

El despliegue del teléfono IP de Vocera en Cisco unificó la infraestructura de red inalámbrica

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Documento de síntesis](#)

[Descripción de la insignia de Vocera](#)

[Consideraciones de la capacidad de llamada de Vocera](#)

[Capacidad del servidor de las comunicaciones de Vocera](#)

[La solución de Vocera](#)

[Hojas de operación \(planning\) de la infraestructura de Vocera](#)

[Descripción general de la arquitectura](#)

[Multicast en un despliegue LWAPP](#)

[Método de entrega del Unicast-Multicast](#)

[Método de entrega del Multicast-Multicast](#)

[Configuración del Multicast del router y del conmutador](#)

[Encaminamiento del Multicast IP del permiso](#)

[Permiso PIM en un interfaz](#)

[Vigilancia del tráfico del VLA N IGMP del conmutador de la neutralización](#)

[Mejoras del Multicast en la versión 4.0.206.0 y más adelante](#)

[Escenarios de instrumentación](#)

[Solo despliegue del regulador](#)

[Despliegue de la capa 2 del controlador múltiple](#)

[Despliegue de la capa 3 del controlador múltiple](#)

[Implementaciones de VoWLAN: Recommendations de Cisco](#)

[Recomendaciones para los edificios, los hospitales, y los almacenes del Multi-suelo](#)

[Mecanismos de seguridad utilizados](#)

[Consideraciones del SALTO](#)

[Infraestructura de red inalámbrica](#)

[Voz, datos y VLA N de Vocera](#)

[Apresto de la red](#)

[Cambie las recomendaciones](#)

[Implementaciones y configuración](#)

[Configuración de la insignia](#)

[Tono AutoRF para su entorno](#)

[Configuración de la infraestructura de red inalámbrica](#)

[Cree los interfaces](#)

[Cree la interfaz de voz de Vocera](#)

[Configuración Tecnología inalámbrica-específica](#)

[Configuración de la red inalámbrica \(WLAN\)](#)

[Configure el detalle del Punto de acceso](#)

[Configure la radio 802.11b/g](#)

[Verificación de la Telefonía IP inalámbrica](#)

[Asociación, autenticación, y registro](#)

[Problemas de itinerancia comunes](#)

[La insignia pierde la conexión a la red o pierden al servicio de voz al vagar por](#)

[La insignia pierde la Calidad de voz mientras que vaga por](#)

[Problemas de audio](#)

[Audio unilateral](#)

[Audio picado o robótico](#)

[Registro y problemas de autenticación](#)

[Apéndice A](#)

[AP y colocación de la antena](#)

[Interferencia y distorsión de trayectoria múltiple](#)

[Atenuación de la 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: La ayuda para los Productos de Vocera se debe obtener directamente de los canales de la ayuda de Vocera. El Soporte técnico de Cisco no se entrena para utilizar los problemas Vocera-relacionados.

Esta guía es un suplemento al Guía de despliegue inalámbrico del regulador LAN de Cisco y dirige solamente los parámetros de la configuración que son determinados a los dispositivos de Vocera VoWLAN en una arquitectura ligera. Refiera a los [reguladores inalámbricos LAN de las Cisco 440X Series que despliegan](#) para más información.

[prerrequisitos](#)

[Requisitos](#)

Se asume que los programas de lectura son familiares con los términos y los conceptos presentados en la Telefonía IP SRND y el LAN SRND de Cisco de la Tecnología inalámbrica de Cisco.

Guía de diseño inalámbrica UC [=](#)

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns818/landing_wireless_uc.html

Comunicaciones unificadas SRND de Cisco basadas en el encargado 7.x de las Comunicaciones unificadas de Cisco ==

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 Técnicos Cisco](#) para obtener más información sobre las convenciones del documento.

Documento de síntesis

Esta tabla resume las cuatro funciones claves y cómo se comportan dentro de una red inalámbrica unificada Cisco.

	Solo regulador	Capa 2 del Regulador-a-regulador que vaga por	Capa 3 del Regulador-a-regulador que vaga por
Insignia-a-insignia	Ninguna configuración especial	Ninguna configuración especial	Ninguna configuración especial
Insignia-a-teléfono	Ninguna configuración especial	Ninguna configuración especial	Ninguna configuración especial
Insignia-a-difusión	Multicast del regulador del permiso	IGMP-vigilancia del tráfico del VLAN de Vocera de la neutralización del Multicast del regulador del permiso o 4.0.206.0 ejecutado o más adelante	4.0.206.0 o más adelante
Ubicación de la insignia	Ninguna configuración especial	Ninguna configuración especial	Ninguna configuración especial

Descripción de la insignia de Vocera

Las insignias de la comunicación no prohíben a portador la comunicación inmediata con ningún otro portador de la insignia también un seguimiento de la ubicación de la integración y de la insignia de la Central telefónica privada (PBX). La utilización de una red inalámbrica 802.11b/g requiere el uso del Multicast y la entrega del paquete de la unidifusión UDP con los requisitos limitados para el Calidad de Servicio (QoS) a partir de la versión de software del servidor de Vocera 3.1 (estructura 1081). Las capacidades del cifrado son 64/128 Wired Equivalent Privacy (WEP) del bit, Temporal Key Integrity Protocol (TKIP), el control de la Integridad del mensaje (MIC), y Protocolo de integridad de clave temporal de Cisco (CKIP) combinado con las capacidades de la autenticación Open, de la clave Acceso-Pre-compartida protegida Wi-Fi (WPA-PSK), del protocolo extensible authentication WPA-protegido (PEAP) y del protocolo lightweight extensible authentication (SALTO).

Con el empuje de un botón, el servidor de Vocera responde con `vocera`, que es un mensaje para publicar los comandos tales como **expediente, donde (soy) /is.. , llamada, juego, difusión, mensajes**, y así sucesivamente. El servidor de Vocera proporciona a los servicios y/o a la configuración de la llamada necesarios para completar la petición.

El sistema de comunicación capaz del 802.11b de Vocera hace uso de la compresión de la voz propietaria y del uso de un rango del puerto UDP. El software del sistema de Vocera se ejecuta en un Servidor Windows que maneje los perfiles de la configuración de la llamada, de la conexión de llamada y de usuario. Partnered con el software del reconocimiento del discurso y del espectrograma de la voz del matiz 8.5 para activar las comunicaciones por voz de la insignia. Vocera recomienda un servidor de las ventanas separadas para funcionar con el software de las soluciones de telefonía de Vocera para activar la Conectividad del Servicio telefónico sencillo antiguo (POTS) con las insignias.

Consideraciones de la capacidad de llamada de Vocera

Vea la sección del [apresto de la red de](#) este documento para otros detalles.

Capacidad del servidor de las comunicaciones de Vocera

Refiera a las [especificaciones de sistema de comunicaciones de Vocera](#) para más información sobre la matriz del apresto del servidor de Vocera.

La solución de Vocera

La insignia de Vocera utiliza el unicast y la salida del paquete de multidifusión para proporcionar a varias características fundamentales que compongan esta solución completa. Aquí están cuatro de las Funciones esenciales que confían en la entrega del paquete apropiada. También se proporciona una comprensión básica de cómo cada característica utiliza la red subyacente para la salida y las funciones.

- Insignia para badge las comunicaciones — Cuando un usuario de Vocera llama a otro usuario, la insignia primero entra en contacto con el servidor de Vocera, que mira para arriba la dirección IP de la insignia del calleo y entra en contacto con al usuario de la insignia para preguntar al usuario si él puede tomar una llamada. Si el calleo valida la llamada, el servidor

de Vocera notifica la insignia de llamada de la dirección IP de la insignia del calleo para poner la comunicación directa entre las insignias sin la intervención adicional del servidor. Toda la comunicación con el servidor de Vocera utiliza el codificador-decodificador de G.711 y toda la comunicación de la insignia-a-insignia utiliza un codificador-decodificador del propietario de Vocera.

- Comunicación de la telefonía de la insignia — Cuando un servidor de la telefonía de Vocera está instalado y disposición con una conexión a un PBX, un usuario puede suspender las Extensiones internas de las líneas telefónicas PBX o del exterior. Vocera permite que los usuarios hagan las llamadas o 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 la función en ese número (por ejemplo, farmacia, hogar, pizza) el servidor de Vocera determina el número que está siendo llamado, interceptando los números en la extensión o mirando el nombre para arriba en la base de datos y seleccionando el número. El servidor de Vocera entonces pasa esa información al servidor de la telefonía de Vocera que conecta con el PBX y genera la Señalización de telefonía apropiada (por ejemplo, DTMF). Toda la comunicación entre la insignia y el servidor de Vocera y el servidor de Vocera y el servidor de la telefonía de Vocera utiliza el codificador-decodificador de G.711 sobre el unicast UDP.
- Difusión de Vocera — Un usuario de la insignia de Vocera puede llamar y comunicar a un grupo de portadores de la insignia de Vocera al mismo tiempo usando el comando broadcast. Cuando un usuario difunde a un grupo, la insignia del usuario envía el comando al servidor de Vocera que entonces mira para arriba a los miembros de un grupo, determina qué miembros del grupo son activos, asigna un direccionamiento del Multicast para utilizar para esta sesión de la difusión, y envía un mensaje a la insignia de cada usuario activo que lo da instrucciones para unirse a al grupo de multidifusión con el direccionamiento asignado del Multicast.
- Función de la ubicación de la insignia — El servidor de Vocera no pierde de vista el Punto de acceso al cual se asocia cada insignia activa mientras que cada insignia envía una segundo señal de mantenimiento 30 al servidor con el BSSID asociado. Esto permite que el sistema de Vocera estime áspero la ubicación de un usuario de la insignia. Esta función tiene un grado de precisión relativamente bajo porque una insignia no se pudo asociar al Punto de acceso al cual está la más cercana.

[Hojas de operación \(planning\) de la infraestructura de Vocera](#)

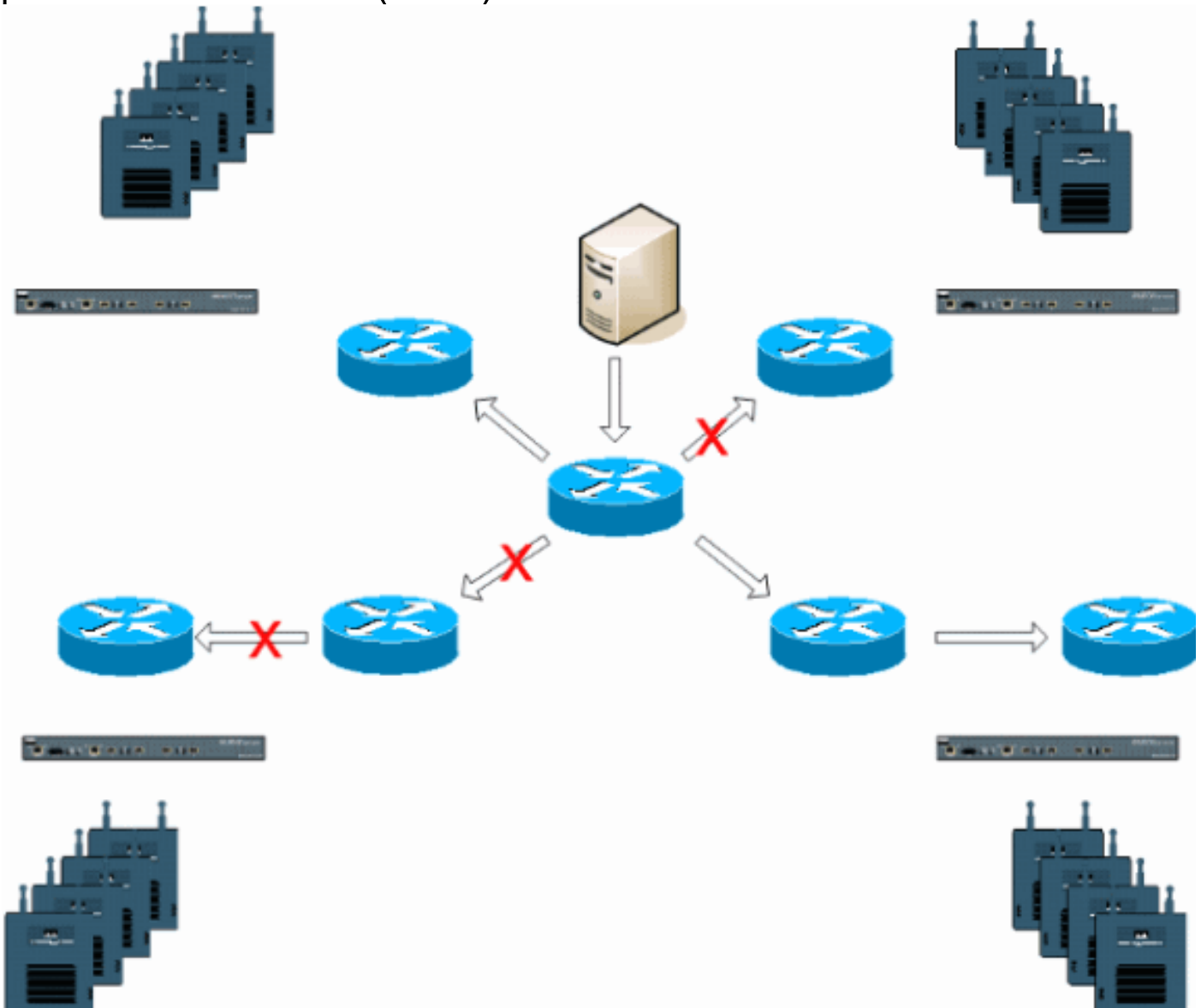
[El Guía de planificación de la infraestructura de Vocera del](#) whitepaper de Vocera , describe los requerimientos mínimos del estudio sobre el sitio que muestran que la insignia debe tener un mínimo de la potencia de la señal de la recepción del dBm -65, de una mayor separación DB de 25 del relación señal-ruido y de la coincidencia y de canal de la punta de acceso adecuado.

[Aunque las insignias utilicen una antena direccional similar del omni como cuaderno que se utilice para un estudio sobre el sitio, no imita el comportamiento de la insignia muy bien, dado las influencias de los portadores en la potencia de la señal. Dado este requerimiento único y este comportamiento del dispositivo que transmite, el uso de la arquitectura Cisco y la administración de recursos de la radio es ideales para asegurarse de que hay una falta de características inusuales del sitio del Radiofrecuencia \(RF\).](#)

La insignia de Vocera es un dispositivo accionado del punto bajo, desgastado al lado del cuerpo con las capacidades limitadas de la corrección de error de la señal. Los requisitos de Vocera en este documento pueden ser alcanzados fácilmente. Sin embargo, puede abrumarse si hay demasiados SSID para que procese y permita que la insignia trabaje eficazmente.

Descripción general de la arquitectura

Cuadro 1 — Multidifusión general delantera y pasa con la Tecnología inalámbrica ligera del protocolo del Punto de acceso (LWAPP)



Multicast en un despliegue LWAPP

La comprensión del Multicast dentro de un despliegue LWAPP es necesaria desplegar la función de la difusión de Vocera. Este documento cubre más adelante los pasos esenciales para activar el Multicast dentro de la solución regulador-basada. Hay actualmente dos métodos de entrega que el regulador LWAPP utiliza para entregar el Multicast a los clientes:

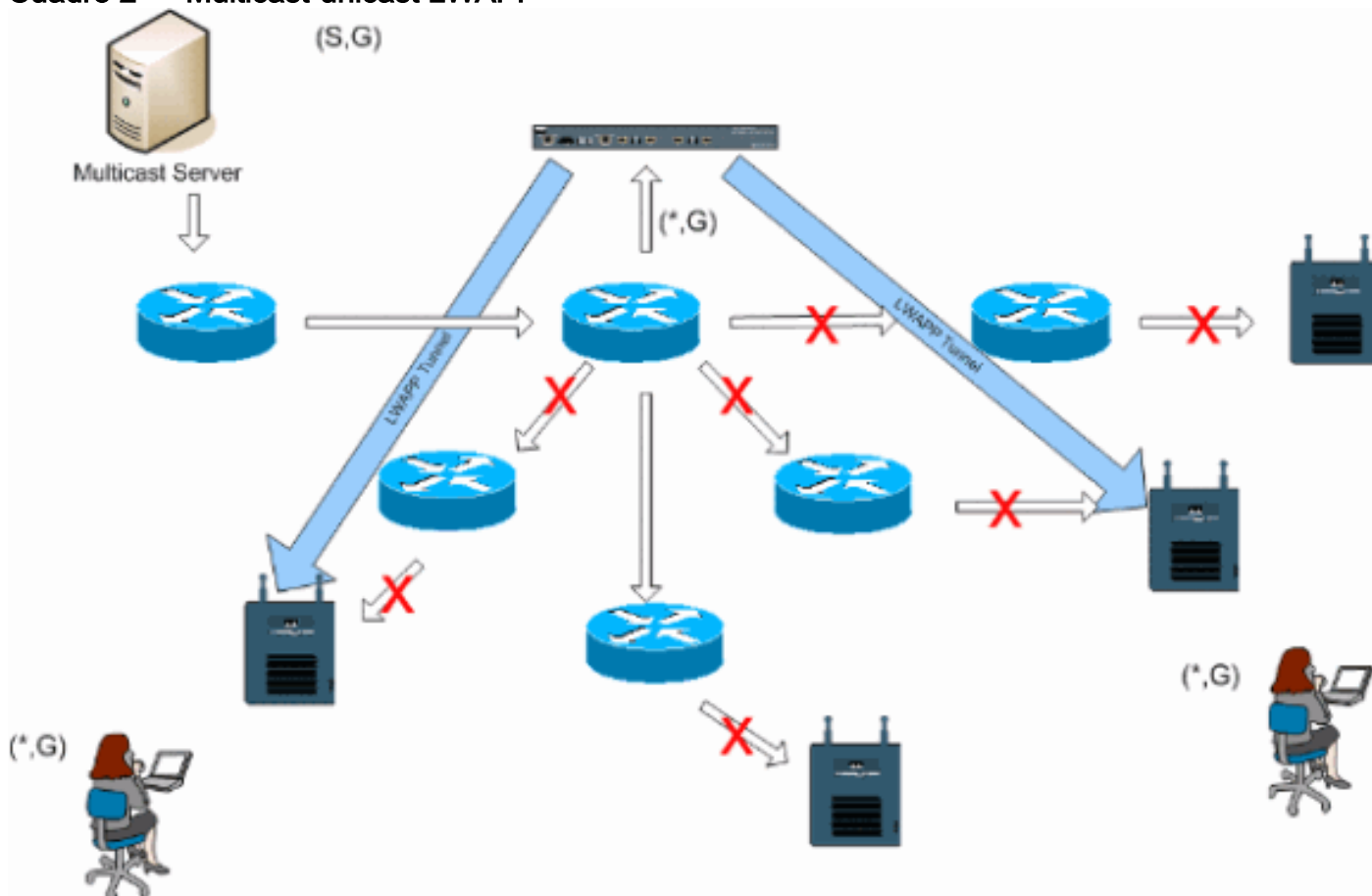
- [Unicast-Multicast](#)
- [Multicast-Multicast](#)

Método de entrega del Unicast-Multicast

El método de entrega del unicast-Multicast crea una copia de cada paquete de multidifusión y adelante él a cada acceso-punta. Cuando un cliente envía un Multicast únase a al LAN de la Tecnología inalámbrica, el Punto de acceso adelante que esto se une a través del túnel LWAPP

al regulador. El regulador puentea este Multicast se une a sobre él es directamente la conexión de red de área local conectada que es el VLA N del valor por defecto para la red inalámbrica (WLAN) asociada del cliente. Cuando un paquete del Multicast IP llega de la red al regulador, el regulador replica este paquete con una encabezado LWAPP para cada Punto de acceso que tenga un cliente dentro del dominio de red inalámbrica que se ha unido a este grupo específico. Cuando la fuente del Multicast es también un receptor dentro del dominio de red inalámbrica, este paquete también se duplica y se remite de nuevo al mismo cliente que envió este paquete. Para las insignias de Vocera, éste no es el método preferido de salida del Multicast dentro de la solución del regulador LWAPP. El método de entrega del unicast trabaja con las pequeñas implementaciones. Sin embargo, debido a los considerables gastos indirectos en el regulador LAN de la Tecnología inalámbrica (WLC), éste nunca es el método de entrega recomendado del Multicast.

Cuadro 2 — Multicast-unicast LWAPP



Nota: Si se configuran los VLA N del grupo AP, y un IGMP se une a se envía de un cliente a través del regulador, se coloca en el VLA N del valor por defecto de la red inalámbrica (WLAN) que el cliente está encendido. Por lo tanto, el cliente no pudo recibir este tráfico Multicast a menos que el cliente sea un miembro de este dominio de broadcast del valor por defecto.

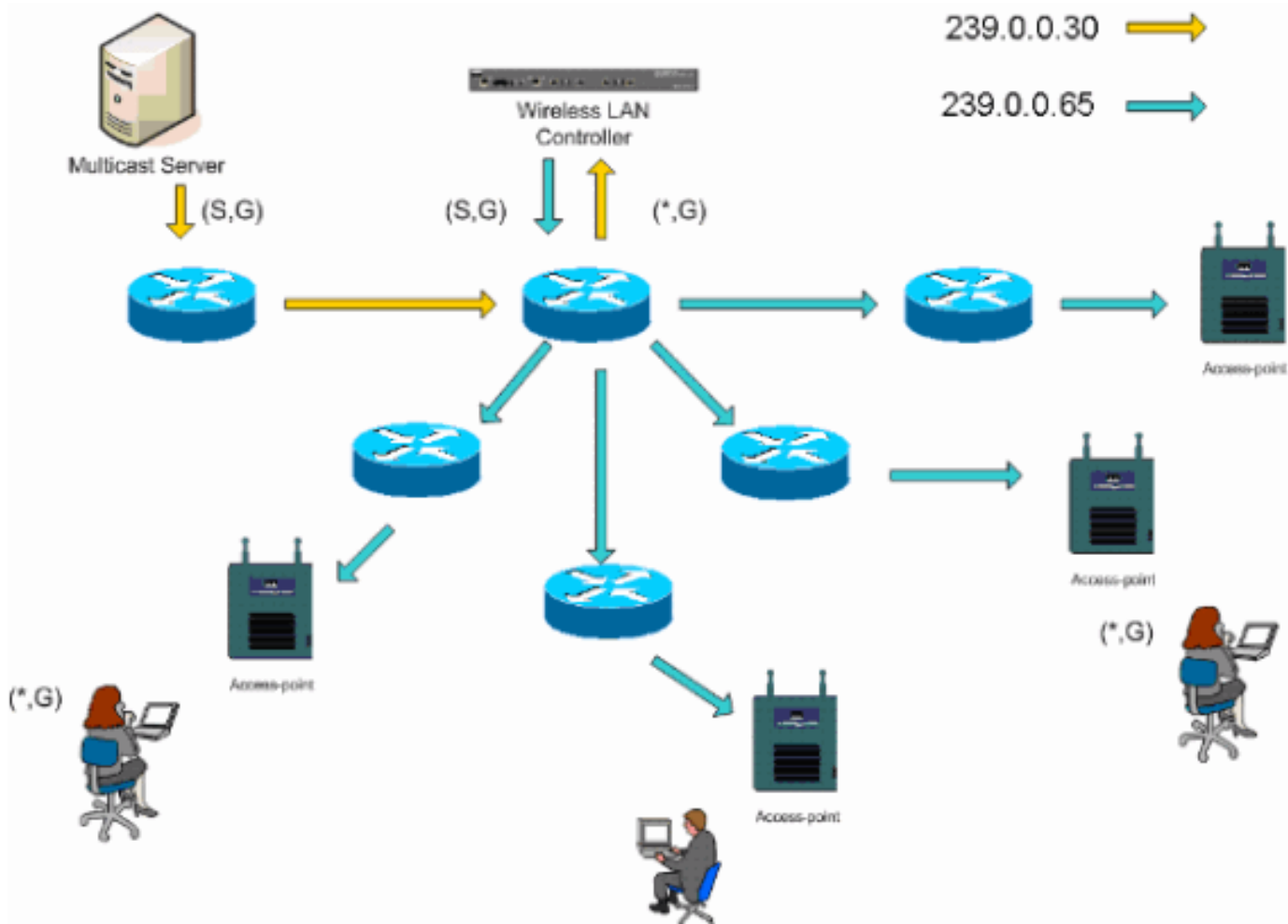
Método de entrega del Multicast-Multicast

El método de entrega del Multicast-Multicast no requiere al regulador replicar cada paquete de multidifusión recibido. El regulador se configura para una dirección de grupo de multidifusión inusitada que siente bien cada Punto de acceso a un miembro de. Con el cuadro 3, el grupo de multidifusión definido del WLC al Punto de acceso es 239.0.0.65. Cuando un cliente envía un Multicast únase a la red inalámbrica (WLAN), el Punto de acceso adelante que esto se une a través del túnel LWAPP al regulador. El regulador adelante este protocolo de la capa del link sobre él es directamente la conexión de red de área local conectada que es el VLA N del valor por

defecto para la red inalámbrica (WLAN) asociada del cliente. El router que es local al regulador después agrega a esta dirección de grupo de multidifusión a ese interfaz para remitir ((*, G)) entrada. Con el cuadro 3, el Multicast del ejemplo se une a fue enviado al grupo de multidifusión 239.0.0.30. Cuando de la red el tráfico Multicast ahora adelante, el direccionamiento del Multicast de 239.0.0.30 se remite al regulador. El regulador entonces encapsula el paquete de multidifusión en un paquete de multidifusión LWAPP dirigido a la dirección de grupo de multidifusión (el ejemplo aquí es 239.0.0.65) que se configura en el regulador y se remite a la red. Cada Punto de acceso en el regulador recibe este paquete como miembro del grupo de multidifusión de los reguladores. El Punto de acceso entonces adelante los clientes/el paquete de multidifusión de los servidores (el ejemplo aquí es 239.0.0.30) como difusión al WLAN/SSID identificado dentro del paquete de multidifusión LWAPP.

Nota: Si usted configura incorrectamente su red de multidifusión, usted podría terminar para arriba la recepción de los paquetes de multidifusión del Punto de acceso de otro regulador. Si el primer regulador tiene que hacer fragmentos de este paquete de multidifusión, el fragmento se remite a la red y cada Punto de acceso debe pasar el tiempo para caer este fragmento. Si usted permite todo el tráfico tal como cualquier cosa del rango del Multicast 224.0.0.x, esto también es encapsulada y remitida posteriormente por cada Punto de acceso.

Cuadro 3 — Multicast-Multicast LWAPP



[Configuración del Multicast del router y del conmutador](#)

Este documento no es una guía de configuración del Multicast de la red. Refiera a [configurar el Multicast IP que encamina](#) para una historia completa de la puesta en práctica. Este documentos abarca los fundamentos para activar el Multicast dentro de su entorno de red.

Encaminamiento del Multicast IP del permiso

El encaminamiento del Multicast IP permite que el software de Cisco IOS® remita los paquetes de multidifusión. Requieren al **comando ip multicast-routing global configuration** permitir que el Multicast funcione en cualquier red activada Multicast. El **comando ip multicast-routing** debe ser activado en todo el Routers dentro de su red entre el WLC y sus Puntos de acceso respectivos.

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

Permiso PIM en un interfaz

Esto activa el interfaz de la encaminamiento para la operación del Internet Group Management Protocol (IGMP). El modo de la multidifusión independiente de protocolo (PIM) determina cómo el router puebla su tabla de encaminamiento del Multicast. El ejemplo proporcionado aquí no requiere el (RP) del punto de encuentro ser sabido para el grupo de multidifusión y por lo tanto el escaso-denso-MODE es el más deseable dado la naturaleza desconocida de su entorno del Multicast. Esto no es una recomendación del Multicast de ser configurado para trabajar aunque el interfaz de la capa 3 conectado directamente con su regulador deba ser PIM activado para que funcione el Multicast. Todos los interfaces entre su WLC y sus Puntos de acceso respectivos deben ser activados.

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

Vigilancia del tráfico del VLA N IGMP del conmutador de la neutralización

La vigilancia del tráfico IGMP permite una red de switch con el Multicast activado limitar el tráfico a esos switchports que tengan los usuarios que quisieran que el Multicast fuera visto mientras que poda los paquetes de multidifusión de los switchports que no desean ver la secuencia de multidifusión. En un despliegue de Vocera, puede ser indeseable activar la vigilancia del tráfico CGMP o IGMP en el switchport por aguas arriba al regulador con las versiones de software anterior que 4.0.206.0.

La itinerancia y el Multicast no se definen con un conjunto de los requisitos de verificar que el tráfico Multicast puede seguir a un usuario suscrito. Aunque la insignia del cliente sea consciente que ha vagado por, no remite otro IGMP se une a para asegurarse de que la infraestructura de red continúa entregando el tráfico del Multicast (difusión de Vocera) a la insignia. Al mismo tiempo, el Punto de acceso LWAPP no envía una interrogación de la multidifusión general al cliente vagado por para incitar para este IGMP se une a. Con un diseño de red de Vocera de la capa 2, inhabilitar la vigilancia del tráfico IGMP permite que el tráfico sea remitido a todos los miembros de la red de Vocera no importa dónde vagan por. Esto se asegura de que la característica de la difusión de Vocera trabaje con independencia de donde el cliente vaga por. Inhabilitar la vigilancia del tráfico IGMP global es una tarea muy indeseable. Se recomienda que la vigilancia del tráfico IGMP solamente esté inhabilitada en el VLA N de Vocera que está conectado directamente con cada WLC.

Refiera a [configurar la vigilancia del tráfico IGMP](#) para más información.

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

Mejoras del Multicast en la versión 4.0.206.0 y más adelante

Con la versión de 4.0.206.0, Cisco introduce una interrogación IGMP para permitir que los usuarios vaguen por en la capa 2 enviando una interrogación general IGMP cuando ocurre éste. El cliente entonces responde con el grupo IGMP que son un miembro de y esto está puenteada a la red alámbrica según lo descrito anterior en este documento. Cuando un cliente vaga por a un regulador que no tenga Conectividad de la capa 2, o una capa 3 vaga por, la encaminamiento síncrona se agrega para los paquetes del origen de multidifusión. Cuando un cliente, que ha completado una capa 3 vaga por las fuentes un paquete de multidifusión de la red inalámbrica, el regulador no nativo encapsula este paquete en los Ethernetes sobre IP (EoIP) en el túnel IP al regulador del ancla. El regulador del ancla entonces adelante que a los clientes de red inalámbrica localmente asoció así como puentea esto de nuevo a la red alámbrica en donde se encamina usando los métodos de ruteo normales del Multicast.

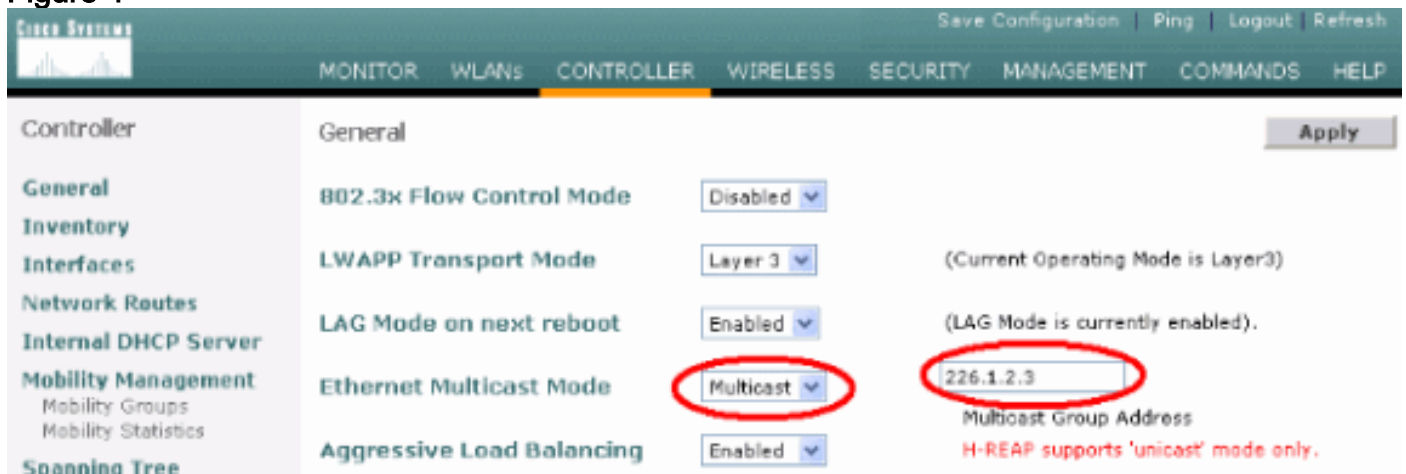
Escenarios de instrumentación

Estos tres escenarios de instrumentación cubren las mejores prácticas y los parámetros de diseño a ayudar con un Vocera acertado Badge el despliegue:

- [Solo despliegue del regulador](#)
- [Despliegue de la capa 2 del controlador múltiple](#)
- [Despliegue de la capa 3 del controlador múltiple](#)

Entendiendo cómo las características de la insignia de Vocera interactivas dentro de un entorno partido LWAPP MAC son esenciales. Con todos los escenarios de instrumentación, el Multicast debe ser activado y el Equilibrio de carga agresivo debe ser inhabilitado. Todas las redes inalámbricas (WLAN) de la insignia se deben contener dentro del mismo dominio de broadcast a través de su toda la red.

Figure 4



The screenshot shows the Cisco Systems Controller configuration interface. The 'CONTROLLER' tab is selected, and the 'General' configuration page is displayed. The 'Ethernet Multicast Mode' is set to 'Multicast', and the 'Multicast Group Address' is set to '226.1.2.3'. Both the dropdown menu for 'Ethernet Multicast Mode' and the text input field for 'Multicast Group Address' are circled in red. Other settings include 'B02.3x Flow Control Mode' set to 'Disabled', 'LWAPP Transport Mode' set to 'Layer 3', 'LAG Mode on next reboot' set to 'Enabled', and 'Aggressive Load Balancing' set to 'Enabled'. A red warning message at the bottom states: 'H-REAP supports 'unicast' mode only.'

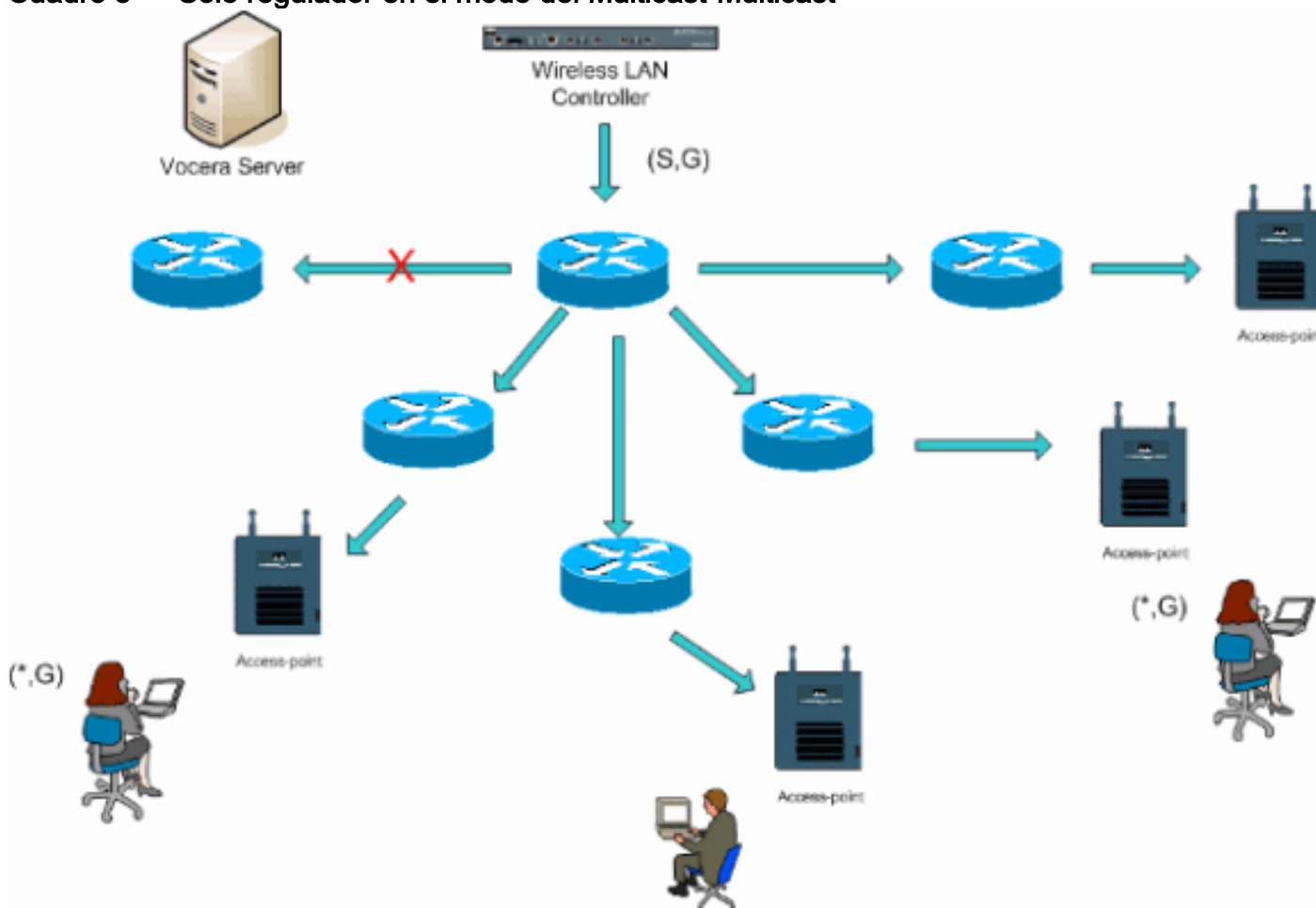
Solo despliegue del regulador

Éste es el escenario de instrumentación más directo. Permite que usted despliegue la solución de la insignia de Vocera con pocas preocupaciones del despliegue. Su red se debe activar para el Multicast IP que encamina para permitir solamente que los Puntos de acceso reciban los paquetes de multidifusión LWAPP. Si procede, usted puede limitar la complejidad del Multicast de la red configurando todo el Routers y Switches con el grupo de multidifusión de los reguladores.

Con el Multicast configurado global en el regulador, el SSID apropiado, los ajustes de seguridad, y todos los Puntos de acceso registraron la solución de la insignia de Vocera y todas sus funciones actúan como se esperaba. Con la función de la difusión de Vocera, un usuario vaga por y el tráfico Multicast sigue como se esperaba. No hay Configuraciones extra requeridas ser configurado para permitir que esta solución funcione correctamente.

Cuando una insignia de Vocera envía un mensaje de multidifusión, como hace con la difusión de Vocera, se remite al regulador. El regulador entonces encapsula este paquete de multidifusión dentro de un paquete de multidifusión LWAPP. La infraestructura de red adelante este paquete a cada Punto de acceso que está conectado con este regulador. Cuando el Punto de acceso recibe este paquete, entonces mira la encabezado del Multicast LWAPP para determinar qué WLAN/SSID entonces difunde este paquete.

Cuadro 5 — Solo regulador en el modo del Multicast-Multicast



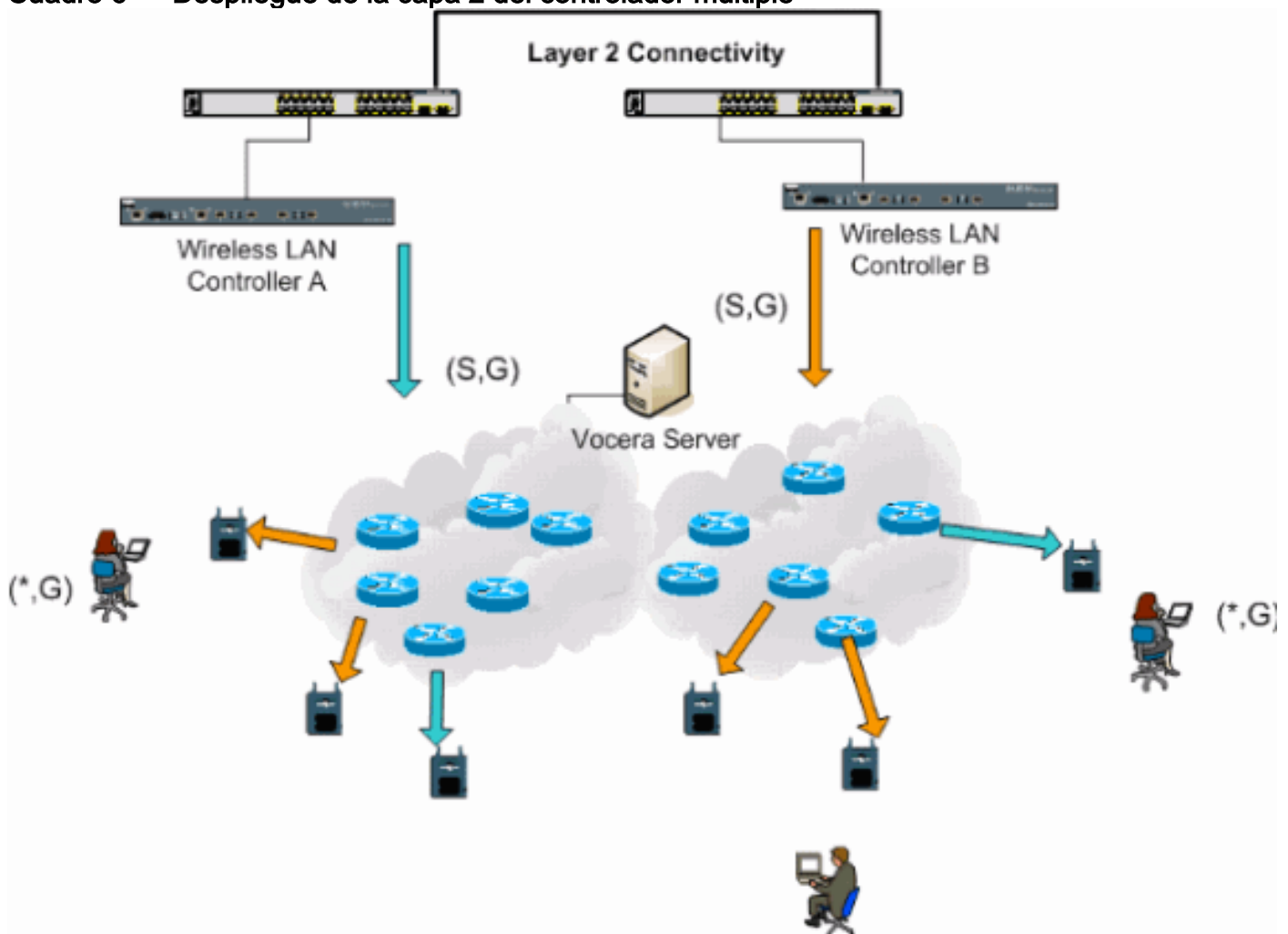
Despliegue de la capa 2 del controlador múltiple

Los controladores múltiples deben todos tener Conectividad el uno al otro vía el mismo dominio de broadcast de la capa 2. Ambos reguladores se configuran para el Multicast como se muestra, usando los grupos de multidifusión idénticos del Punto de acceso en cada regulador para limitar la fragmentación. Con la suposición que este dominio de broadcast de la capa 2 está conectado vía un conmutador común o un conjunto común de Switches, la vigilancia del tráfico CGMP/IGMP en este Switches se debe inhabilitar para este solo VLA N o funcionamiento 4.0.206.0 o software WLC posterior. Con la función de la difusión de Vocera y un usuario vague por de un Punto de acceso en un regulador a un Punto de acceso en un diverso regulador, allí no es ningún mecanismo para IGMP se une a para ser remitido al nuevo puerto de la capa 2 para que la vigilancia del tráfico IGMP trabaje. Sin un paquete IGMP que alcanza el conmutador capaz por aguas arriba CGMP o IGMP, no remiten al regulador y por lo tanto no son recibido el grupo de

multidifusión especificado por el cliente. Esto pudo trabajar en algunos casos, si un cliente que es parte del mismo grupo de la difusión de Vocera ha enviado ya este paquete IGMP antes de que el cliente de itinerancia vague por sobre el nuevo regulador con las ventajas de la versión 4.0.206.0, un cliente que vaga por a otro regulador mientras que una capa 2 vaga por recibe una interrogación general IGMP inmediatamente después de la autenticación. El cliente debe entonces responder con los grupos interesados y el nuevo regulador entonces se puentea esto localmente al switch conectado. Esto permite las ventajas de IGMP y de CGMP en su Switches por aguas arriba.

Usted puede crear la insignia adicional SSID y acodar 2 dominios para las redes separadas de la insignia mientras su red se configure para pasar el tráfico Multicast apropiadamente. También, cada dominio de broadcast de la capa 2 de Vocera creado debe existir por todas partes un regulador está conectado con la red para no romper el Multicast.

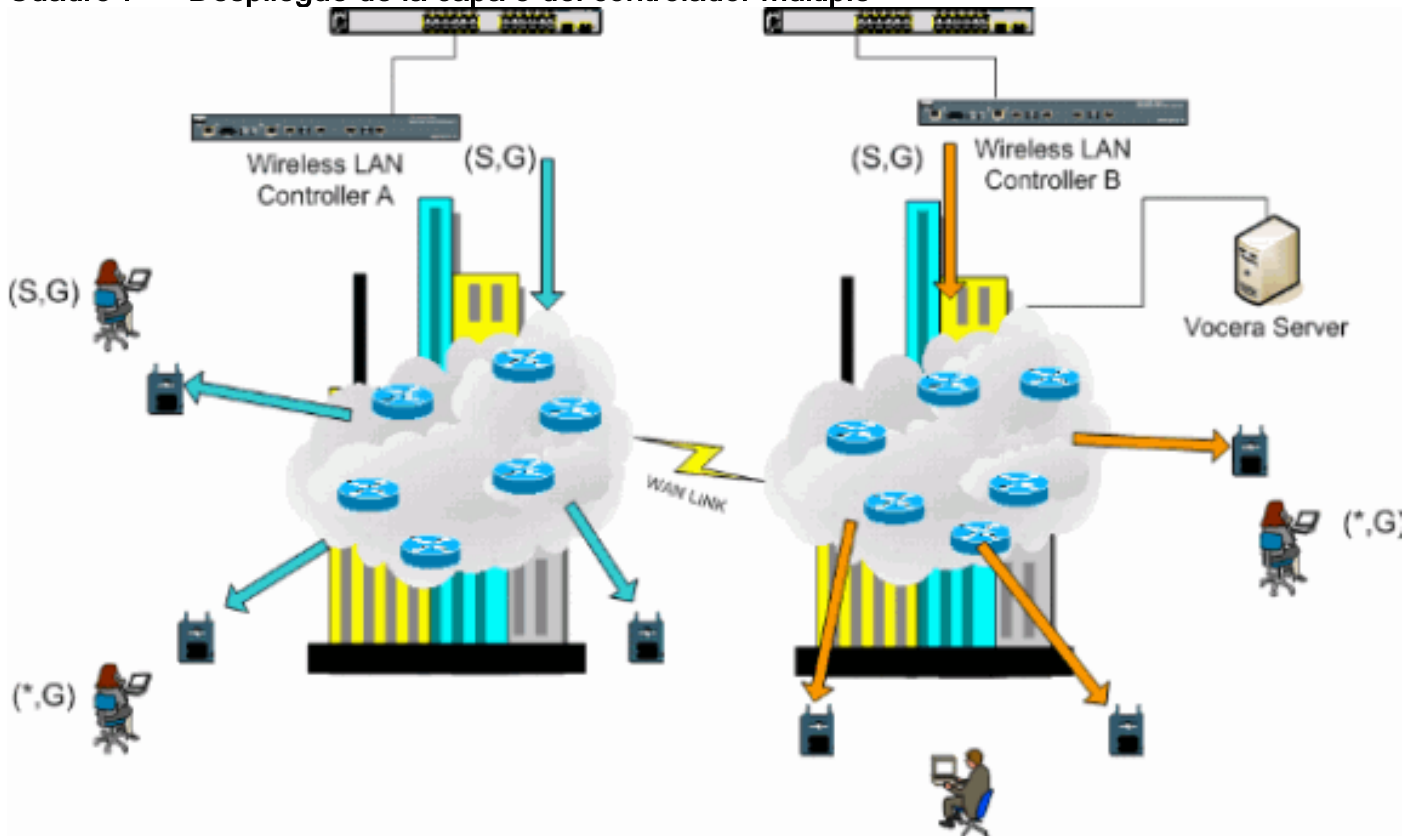
Cuadro 6 — Despliegue de la capa 2 del controlador múltiple



Despliegue de la capa 3 del controlador múltiple

La Estrategia de implementación de itinerancia de la capa 3 debe ser utilizada solamente con el regulador-a-regulador que vaga por con versión de software WLC 4.0.206.0 o más adelante. Si preguntan a un cliente que ha estado conectado con el grupo de la difusión de Vocera y recibe la secuencia de multidifusión apropiada y vaga por a otro regulador mientras que una capa 3 vaga por con la itinerancia de la capa 3 LWAPP configurada, él para los grupos de multidifusión interesados. El cliente, cuando compra de componentes al mismo grupo de la difusión de Vocera, tiene estos paquetes entregados al regulador del ancla a través del túnel de EoIP y tiene estos paquetes encaminados con los métodos de ruteo normales del Multicast.

Cuadro 7 — Despliegue de la capa 3 del controlador múltiple



Implementaciones de VoWLAN: Recommendations de Cisco

Las redes de la Telefonía IP inalámbrica requieren las hojas de operación (planning) cuidadosas RF. Un estudio sobre el sitio completo de la Voz se requiere a menudo para determinar los niveles apropiados de cobertura de red inalámbrica y para identificar las fuentes de interferencia. Las opciones de la colocación y de la selección de antena del Punto de acceso se pueden facilitar grandemente con la ayuda de los resultados de un estudio sobre el sitio válido de la Voz. La consideración más importante es la potencia de transmisión del teléfono inalámbrico. El teléfono aprende idealmente la potencia de transmisión del Punto de acceso y ajusta su potencia de transmisión a la del Punto de acceso.

Aunque despliegan a la mayoría de las redes inalámbricas hoy después de un estudio sobre el sitio extenso RF, se hacen con tener el servicio de datos presente también. Los teléfonos de VoWLAN son probables tener diversas características de itinerancia y diversos requisitos de la cobertura que los de un adaptador típico de la red inalámbrica (WLAN) para un cliente móvil tal como una computadora portátil. Por lo tanto, un estudio sobre el sitio adicional para la Voz se recomienda a menudo para prepararse para los requisitos de rendimiento de los clientes múltiples de VoWLAN. Esta encuesta adicional da la oportunidad de adaptar los Puntos de acceso para asegurarse de que los teléfonos de VoWLAN tienen bastante cobertura y ancho de banda RF para proporcionar a la Calidad de voz apropiada.

Para más información sobre los aspectos del diseño RF, refiera al capítulo en los aspectos del diseño del Radiofrecuencia (RF) de la red inalámbrica (WLAN) en la guía de diseño inalámbrica LAN de Cisco, disponible en <http://cisco.com/go/srnd>.

Recomendaciones para los edificios, los hospitales, y los almacenes del Multi-suelo

Considere los factores enumerados en esta sección cuando usted examina los edificios, los

hospitales, y los almacenes del multi-suelo.

Métodos y materiales de la construcción

Muchos aspectos de la construcción de edificios son desconocidos u ocultados del estudio sobre el sitio, así que usted puede ser que tenga que adquirir esa información de otras fuentes (tales como gráficos arquitectónicos). Algunos ejemplos de los métodos y materiales típicos de la construcción que afectan al rango y la área de cobertura de los Puntos de acceso incluye la película metálica en el vidrio de la ventana, vidrio plomado, las paredes acero-tachonadas, los suelos del cemento y las paredes con el refuerzo de acero, aislante hoja-apoyado, las escaleras y los ejes de elevador, sondeando los tubos y las bases, y muchos otros.

Inventario

Los diversos tipos de inventario pueden afectar al rango RF, determinado a éstos con el alto acero o al contenido de agua. Algunos items a mirar para incluyen las cajas de cartón, alimento para animales, pintura, los productos petrolíferos, las piezas del motor, y así sucesivamente.

Niveles de inventario

Asegúrese de le para realizar un estudio sobre el sitio en los niveles de inventario máximos o en tiempos de la actividad más alta. Un almacén en un nivel de media del 50% tiene una huella muy diversa RF que el mismo almacén en un nivel de inventario del 100%.

Niveles de actividad

Semejantemente, un área de la oficina después de las horas (sin la gente) tiene una diversa huella RF que la misma área por completo de la gente durante el día. Aunque muchas partes del estudio sobre el sitio puedan ser dirigidas sin el empleo completo, es esencial conducir la verificación del estudio sobre el sitio y pellizcar los valores de la clave durante una época en que se ocupa la ubicación. Cuanto más altos son los requisitos de la utilización y la densidad de los usuarios, más importante es tener una solución bien diseñada de la diversidad. Cuando más usuarios están presentes, más señales se reciben en el dispositivo de cada usuario. Las señales adicionales causan más contención, más puntos nulos, y una distorsión más de trayectoria múltiple. La diversidad en las ayudas del Punto de acceso (Antenas) minimiza estas condiciones.

Edificios del Multi-suelo

Tenga presente estas guías de consulta cuando usted conduce un estudio sobre el sitio para un edificio de oficinas típico:

- Los ejes de elevador bloquean y reflejan las señales RF.
- Los cuartos de la fuente con el inventario absorben las señales.
- Las oficinas interiores con las paredes duras absorben las señales RF.
- Los cuartos de la rotura (cocinas) pueden producir 2.4 gigahertz de interferencia con el uso de los hornos de microondas.
- Los laboratorios de prueba pueden producir 2.4 gigahertz o 5 gigahertz de interferencia, creando la distorsión de trayectoria múltiple y las sombras RF.
- Los cubículos tienden a absorber y las señales de bloque.

- Las salas de conferencia requieren la alta cobertura del Punto de acceso porque son áreas de la utilización intensa.

La precaución adicional debe ser administrada cuando usted examina los recursos del multi-suelo. Los Puntos de acceso en diversos suelos pueden interferir con uno a tan fácilmente como los Puntos de acceso situados en el mismo suelo. Es posible utilizar este comportamiento a su ventaja durante una encuesta. Usando las Antenas del alto-aumento, puede ser que sea posible penetrar los suelos y los techos y proporcionar a la cobertura a los suelos sobre así como debajo del suelo donde se monta el Punto de acceso. Tenga cuidado de no solapar los canales entre los Puntos de acceso en diversos suelos o los Puntos de acceso en el mismo suelo. En los edificios del multi-arrendatario, pudo haber los problemas de seguridad que requieren el uso de energías de transmisión más bajas y más bajo ganan las Antenas para guardar las señales fuera de las oficinas vecinas.

Hospitales

El proceso de la encuesta para un hospital es mucho el lo mismo que ése para una empresa, pero la disposición de un recurso del hospital tiende a diferenciar de estas maneras:

- Los edificios del hospital tienden a pasar a través de muchos proyectos y adiciones de la reconstrucción. Cada construcción adicional es probable tener diversos materiales de construcción con diversos niveles de atenuación.
- La penetración de la señal a través de las paredes y de los suelos en las áreas pacientes es típicamente mínima, que las ayudas crean las micro-células y las variaciones de trayectoria múltiple.
- La necesidad del ancho de banda aumenta con el uso cada vez mayor del equipo del ultrasonido de la red inalámbrica (WLAN) y de otras aplicaciones portátiles de la proyección de imagen. La necesidad de los aumentos del ancho de banda con la adición de la Voz inalámbrica también.
- Las células de la atención sanitaria son pequeñas, y la itinerancia inconsútil es esencial, especialmente con las Aplicaciones de voz.
- La coincidencia de la célula puede ser alta, y así que puede canalizar la reutilización.
- Los hospitales pueden tener varios tipos de redes inalámbricas instaladas. Esto incluye 2.4 gigahertz del equipo non-802.11. Este equipo puede causar la contención con otras redes 2.4 gigahertz.
- Las Antenas montadas en la pared de la corrección de la diversidad y las Antenas omnidireccionales techo-montadas de la diversidad son populares, pero tienen presente que la diversidad está requerida.

Almacenes

Los almacenes tienen áreas abiertas grandes que contengan a menudo los altos estantes del almacenamiento. Muchas veces, estos estantes casi alcanzan al techo, donde los Puntos de acceso se ponen típicamente. Tales estantes del almacenamiento pueden limitar el área que el Punto de acceso puede cubrir. En estos casos, considere poner los Puntos de acceso en otras ubicaciones además del techo, tal como paredes laterales y pilares del cemento. También considere estos factores cuando usted examina un almacén:

- Los niveles de inventario afectan a los números de punto de acceso necesarios. Pruebe la cobertura con dos o tres Puntos de acceso en las ubicaciones estimadas de la colocación.

- Las coincidencias inesperadas de la célula son probables debido a las variaciones de trayectoria múltiple. La calidad de la señal varía más que la fuerza de esa señal. Los clientes pudieron asociarse y actuar mejor con los Puntos de acceso más lejos lejos que con los Puntos de acceso próximos.
- Durante una encuesta, los Puntos de acceso y las Antenas no tienen generalmente un Cable de antena que los conecta. Pero en un entorno de producción, el Punto de acceso y la antena pudieron requerir los Cables de antena. Todos los Cables de antena introducen la pérdida de la señal. La encuesta más exacta incluye el tipo de antena que se instalará y la longitud del cable que se instalará. Una buena herramienta a utilizar para simular el cable y su pérdida es un atenuador en un equipo de la encuesta.

Examinar una instalación de fabricación es similar a examinar un almacén, salvo que pudo haber muchas más fuentes de interferencia RF en una instalación de fabricación. Además, las aplicaciones en una instalación de fabricación requieren generalmente más ancho de banda que los de un almacén. Estas aplicaciones pueden incluir la proyección de imagen video y la Voz inalámbrica. La distorsión de trayectoria múltiple es probable ser el problema de rendimiento más grande de una instalación de fabricación.

Mecanismos de seguridad utilizados

Además del WEP estático y del SALTO de Cisco para la autenticación y la encriptación de datos, las insignias de Vocera también utilizan WPA-PEAP (MS-CHAP v2)/WPA2-PSK.

Consideraciones del SALTO

El SALTO permite que los dispositivos sean autenticados mutuamente (punta del insignia-a-acceso y punta-a-insignia del acceso) basó en un Nombre de usuario y una contraseña. Sobre la autenticación, una clave dinámica se utiliza entre el teléfono y el Punto de acceso para cifrar el tráfico. Sin embargo, el ataque de diccionario ASLEAP debe ser considerado cuando usted decide utilizar el SALTO como su solución de la Seguridad:

Refiera al [ataque de diccionario en la vulnerabilidad del SALTO de Cisco](#) para más información.

Si se utiliza el SALTO, requieren a un servidor de RADIUS Salto-obediente, tal como el servidor del control de acceso de Cisco (ACS), proporcionar al acceso a la base de datos de usuarios. Cisco ACS puede o salvar el Nombre de usuario y la base de datos de contraseñas localmente, o puede tener acceso a esa información de un directorio externo de Microsoft Windows NT. Al usar el SALTO, asegúrese de que las contraseñas fuertes están utilizadas en todos los dispositivos de red inalámbrica. Las contraseñas fuertes se definen como estar entre 10 y 12 caracteres de largo y pueden incluir el mayúscula y los caracteres en minúscula así como los caracteres especiales.

Porque todas las insignias utilizan la misma contraseña y se salva dentro de la insignia, Cisco recomienda que usted utiliza los diversos Nombres de usuario y contraseñas en los clientes de los datos y los clientes inalámbricos de la Voz. Esta práctica ayuda con el seguimiento y resolver problemas así como la Seguridad. Aunque sea una opción de configuración válida para utilizar una base de datos externa (del off-ACS) para salvar los Nombres de usuario y las contraseñas para las insignias, Cisco no recomienda esta práctica. Porque el ACS debe ser preguntado siempre que la insignia vague por entre los Puntos de acceso, el retraso imprevisible para tener acceso a una base de datos del off-ACS podría causar el Retraso excesivo y la calidad de voz deficiente.

Infraestructura de red inalámbrica

La red de la Telefonía IP inalámbrica, apenas como una red de telefonía IP atada con alambre, requiere las hojas de operación (planning) cuidadosas para la configuración del VLA N, el apresto de la red, el transporte del Multicast, y las opciones del equipo. Para las redes atada con alambre y de la Telefonía IP inalámbrica, separe la Voz y los VLA N de los datos son a menudo la mayoría del modo eficaz de despliegue sugerido de asegurar el suficientes ancho de banda de la red y facilidad del troubleshooting.

Voz, datos y VLA N de Vocera

Los VLA N proporcionan a un mecanismo para dividir las redes en segmentos en uno o más dominios de broadcast. Los VLA N son especialmente importantes para las redes de telefonía IP, donde está separar la recomendación típica el tráfico de voz y de datos en diversos dominios de la capa 2. Cisco recomienda que usted configura los VLAN distintos para las insignias de Vocera del otro tráfico de voz y de datos: un VLA N nativo para el tráfico de administración del Punto de acceso, el VLA N de los datos para el tráfico de datos, una Voz o un VLA N auxiliar para el tráfico de voz, y un VLA N para el Vocera Badges. Un VLA N separado de la Voz permite a la red aprovecharse de la marca de la capa 2 y proporciona a la cola prioritaria en el puerto del switch de acceso de la capa 2. Esto se asegura de que QoS apropiado esté proporcionado para las diversas clases de tráfico y ayuda a resolver abordar los problemas tales como dirección IP, Seguridad, y dimensionalización de la red. Las insignias de Vocera utilizan una característica de la difusión que utilice el Multicast para entregar. Este VLA N común se asegura de que cuando una insignia vaga por entre los reguladores, siga siendo parte del grupo de multidifusión. Este último proceso se discute detalladamente cuando el Multicast se dirige más adelante en este documento.

Apresto de la red

El apresto de la red de telefonía IP es esencial asegurarse de que el ancho de banda adecuado y los recursos están disponibles cubrir las demandas presentadas por la presencia de tráfico de voz. Además de las guías de consulta de diseño de telefonía IP usuales para los componentes de clasificación tales como puertos del gateway PSTN, los transcodificadores, ancho de banda WAN, y así sucesivamente, también consideran estos problemas del 802.11b cuando usted clasifica su red de la Telefonía IP inalámbrica. Las insignias de Vocera son una aplicación especializada que estiran el número de clientes atados con alambre más allá de nuestras recomendaciones de la instalación típica.

Número de dispositivos del 802.11b por el Punto de acceso

Cisco recomienda que usted tiene no más que 15 a 25 dispositivos del 802.11b por el Punto de acceso.

Número de llamadas del Active por el Punto de acceso

Vocera utiliza dos diversos codificadores-decodificador basados encendido si es una llamada de la insignia-a-insignia (codificador-decodificador propietario de la baja velocidad de bits) o una llamada del insignia-a-teléfono (codificador-decodificador de G.711). Esta tabla muestra un porcentaje del ancho de banda disponible por las tarifas de datos y le da una imagen más clara de la producción prevista:

Proceso de la llamada	1 Mbp s	2 Mbp s	5.5 Mbp s	11 Mbp s
Insignia-a-teléfono (G.711)	20.7 %	11.8 %	6,3 %	4.7 %
Insignia-a-insignia (codificador-decodificador propietario de la baja velocidad de bits)	9.4%	6.1%	4.2 %	3.6 %

Cambie las recomendaciones

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

Usted puede crear una plantilla del puerto del switch para el uso cuando usted configura cualquier puerto del switch para la conexión a un Punto de acceso. Esta plantilla debe agregar todas las características de la seguridad de línea de base y de la elasticidad de la plantilla de escritorio estándar. Además, cuando usted asocia el Punto de acceso a un Cisco Catalyst 3750 Switch, usted puede optimizar el funcionamiento del Punto de acceso usando los comandos qos de múltiples capas de la transferencia (MLS) de limitar la velocidad de puerto y al map class del servicio (CoS) a las configuraciones del punto del código de los Servicios diferenciados (DSCP).

Ningún tráfico que no sea requerido por los clientes de la red inalámbrica (WLAN) no se debe enviar a un Punto de acceso. Una plantilla debe ser diseñada de una manera tal que las ayudas creen una conexión segura y de red fuerte con estas características:

- Vuelva las configuraciones del puerto para omitir — Previene los conflictos de configuración borrando cualquier configuración del puerto preexistente.
- Dynamic Trunking Protocol (DTP) de la neutralización — Inhabilita el enlace dinámico, que no es necesario para la conexión a un Punto de acceso.
- Port Aggregation Protocol (PAgP) de la neutralización — PagP se activa por abandono pero no es necesario para los puertos del usuario-revestimiento.
- Puerto del permiso rápido — Permite que un conmutador reanude rápidamente el tráfico de reenvío si el atravesar - el link del árbol va abajo.
- Configure el VLAN inalámbrico — Crea un VLAN de la red inalámbrica única que aisle el tráfico de red inalámbrica de otros datos, Voz, y VLAN de administraciones. Esto aísla el tráfico y asegura el mayor control del tráfico.
- Calidad de Servicio (QoS) del permiso; no confíe en el puerto (marca abajo a 0) — asegura el tratamiento apropiado del tráfico de prioridad alta, incluyendo los softphones, y previene a los usuarios del ancho de banda excesivo consumidor configurando de nuevo sus PC.

Los botones interruptores de encendido en línea WS-C3750-48PS-S se pueden utilizar para proporcionar a la potencia a los Puntos de acceso que son capaces de recibir la potencia en línea.

El catalizador 6500 permite que usted remita los paquetes en la línea tarifa con todas las características descritas aquí así como los módulos de servicio numerosos de integración. El módulo de servicio de red inalámbrica (WiSM) permite que usted tenga dos reguladores cada uno

con la capacidad para controlar 150 Puntos de acceso por cada uno. Con hasta cinco WiSMs por el chasis, esto permite que usted controle sobre 1500 Puntos de acceso que apoyen a 50,000 clientes dentro de un solo Switching Architecture del rendimiento alto.

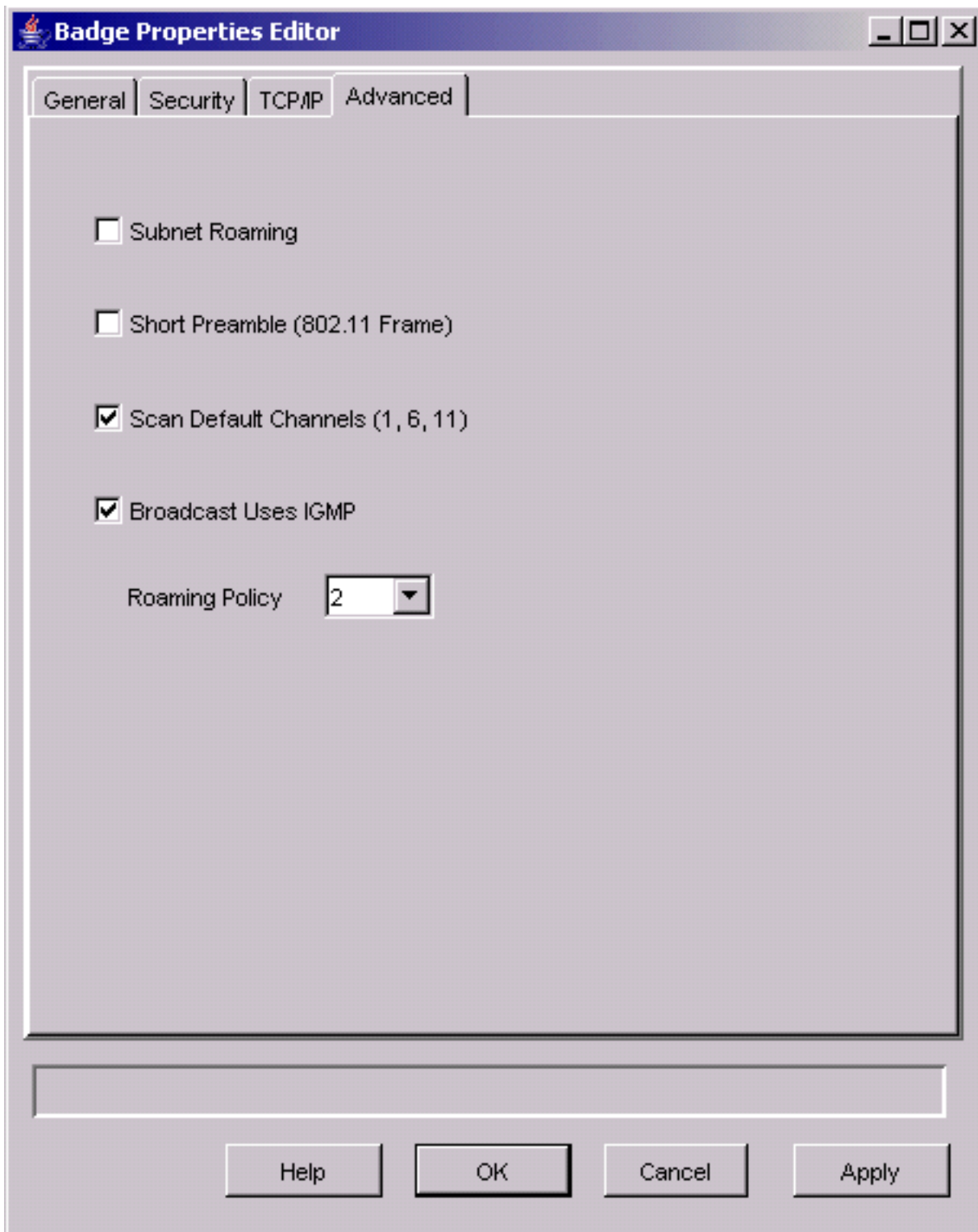
Implementaciones y configuración

Configuración de la insignia

La utilidad de configuración de la insignia de Vocera (BCU) y la configuración de la insignia pueden introducir la itinerancia y el tiempo de espera en su entorno si está hecha incorrectamente. Usando el BCU y el editor de las propiedades de la insignia (BPE), verifique estas configuraciones (véase el cuadro 8):

- **La subred que vaga por se inhabilita.**
- **Se controlan los canales del valor por defecto de la exploración (1,6,11).**
- **Se activan las aplicaciones IGMP de la difusión.**
- **La directiva de itinerancia se fija a 2 o más alto.**

Cuadro 8 — Ficha Avanzadas de Vocera BCU



Cuando la **subred que vaga por** se controla, da instrucciones la insignia para pedir una nueva dirección IP después de cada uno vaga por. En el entorno LWAPP, las ayudas de la infraestructura mantienen la Conectividad del cliente en la capa 3. Cuando un cliente de la Voz debe esperar el servidor del DHCP para responder antes de que pueda enviar o recibir los paquetes, se introduce la fluctuación y retraso. Si los **canales del valor por defecto de la exploración (1,6,11)** no se controlan, la insignia analiza todos los canales del 802.11b cuando la insignia mira para vagar por. Esto previene la expedición de los paquetes y de la itinerancia inconsútil.

[Tono AutoRF para su entorno](#)

Según lo descrito en la sección de las [recomendaciones de](#) este documento, es importante entender que cada sitio lo tiene es poseer las características RF. AutoRF o el Administración de recursos de radio (RRM) pudo necesitar ser adaptado, con la comprensión que cada sitio es diferente y AutoRF/RRM se debe adaptar para su entorno.

Antes de que usted ajuste AutoRF, refiera a la [administración de recursos de radio bajo redes inalámbricas unificadas](#) para más información.

RRM permite que usted ajuste la potencia de transmisión de cada Punto de acceso, ajustando cómo es fuerte cada Punto de acceso oye a su tercer vecino más fuerte. Este valor se puede ajustar solamente desde el CLI usando el **802.11b avanzado los config tx-potencia-trilla el** comando según lo descrito en [Alimentación de TX las configuraciones llanas de la asignación](#).

Antes de que usted ajuste AutoRF, recorre el sitio del despliegue usando la insignia de Vocera según lo desgastado por el usuario final y utiliza una herramienta del estudio sobre el sitio para ganar un conocimiento profundo de cómo la insignia vaga por y en de qué potencia se considera cada Punto de acceso. Una vez que esto es completo y se determina que el ajuste de este valor está requerido, comience con un valor – del dBm 71 para el algoritmo de control de potencia de transmisión. Utilice este parámetro CLI:

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

Permita que la red trabaje con este ajuste con un mínimo de 30 minutos a una hora antes de que usted observe cualquier cambio. Una vez que la red se da una cantidad suficiente de hora, recorre el sitio usando la misma herramienta e insignias de la encuesta otra vez. Observe las mismas características y potencia de itinerancia del Punto de acceso. La meta aquí es intentar hacer que las insignias vaguen por en o antes del Punto de acceso siguiente para conseguir la relación señal-ruido mejor.

- **¿Cómo sé si la potencia de transmisión es demasiado caliente o demasiado fría?**La determinación si usted tiene de su umbral de la potencia de transmisión demasiado alto o demasiado bajo requiere una buena comprensión de su entorno. Si usted ha recorrido su área entera del despliegue (donde usted espera que su Vocera badges para funcionar), usted debe saber dónde se localizan sus Puntos de acceso así como experimentar el comportamiento de itinerancia de la insignia.
- **¿Qué hago si mi potencia de transmisión es demasiado caliente?**La insignia de Vocera vaga por basado solamente en la potencia de la señal bastante que la calidad de la señal. Si la insignia de Vocera no vaga por después de que pase varios Puntos de acceso mientras que esté enganchada al preceptoral agradable o el tono de prueba, la insignia se considera ser Sticky. Si este comportamiento es indicativo del área entera del despliegue del campus, después su umbral de la potencia de transmisión es demasiado caliente y se debe retroceder. Si solamente uno o dos áreas aisladas muestran este comportamiento y el resto de las características de itinerancia más idealistas de las demostraciones del área del despliegue ésta no es una indicación que su red está ejecutando demasiado caliente.
- **¿Qué hago si mi potencia de transmisión es demasiado fría?**El valor por defecto transmite el umbral debe casi nunca proporcionarle a un área del despliegue donde su red ejecuta demasiado frío. Si el umbral de la potencia de transmisión se ajusta abajo, y el recorrer los pasillos con la insignia de Vocera provee de usted un entorno donde la insignia vaga por bien, pero pierde la Conectividad y/o los muertos/la cobertura irregular, después su red pudo haber

sido demasiado baja adaptado. Si esto no es característico de su toda la red pero aislado a uno o dos áreas, después es más indicativo de un agujero de la cobertura bastante que un problema para toda la red.

- **Comportamiento aislado** Si usted encuentra que en uno o dos áreas, la insignia se pega a un Punto de acceso bastante que vagando por de una manera idealista, examine esta área. ¿Cómo es esta área diferente del resto del campus? ¿Si ésta/estas áreas es salidas o áreas cercanas del edificio bajo construcción, podría la detección del agujero de la cobertura forzar estos Puntos de acceso para aumentar la potencia? Mire las listas vecinas del archivo del registro y del Punto de acceso WLC para ayudar a determinar porqué tal anomalía podría ocurrir. Si usted encuentra que en una o más áreas aisladas, las experiencias de la insignia muertas o la cobertura irregular, después usted necesita examinar estas áreas por separado. ¿Está esta área cerca de un eje de elevador, de radiología, o de un cuarto de la rotura? Estas áreas se pudieron adaptar mejor por la instalación o la mejor colocación de un Punto de acceso para tener en cuenta una mejor cobertura de la Voz. En ambos casos, es siempre recomendable entender que usted está trabajando en un espectro de radio no autorizado y el comportamiento idealista no pudo nunca ser realizable. Esto podría suceder cuando le sitúan al lado de una torre o un dispositivo de la transmisión de radio, un transmisor de televisión o posiblemente un non-802.11 recurso de la reparación 2.4 gigahertz (teléfonos inalámbricos, y así sucesivamente).

[Configuración de la infraestructura de red inalámbrica](#)

Cisco unificó el diseño de red inalámbrica y el Guía de despliegue se debe seguir para la configuración general de su WLC. Esta sección proporciona a las recomendaciones adicionales específicas a las insignias de la comunicación de Vocera®.

Nota: Los cambios se dejan unsaved si usted no presiona el **botón Apply Button** antes de que usted se traslade al siguiente paso.

Complete estos pasos bajo menú del nivel superior del **regulador**:

1. Cambie al modo de multidifusión de los Ethernetes al **Multicast**.
2. Fije la dirección de grupo de multidifusión a **239.0.0.255** (o a una cierta otra dirección de grupo de multidifusión inusitada).
3. Fije el nombre del Domain Name y de la RF-red de la movilidad del valor por defecto a su diseño de red.
4. Inhabilite el **Equilibrio de carga agresivo**. Cuadro 9 — Configuración general WLC

Cisco Systems Save Configuration | Ping | Logout | Refresh

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Controller

General Apply

General
Inventory
Interfaces
Network Routes
Internal DHCP Server
Mobility Management
 Mobility Groups
 Mobility Statistics
Spanning Tree
Ports
Master Controller Mode
Network Time Protocol
QoS Profiles

General
 802.3x Flow Control Mode (Current Operating Mode is Layer3)
 LWAPP Transport Mode (LAG Mode is currently enabled).
 LAG Mode on next reboot
 Ethernet Multicast Mode
 Multicast Group Address
 H-REAP supports 'unicast' mode only.
 Aggressive Load Balancing
 Peer to Peer Blocking Mode
 Over The Air Provisioning of AP
 AP Fallback
 Apple Talk Bridging
 Fast SSID change
 Default Mobility Domain Name
 RF-Network Name
 User Idle Timeout (seconds)
 ARP Timeout (seconds)
 Web Radius Authentication
 Operating Environment Commercial (0 to 40 C)
 Internal Temp Alarm Limits 0 to 65 C

[Cree los interfaces](#)

Haga clic el regulador > los interfaces.

Nota: Su VLA N y dirección IP varía. Las capturas de pantalla aquí proporcionan a dirección de la muestra que no debe ser seguida directamente.

Cuadro 10 — Lista de interfaces WLC

[Cree la interfaz de voz de Vocera](#)

Complete estos pasos:

1. Haga clic en **New**.
2. Ingrese un representante del nombre de la etiqueta de su red de Vocera VoWLAN en el campo de nombre del interfaz.
3. Ingrese el número del VLA N de esa red de VoWLAN en el campo identificación del VLA N.
4. El teclado **se aplica** y después hace clic **corrige** para corregir el interfaz que usted acaba de crear.
5. Ingrese el IP que dirige para este interfaz que esté en el rango del VLA N y de la otra información relacionada.
6. Haga clic en Apply (Aplicar).

[Configuración Tecnología inalámbrica-específica](#)

Para una red inalámbrica (WLAN) que tenga solamente Vocera Badges, esta configuración proporciona a las configuraciones de ejemplo que el mejor utilice la aplicación de la difusión de Vocera.

- El período DTIM es 1.
- La ayuda para 802.11g se inhabilita. Solamente el índice de datos del 802.11b de **11 Mbps** es **obligatorio**.
- Se inhabilita el preámbulo corto.
- Se inhabilita DTPC.

Cuadro 11 — configuración 802.11b/g

Save Configuration | Ping | Logout | Refresh

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Wireless 802.11b/g Global Parameters Apply Auto RF...

Access Points 802.11b/g Network Status Enabled

802.11a Radios

802.11b/g Radios

Bridging

802.11g Support Enabled

802.11n Support

Data Rates**

1 Mbps Supported

2 Mbps Supported

5.5 Mbps Supported

11 Mbps Mandatory

Beacon Period (milliseconds) DTIM Period (beacon intervals)

Fragmentation Threshold (bytes)

Short Preamble Enabled

Pico Cell Mode Enabled

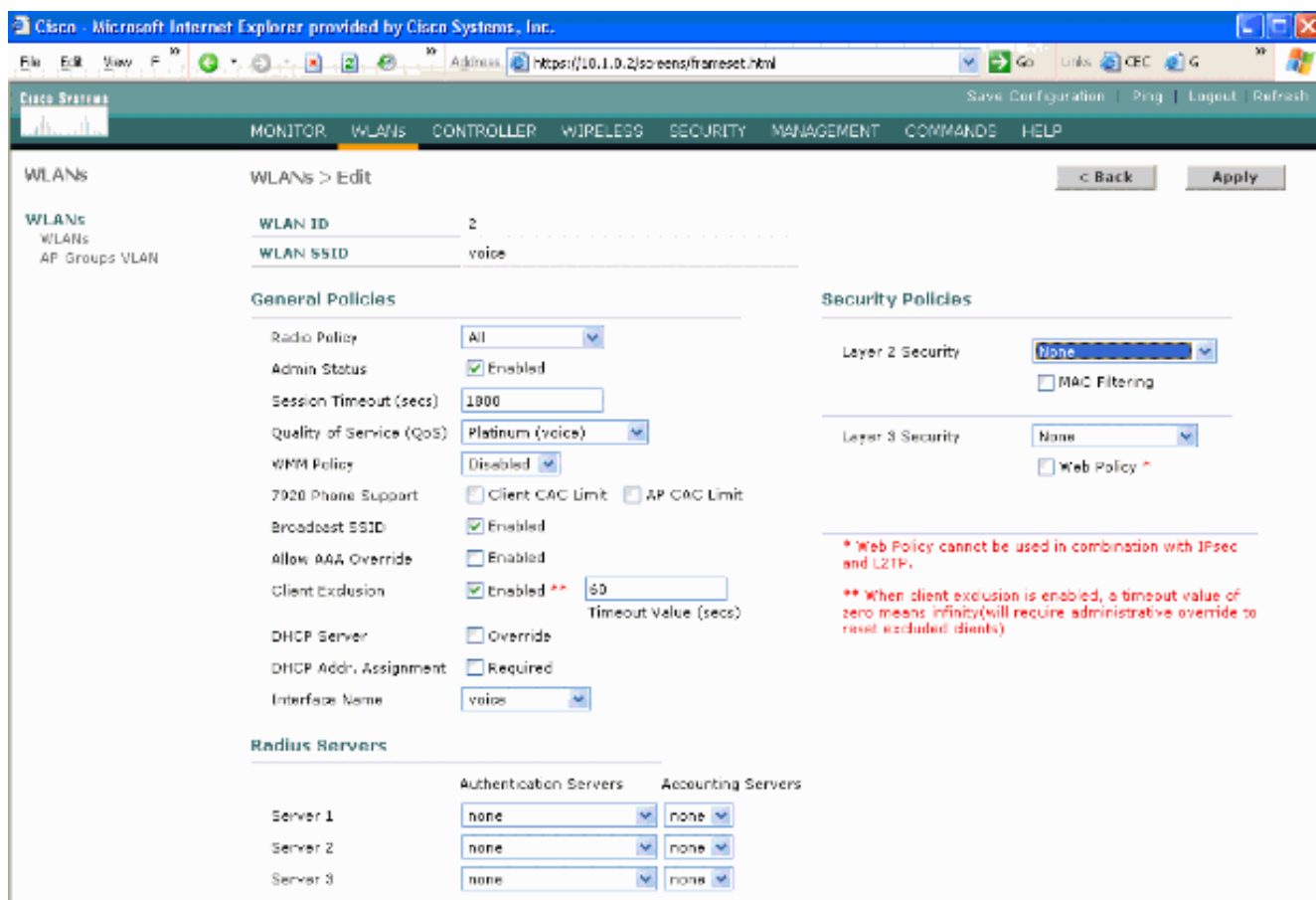
DTPC Support Enabled

** Data Rate 'Mandatory' implies that clients who do not support that specific rate will not be able to associate. Data Rate 'Supported' implies that any associated client that also supports that same rate may communicate with the AP using that rate. But it is not required that a client be able to use the rates marked supported in order to associate.

[Configuración de la red inalámbrica \(WLAN\)](#)

Complete estos pasos:

1. Ponga al día el campo de radio de la directiva a un valor que los mejores ajustes usted necesiten.
2. Cambie el estado del administrador a **activado**.
3. Fije el tiempo de espera de la sesión a **1800**.
4. Fije la calidad de servicio al **platino**.
5. Fije la difusión SSID a **activado**.
6. Fije el nombre del interfaz al interfaz creado para las insignias de la comunicación de Vocera.
7. Fije las opciones de seguridad de hacer juego sus directivas corporativas. **Cuadro 12 — Configuración de la red inalámbrica (WLAN)**



[Configure el detalle del Punto de acceso](#)

Complete estos pasos:

1. Haga clic el **detalle**.
2. Configure el nombre AP.
3. Asegúrese de que el Punto de acceso esté configurado para el DHCP.
4. Asegúrese de que **activen** al estado del administrador.
5. La Mod AP" se debe fijar al **local**.
6. Ingrese la ubicación del Punto de acceso.
7. Ingrese el nombre del regulador que el Punto de acceso pertenece a. El nombre del regulador se puede encontrar en la página del monitor.
8. Haga clic en Apply (Aplicar). **Cuadro 13 — Detalle AP**

Wireless

Access Points
All APs
802.11a Radios
802.11b/g Radios

Mesh

Regues
Regue APs
Known Regue APs
Regue Clients
Adhoc Regues

Clients
802.11a
Network
Client Roaming
Voice
Video
802.11h

802.11b/g
Network
Client Roaming
Voice
Video

Country

Timers

All APs

Search by Ethernet MAC Search

AP Name	AP ID	Ethernet MAC	Admin Status	Operational Status	Port
ap:54:cb:30	0	00:0c:85:54:cb:30	Enable	REG	4 Detail

[Configure la radio 802.11b/g](#)

Complete estos pasos:

1. Haga clic la **Tecnología inalámbrica** situada en la cima del WLC y verifique que todos los Puntos de acceso bajo estado del administrador están fijados **para activar**. **Figura 14**

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

All APs

Search by Ethernet MAC Search

AP Name	AP ID	Ethernet MAC	Admin Status	Operational Status	Port
AP0016.47cc.2d28	0	00:16:47:cc:2d:28	Enable	REG	29 Detail
AP0016.47cc.2c08	1	00:16:47:cc:2c:08	Enable	REG	29 Detail

2. **Red del teclado** (situada cerca de 802.11b/g).
3. Teclado **AutoRF**.
4. Utilice AutoRF para crear una cobertura completa con el canal sin traslapo RF y una potencia de transmisión. Para hacer esto, **automático** selecto para la asignación del canal RF y Alimentación de TX la asignación llana. **Figura 15**

802.11b/g Global Parameters > Auto RF

RF Group

Group Mode	<input checked="" type="checkbox"/> Enabled
Group Update Interval	600 secs
Group Leader	00:14:a9:be:50:40
Is this Controller a Group Leader	Yes
Last Group Update	557 secs ago

RF Channel Assignment

Channel Assignment Method	<input checked="" type="radio"/> Automatic Every 600 sec <input type="radio"/> On Demand Invoke Channel Update now <input type="radio"/> OFF
Avoid Foreign AP interference	<input checked="" type="checkbox"/> Enabled
Avoid Cisco AP load	<input type="checkbox"/> Enabled
Avoid non-802.11b noise	<input checked="" type="checkbox"/> Enabled
Signal Strength Contribution	Enabled
Channel Assignment Leader	00:14:a9:be:50:40
Last Channel Assignment	557 secs ago

Tx Power Level Assignment

Power Level Assignment Method	<input checked="" type="radio"/> Automatic Every 600 sec <input type="radio"/> On Demand Invoke Power Update now <input type="radio"/> Fixed <input type="text" value="1"/>
Power Threshold	-65 dBm
Power Neighbor Count	3
Power Update Contribution	SNI
Power Assignment Leader	00:14:a9:be:50:40
Last Power Level Assignment	557 secs ago

- Haga clic en Apply (Aplicar).
- Haga clic la configuración de la salvaguardia y vea el [tono AutoRF para su](#) sección del [entorno de](#) este documento.
- Elija la **Tecnología inalámbrica > los Puntos de acceso > las radios 802.11b/g**. Figura 16

802.11b/g Radios

AP Name	Base Radio MAC	Admin Status	Operational Status	Channel	Power Level	Antenna	
AP1	00:0b:85:54:c3:30	Enable	UP	11 *	1 *	Internal	Configure Detail 802.11b/gTSM

* global assignment

Verificación de la Telefonía IP inalámbrica

Después de que usted conduzca un estudio sobre el sitio RF y configure los Puntos de acceso y los teléfonos, es crucial conducir las Pruebas de verificación para asegurarse de que todo trabaja según lo deseado. Estas pruebas se deben realizar en absoluto de estas ubicaciones:

- El área primaria de cada célula del Punto de acceso (donde están más probable las insignias de conectar con ese Punto de acceso determinado).
- Cualquier ubicación en donde pudo haber volumen alto de llamada.
- Las ubicaciones en donde el uso pudo ser infrecuente solamente la cobertura todavía tiene que ser certificadas (por ejemplo, las escaleras, los lavabos, y así sucesivamente).
- En las franjas de la área de cobertura del Punto de acceso.
- Estas pruebas se pueden realizar paralelamente o serie. Si está realizado paralelamente, asegúrese de que los teléfonos están accionados apagado entre las puntas de prueba para probar la asociación, la autenticación, y el registro completos en cada ubicación. Las pruebas de la itinerancia y de carga deben ser las Pruebas finales.

Asociación, autenticación, y registro

Esta sección explica cómo verificar que la insignia se asocia, autentica, y se registra correctamente.

- En los puntos múltiples en el entorno, el ciclo inicial las insignias y verifica la asociación con el Punto de acceso. Si la insignia no se asocia al Punto de acceso, realice estos controles: Controle la configuración de la insignia para asegurar el SSID apropiado, tipo de la autenticación, y así sucesivamente. Controle la configuración WLC para asegurar el SSID apropiado, tipo de la autenticación, los canales de radio, y así sucesivamente. Controle su estudio sobre el sitio para asegurarse que la ubicación tiene cobertura adecuada RF.
- En los puntos múltiples en el entorno, asegúrese de que el teléfono autentique a través del Punto de acceso con éxito. Si el cliente no autentica, controle la clave WEP o el nombre de usuario y contraseña del SALTO en las insignias. También, controle el nombre de usuario y contraseña en el servidor AAA usando una computadora portátil inalámbrica con las credenciales idénticas.
- En los puntos múltiples en el entorno, asegúrese de que las insignias se registren con el Vocera Communication Server (Servidor de comunicación). Si el cliente no se registra, realice estos controles: Verifique que la insignia tenga el la dirección IP correcta, la máscara de subred, el gateway principal, el TFTP, primarios primario/secundarios y DNS.
- Llamadas de Voz inmóviles: En los puntos múltiples en el entorno, mientras que usted todavía se coloca, haga una llamada a otra insignia y conduzca 60 a las pruebas de la Voz 120-second para controlar la Calidad de voz. Si la Calidad de voz es inaceptable, mueva una insignia a una mejor ubicación y pruebe otra vez. ¿Es la Calidad de voz aceptable? Si no, controle su cobertura de red inalámbrica. Si el servidor de la telefonía se configura, en los puntos múltiples en el entorno, todavía colóquese y haga una llamada a un teléfono atado con alambre y conduzca 60 a las pruebas de la Voz 120-second para controlar la Calidad de voz. Si la Calidad de voz es inaceptable, pregunte si usted hace una llamada usando el teléfono atado con alambre. ¿Es la Calidad de voz aceptable? Si no, verifique el diseño de red alámbrica contra las guías de consulta.

- Utilice las herramientas del estudio sobre el sitio para verificar que hay no más que un Punto de acceso por el canal RF de esa ubicación con una potencia de la señal ([RSSI] del indicador de la fuerza de señal recibida) mayor de 35. Si hay dos Puntos de acceso presentes en el mismo canal, asegúrese de que el relación señal-ruido (SNR) sea tan alto como sea posible minimizar interferencia. Por ejemplo, si el Punto de acceso más fuerte tiene un RSSI de 35, idealmente el Punto de acceso más débil debe tener un RSSI de menos de 20. Para alcanzar esta meta, usted puede ser que tenga que reducir la una potencia de transmisión del Punto de acceso o mover el Punto de acceso.
- Controle las configuraciones de QoS en el Punto de acceso para confirmar las configuraciones recomendadas apropiadas.
- Llamadas de itinerancia de la insignia: Si el servidor de la telefonía no está disponible, inicie la guía de Vocera con el comando **comienzan la guía**. Si el servidor de la telefonía está disponible, inicie una llamada con un dispositivo inmóvil a la insignia. Controle continuamente la Calidad de voz mientras que usted atraviesa el área total de la cobertura de red inalámbrica. Si la Calidad de voz es escasa, realice estas tareas: Esté atentos todos los cambios inaceptables en la Calidad de voz y tome la nota de la ubicación y de los valores de radio en su computadora portátil y los valores CQ de la insignia. Mire y esté atenta la insignia para vagar por al Punto de acceso siguiente. Observe los otros Puntos de acceso disponibles en el estudio sobre el sitio para controlar la cobertura e interferencia.
- Haga los ajustes a la colocación y a las configuraciones del Punto de acceso para ajustar la red inalámbrica (WLAN), y realice estos controles para asegurar la Calidad de voz: Utilice las herramientas del estudio sobre el sitio y verifique que hay no más que un Punto de acceso por el canal con un valor RSSI mayor de 35 en cualquier ubicación dada. Idealmente, el resto de los Puntos de acceso en el mismo canal deben tener valores RSSI que bajos como sea posible (preferiblemente menos de 20). En la frontera de la área de cobertura donde está 35 el RSSI, el RSSI para el resto de los Puntos de acceso en el mismo canal debe idealmente ser menos de 20. Utilice las herramientas del estudio sobre el sitio para verificar que hay por lo menos dos Puntos de acceso (totales, en los canales diferentes) visibles en toda la ubicación con la suficiente potencia de la señal. Controle que los Puntos de acceso en un área de itinerancia dada son todos en una red de la capa 2.

Problemas de itinerancia comunes

Estos problemas de itinerancia pueden ocurrir:

- La insignia no vaga por cuando está colocada directamente conforme al Punto de acceso.
- La insignia es más probable no alcanzando los umbrales diferenciados de itinerancia para el indicador de la fuerza de señal recibida (RSSI) y el uso del canal (CU). Ajuste la forma del umbral de la potencia de transmisión el WLC.
- La insignia no recibe los faros ni sonda las respuestas del Punto de acceso.
- La insignia vaga por demasiado lentamente.

La insignia pierde la conexión a la red o pierden al servicio de voz al vagar por

- Controle la autenticación para saber si hay una discordancia posible WEP.
- La insignia no envía IGMP se une a o la red envía las interrogaciones IGMP durante una itinerancia. Por lo tanto, la función de la difusión de Vocera falla durante una capa 2/Layer 3

vaga por.

- La insignia es capaz de la capa inconsútil 2 que vaga por solamente (a menos que se configura un mecanismo de la movilidad de la capa 3). Asegúrese de que el nuevo WLC no esté sirviendo una diversa subred IP.
- Verifique que el Punto de acceso asociado/regulador tenga Conectividad IP al Vocera Communication Server (Servidor de comunicación).
- Controle los valores CQ de la potencia de la señal y de la insignia RF.

[La insignia pierde la Calidad de voz mientras que vaga por](#)

- Controle para saber si hay el RSSI bajo en el Punto de acceso del destino.
- La coincidencia del canal pudo ser escasa. La insignia debe tener tiempo para dar de la llamada suavemente antes de que pierda su señal con el Punto de acceso original.
- La señal del Punto de acceso original pudo ser perdida.

[Problemas de audio](#)

Hay algunos errores de la configuración común que pueden causar algunos Problemas de audio fácilmente resueltos. Si es posible, controle los problemas de audio contra una insignia inmóvil (de la referencia) para ayudar al estrecho el problema a un problema inalámbrico. Los problemas de audio comunes incluyen:

- [Audio unilateral](#)
- [Audio picado o robótico](#)
- [Registro y problemas de autenticación](#)

[Audio unilateral](#)

- Este problema puede ocurrir en las áreas de la franja de un Punto de acceso, donde una señal pudo ser demasiado débil en el lado de la insignia o el lado del Punto de acceso. Corresponder con las configuraciones de energía en el Punto de acceso a la insignia (20 mW), cuando es posible, puede fijar este problema. Este problema es el más común cuando la variación entre la configuración del Punto de acceso y la configuración de la insignia es grande (por ejemplo, 100 mW en el Punto de acceso y 28 mW en la insignia).
- Controle el gateway y el Routing IP para saber si hay Calidad de voz.
- Controle para ver si un Firewall o un NAT está en la trayectoria de los paquetes UDP propietarios. Por abandono, los Firewall y NATs causan el audio unidireccional o no audios. Cisco IOS® y PIX NATs y Firewall tiene la capacidad de modificar esas conexiones de modo que el audio de dos vías pueda fluir. Si usted utiliza la movilidad de la capa 3, su red podría bloquear el tráfico por aguas arriba con los controles del Unicast Reverse Path Forwarding (uRPF).
- El audio unidireccional puede ocurrir si el almacenamiento en memoria inmediata ARP no se configura en el WLC.

[Audio picado o robótico](#)

- Las razones comunes para el audio picado o robótico son cuando una microonda actúa

- cerca. Las microondas comienzan en el canal 9 y pueden extender de los canales 6 a 14.
- Controle para saber si hay teléfonos inalámbricos 2.4 gigahertz y otros dispositivos de red inalámbrica de la llamada de la enfermera usando las herramientas como Cognio.

Registro y problemas de autenticación

Cuando usted encuentra los problemas con la autenticación, realice estos controles:

- Controle los SSID para asegurarse de que hacen juego en la insignia y el Punto de acceso (o red). También esté seguro que la red tiene una ruta al servidor de Vocera.
- Controle las claves WEP para asegurarse de que hacen juego. Es una buena idea entrarlos de nuevo en la utilidad de configuración de la insignia (BCU) y reprogramar la insignia, porque es fácil hacer un error de tipeo cuando usted ingresa una clave WEP o una contraseña.

Estos mensajes o síntomas pueden ocurrir:

- No puede utilizar todas las capacidades pedidas — Esto es más probable una discordancia del cifrado entre el Punto de acceso y el cliente.
- Autenticación fallada/ningún AP encontrado — Asegure los tipos coincidencia de la autenticación en el Punto de acceso y el cliente.
- Ningún servicio – Config IP fallados — Si usted utiliza el WEP estático, asegúrese que las claves estén configuradas correctamente. Asegúrese que otros clientes puedan recibir el DHCP usando el mismo SSID.
- De-autentique a todos los clientes TKIP del AP — Este problema sucede cuando el Punto de acceso detecta dos errores MIC en el plazo de 60 segundos. Este las contramedidas guardan a todos los clientes TKIP de la re-autenticidad por 60 segundos.
- Re-autenticación/tiempo de espera de la sesión — Si está configurado, un tiempo de espera de la sesión acciona una re-autenticación que cause los huecos en la secuencia de voz (ms 300 + retraso PÁLIDO para la autenticación del 802.1x).

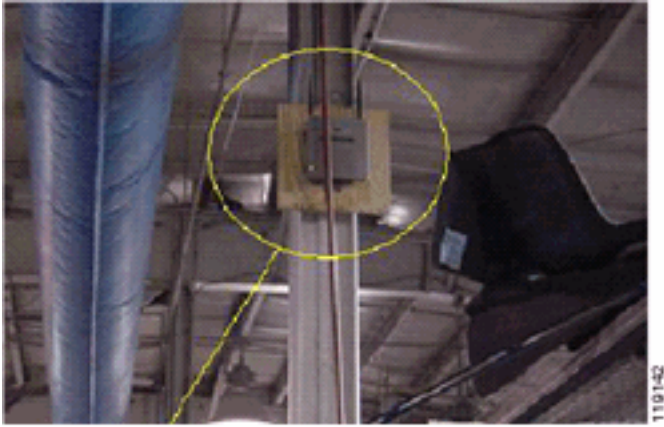
Apéndice A

AP y colocación de la antena

Esta sección da los ejemplos de la colocación apropiada e incorrecta de los Puntos de acceso (APs) y de las Antenas.

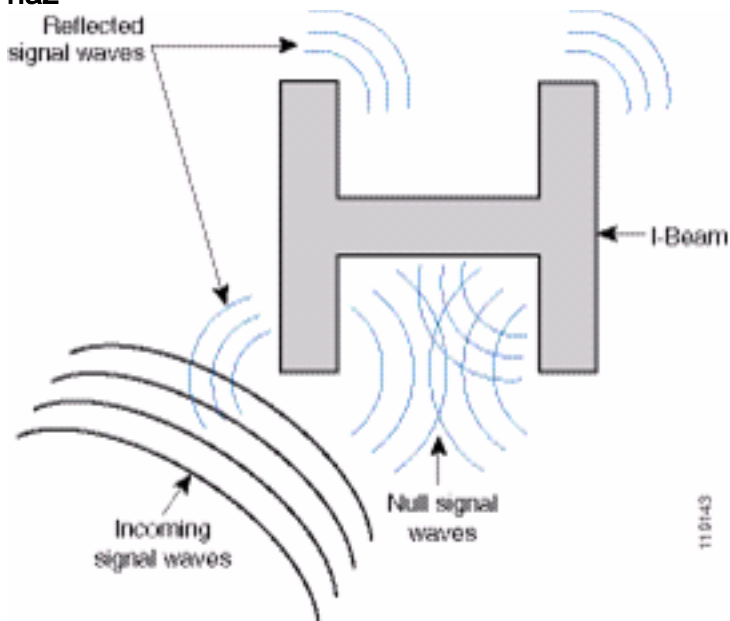
El cuadro 17 muestra la colocación incorrecta de un Punto de acceso y de las Antenas cerca de un Yo-haz, que crea los modelos torcidos de la señal. Un punto nulo RF es creado por la travesía de las ondas de la señal, y se crea la distorsión de trayectoria múltiple cuando se reflejan las ondas de la señal. Esta colocación da lugar a la cobertura muy pequeña detrás del Punto de acceso y de la calidad de la señal reducida delante del Punto de acceso.

Cuadro 17 — Colocación incorrecta de las Antenas cerca de un Yo-haz



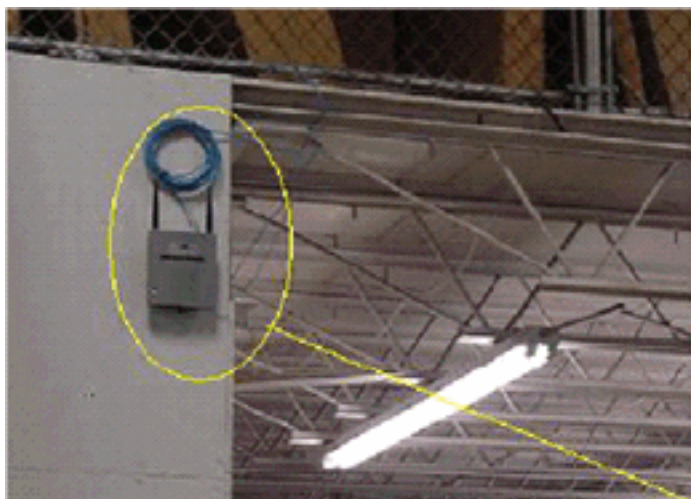
El cuadro 18 muestra los cambios o las distorsiones de la propagación de la señal causados por un Yo-haz. El Yo-haz crea muchas reflexiones de los paquetes recibidos y de los paquetes transmitidos. Las señales reflejadas dan lugar a la calidad de la señal muy pobre debido a los puntos nulos y interferencia de trayecto múltiple. Sin embargo, la potencia de la señal es alta porque las antenas del punto de acceso están tan cerca al Yo-haz.

Cuadro 18 — Distorsiones de señal causadas colocando las Antenas demasiado cerca a un Yo-haz



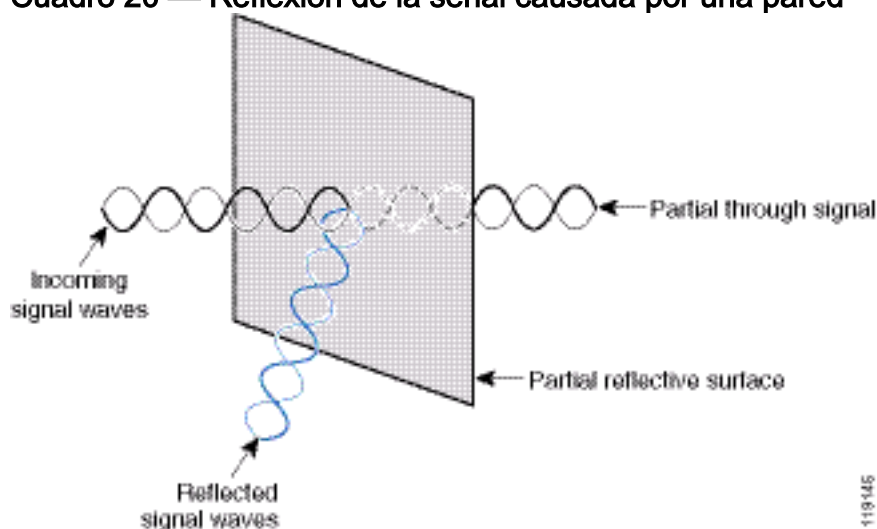
El Punto de acceso y la colocación de la antena en el cuadro 19 es mejores porque está lejos de los Yo-haces y hay menos señales reflejadas, menos puntos nulos, y menos interferencia de trayecto múltiple. Esta colocación todavía no es perfecta porque el cable de Ethernetes no se debe arrollar encima así que cercano a la antena. También, el Punto de acceso se podía dar vuelta con las Antenas 2.4GHz señaladas al suelo. Esto proporciona a una mejor cobertura directamente debajo del Punto de acceso. No hay usuarios sobre el Punto de acceso.

Cuadro 19 — Punto de acceso y Antenas montados en una pared, lejos de los Yo-haces



El cuadro 20 muestra la propagación de la señal causada por la pared en la cual se monta el Punto de acceso.

Cuadro 20 — Reflexión de la señal causada por una pared

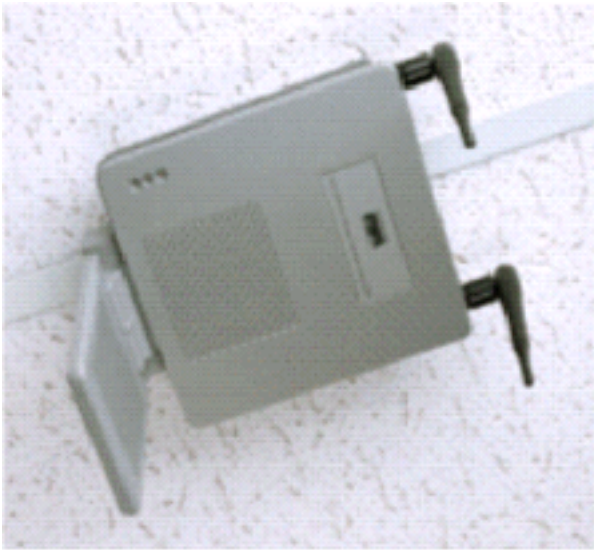


Los ejemplos anteriores también se aplican cuando usted coloca los Puntos de acceso y las Antenas en o cerca del techo en un entorno estándar de la empresa. Si hay tubos de aire del metal, ejes de elevador, u otras barreras físicas que pueden causar la reflexión o interferencia de trayecto múltiple de la señal, Cisco recomienda altamente que usted mueva las Antenas lejos de esas barreras. En el caso del elevador, mueva la antena algunos pies lejos para ayudar a eliminar la reflexión y la distorsión de la señal. Lo mismo es verdad con los tubos de aire en el techo.

Una encuesta conducida sin el envío y la recepción de los paquetes no es suficiente. El ejemplo del Yo-haz muestra la creación de los puntos nulos que pueden resultar de los paquetes que tienen errores CRC. Los paquetes de voz con los errores CRC son los paquetes faltados que afectan al contrario a la Calidad de voz. En este ejemplo, esos paquetes podían estar sobre el suelo del ruido medido por una herramienta de la encuesta. Por lo tanto, es muy importante que los niveles de la señal de las medidas del estudio sobre el sitio no sólo pero también generan los paquetes y después señalan los errores de paquete.

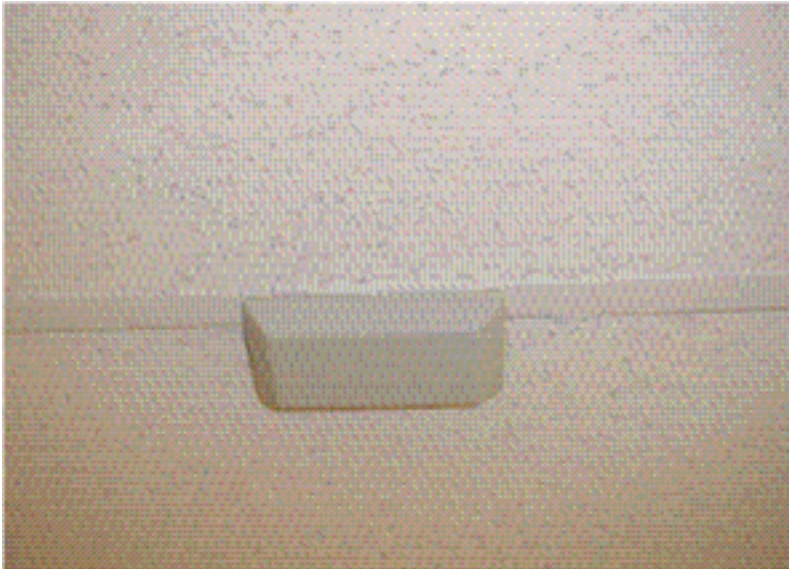
El cuadro 21 muestra Cisco AP1200 montado correctamente a una T-barra del techo, con las Antenas en una posición omnidireccional.

Cuadro 21 — Cisco AP1200 montado a un techo



El cuadro 22 muestra una antena de diversidad omnidireccional de Cisco Aironet 5959 montada correctamente a una T-barra del techo. En este caso, Cisco AP1200 se monta sobre la teja del techo.

Cuadro 22 — Antena de Cisco Aironet 5959 montada a un techo



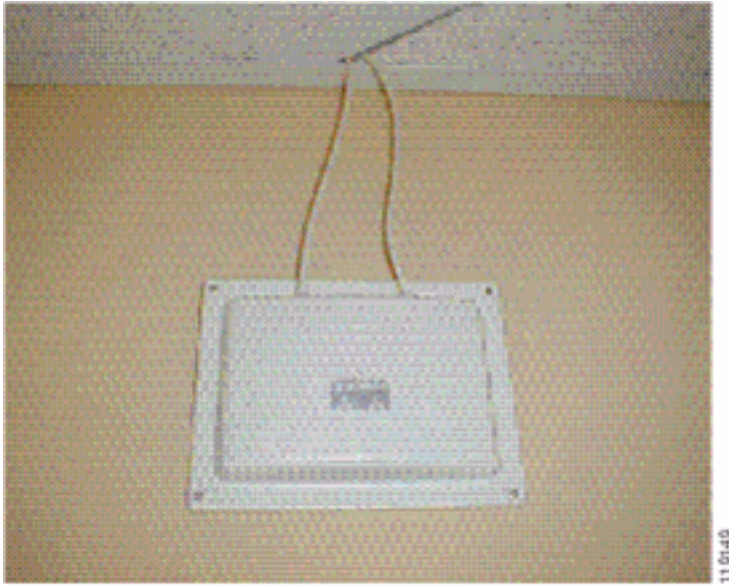
El cuadro 23 muestra Cisco AP1200 montado correctamente a una pared.

Cuadro 23 — Cisco AP1200 montado a una pared



El cuadro 24 muestra la antena de la corrección de la diversidad de Cisco Aironet 2012 montada a una pared. En este caso, Cisco AP1200 se monta sobre la teja del techo.

Cuadro 24 — Antena de Cisco Aironet 2012 montada a una pared



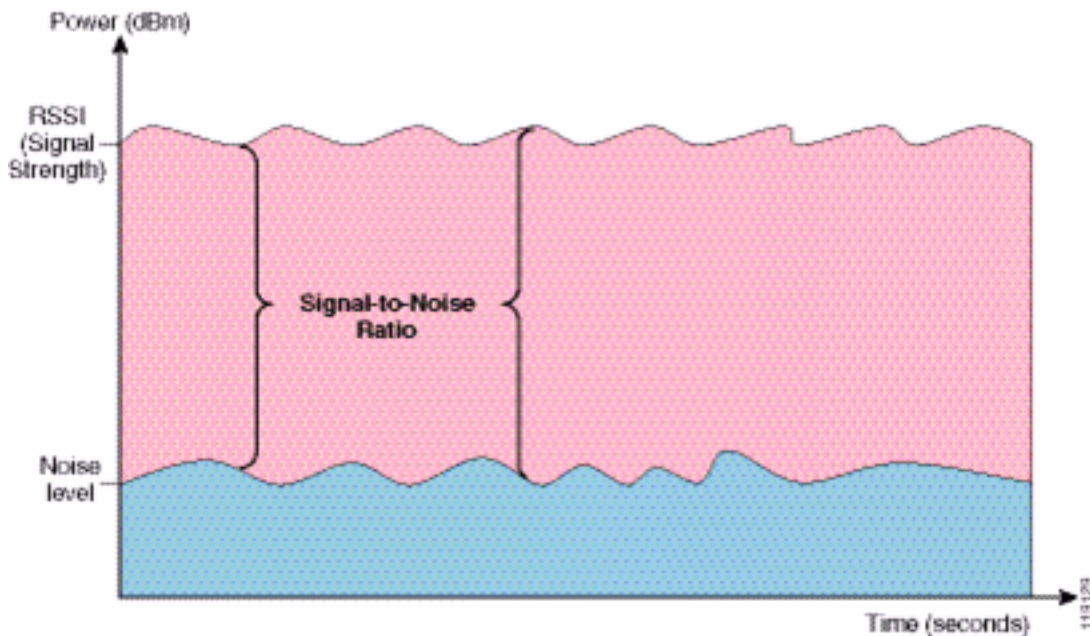
Para las áreas donde está alto el tráfico de usuarios (por ejemplo los espacios de oficina, las escuelas, las empresas minoristas, y los hospitales), Cisco recomienda que usted pone el acceso señala de la vista y coloca las Antenas discretas debajo del techo. La separación para las Antenas de la no-diversidad no debe exceder 18 pulgadas.

[Interferencia y distorsión de trayectoria múltiple](#)

El desempeño del rendimiento de procesamiento de la red de la red inalámbrica (WLAN) es afectado por las señales inutilizables. Interferencia de la red inalámbrica (WLAN) se puede generar por los hornos de microondas, los 2.4 dispositivos de los teléfonos inalámbricos GHz, de Bluetooth, o el otro equipo electrónico que actúa en la banda 2.4 gigahertz. Interferencia también viene típicamente de otros Puntos de acceso y dispositivos cliente que pertenezcan en la red inalámbrica (WLAN) pero que esté suficientemente lejos ausente para debilitar o se haya corrompido su señal. Los Puntos de acceso que no son parte de la infraestructura de red pueden también causar interferencia de la red inalámbrica (WLAN) y se identifican como puntos de acceso no autorizado.

Interferencia y la distorsión de trayectoria múltiple causan la señal transmitida de fluctuar. Interferencia disminuye el relación señal-ruido (SNR) para una tarifa de datos determinada. Las cuentas de reintentos del paquete entran para arriba en un área donde están altas interferencia y/o la distorsión de trayectoria múltiple. Interferencia también se refiere como suelo del nivel de ruido o del ruido. La fuerza de la señal recibida de su Punto de acceso asociado debe estar arriba bastante sobre el nivel de ruido del receptor que se decodificará correctamente. Este nivel de fuerza se refiere como el relación señal-ruido, o SNR. El SNR ideal para la insignia de Vocera es DB 25. Por ejemplo, si el suelo del ruido es 95 decibeles por milivatio (dBm) y la señal recibida en el teléfono es el dBm 70, después el relación señal-ruido es DB 25. (Véase el cuadro 25.)

Cuadro 25 — Relación señal-ruido (SNR)



Cuando usted cambia el tipo y la ubicación de la antena, puede reducir la distorsión e interferencia de trayectoria múltiple. El aumento de la antena agrega a la ganancia del sistema y puede reducir interferencia si el transmisor de interferencia no está directamente delante de la antena direccional.

Mientras que las antenas direccionales pueden estar de las aplicaciones internas del mucho valor con certeza, el amplia mayoría de las instalaciones interiores utiliza las Antenas omnidireccionales. La direccionalidad se debe determinar estrictamente por un estudio sobre el sitio correcto y apropiado. Si usted utiliza un omnidireccional o parchea la antena, los entornos interiores requieren las antenas de diversidad atenuar la distorsión de trayectoria múltiple. Las radios del Punto de acceso de la serie de Cisco Aironet permiten la ayuda de la diversidad.

Atenuación de la señal

La atenuación de la señal o la pérdida de la señal ocurre incluso durante la señal pasa a través del aire. La fuerza de la pérdida de señal es pronunciada pues la señal pasa a través de diversos objetos. Una potencia de transmisión de 20 mW es equivalente al dBm 13. Por lo tanto, si la potencia transmitida en el punto de entrada de una pared del cartón yeso está en el dBm 13, la potencia de la señal se reduce al dBm 10 al salir esa pared. Esta tabla muestra la pérdida probable en la potencia de la señal causada por los diversos tipos de objetos.

Atenuación de la señal causada por los diversos tipos de objetos

Objeto en el trayecto de la señal	Atenuación de la señal a través del objeto
Pared del cartón yeso	DB 3
Pared de cristal con el marco metálico	DB 6
Pared del bloque de escoria	DB 4
Ventana de la oficina	DB 3
Puerta del metal	DB 6
Puerta del metal en la	DB 12

pared de ladrillo	
Cuerpo humano	DB 3

Cada sitio examinado tiene diversos niveles de distorsión de trayectoria múltiple, la señal pierde, y ruido de la señal. Los hospitales son típicamente el entorno más desafiador para examinar debido a la alta distorsión de trayectoria múltiple, pérdidas de la señal y ruido de la señal. Los hospitales duran para examinar, para requerir una población más densa de Puntos de acceso, y para requerir los estándares de mayor rendimiento. La fabricación y las plantas de producción son las siguientes lo más difícilmente posible a examinar. Estos sitios tienen generalmente apartadero del metal y muchos metal los objetos en el suelo, que dan lugar a las señales reflejadas que reconstruyen la distorsión de trayectoria múltiple. Los edificios de oficinas y los sitios de la hospitalidad tienen generalmente la alta atenuación de la señal pero un grado menor de distorsión de trayectoria múltiple.

[Información Relacionada](#)

- [Implementación de Cisco 440X Series Cisco 440X Series que despliegan](#)
- [Diseño de red de la referencia de la solución](#)
- [Especificaciones de sistema de comunicaciones de Vocera](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)