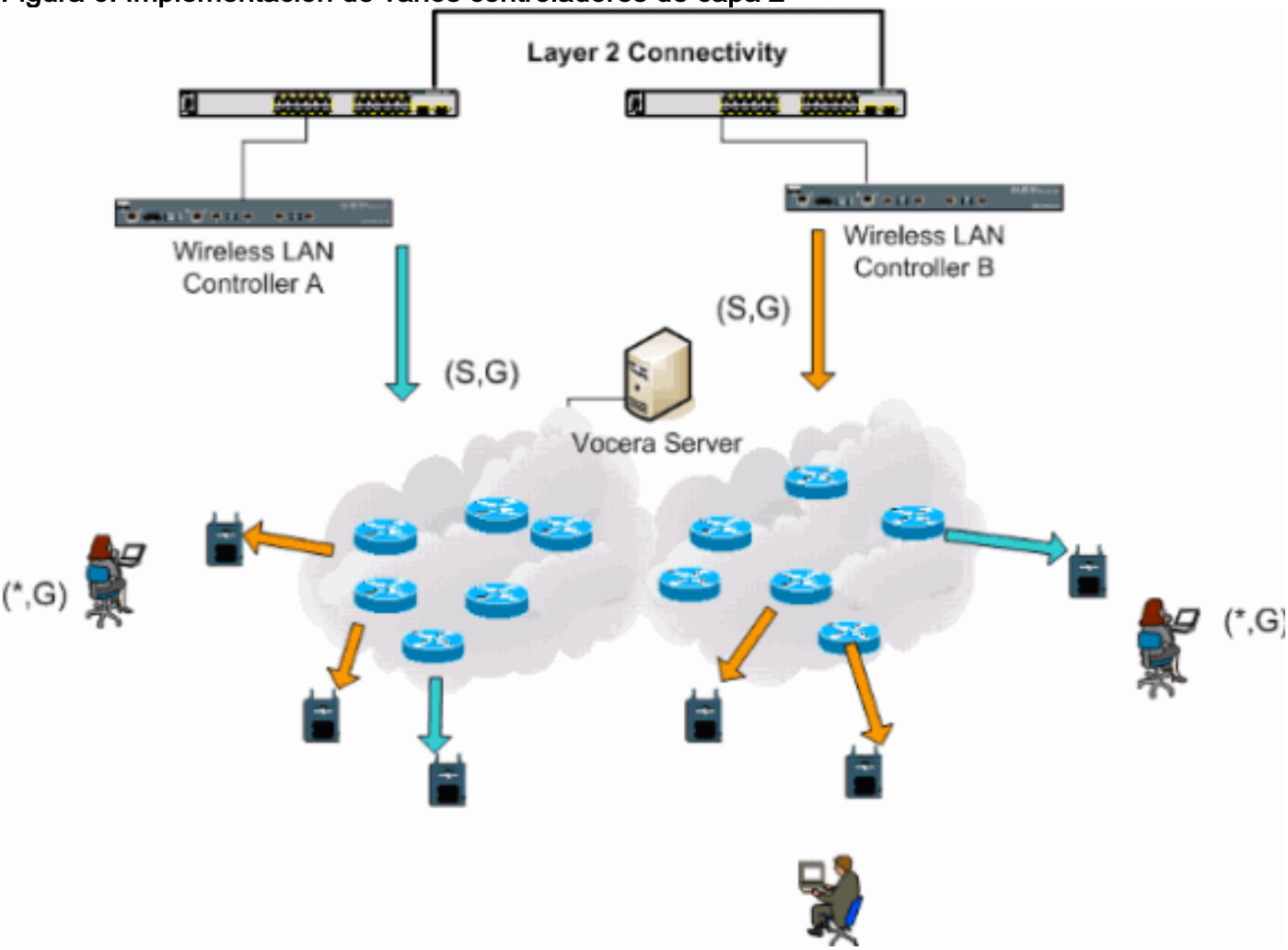
Implementación de nivel 2 de controlador múltiple

Todos los controladores múltiples deben tener conectividad entre sí a través del mismo dominio de broadcast de Capa 2. Ambos controladores se configuran para multicast como se muestra, usando los grupos multicast de punto de acceso idénticos en cada controlador para limitar la fragmentación. Con la suposición de que este dominio de broadcast de Capa 2 está conectado a través de un switch común o un conjunto común de switches, la indagación CGMP/IGMP en estos switches debe ser inhabilitada para esta VLAN única o ejecutar el software WLC 4.0.206.0 o posterior. Con la función de difusión de Vocera y un usuario itinerante desde un punto de acceso en un controlador a un punto de acceso en un controlador diferente, no hay ningún mecanismo para que las uniones IGMP se reenvíen al nuevo puerto de Capa 2 para que la indagación IGMP funcione. Sin un paquete IGMP que alcance el switch con capacidad de CGMP o IGMP ascendente, el grupo multicast especificado no se reenvía al controlador y, por lo tanto, el cliente no lo recibe. En algunos casos esto podría funcionar, si un cliente que forma parte del mismo grupo de broadcast de Vocera ya ha enviado este paquete IGMP antes de que el cliente de roaming se desplace hacia el nuevo controlador Con las ventajas de la versión 4.0.206.0, un cliente que se traslada a otro controlador como roaming de Capa 2 recibe una consulta IGMP general inmediatamente después de la autenticación. El cliente debe responder entonces con los grupos interesados y el nuevo controlador se conecta con el switch conectado localmente. Esto permite las ventajas de IGMP y CGMP en sus switches ascendentes.

Puede crear SSID de placa adicionales y dominios de Capa 2 para redes de placa independientes

siempre y cuando la red esté configurada para pasar tráfico multidifusión de forma adecuada. Además, cada dominio de broadcast de Capa 2 de Vocera creado debe existir en cualquier lugar en el que se conecte un controlador a la red para no interrumpir el multicast.

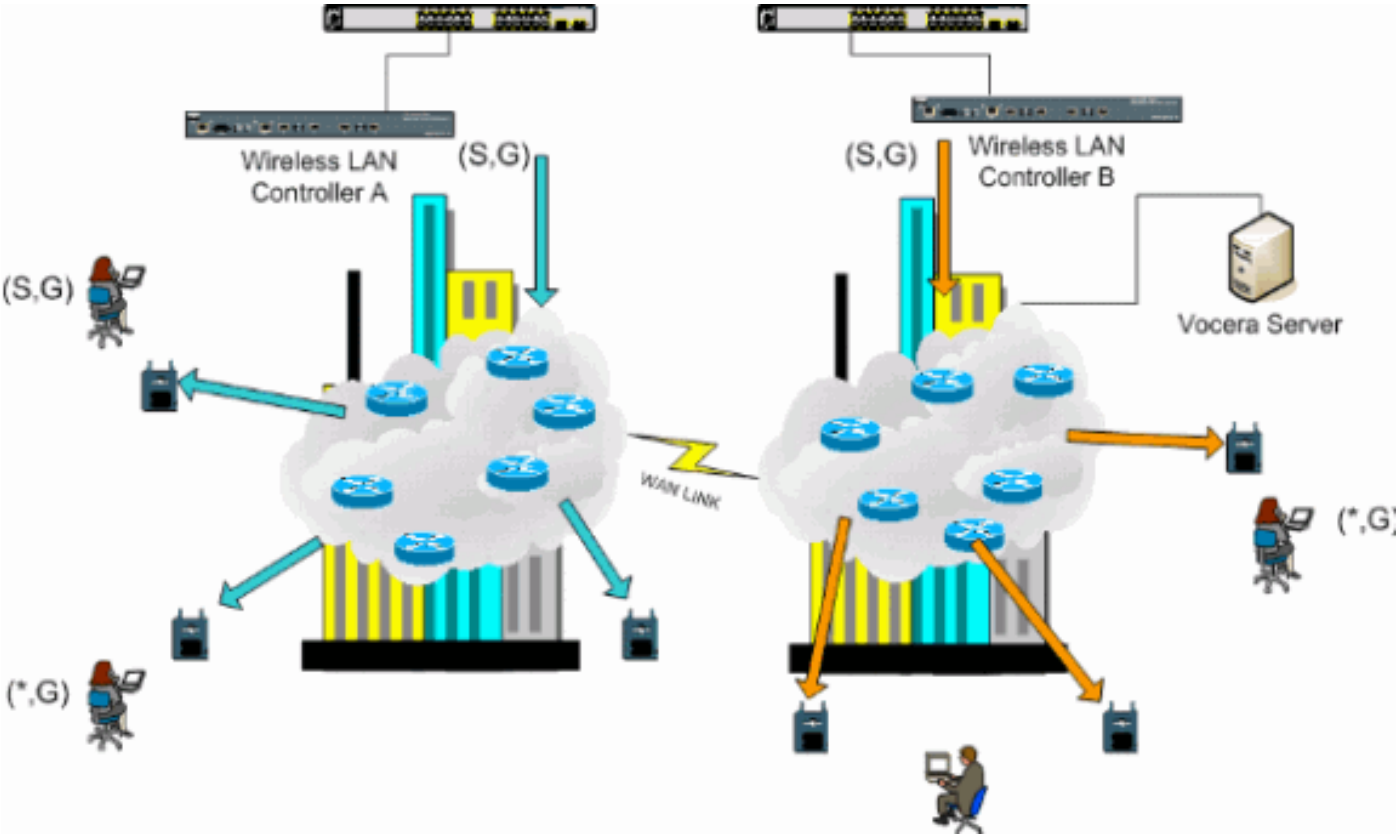
Figura 6: Implementación de varios controladores de capa 2



Implementación de varios controladores de capa 3

La estrategia de implementación de roaming de Capa 3 sólo se debe utilizar con la itinerancia de controlador a controlador con la versión 4.0.206.0 o posterior del software WLC. Si un cliente que se ha conectado al grupo de broadcast de Vocera y recibe el flujo de multidifusión apropiado y se traslada a otro controlador como itinerario de Capa 3 con el roaming de Capa 3 de LWAPP configurado, se le consulta para los grupos de multicast interesados. El cliente, cuando se envía al mismo grupo de broadcast de Vocera, tiene estos paquetes entregados al controlador de anclaje a través del túnel EoIP y hace que estos paquetes sean enrutados a través de métodos de ruteo multicast normales.

Figura 7: Implementación de varios controladores de capa 3



Implementaciones de VoWLAN: Recomendaciones de Cisco

Las redes de telefonía IP inalámbrica requieren una cuidadosa planificación de RF. A menudo se requiere un sondeo detallado del sitio de voz para determinar los niveles adecuados de cobertura inalámbrica e identificar las fuentes de interferencia. La ubicación de los puntos de acceso y las opciones de selección de antena se pueden facilitar en gran medida con la ayuda de los resultados de un sondeo del sitio de voz válido. La consideración más importante es la potencia de transmisión del teléfono inalámbrico. Idealmente, el teléfono aprende la potencia de transmisión del punto de acceso y ajusta su potencia de transmisión a la del punto de acceso.

Aunque la mayoría de las redes inalámbricas de hoy en día se implementan tras un extenso sondeo del sitio de RF, también se realizan teniendo en cuenta el servicio de datos. Es probable que los teléfonos VoWLAN tengan diferentes características de itinerancia y diferentes requisitos de cobertura que los de un adaptador WLAN típico para un cliente móvil como un portátil. Por lo tanto, a menudo se recomienda realizar un sondeo adicional del sitio para la voz a fin de prepararse para los requisitos de rendimiento de varios clientes VoWLAN. Esta encuesta adicional ofrece la oportunidad de ajustar los puntos de acceso para garantizar que los teléfonos VoWLAN tengan suficiente cobertura de RF y ancho de banda para proporcionar una calidad de voz adecuada.

Para obtener información adicional sobre consideraciones de diseño de RF, refiérase al capítulo sobre Consideraciones de Diseño de Radiofrecuencia WLAN (RF) de la Guía de Diseño de LAN Inalámbrica de Cisco, disponible en http://cisco.com/go/srnd.

Recomendaciones para edificios de varias plantas, hospitales y almacenes

Tenga en cuenta los factores enumerados en esta sección cuando realice un estudio de edificios, hospitales y almacenes de varios pisos.

Métodos y materiales de construcción

Muchos aspectos de la construcción del edificio se desconocen o se ocultan del estudio del lugar, por lo que es posible que deba adquirir esa información de otras fuentes (como los dibujos arquitectónicos). Algunos ejemplos de métodos y materiales de construcción típicos que afectan el alcance y la cobertura de los puntos de acceso son la película metálica sobre vidrio de ventana, vidrio plomo, paredes encastradas en acero, suelos de cemento y paredes con refuerzo de acero, aislamiento con respaldo de lámina, pozos de escalera y trampas para ascensores, tuberías y accesorios de plomería, y muchos otros.

Inventario

Diversos tipos de inventario pueden afectar el rango de RF, particularmente aquellos con alto contenido de acero o agua. Algunos artículos a tener en cuenta incluyen cajas de cartón, comida para mascotas, pintura, productos petrolíferos, piezas de motor, etc.

Niveles de inventario

Asegúrese de realizar un sondeo del sitio a niveles máximos de inventario o en momentos de mayor actividad. Un almacén con un nivel de existencias del 50% tiene una huella de radiofrecuencia muy diferente que el mismo almacén con un nivel de inventario del 100%.

Niveles de actividad

De manera similar, un área de oficinas fuera de horario (sin gente) tiene una huella de RF diferente a la misma área llena de gente durante el día. Aunque muchas partes del sondeo del sitio pueden realizarse sin ocupación total, es esencial llevar a cabo la verificación del sondeo del sitio y ajustar los valores clave durante un momento en que el lugar está ocupado. Cuanto mayores sean los requisitos de utilización y la densidad de los usuarios, más importante será contar con una solución de diversidad bien diseñada. Cuando hay más usuarios, se reciben más señales en el dispositivo de cada usuario. Las señales adicionales causan más contención, más puntos nulos y más distorsión de múltiples rutas. La diversidad en el punto de acceso (antenas) ayuda a minimizar estas condiciones.

Edificios de varios pisos

Tenga en cuenta estas directrices al realizar un sondeo del sitio de un edificio de oficina típico:

- Los ejes del ascensor bloquean y reflejan las señales de RF.
- Proporcione a las habitaciones señales de absorción de inventario.
- Las oficinas interiores con paredes rígidas absorben las señales de radiofrecuencia.
- Las salas de descanso (cocinas) pueden producir interferencias de 2,4 GHz mediante el uso de hornos microondas.
- Los laboratorios de pruebas pueden producir interferencias de 2,4 GHz o 5 GHz, lo que crea distorsión de múltiples rutas y sombras de RF.
- Los cubículos tienden a absorber y bloquear las señales.
- Las salas de conferencias requieren una alta cobertura de puntos de acceso, ya que son áreas de alta utilización.

Se debe tomar una precaución adicional cuando estudie instalaciones de varias plantas. Los

puntos de acceso de diferentes plantas pueden interferir entre sí tan fácilmente como los puntos de acceso ubicados en la misma planta. Es posible utilizar este comportamiento en su beneficio durante una encuesta. Mediante antenas de mayor ganancia, podría ser posible penetrar en los pisos y techos y proporcionar cobertura a los pisos superiores y inferiores del piso donde está montado el punto de acceso. Tenga cuidado de no solapar los canales entre los puntos de acceso en diferentes pisos o puntos de acceso en la misma planta. En los edificios de varios arrendatarios, puede haber problemas de seguridad que requieran el uso de menos potencia de transmisión y antenas de menor ganancia para mantener las señales fuera de las oficinas vecinas.

Hospitales

El proceso de encuesta de un hospital es muy similar al de una empresa, pero la distribución de una instalación hospitalaria tiende a diferir de estas maneras:

- Los edificios de los hospitales tienden a pasar por muchos proyectos de reconstrucción y adiciones. Cada construcción adicional probablemente tenga diferentes materiales de construcción con diferentes niveles de atenuación.
- La penetración de la señal a través de paredes y pisos en las zonas de los pacientes es típicamente mínima, lo que ayuda a crear microcélulas y variaciones de múltiples rutas.
- La necesidad de ancho de banda aumenta con el creciente uso del equipo de ultrasonido WLAN y otras aplicaciones de imágenes portátiles. La necesidad de ancho de banda aumenta con la adición de voz inalámbrica.
- Las células sanitarias son pequeñas y la itinerancia fluida es esencial, especialmente con las aplicaciones de voz.
- La superposición de celdas puede ser alta, al igual que la reutilización del canal.
- Los hospitales pueden tener instalados varios tipos de redes inalámbricas. Esto incluye equipos de 2,4 GHz que no sean 802.11. Este equipo puede provocar contención con otras redes de 2,4 GHz.
- Las antenas de parche de diversidad montadas en pared y las antenas omnidireccionales montadas en techo son populares, pero tenga en cuenta que se requiere diversidad.

Almacenes

Los almacenes tienen grandes áreas abiertas que a menudo contienen altos racks de almacenamiento. Muchas veces, estos racks llegan casi al techo, donde normalmente se ubican los puntos de acceso. Estos racks de almacenamiento pueden limitar el área que el punto de acceso puede cubrir. En estos casos, considere la posibilidad de colocar puntos de acceso en otros lugares además del techo, como paredes laterales y pilares de cemento. Tenga en cuenta también estos factores al realizar una encuesta en un almacén:

- Los niveles de inventario afectan al número de puntos de acceso necesarios. Pruebe la cobertura con dos o tres puntos de acceso en ubicaciones de ubicación estimadas.
- Es probable que se superpongan celdas inesperadas debido a las variaciones de múltiples rutas. La calidad de la señal varía más que la intensidad de esa señal. Los clientes pueden asociarse y funcionar mejor con puntos de acceso más alejados que con puntos de acceso cercanos.
- Durante una encuesta, los puntos de acceso y las antenas no suelen tener un cable de antena que los conecte. Sin embargo, en un entorno de producción, el punto de acceso y la

antena pueden requerir cables de antena. Todos los cables de antena introducen la pérdida de señal. La encuesta más precisa incluye el tipo de antena que se va a instalar y la longitud del cable que se va a instalar. Una buena herramienta para simular el cable y su pérdida es un atenuador en un kit de encuesta.

La inspección de una instalación de fabricación es similar a la inspección de un almacén, con la excepción de que podría haber muchas más fuentes de interferencias de radiofrecuencia en una instalación de fabricación. Además, las aplicaciones de una instalación de fabricación suelen requerir más ancho de banda que las de un almacén. Estas aplicaciones pueden incluir imágenes de vídeo y voz inalámbrica. Es probable que la distorsión de múltiples rutas sea el mayor problema de rendimiento en una instalación de fabricación.

Mecanismos de seguridad admitidos

Además de WEP estática y Cisco LEAP para la autenticación y el cifrado de datos, los distintivos Vocera también admiten WPA-PEAP (MS-CHAP v2)/WPA2-PSK.

Consideraciones sobre LEAP

LEAP permite que los dispositivos se autentiquen mutuamente (placa a punto de acceso y punto de acceso a placa) basándose en un nombre de usuario y una contraseña. Tras la autenticación, se utiliza una clave dinámica entre el teléfono y el punto de acceso para cifrar el tráfico. Sin embargo, el ataque del diccionario ASLEAP debe considerarse cuando decide utilizar LEAP como solución de seguridad:

Consulte Ataque del diccionario sobre la vulnerabilidad de Cisco LEAP para obtener más información.

Si se utiliza LEAP, se necesita un servidor RADIUS compatible con LEAP, como Cisco Access Control Server (ACS), para proporcionar acceso a la base de datos de usuarios. Cisco ACS puede almacenar localmente el nombre de usuario y la base de datos de contraseñas, o puede acceder a esa información desde un directorio externo de Microsoft Windows NT. Cuando utilice LEAP, asegúrese de que se utilizan contraseñas seguras en todos los dispositivos inalámbricos. Las contraseñas seguras se definen como de entre 10 y 12 caracteres y pueden incluir caracteres en mayúsculas y minúsculas, así como caracteres especiales.

Dado que todos los insignios utilizan la misma contraseña y se almacenan en el distintivo, Cisco recomienda que utilice nombres de usuario y contraseñas diferentes en clientes de datos y clientes de voz inalámbricos. Esta práctica ayuda con el seguimiento y la resolución de problemas, así como con la seguridad. Aunque es una opción de configuración válida utilizar una base de datos externa (fuera de ACS) para almacenar los nombres de usuario y las contraseñas de los identificadores, Cisco no recomienda esta práctica. Debido a que el ACS debe ser consultado cada vez que el distintivo se traslada entre los puntos de acceso, el impredecible retraso para acceder a una base de datos fuera de ACS podría causar un retraso excesivo y una calidad de voz deficiente.

Infraestructura de red inalámbrica

La red de telefonía IP inalámbrica, al igual que una red de telefonía IP por cable, requiere una cuidadosa planificación de la configuración de VLAN, el tamaño de la red, el transporte multidifusión y las opciones de equipos. Tanto para las redes de telefonía IP por cable como

inalámbricas, las VLAN de voz y de datos independientes suelen ser la forma más eficaz de realizar la implementación sugerida para garantizar un ancho de banda de red suficiente y la facilidad de resolución de problemas.

VLAN de voz, datos y vocera

Las VLAN proporcionan un mecanismo para segmentar las redes en uno o más dominios de broadcast. Las VLAN son especialmente importantes para las redes de telefonía IP, donde la recomendación típica es separar el tráfico de voz y datos en diferentes dominios de capa 2. Cisco recomienda que configure VLAN separadas para los distintivos de Vocera de otro tráfico de voz y datos: una VLAN nativa para el tráfico de administración de puntos de acceso, VLAN de datos para el tráfico de datos, una VLAN de voz o auxiliar para el tráfico de voz y una VLAN para los distintivos Vocera. Una VLAN de voz independiente permite a la red aprovechar el marcado de Capa 2 y proporciona colas de prioridad en el puerto del switch de acceso de Capa 2. Esto garantiza que se proporciona una QoS adecuada para diversas clases de tráfico y ayuda a resolver problemas como el direccionamiento IP, la seguridad y la dimensionamiento de la red. Los distintivos Vocera utilizan una función de difusión que utiliza la multidifusión para ofrecer. Esta VLAN común garantiza que cuando una placa se traslada entre los controladores, siga siendo parte del grupo multicast. Este último proceso se analiza en detalle cuando se trata la multidifusión más adelante en este documento.

Dimensionamiento de la red

El dimensionamiento de la red de telefonía IP es esencial para garantizar que haya suficiente ancho de banda y recursos disponibles para satisfacer las demandas presentadas por la presencia del tráfico de voz. Además de las directrices de diseño habituales de telefonía IP para el dimensionamiento de componentes como puertos de gateway PSTN, transcodificadores, ancho de banda WAN, etc., tenga en cuenta estos problemas de 802.11b al dimensionar la red de telefonía IP inalámbrica. Los distintivos Vocera son una aplicación especializada que amplía el número de clientes conectados por cable más allá de nuestras recomendaciones de implementación habituales.

Número de dispositivos 802.11b por punto de acceso

Cisco recomienda que no tenga más de 15 a 25 dispositivos 802.11b por punto de acceso.

Número de llamadas activas por punto de acceso

Vocera utiliza dos códecs diferentes en función de si se trata de una llamada de placa a placa (códec propietario de velocidad de bits baja) o de una llamada de placa a teléfono (códec G.711). Esta tabla muestra un porcentaje del ancho de banda disponible según las velocidades de datos y le ofrece una imagen más clara del rendimiento esperado:

Proceso de llamada	1 Mbps	2 Mbps	5,5 Mbps	11 Mbps
Badge-to-Phone (G.711)	20.7%	11.8%	6,3%	4.7%
Badge-to-Badge (códec de velocidad de bits baja propiedad)	9.4%	6.1%	4.2%	3.6%

Recomendaciones del switch

Nota: Si utiliza un Cisco Catalyst 4000 Series Switch como router principal en la red, asegúrese de que contenga, como mínimo, un módulo Supervisor Engine 2+ (SUP2+) o Supervisor Engine 3 (SUP3). El módulo SUP1 o SUP2 puede causar retrasos en el roaming, al igual que los switches Cisco Catalyst 2948G, 2980G, 2980G-A, 4912 y 2948G-GE-TX.

Puede crear una plantilla de puerto de switch para utilizarla cuando configure cualquier puerto de switch para la conexión a un punto de acceso. Esta plantilla debe agregar todas las funciones básicas de seguridad y resistencia de la plantilla de escritorio estándar. Además, cuando se conecta el punto de acceso a un switch Cisco Catalyst 3750, se puede optimizar el rendimiento del punto de acceso mediante el uso de comandos QoS de switching multicapa (MLS) para limitar la velocidad de los puertos y asignar la configuración de Clase de servicio (CoS) a Punto de código de servicios diferenciados (DSCP).

No se debe enviar a un punto de acceso ningún tráfico que no sea necesario para los clientes de WLAN. Una plantilla debe diseñarse de forma que ayude a crear una conexión de red segura y resistente con estas funciones:

- Devolver configuraciones de puerto al valor predeterminado: evita conflictos de configuración al borrar cualquier configuración de puerto existente.
- Desactivar protocolo de enlace troncal dinámico (DTP): desactiva el enlace troncal dinámico, que no es necesario para la conexión a un punto de acceso.
- Desactivar el protocolo de agregación de puertos (PagP): PagP está activado de forma predeterminada, pero no es necesario para los puertos orientados al usuario.
- Enable Port Fast (Activar puerto rápido): permite que un switch reanude rápidamente el tráfico de reenvío si se desactiva un link de árbol de expansión.
- Configurar VLAN inalámbrica: crea una VLAN inalámbrica única que aísla el tráfico inalámbrico de otras VLAN de datos, voz y gestión. Esto aísla el tráfico y garantiza un mayor control del tráfico.
- Habilitar calidad de servicio (QoS); no confiar en el puerto (marca hasta 0): garantiza el tratamiento adecuado del tráfico de alta prioridad, incluidos los softphones, y evita que los usuarios consuman un ancho de banda excesivo reconfigurando sus PC.

Los switches de alimentación en línea WS-C3750-48PS-S se pueden utilizar para proporcionar alimentación a los puntos de acceso que pueden recibir alimentación en línea.

El Catalyst 6500 le permite reenviar paquetes a velocidad de línea con todas las funciones descritas aquí, así como integrar numerosos módulos de servicio. El Wireless Service Module (WiSM) permite tener dos controladores cada uno con la capacidad de controlar 150 puntos de acceso cada uno. Con hasta cinco WiSM por chasis, esto le permite controlar más de 1500 puntos de acceso que admiten 50 000 clientes en una única arquitectura de switching de alto rendimiento.

Implementaciones y configuración

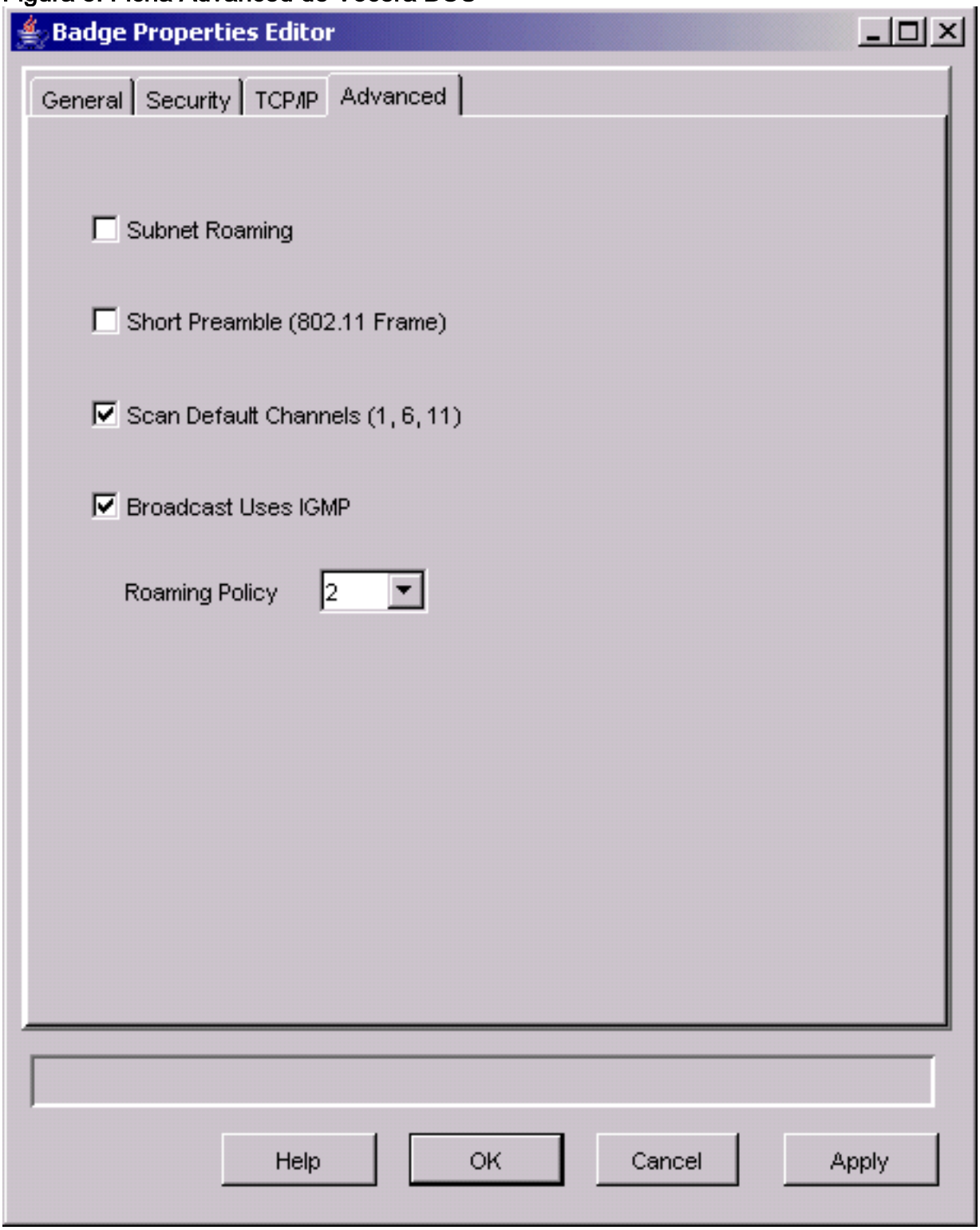
Configuración de la placa

La utilidad de configuración de distintivos de Vocera (BCU) y la configuración de la placa pueden introducir itinerancia y latencia en el entorno si se realiza de forma incorrecta. Utilice la BCU y el

Editor de propiedades de la placa (BPE) para comprobar estos parámetros (consulte la figura 8):

- **El roaming de subred** está desactivado.
- **La opción Buscar canales predeterminados (1,6,11)** está activada.
- **La difusión utiliza IGMP** está habilitada.
- La política de roaming se establece en **2** o superior.

Figura 8: Ficha Advanced de Vocera BCU



Cuando se marca **Subnet Roaming**, indica a la insignia que solicite una nueva dirección IP después de cada roaming. En el entorno LWAPP, la infraestructura ayuda a mantener la conectividad del cliente en la Capa 3. Cuando un cliente de voz debe esperar a que el servidor DHCP responda antes de poder enviar o recibir paquetes, se introducen el retardo y la

fluctuación. Si **Scan Default Channels (1,6,11)** no está activado, la insignia escanea todos los canales 802.11b cuando la insignia parece romar. Esto evita el reenvío de paquetes y el roaming sin problemas.

Ajuste de AutoRF para su entorno

Como se describe en la sección Recomendaciones de este documento, es importante entender que cada sitio tiene sus propias características de RF. Es posible que sea necesario ajustar AutoRF o Radio Resource Management (RRM), en el entendimiento de que cada sitio es diferente y que AutoRF/RRM debe ajustarse para su entorno.

Antes de ajustar AutoRF, consulte Administración de recursos de radio en Redes Inalámbricas Unificadas para obtener más información.

RRM le permite ajustar la potencia de transmisión de cada punto de acceso, ajustando la intensidad con la que cada punto de acceso oye a su tercer vecino más fuerte. Este valor sólo se puede ajustar desde la CLI mediante el comando **config advanced 802.11b tx-power-threshold** como se describe en Configuración de Asignación de Nivel de Potencia Tx.

Antes de ajustar AutoRF, camine por el sitio de implementación usando la insignia Vocera tal como la usa el usuario final y utilice una herramienta de sondeo del sitio para obtener una comprensión sólida de cómo se mueve la insignia y a qué potencia se ve cada punto de acceso. Una vez que esto se complete y se determine que se requiere ajustar este valor, comience con un valor de -71 dBm para el algoritmo de control de potencia de transmisión. Utilice este parámetro CLI:

```
config advanced 802.11b tx-power-thresh -71
```

Deje que la red funcione con este ajuste con un mínimo de 30 minutos a una hora antes de observar cualquier cambio. Una vez que se haya dado a la red un tiempo suficiente, camine por el sitio utilizando la misma herramienta de sondeo y las mismas insignias de nuevo. Observe las mismas características de itinerancia y potencia del punto de acceso. El objetivo aquí es intentar que las insignias deambulen en o antes del siguiente punto de acceso para obtener la mejor relación señal-ruido posible.

- **¿Cómo sé si la potencia de transmisión está demasiado caliente o demasiado fría?**Determinar si su umbral de potencia de transmisión es demasiado alto o demasiado bajo requiere una buena comprensión de su entorno. Si ha recorrido todo el área de implementación (donde espera que funcionen las insignias de Vocera), debe saber dónde se encuentran sus puntos de acceso, así como experimentar el comportamiento de itinerancia de la insignia.
- **¿Qué hago si mi potencia de transmisión está demasiado caliente?**El distintivo Vocera se basa únicamente en la potencia de la señal en lugar de en la calidad de la señal. Si la barra de vocera no se mueve después de pasar varios puntos de acceso mientras se encuentra en el tutorial de bienvenida o en el tono de prueba, la insignia se considera pegajosa. Si este comportamiento indica el área de implementación de campus completa, el umbral de potencia de transmisión está demasiado caliente y se debe realizar una copia de seguridad. Si sólo una o dos áreas aisladas muestran este comportamiento y el resto del área de implementación muestra características de itinerancia más idealistas, esto no indica que su red esté demasiado caliente.

- **¿Qué hago si mi potencia de transmisión está demasiado fría?**El umbral de transmisión predeterminado casi nunca debería proporcionarle un área de implementación donde su red se ejecuta demasiado fría. Si el umbral de potencia de transmisión se ajusta hacia abajo, y caminar por las salas con la barra de Vocera le proporciona un entorno en el que la placa se mueve bien, pero pierde conectividad y/o cobertura muerta/irregular, entonces su red podría haber sido ajustada demasiado baja. Si esto no es característico de toda la red, sino aislado en una o dos áreas, entonces es más indicativo de un agujero de cobertura que de un problema en toda la red.
- **Comportamiento aislado**Si encuentra que en una o dos áreas, la insignia se pega a un punto de acceso en lugar de vagar de una manera idealista, examine esta área.¿En qué se diferencia este área del resto del campus?Si estas áreas están cerca de salidas de edificios o áreas en construcción, ¿podría la detección de agujeros de cobertura obligar a estos puntos de acceso a aumentar la potencia?Observe el archivo de registro del WLC y las listas de vecinos del punto de acceso para ayudar a determinar por qué podría ocurrir tal anomalía.Si descubre que en una o más áreas aisladas, la insignia experimenta cobertura muerta o irregular, entonces necesita examinar estas áreas por separado.¿Esta zona está cerca de un eje de ascensores, radiología o una sala de descanso?Estas áreas podrían ser más adecuadas por la instalación o mejor ubicación de un punto de acceso para permitir una mejor cobertura de voz.En ambos casos, siempre es aconsejable entender que está trabajando en un espectro de radio sin licencia y que es posible que el comportamiento idealista no se pueda lograr nunca. Esto podría ocurrir cuando se encuentra junto a una torre o dispositivo de transmisión de radio, un transmisor de televisión o posiblemente una instalación de reparación de 2,4 GHz que no sea 802.11 (teléfonos inalámbricos, etc.).

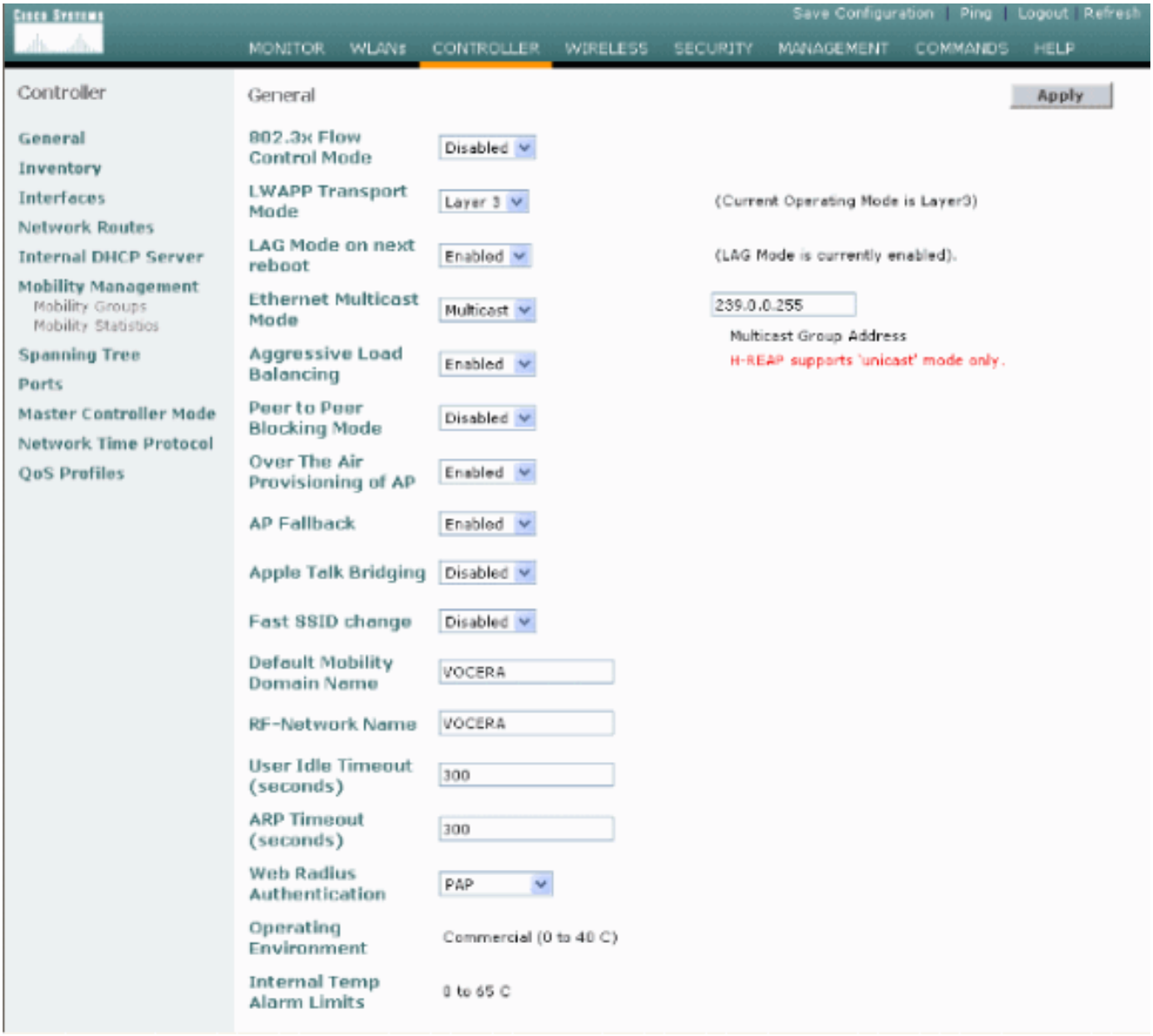
Configuración de la infraestructura de red inalámbrica

Se debe seguir la guía de diseño e implementación de Cisco Unified Wireless Network para la configuración general de sus WLC. Esta sección proporciona recomendaciones adicionales específicas para los distintivos de comunicación de Vocera®.

Nota: Los cambios se dejan sin guardar si no pulsa el botón **Aplicar** antes de pasar al paso siguiente.

Complete estos pasos en el menú **Controller** de nivel superior:

1. Cambie el modo de multidifusión Ethernet a **multidifusión**.
2. Establezca la dirección de grupo de multidifusión en **239.0.0.255** (o alguna otra dirección de grupo de multidifusión no utilizada).
3. Establezca el nombre de dominio de movilidad predeterminado y el nombre de red de radiofrecuencia en el diseño de red.
4. Inhabilite **Balanceo de Carga Agresivo**.**Figura 9: Configuración general del WLC**

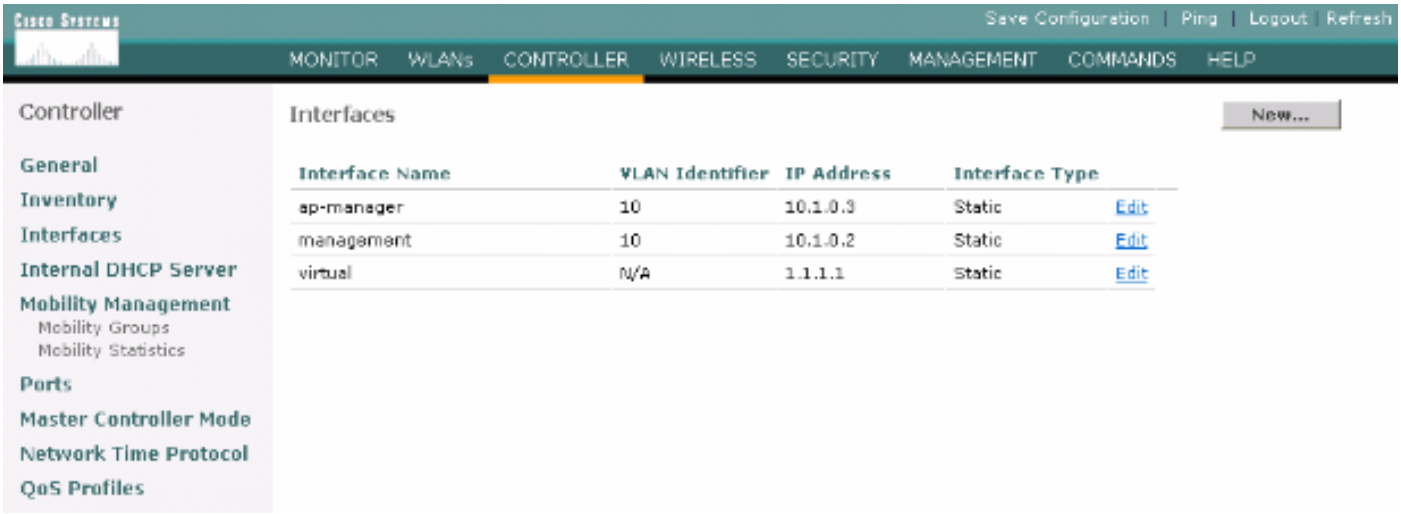


Crear interfaces

Haga clic en **Controlador > Interfaces**.

Nota: Su VLAN y dirección IP varían. Las capturas de pantalla aquí proporcionan un direccionamiento de muestra que no debe seguirse directamente.

Figura 10: Lista de interfaces WLC



Crear la interfaz de voz de Vocera

Complete estos pasos:

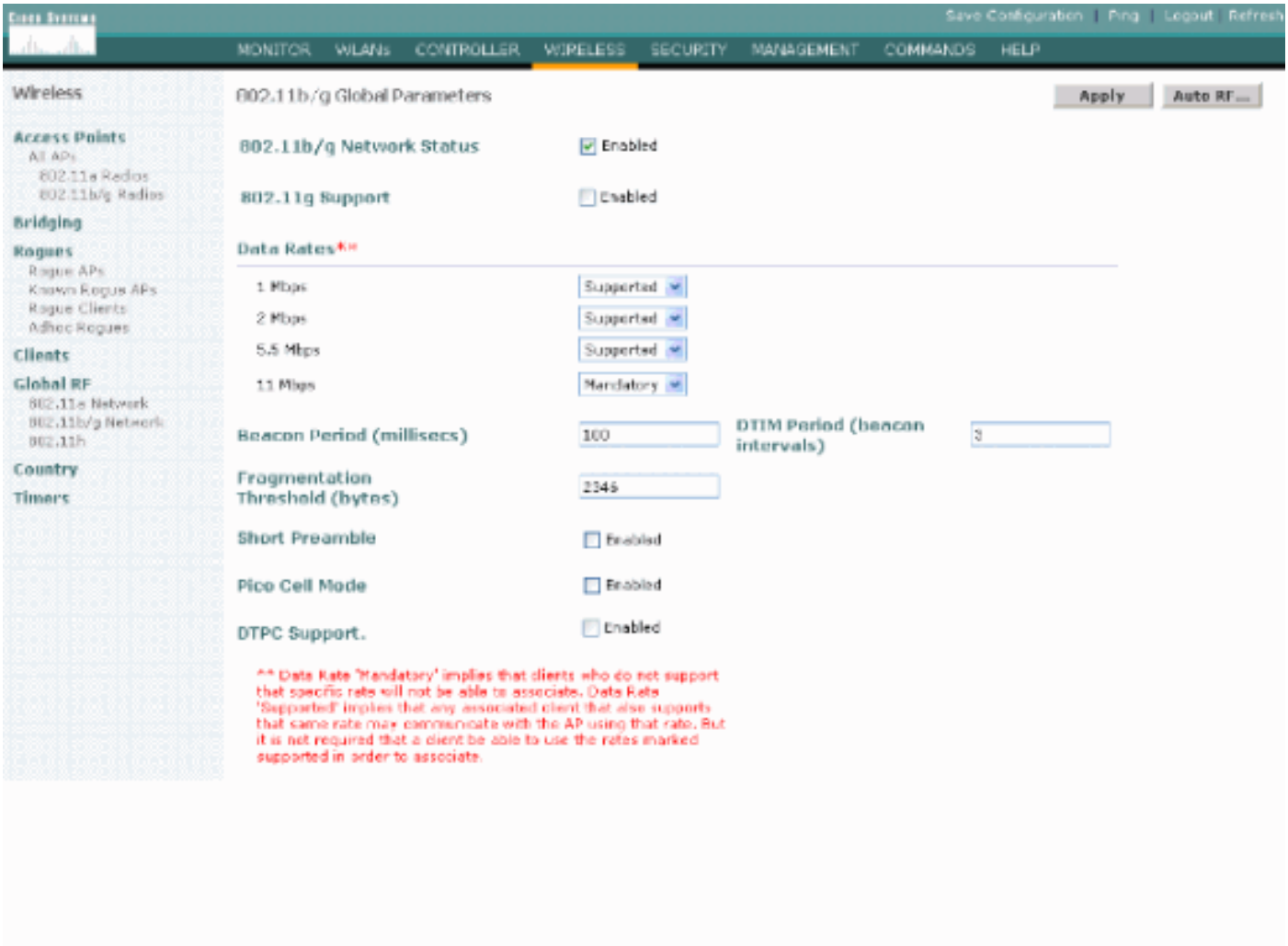
1. Haga clic en **New**.
2. Introduzca un nombre de etiqueta representativo de la red VoWLAN de Vocera en el campo Interface Name (Nombre de la interfaz).
3. Introduzca el número de VLAN de esa red VoWLAN en el campo ID de VLAN.
4. Haga clic en **Aplicar** y luego haga clic en **Editar** para editar la interfaz que acaba de crear.
5. Ingrese el direccionamiento IP para esta interfaz que está en el rango de la VLAN y otra información relacionada.
6. Haga clic en Apply (Aplicar).

Configuración específica de la conexión inalámbrica

En el caso de una WLAN que sólo tenga distintivos Vocera, esta configuración proporciona la configuración de ejemplo que mejor admite la aplicación de difusión Vocera.

- El periodo DTIM es **1**.
- La compatibilidad con 802.11g está desactivada. Sólo la velocidad de datos 802.11b de **11 Mpbs** es **obligatoria**.
- El preámbulo corto está desactivado.
- DTPC está desactivado.

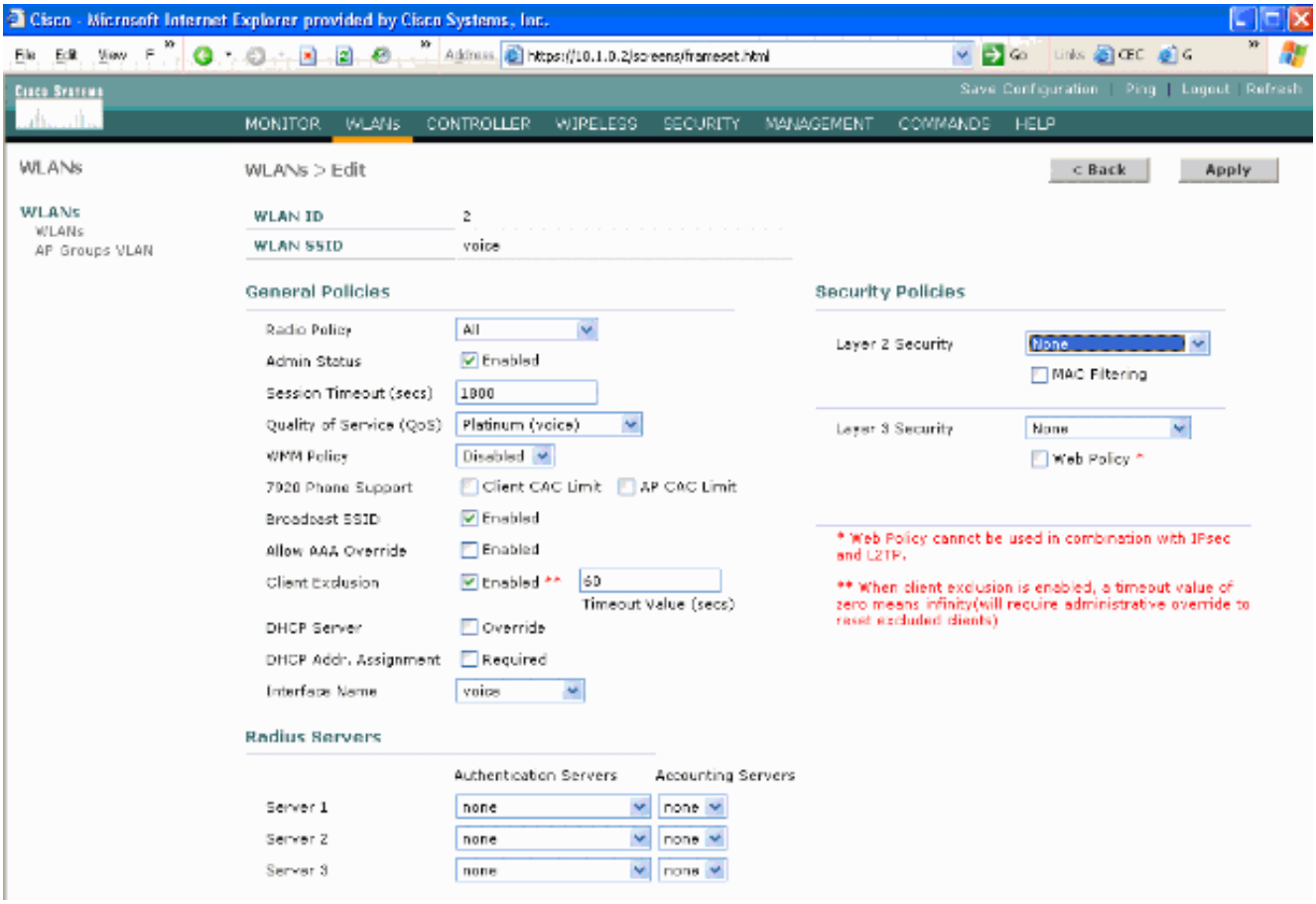
Figura 11—Configuración de 802.11b/g



Configuración de WLAN

Complete estos pasos:

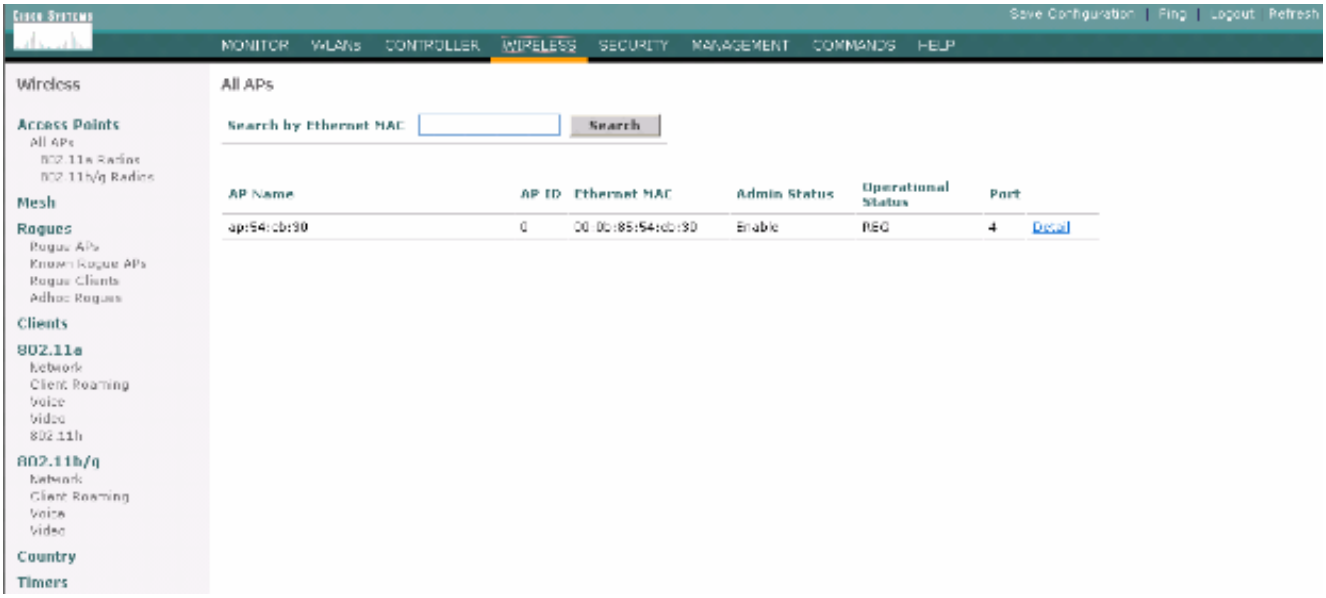
1. Actualice el campo Política de radio a un valor que se ajuste mejor a sus necesidades.
2. Cambiar estado de administrador a **Habilitado**.
3. Establezca el tiempo de espera de la sesión en **1800**.
4. Establezca Calidad de Servicio en **Platinum**.
5. Establezca Broadcast SSID en **Enabled**.
6. Establezca el nombre de la interfaz en la interfaz creada para los distintivos de comunicación de Vocera.
7. Establezca las opciones de seguridad para que coincidan con las políticas corporativas.**Figura 12: Configuración de WLAN**



Configurar detalles del punto de acceso

Complete estos pasos:

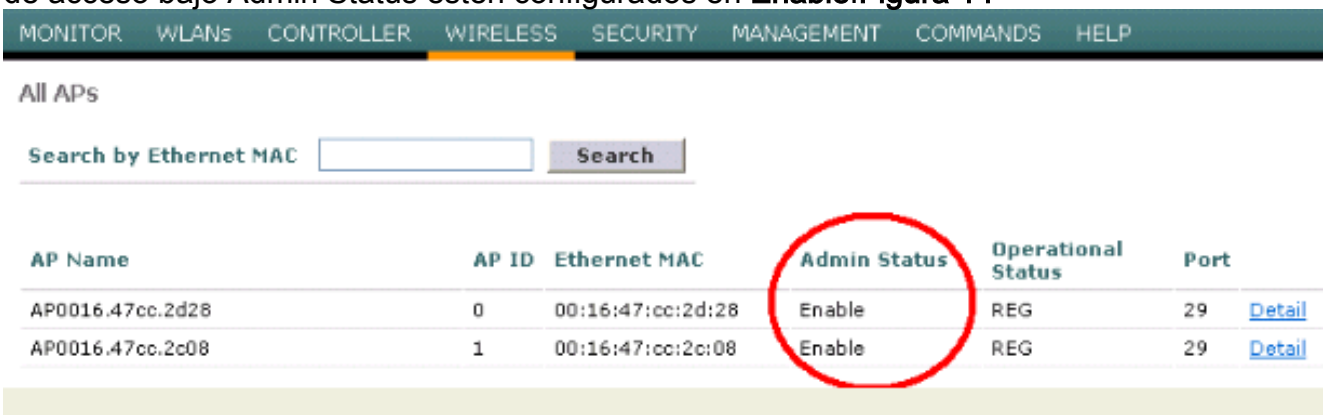
1. Haga clic en **Detalle**.
2. Configure el nombre AP.
3. Asegúrese de que el punto de acceso esté configurado para DHCP.
4. Asegúrese de que Admin Status esté **habilitado**.
5. AP Mod" debe configurarse en **local**.
6. Introduzca la ubicación del punto de acceso.
7. Introduzca el nombre del controlador al que pertenece el punto de acceso. El nombre del controlador se puede encontrar en la página Monitor.
8. Haga clic en Apply (Aplicar).**Figura 13: detalle de punto de acceso**



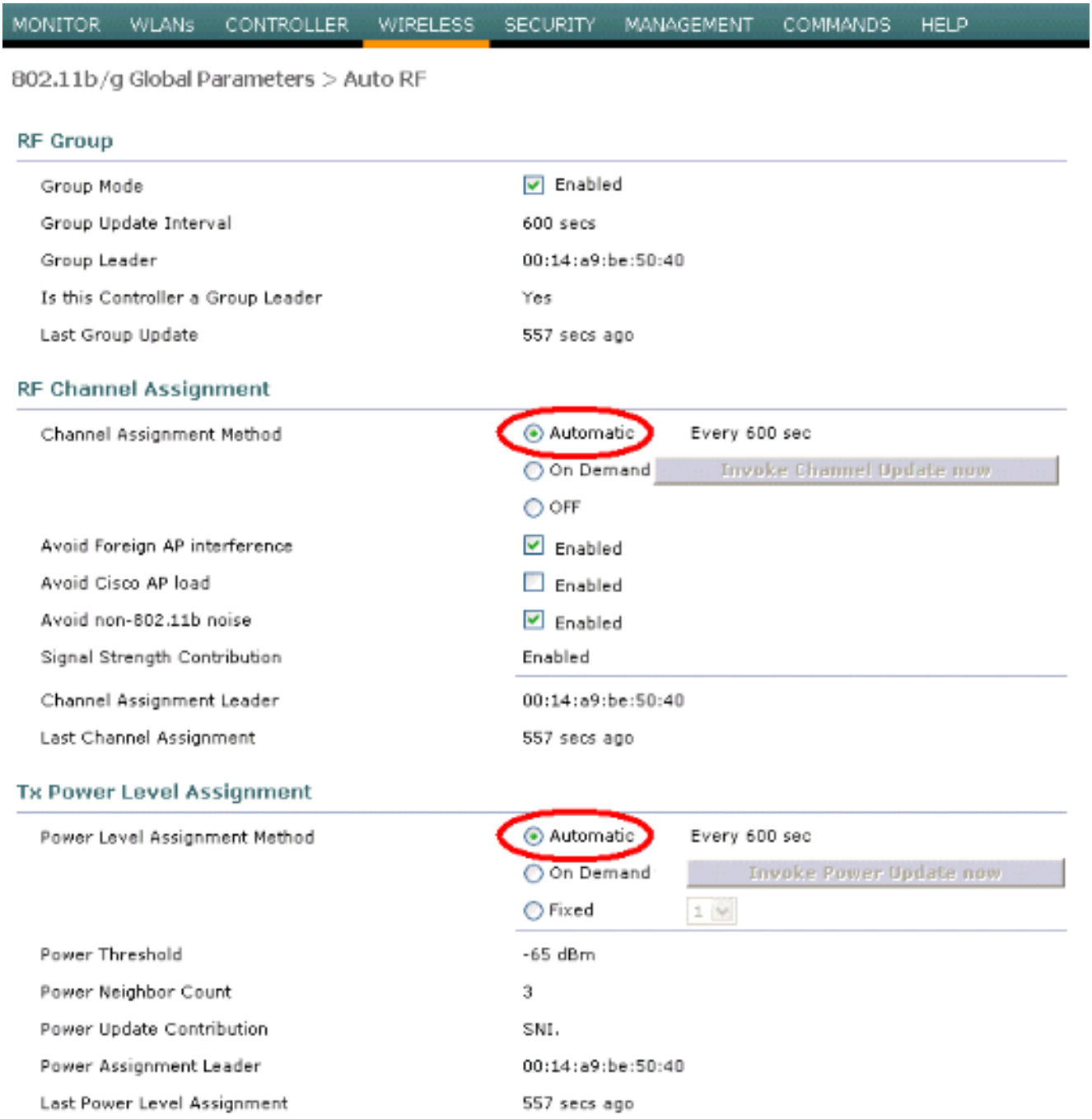
Configuración de la radio 802.11b/g

Complete estos pasos:

1. Haga clic en **Wireless** ubicado en la parte superior del WLC y verifique que todos los puntos de acceso bajo Admin Status estén configurados en **Enable**.**Figura 14**



2. Haga clic en **Red** (ubicado cerca de 802.11b/g).
3. Haga clic en **AutoRF**.
4. Utilice AutoRF para crear una cobertura completa con un canal de RF no superpuesto y una potencia de transmisión. Para hacer esto, seleccione **Automático** para la Asignación de Canal RF y Asignación de Nivel de Potencia Tx.**Figura 15**



5. Haga clic en Apply (Aplicar).
6. Haga clic en **Guardar configuración** y vea la sección Ajustar AutoRF para su entorno de este documento.
7. Elija **Wireless > Access Points > 802.11b/g Radios**.Figura 16

Verificación de telefonía IP inalámbrica

Después de realizar un sondeo del sitio de RF y configurar los puntos de acceso y los teléfonos, es fundamental realizar pruebas de verificación para asegurarse de que todo funciona según lo deseado. Estas pruebas deben realizarse en todas estas ubicaciones:

- El área principal de cada celda de punto de acceso (donde es más probable que las insignias se conecten a ese punto de acceso concreto).
- Cualquier ubicación en la que pueda haber un gran volumen de llamadas.
- Ubicaciones donde el uso puede ser poco frecuente pero la cobertura aún tiene que ser certificada (por ejemplo, escaleras, baños, etc.).
- En los extremos del área de cobertura del punto de acceso.
- ·Estas pruebas pueden realizarse en paralelo o en serie. Si se realiza en paralelo, asegúrese de que los teléfonos se apagan entre puntos de prueba para probar la asociación completa, la autenticación y el registro en cada ubicación. Las pruebas de roaming y carga deben ser las pruebas finales.

Asociación, autenticación y registro

Esta sección explica cómo verificar que el distintivo asocia, autentica y se registra correctamente.

- En varios puntos del entorno, encienda las insignias y verifique la asociación con el punto de acceso. Si el identificador no se asocia al punto de acceso, realice estas comprobaciones:Verifique la configuración de la placa para asegurarse de que el SSID, el tipo de autenticación, etc.Verifique la configuración del WLC para asegurar el SSID adecuado, el tipo de autenticación, los canales de radio, etc.Consulte el sondeo del sitio para asegurarse de que la ubicación tiene una cobertura de RF adecuada.
- En varios puntos del entorno, asegúrese de que el teléfono se autentica correctamente a través del punto de acceso. Si el cliente no se autentica, verifique la clave WEP o el nombre de usuario y contraseña LEAP en las insignias. Además, verifique el nombre de usuario y la contraseña en el servidor AAA usando un portátil inalámbrico con credenciales idénticas.
- En varios puntos del entorno, asegúrese de que las insignias se registran en el servidor de comunicación de Vocera. Si el cliente no se registra, realice estas comprobaciones:Verifique que el identificador tenga la dirección IP, la máscara de subred, el gateway principal, el TFTP primario, el primario/secundario y el DNS correctos.
- Llamadas de voz estacionarias:En varios puntos del entorno, mientras se mantiene parado, realice una llamada a otra insignia y pruebas de voz de entre 60 y 120 segundos para comprobar la calidad de la voz. Si la calidad de voz es inaceptable, mueva una insignia a una mejor ubicación y vuelva a probar. ¿Es aceptable la calidad de voz? Si no es así, consulte su cobertura inalámbrica.Si el servidor de telefonía está configurado, en varios puntos del entorno, se parará y realizará una llamada a un teléfono con cables y realizará pruebas de voz de 60 a 120 segundos para comprobar la calidad de la voz. Si la calidad de voz es inaceptable, pregunte si realiza una llamada con el teléfono por cable. ¿Es aceptable la calidad de voz? Si no es así, verifique el diseño de la red por cable según las directrices.
- Utilice las herramientas de sondeo del sitio para verificar que no haya más de un punto de acceso por canal RF desde esa ubicación con una potencia de señal (indicador de potencia de la señal recibida [RSSI]) superior a 35. Si hay dos puntos de acceso presentes en el

mismo canal, asegúrese de que la relación señal-ruido (SNR) sea lo más alta posible para minimizar las interferencias. Por ejemplo, si el punto de acceso más fuerte tiene un RSSI de 35, idealmente el punto de acceso más débil debería tener un RSSI inferior a 20. Para lograr este objetivo, es posible que tenga que reducir la potencia de transmisión de un punto de acceso o mover el punto de acceso.
- Verifique los parámetros de QoS en el punto de acceso para confirmar los ajustes recomendados adecuados.
- Llamadas de identificación de roaming:Si el servidor de telefonía no está disponible, inicie Vocera Tutorial con el comando **Begin Tutorial**.OSi el servidor de telefonía está disponible, inicie una llamada con un dispositivo estacionario a la placa.Compruebe continuamente la calidad de voz mientras atraviesa el área de cobertura inalámbrica total. Si la calidad de voz es insuficiente, realice estas tareas:Escuche todos los cambios inaceptables en la calidad de voz y tome nota de la ubicación y los valores de radio de su portátil y los valores de CQ de la placa.Esté atento y escuche la insignia para desplazarse hasta el siguiente punto de acceso.Observe los otros puntos de acceso disponibles en el sondeo del sitio para comprobar la cobertura y las interferencias.
- Realice ajustes en la ubicación y la configuración del punto de acceso para ajustar la WLAN y realice estas comprobaciones para garantizar la calidad de voz:Utilice las herramientas de sondeo del sitio y verifique que no haya más de un punto de acceso por canal con un valor RSSI superior a 35 en cualquier ubicación dada. Lo ideal es que todos los demás puntos de acceso del mismo canal tengan valores RSSI lo más bajos posible (preferiblemente menos de 20). En el borde del área de cobertura donde el RSSI es 35, el RSSI para todos los demás puntos de acceso en el mismo canal debería ser idealmente menor a 20.Utilice las herramientas de sondeo del sitio para verificar que haya al menos dos puntos de acceso (total, en canales independientes) visibles en todas las ubicaciones con una potencia de señal suficiente.Verifique que los puntos de acceso en un área de roaming dada estén todos en una red de Capa 2.

Problemas comunes de roaming

Estos problemas de roaming pueden ocurrir:

- La insignia no se mueve cuando se coloca directamente debajo del punto de acceso.
- Es muy probable que la placa no alcance los umbrales diferenciales de itinerancia para el indicador de potencia de la señal recibida (RSSI) y la utilización del canal (CU). Ajuste el umbral de potencia de transmisión del WLC.
- La insignia no recibe las balizas ni las respuestas de sonda del punto de acceso.
- La placa camina demasiado despacio.

El distintivo pierde la conexión a la red o el servicio de voz se pierde al roaming

- Verifique la autenticación para ver una posible discordancia WEP.
- La insignia no envía las uniones IGMP o la red envía las consultas IGMP durante un roaming. Por lo tanto, la función de broadcast de Vocera falla durante un roaming de Capa 2/Capa 3.
- La insignia es capaz de itinerancia de capa 2 sin problemas solamente (a menos que se configure un mecanismo de movilidad de capa 3). Asegúrese de que el nuevo WLC no esté sirviendo a una subred IP diferente.

- Verifique que el punto de acceso/controlador asociado tenga conectividad IP con Vocera Communication Server.
- Compruebe la potencia de la señal RF y los valores de la placa CQ.

El distintivo pierde calidad de voz mientras se desplaza

- Verifique si hay un RSSI bajo en el punto de acceso de destino.
- La superposición del canal puede ser insuficiente. La insignia debe tener tiempo para entregar la llamada sin problemas antes de que pierda su señal con el punto de acceso original.
- Es posible que se pierda la señal del punto de acceso original.

Problemas de audio

Hay algunos errores de configuración comunes que pueden causar algunos problemas de audio fácilmente resueltos. Si es posible, verifique los problemas de audio con una insignia (de referencia) estacionaria para ayudar a reducir el problema a un problema inalámbrico. Los problemas de audio comunes incluyen:

- Audio de un solo lado
- Audio irregular
- Problemas de registro y autenticación

Audio de un solo lado

- Este problema puede ocurrir en las áreas marginales de un punto de acceso, donde una señal puede ser demasiado débil en el lado del indicador o en el del punto de acceso. La coincidencia de los parámetros de alimentación del punto de acceso con el indicador (20 mW), siempre que sea posible, puede solucionar este problema. Este problema es más común cuando la variación entre la configuración del punto de acceso y la configuración de la placa es grande (por ejemplo, 100 mW en el punto de acceso y 28 mW en la placa).
- Verifique la gateway y el ruteo IP para la calidad de voz.
- Verifique si un firewall o NAT está en la trayectoria de los paquetes UDP patentados. De forma predeterminada, los firewalls y las NAT provocan audio unidireccional o sin audio. Los firewalls y NAT de Cisco IOS® y PIX tienen la capacidad de modificar esas conexiones para que pueda fluir el audio bidireccional.Si utiliza la movilidad de capa 3, la red podría estar bloqueando el tráfico ascendente con comprobaciones de Unicast Reverse Path Forwarding (uRPF).
- El audio unidireccional puede ocurrir si el almacenamiento en caché ARP no está configurado en el WLC.

Audio irregular

- Una razón común para el audio amapotado o robótico es cuando un microondas opera cerca. Las microondas comienzan en el canal 9 y pueden extenderse de los canales 6 a 14.
- Compruebe la existencia de teléfonos inalámbricos de 2,4 Ghz y otros dispositivos de enfermería que llaman a dispositivos inalámbricos con herramientas como Cognio.

Problemas de registro y autenticación

Cuando encuentre problemas con la autenticación, realice estas comprobaciones:

- Compruebe los SSID para asegurarse de que coinciden con el distintivo y el punto de acceso (o red). También asegúrese de que la red tenga una ruta al servidor Vocera.
- Compruebe las claves WEP para asegurarse de que coinciden. Es una buena idea volver a introducirlos en la utilidad de configuración de distintivos (BCU) y volver a programar la insignia, ya que es fácil cometer un error al escribir una clave o contraseña WEP.

Estos mensajes o síntomas pueden ocurrir:

- No se pueden admitir todas las capacidades solicitadas: lo más probable es que haya una discordancia de cifrado entre el punto de acceso y el cliente.
- Error de autenticación / No se encontró ningún AP: asegúrese de que los tipos de autenticación coincidan en el punto de acceso y el cliente.
- No Service - IP Config Failed: si utiliza WEP estático, asegúrese de que las claves están configuradas correctamente. Asegúrese de que otros clientes puedan recibir DHCP usando el mismo SSID.
- Desautenticar todos los clientes TKIP del AP: este problema ocurre cuando el punto de acceso detecta dos errores MIC en 60 segundos. Esta contramedida evita que todos los clientes TKIP se vuelvan a autenticar durante 60 segundos.
- Reautenticación / Tiempo de espera de sesión: si se configura, un tiempo de espera de sesión activa una reautenticación que causa lagunas en el flujo de voz (300 ms + demora WAN para la autenticación 802.1x).

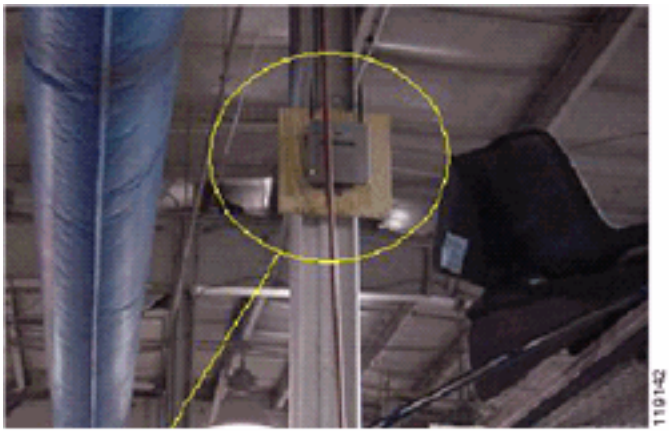
Apéndice A

Colocación de antena y punto de acceso

Esta sección ofrece ejemplos de la ubicación adecuada e inadecuada de puntos de acceso (AP) y antenas.

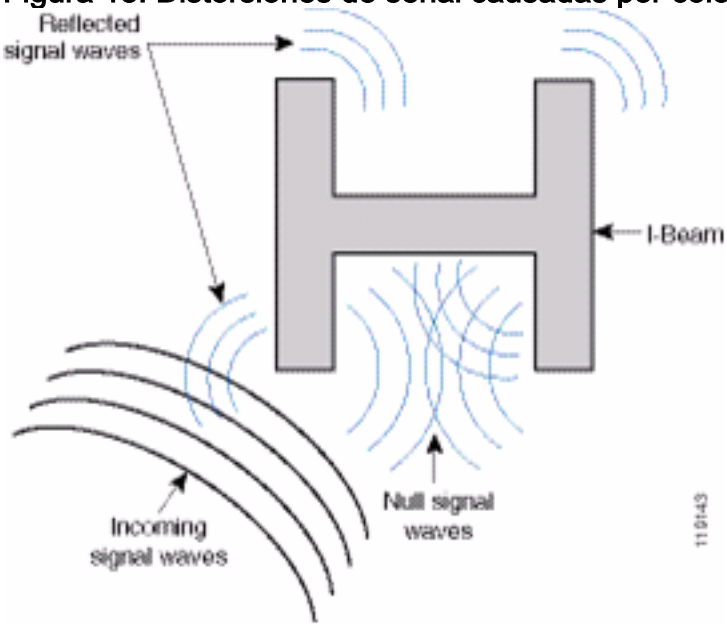
La figura 17 muestra la ubicación inadecuada de un punto de acceso y antenas cerca de un haz I, lo que crea patrones de señal distorsionados. El cruce de las ondas de señal crea un punto nulo de RF y se crea una distorsión de trayectoria múltiple cuando se reflejan las ondas de señal. Esta ubicación da como resultado una cobertura muy pequeña detrás del punto de acceso y una calidad de señal reducida frente al punto de acceso.

Figura 17: Colocación incorrecta de antenas cerca de un haz I



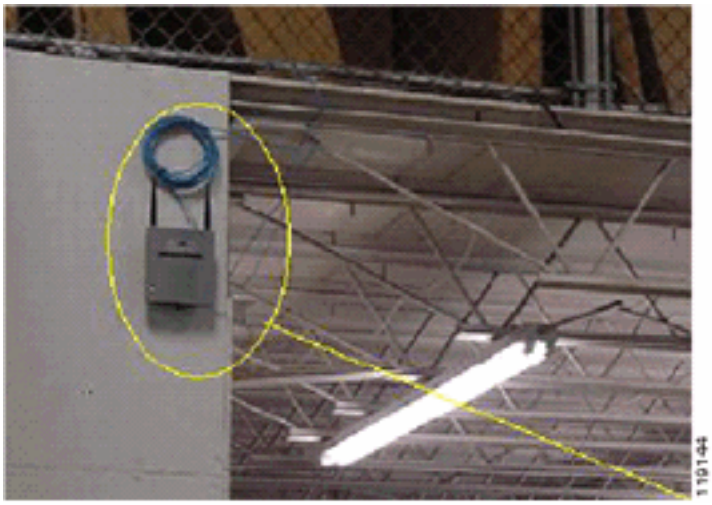
La figura 18 muestra los cambios o distorsiones de propagación de la señal provocados por un haz I. El haz I crea muchas reflexiones tanto de los paquetes recibidos como de los transmitidos. Las señales reflejadas resultan en una calidad de señal muy baja debido a los puntos nulos y la interferencia de múltiples rutas. Sin embargo, la potencia de la señal es alta porque las antenas del punto de acceso están tan cerca del haz I.

Figura 18: Distorsiones de señal causadas por colocar las antenas demasiado cerca de un haz I



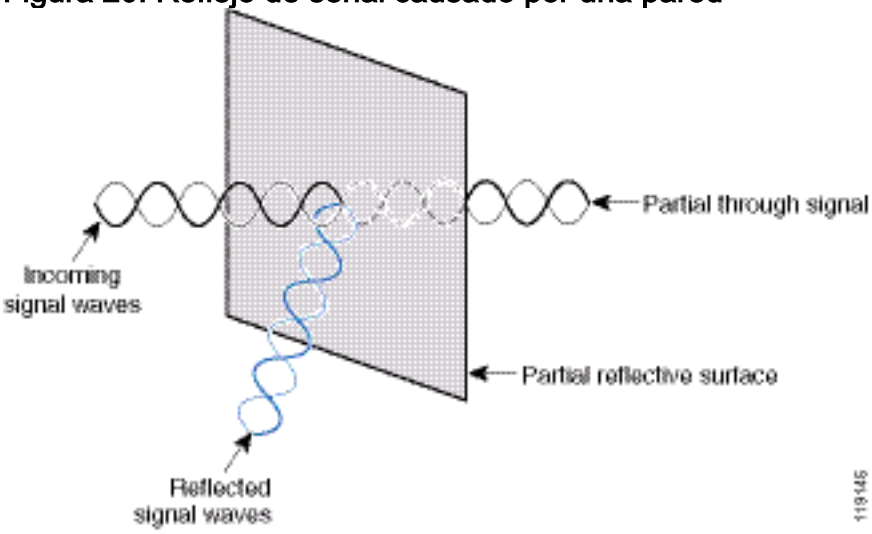
La ubicación del punto de acceso y de la antena en la figura 19 es mejor porque está lejos de los haces de luz y hay menos señales reflejadas, menos puntos nulos y menos interferencias de múltiples rutas. Esta posición todavía no es perfecta porque el cable Ethernet no debe enrollarse tan cerca de la antena. Además, el punto de acceso se podía girar con las antenas de 2,4 GHz apuntadas al suelo. Esto proporciona una mejor cobertura directamente por debajo del punto de acceso. No hay usuarios por encima del punto de acceso.

Figura 19: punto de acceso y antenas montadas en una pared, lejos de los rayos I



La figura 20 muestra la propagación de la señal causada por la pared en la que se monta el punto de acceso.

Figura 20: Reflejo de señal causado por una pared

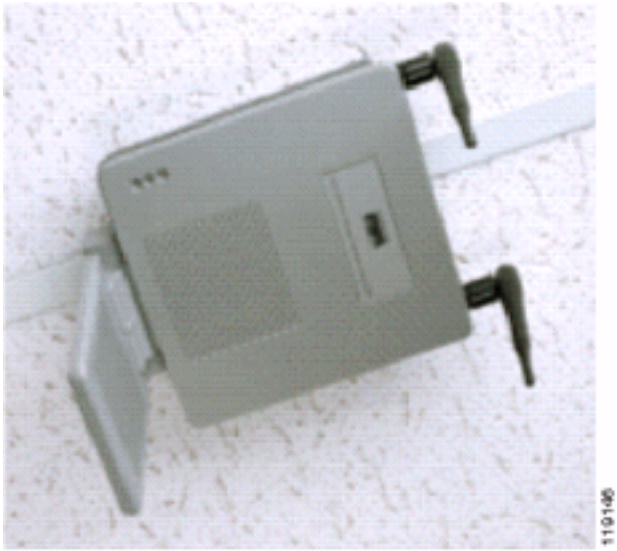


Los ejemplos anteriores también se aplican cuando coloca puntos de acceso y antenas en el techo o cerca del mismo en un entorno empresarial estándar. Si hay conductos de aire metálicos, barras de elevador u otras barreras físicas que puedan causar la reflexión de la señal o interferencias de múltiples rutas, Cisco recomienda encarecidamente que aleje las antenas de esas barreras. En el caso del elevador, mueva la antena a unos metros para ayudar a eliminar el reflejo y la distorsión de la señal. Lo mismo ocurre con los conductos de aire en el techo.

Una encuesta realizada sin enviar y recibir paquetes no es suficiente. El ejemplo I-beam muestra la creación de puntos nulos que pueden resultar de paquetes que tienen errores CRC. Los paquetes de voz con errores CRC son paquetes perdidos que afectan negativamente la calidad de voz. En este ejemplo, esos paquetes podrían estar por encima del nivel mínimo de ruido medido por una herramienta de sondeo. Por lo tanto, es muy importante que el sondeo del sitio no sólo mida los niveles de señal sino que también genere paquetes y luego informe de errores de paquetes.

La figura 21 muestra un Cisco AP1200 correctamente montado en una barra T del techo, con las antenas en una posición omnidireccional.

Figura 21: Cisco AP1200 montado en un techo



La figura 22 muestra una antena de diversidad omnidireccional Cisco Aironet 5959 montada correctamente en una barra T del techo. En este caso, el Cisco AP1200 se monta sobre el mosaico del techo.

Figura 22: Antena Cisco Aironet 5959 montada en un techo

La figura 23 muestra un Cisco AP1200 correctamente montado en una pared.

Figura 23: Cisco AP1200 montado en una pared

La figura 24 muestra la antena de parche de diversidad Cisco Aironet 2012 montada en una pared. En este caso, el Cisco AP1200 se monta sobre el mosaico del techo.

Figura 24: Antena Cisco Aironet 2012 montada en una pared

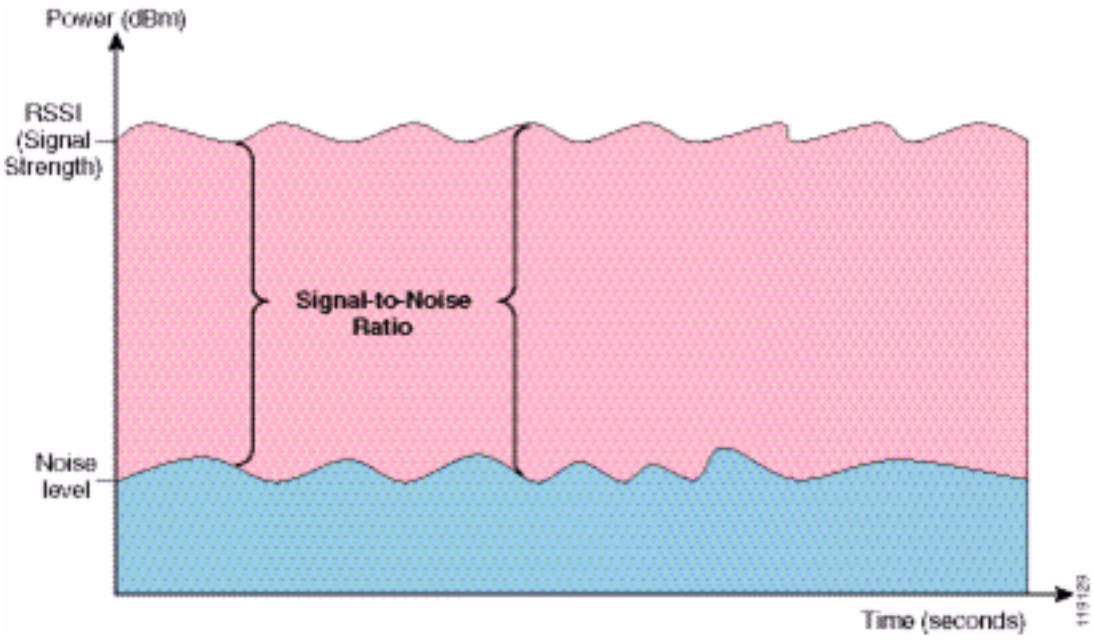
En las áreas en las que el tráfico de usuarios es elevado (como los espacios de oficinas, las escuelas, las tiendas minoristas y los hospitales), Cisco recomienda que coloque el punto de acceso fuera de la vista y coloque las antenas discretas debajo del techo. La separación de las antenas que no son de diversidad no debe superar los 18 pulgadas.

Distorsión de interferencias y múltiples rutas

El rendimiento de la red WLAN se ve afectado por las señales inutilizables. Las interferencias WLAN se pueden generar mediante hornos microondas, teléfonos inalámbricos de 2,4 GHz, dispositivos Bluetooth u otros equipos electrónicos que funcionan en la banda de 2,4 GHz. La interferencia también proviene normalmente de otros puntos de acceso y dispositivos cliente que pertenecen a la WLAN pero que están lo suficientemente alejados como para que su señal se debilite o se dañe. Los puntos de acceso que no forman parte de la infraestructura de red también pueden provocar interferencias WLAN y se identifican como puntos de acceso no autorizados.

La interferencia y la distorsión de múltiples rutas hacen que la señal transmitida fluctúe. La interferencia disminuye la relación señal-ruido (SNR) para una velocidad de datos determinada. Los recuentos de reintentos de paquetes aumentan en un área donde la interferencia y/o la distorsión de múltiples rutas son altas. La interferencia también se denomina nivel de ruido o nivel de ruido. La potencia de la señal recibida desde su punto de acceso asociado debe ser lo suficientemente alta por encima del nivel de ruido del receptor para ser decodificada correctamente. Este nivel de resistencia se denomina relación señal-ruido o SNR. El SNR ideal para la placa Vocera es de 25 dB. Por ejemplo, si el piso de ruido es de 95 decibelios por milivatio (dBm) y la señal recibida en el teléfono es de 70 dBm, la relación señal-ruido es de 25 dB. (Consulte la Figura 25).

Figura 25: Relación señal-ruido (SNR)



Cuando cambia el tipo y la ubicación de la antena, puede reducir la distorsión y la interferencia de múltiples rutas. La ganancia de la antena se añade a la ganancia del sistema y puede reducir la interferencia si el transmisor que interfiere no está directamente frente a la antena direccional.

Aunque las antenas direccionales pueden ser de gran valor para ciertas aplicaciones interiores, la gran mayoría de las instalaciones interiores utilizan antenas omnidireccionales. La direccionalidad debe determinarse estrictamente mediante un sondeo del sitio correcto y adecuado. Tanto si utiliza una antena omnidireccional como de parche, los entornos interiores requieren antenas de diversidad para mitigar la distorsión de múltiples rutas. Las radios de los puntos de acceso de la serie Cisco Aironet permiten la compatibilidad con la diversidad.

Atenuación de señal

La atenuación de la señal o la pérdida de la señal se produce incluso cuando la señal pasa por el aire. La pérdida de potencia de la señal es más pronunciada a medida que la señal pasa a través de diferentes objetos. Una potencia de transmisión de 20 mW equivale a 13 dBm. Por lo tanto, si la potencia transmitida en el punto de entrada de una pared de placa de yeso es de 13 dBm, la potencia de la señal se reduce a 10 dBm al salir de esa pared. Esta tabla muestra la pérdida probable de intensidad de la señal causada por varios tipos de objetos.

Atenuación de señal causada por varios tipos de objetos

Objeto en Ruta de Señal	Atenuación de la señal a través del objeto
Muro de placa	3 dB
Muro de vidrio con marco metálico	6 dB
Cinturón	4 dB
ventana Office	3 dB
Puerta metálica	6 dB
Puerta metálica en pared de ladrillo	12 dB
Cuerpo humano	3 dB

Cada sitio encuestado tiene diferentes niveles de distorsión de múltiples rutas, pérdidas de señal y ruido de señal. Los hospitales suelen ser el entorno más difícil de estudiar debido a la alta distorsión de múltiples rutas, las pérdidas de señal y el ruido de la señal. Los hospitales tardan más en realizar las encuestas, requieren una mayor cantidad de puntos de acceso y requieren estándares de rendimiento más altos. Las fábricas y las tiendas son las siguientes más difíciles de estudiar. Estos sitios suelen tener costado metálico y muchos objetos metálicos en el suelo, lo que da como resultado señales reflejadas que recrean la distorsión de múltiples rutas. Los edificios de oficinas y los lugares de acogida suelen tener una gran atenuación de la señal, pero un menor grado de distorsión de múltiples rutas.

Información Relacionada

- Implementación de Cisco 440X Series Cisco 440X Series que despliegan
- Diseño de red de referencia de soluciones
- Especificaciones del sistema de comunicaciones de Vocera
- Soporte Técnico y Documentación - Cisco Systems