Implantação de telefone IP Vocera na infraestrutura UWN

Contents

Introduction

Este documento fornece considerações de projeto e diretrizes de implementação para a implementação da tecnologia Vocera® Badge Voice over WLAN (VoWLAN) na infraestrutura Cisco Unified Wireless Network.

Nota: O apoio aos produtos Vocera deve ser obtido diretamente dos canais de suporte da Vocera. O Suporte Técnico da Cisco não é treinado para suportar problemas relacionados à Vocera.

Este guia é um suplemento do Guia de implantação do controlador de LAN sem fio da Cisco e aborda apenas os parâmetros de configuração que são específicos dos dispositivos VoWLAN Vocera em uma arquitetura leve. Consulte Implantação de Cisco 440X Series Wireless LAN Controllers para obter mais informações.

Prerequisites

Requirements

Supõe-se que os leitores estejam familiarizados com os termos e conceitos apresentados no Cisco IP Telephony SRND e no Cisco Wireless LAN SRND. .

Guia de design de UC sem fio—
http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns818/landing_wireless_uc.html

Cisco Unified Communications SRND baseado no 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 não se restringe a versões de software e hardware específicas.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Resumo executivo

Esta tabela resume as quatro principais funções e como elas se comportam em uma rede Cisco Unified Wireless.

	Controlador único	Roaming da camada 2 do controlador para o controlador	Roaming da camada 3 do controlador para o controlador
Crachá a crachá	Nenhuma configuração especial	Nenhuma configuração especial	Nenhuma configuração especial
Crachá ao telefone	Nenhuma configuração especial	Nenhuma configuração especial	Nenhuma configuração especial
Crachá para transmissão	Habilitar multicast do controlador	Habilite o comando multicast disable Vocera VLAN IGMP-Snooping ou execute 4.0.206.0 ou posterior	4.0.206.0 ou posterior
Local do crachá	Nenhuma configuração especial	Nenhuma configuração especial	Nenhuma configuração especial

Visão geral do emblema de voz

Os emblemas de comunicação permitem uma comunicação instantânea ao usuário com qualquer outro usuário de emblema, bem como integração de PBX (Private Branch Exchange) e rastreamento de localização de emblema. A utilização de uma rede sem fio 802.11b/g requer o uso de envio de pacotes unicast multicast e UDP com requisitos limitados para Qualidade de Serviço (QoS) a partir do Software de Servidor Vocera versão 3.1 (Build 1081). Os recursos de criptografia são: WEP (Wired Equivalent Privacy) de 64/128 bits, TKIP (Temporal Key Integrity

Protocol), MIC (Message Integrity Check) e CKIP (Cisco Temporal Key Integrity Protocol) combinados com os recursos de autenticação de chave pré-compartilhada WPA-PSK (Open, Wi-Fi Protected Access-Pre-shared Key), PEAP (WPA-Protected Extensible Authentication Protocol) e Lightweight Extensible Authentication Protocol (LEAP).

Com o pressionamento de um botão, o servidor Vocera responde com Vocera, que é um prompt para emitir comandos como record, onde (am) /is..., call, play, **broadcast**, **mensagens** e assim por diante. O servidor Vocera fornece os serviços necessários e/ou a configuração de chamada para concluir a solicitação.

O Sistema de Comunicação com capacidade para 802.11b da Vocera utiliza a compressão de voz proprietária e o uso de um intervalo de portas UDP. O software Sistema Vocera é executado em um servidor Windows que gerencia a configuração de chamadas, a conexão de chamadas e os perfis de usuário. Eles fizeram uma parceria com o software de reconhecimento de voz e impressão de voz Nuance 8.5 para habilitar comunicações de voz de emblema. A Vocera recomenda um servidor Windows separado para executar o software Vocera Telephony Solutions para habilitar a conectividade do Plain Old Telephone Service (POTS) com os emblemas.

Considerações sobre a capacidade das chamadas de voz

Consulte a seção Dimensionamento de Rede deste documento para obter mais detalhes.

Capacidade do servidor de comunicações Vocera

Consulte as especificações do sistema de comunicações Vocera para obter mais informações sobre a matriz de dimensionamento do servidor Vocera.

A solução Vocera

O Crachá Vocera utiliza a entrega de pacotes unicast e multicast para fornecer vários recursos importantes que compõem essa solução completa. Aqui estão quatro dos recursos essenciais que dependem da entrega adequada de pacotes. Também é fornecida uma compreensão básica de como cada recurso usa a rede subjacente para fornecimento e funcionalidade.

- Badge to Badge Communications—Quando um usuário do Vocera chama outro usuário, o crachá primeiro entra em contato com o servidor Vocera, que procura o endereço IP do crachá do chamador e entra em contato com o usuário do crachá para perguntar ao usuário se ele pode atender uma chamada. Se a chamada aceitar a chamada, o servidor Vocera notifica o crachá chamador do endereço IP do crachá de chamada para configurar a comunicação direta entre os crachás sem nenhuma intervenção adicional do servidor. Toda comunicação com o servidor Vocera usa o codec G.711 e toda comunicação emblemática usa um codec proprietário Vocera.
- Comunicação de telefonia emblema—Quando um servidor de telefonia vocérica é instalado e configurado com uma conexão com um PBX, um usuário pode chamar ramais internos do PBX ou linhas telefônicas externas. A Vocera permite que os usuários façam chamadas dizendo os números (cinco, seis, três, dois) ou criando uma entrada de catálogo de endereços na base de dados Vocera para a pessoa ou função nesse número (por exemplo, farmácia, casa, pizza), o servidor Vocera determina o número que está sendo chamado, seja

interceptando os números na extensão ou procurando o nome na base de dados e selecionando o número. O servidor Vocera então passa essas informações para o servidor Vocera Telephony que se conecta ao PBX e gera a sinalização de telefonia apropriada (por exemplo, DTMF). Toda comunicação entre o crachá e o servidor Vocera e o servidor Vocera e o servidor Vocera Telephony usam o codec G.711 sobre UDP unicast.

- Difusão de Vocera—Um usuário do Crachá de Vocera pode ligar e se comunicar com um grupo de usuários do crachá de Vocera ao mesmo tempo, usando o comando Broadcast. Quando um usuário envia broadcasts para um grupo, o crachá do usuário envia o comando para o servidor Vocera, que então procura os membros de um grupo, determina quais membros do grupo estão ativos, atribui um endereço multicast para usar nesta sessão de broadcast e envia uma mensagem para cada crachá do usuário ativo instruindo-o a se juntar ao grupo multicast com o endereço multicast atribuído.
- Função de localização do crachá—O servidor Vocera rastreia o ponto de acesso ao qual cada crachá ativo está associado à medida que cada crachá envia uma manutenção de 30 segundos ao servidor com o BSSID associado. Isso permite que o sistema Vocera estime aproximadamente a localização de um usuário de crachá. Esta função tem um grau de precisão relativamente baixo porque um Badge pode não estar associado ao ponto de acesso ao qual ele está mais próximo.

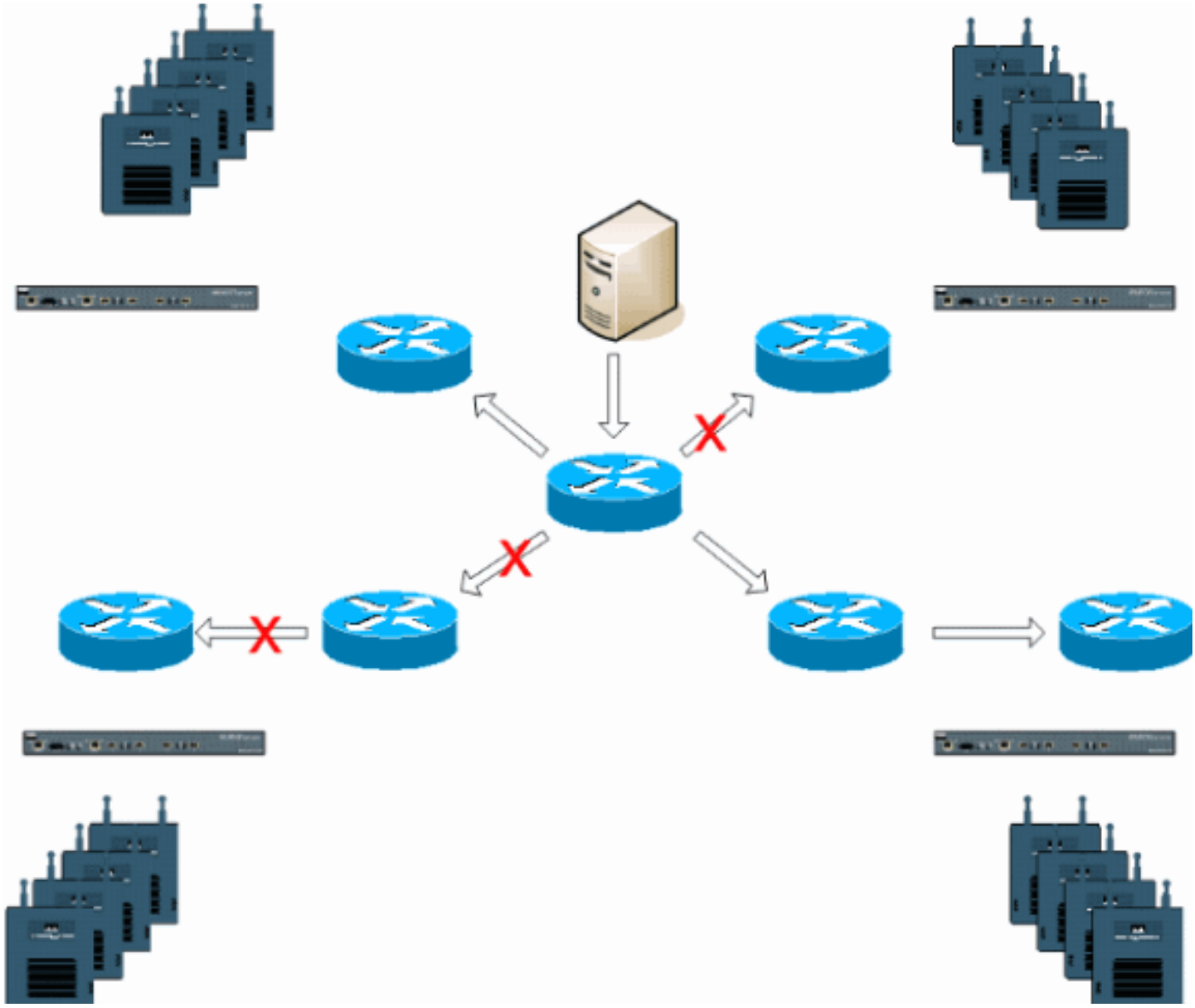
Planejamento de infraestrutura da Vocera

O whitepaper Vocera Vocera Infrastructure Planning Guide , descreve os requisitos mínimos da pesquisa de site que mostram que o crachá deve ter uma intensidade mínima de sinal de recepção de -65 dBm, uma relação sinal-ruído maior que 25 db e sobreposição adequada de ponto de acesso e separação de canais. Embora os crachás utilizem uma antena omni direcional semelhante à de um notebook usado para o levantamento do local, não mimetizam muito bem o comportamento do crachá, dados os efeitos dos usuários na intensidade do sinal. Considerando esse requisito exclusivo e esse comportamento do dispositivo transmissor, o uso da arquitetura da Cisco e do gerenciamento de recursos de rádio é ideal para garantir que não haja características incomuns de site de radiofrequência (RF).

O crachá Vocera é um dispositivo de baixa potência, usado ao lado do corpo com capacidades limitadas de correção de erros de sinal. Os requisitos Vocera neste documento podem ser facilmente alcançados. No entanto, ele pode ficar sobrecarregado se houver muitos SSIDs para que ele processe e permita que o crachá funcione com eficiência.

Visão geral da arquitetura

Figura 1 - Encaminhamento e remoção multicast gerais com conexão sem fio LWAPP (Lightweight Access Point Protocol)



Multicast em uma implantação LWAPP

Énecessário compreender o multicast em uma implantação LWAPP para implantar a função de broadcast Vocera. Este documento aborda posteriormente as etapas essenciais para habilitar o multicast na solução baseada em controlador. Atualmente, há dois métodos de entrega que o controlador LWAPP usa para fornecer multicast aos clientes:

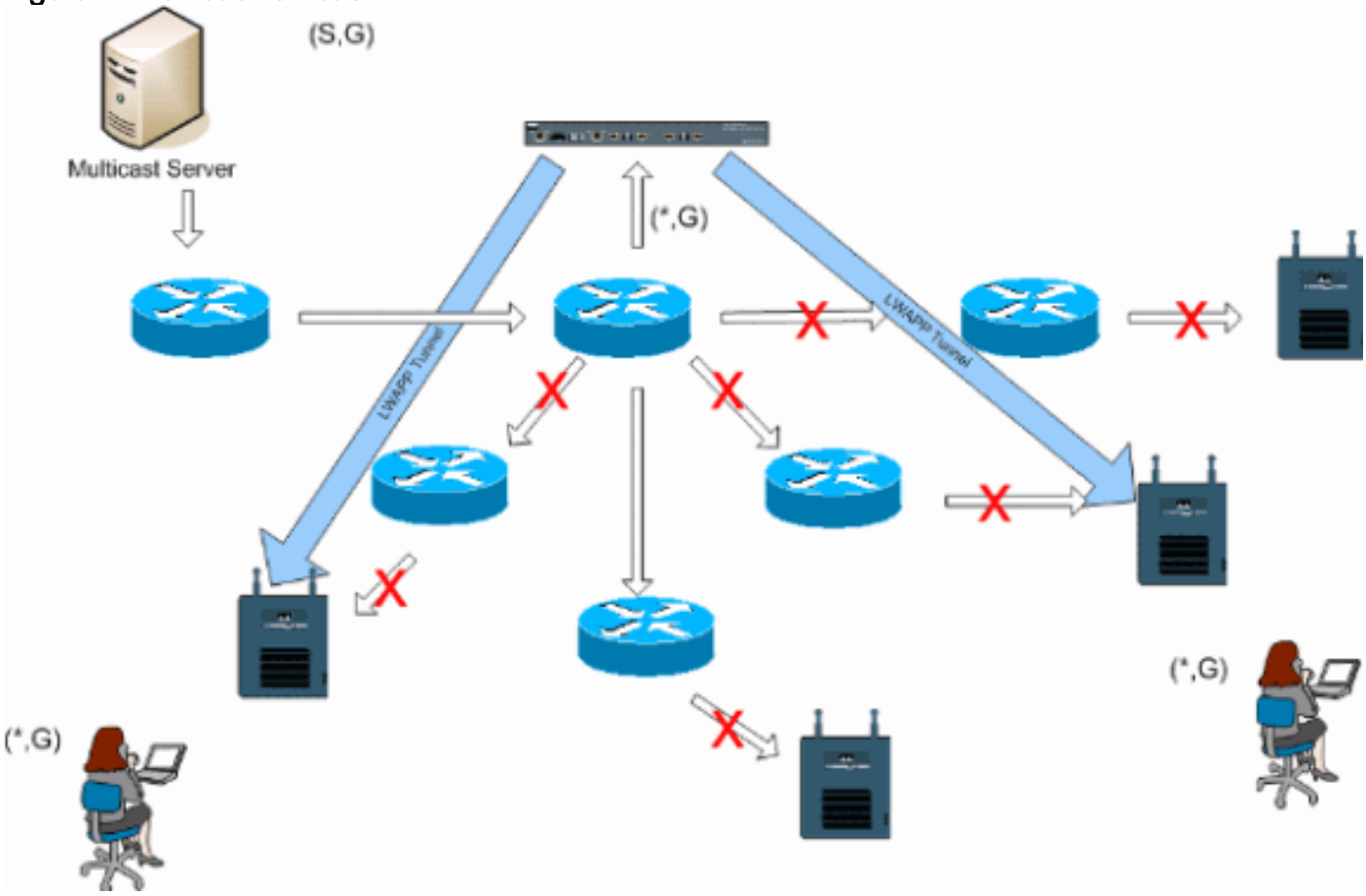
- Unicast-Multicast
- Multicast-Multicast

Método de Entrega Unicast-Multicast

O método de entrega unicast-multicast cria uma cópia de cada pacote multicast e a encaminha a cada ponto de acesso. Quando um cliente envia uma junção multicast à LAN sem fio, o ponto de acesso encaminha essa junção através do túnel LWAPP para o controlador. A controladora liga essa união multicast à conexão de rede local diretamente conectada que é a VLAN padrão para a WLAN associada do cliente. Quando um pacote multicast IP chega da rede ao controlador, o controlador replica esse pacote com um cabeçalho LWAPP para cada ponto de acesso que tenha um cliente dentro do domínio sem fio que se juntou a esse grupo específico. Quando a origem do multicast também é um receptor no domínio sem fio, esse pacote também é duplicado e

encaminhado de volta ao mesmo cliente que enviou esse pacote. Para crachás da Vocera, esse não é o método preferencial de entrega multicast na solução de controlador LWAPP. O método de entrega unicast funciona com pequenas implantações. No entanto, devido à sobrecarga considerável no Wireless LAN Controller (WLC), esse nunca é o método de entrega multicast recomendado.

Figura 2: Multicast-Unicast LWAPP



Observação: se as VLANs do grupo de AP estiverem configuradas e uma junção IGMP for enviada de um cliente através do controlador, ela será colocada na VLAN padrão da WLAN em que o cliente está. Portanto, o cliente pode não receber esse tráfego multicast, a menos que seja um membro desse domínio de broadcast padrão.

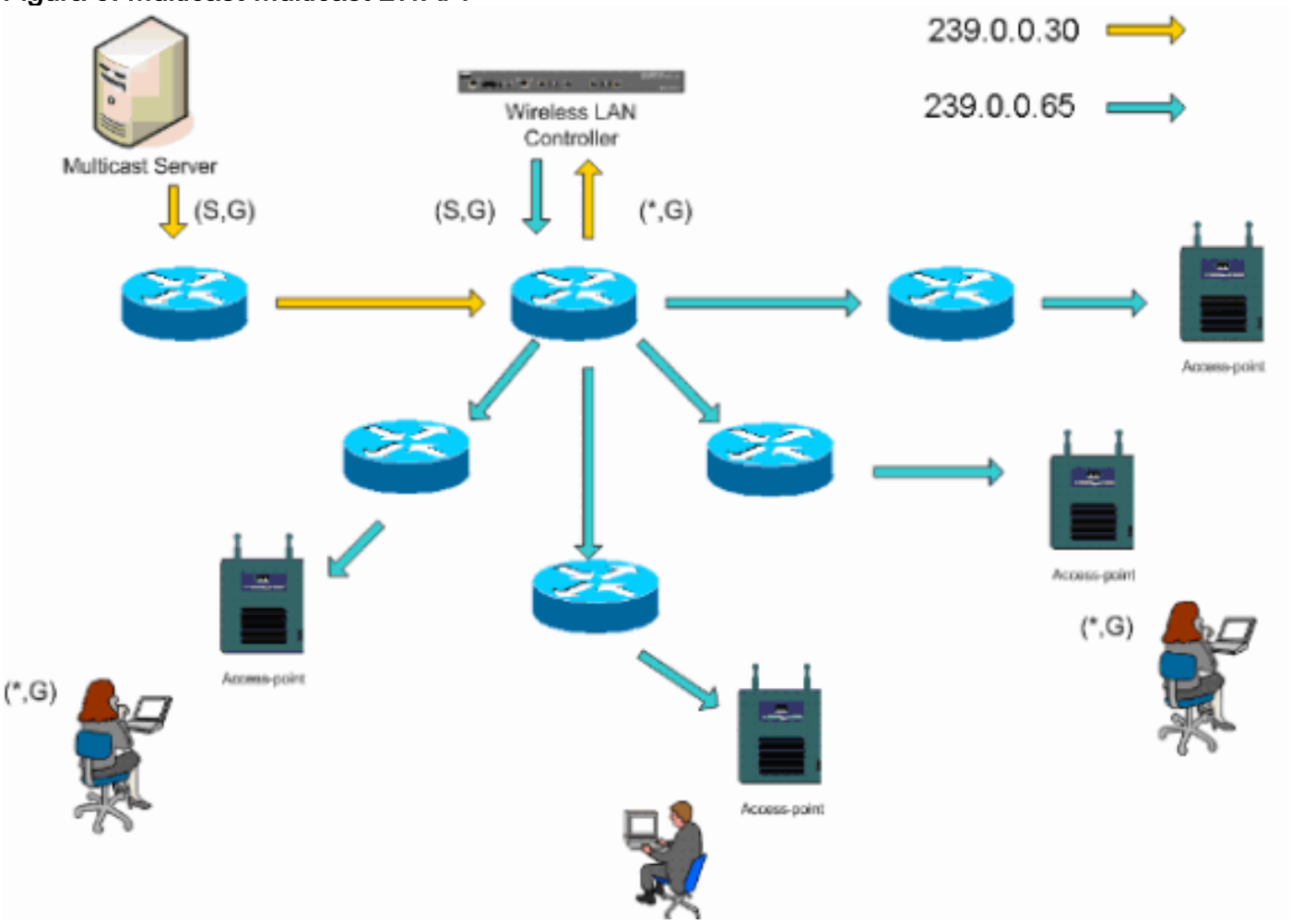
Método de entrega multicast-multicast

O método de entrega multicast-multicast não exige que o controlador replique cada pacote multicast recebido. O controlador é configurado para um endereço de grupo multicast não usado do qual cada ponto de acesso se torna membro. Com a Figura 3, o grupo multicast definido da WLC para o ponto de acesso é 239.0.0.65. Quando um cliente envia uma junção multicast para a WLAN, o ponto de acesso encaminha essa junção através do túnel LWAPP para a controladora. O controlador encaminha esse protocolo de camada de enlace para sua conexão de rede local diretamente conectada que é a VLAN padrão para a WLAN associada do cliente. O roteador que é local para a controladora adiciona esse endereço de grupo multicast àquela interface para encaminhamento ((*,G)). Com a Figura 3, o exemplo de união multicast foi enviado para o grupo multicast 239.0.0.30. Quando a rede agora encaminha o tráfego multicast, o endereço multicast 239.0.0.30 é encaminhado ao controlador. Em seguida, o controlador encapsula o pacote multicast em um pacote multicast LWAPP endereçado ao endereço do grupo multicast (por exemplo, aqui está 239.0.0.65) configurado no controlador e encaminhado à rede. Cada ponto de acesso no controlador recebe esse pacote como membro do grupo multicast de controladores. O

ponto de acesso encaminha o pacote multicast de clientes/servidores (por exemplo, aqui está 239.0.0.30) como um broadcast para a WLAN/SSID identificada no pacote multicast LWAPP.

Observação: se você configurar incorretamente sua rede multicast, poderá acabar recebendo pacotes multicast de outro ponto de acesso do controlador. Se o primeiro controlador tiver que fragmentar esse pacote multicast, o fragmento será encaminhado à rede e cada ponto de acesso deverá gastar tempo para descartar esse fragmento. Se você permitir todo o tráfego, como qualquer coisa do intervalo multicast 224.0.0.x, ele também é encapsulado e encaminhado posteriormente por cada ponto de acesso.

Figura 3: Multicast-Multicast LWAPP



Configuração Multicast de Roteador e Switch

Este documento não é um guia de configuração de multicast de rede. Consulte Configurando o Roteamento Multicast IP para obter um histórico de implementação completo. Este documento aborda os conceitos básicos para habilitar o multicast em seu ambiente de rede.

Ativar o roteamento multicast IP

O roteamento multicast IP permite que o software Cisco IOS® encaminhe pacotes multicast. O comando de configuração global **ip multicast-routing** é necessário para permitir que o multicast funcione em qualquer rede habilitada para multicast. O comando **ip multicast-routing** deve ser ativado em todos os roteadores da rede entre as WLCs e seus respectivos pontos de acesso.

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

Ativar PIM em uma interface

Isso ativa a interface de roteamento para a operação do Internet Group Management Protocol (IGMP). O modo Protocol Independent Multicast (PIM) determina como o roteador preenche sua tabela de roteamento multicast. O exemplo fornecido aqui não exige que o ponto de encontro (RP) seja conhecido para o grupo multicast e, portanto, o modo denso escasso é o mais desejável, dada a natureza desconhecida do seu ambiente multicast. Esta não é uma recomendação multicast para ser configurada para funcionar, embora a interface da Camada 3 diretamente conectada ao seu controlador deva ser PIM ativado para que o multicast funcione. Todas as interfaces entre suas WLCs e seus respectivos pontos de acesso devem ser ativadas.

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

Desabilitar rastreamento IGMP de VLAN de Switch

O rastreamento de IGMP permite que uma rede comutada com multicast habilitado limite o tráfego para as portas de switch que têm usuários que desejam que o multicast seja visto enquanto os pacotes multicast são removidos das portas de switch que não desejam ver o fluxo multicast. Em uma implantação de Vocera, pode ser indesejável ativar o rastreamento de CGMP ou IGMP na porta do switch upstream para o controlador com versões de software anteriores à 4.0.206.0.

O roaming e o multicast não são definidos com um conjunto de requisitos para verificar se o tráfego multicast pode seguir um usuário inscrito. Embora o crachá do cliente esteja ciente de que ele fez roaming, ele não encaminha outro ingresso IGMP para garantir que a infraestrutura de rede continue a entregar o tráfego multicast (broadcast Vocera) ao crachá. Ao mesmo tempo, o ponto de acesso do LWAPP não envia uma consulta multicast geral ao cliente com roaming para solicitar essa junção do IGMP. Com um projeto de rede Vocera de Camada 2, a desativação da espionagem de IGMP permite que o tráfego seja encaminhado a todos os membros da rede Vocera, independentemente de onde eles façam roaming. Isso garante que o recurso de transmissão Vocera funcione independentemente de onde o cliente faça roaming. Desativar globalmente a espionagem de IGMP é uma tarefa muito indesejável. Recomenda-se que o rastreamento IGMP seja desabilitado somente na VLAN Vocera conectada diretamente a cada WLC.

Consulte Configurando o IGMP Snooping para obter mais informações.

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

Aprimoramentos multicast na versão 4.0.206.0 e posterior

Com a versão 4.0.206.0, a Cisco introduz uma consulta IGMP para permitir que os usuários façam roaming na Camada 2 enviando uma consulta IGMP geral quando isso ocorrer. Em seguida, o cliente responde com o grupo IGMP do qual é membro e isso é ligado à rede com fio conforme descrito anteriormente neste documento. Quando um cliente faz roaming para um controlador que não tem conectividade de Camada 2, ou um roaming de Camada 3, o roteamento síncrono é adicionado para pacotes de origem multicast. Quando um cliente, que concluiu um

roaming de Camada 3, origina um pacote multicast da rede sem fio, o controlador externo encapsula esse pacote na Ethernet sobre IP (EoIP) no túnel IP para o controlador âncora. O controlador âncora encaminha isso aos clientes sem fio associados localmente, bem como conecta isso de volta à rede com fio, onde é roteado usando métodos normais de roteamento multicast.

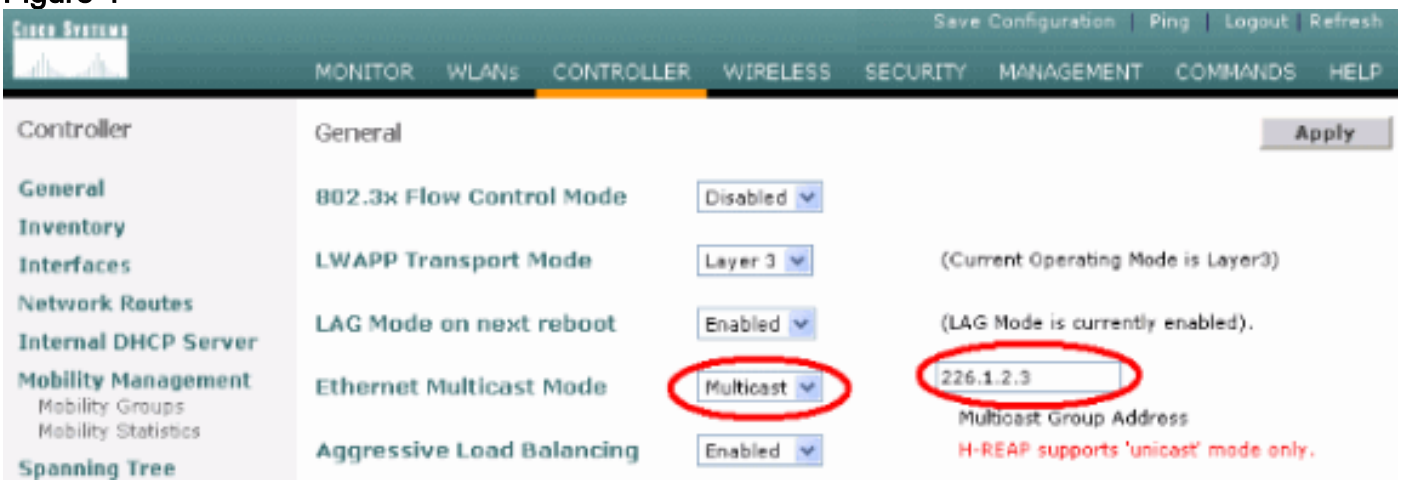
Cenários de implantação

Esses três cenários de implantação abrangem as melhores práticas e parâmetros de projeto para ajudar com uma implantação bem-sucedida do Crachá de Vocera:

- Implantação de controlador único
- Implantação da camada 2 de vários controladores
- Implantação da camada 3 de vários controladores

Éessencial compreender como os recursos do emblema Vocera interagem em um ambiente MAC dividido do LWAPP. Com todos os cenários de implantação, o multicast deve ser ativado e o balanceamento de carga agressivo deve ser desativado. Todas as WLANs de emblema devem estar contidas no mesmo domínio de broadcast em toda a rede.

Figure 4



Implantação de controlador único

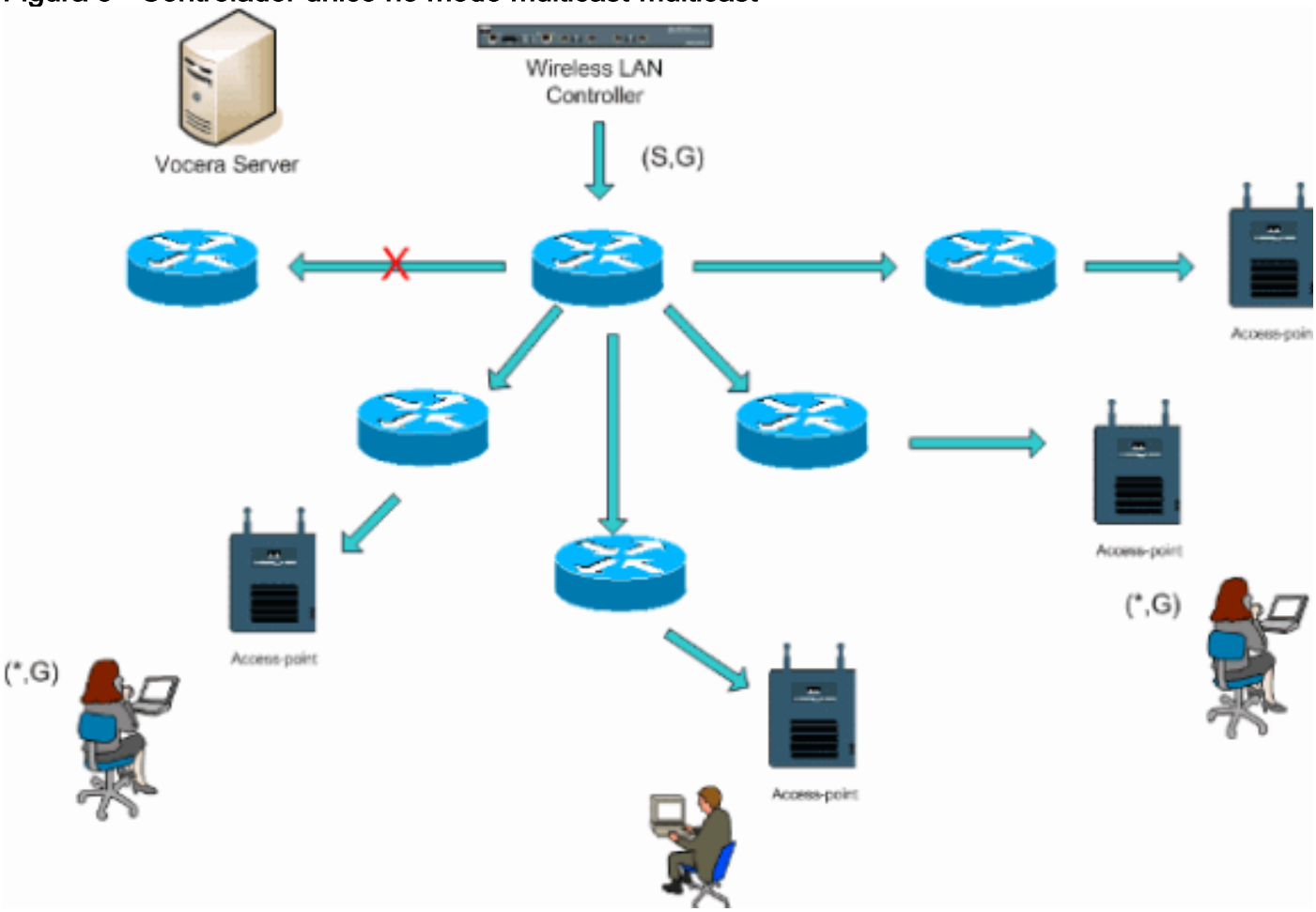
Este é o cenário de implantação mais direto. Ele permite que você implante a solução de emblema Vocera com pequenas preocupações de implantação. Sua rede deve ser habilitada para o roteamento multicast IP somente para permitir que os pontos de acesso recebam os pacotes multicast LWAPP. Se necessário, você pode limitar a complexidade do multicast da rede configurando todos os roteadores e switches com o grupo multicast dos controladores.

Com o multicast configurado globalmente no controlador, o SSID correto, as configurações de segurança e todos os pontos de acesso registraram a solução Vocera Badge e todas as suas funções operam conforme esperado. Com a função de difusão Vocera, um usuário faz roaming e o tráfego multicast segue como esperado. Não é necessário definir configurações adicionais para permitir que esta solução funcione corretamente.

Quando um crachá de voz envia uma mensagem de multicast, como faz com o broadcast de voz, ele é encaminhado ao controlador. Em seguida, o controlador encapsula esse pacote multicast em um pacote multicast LWAPP. A infraestrutura de rede encaminha esse pacote para cada ponto de acesso conectado a esse controlador. Quando o ponto de acesso recebe esse pacote,

ele examina o cabeçalho multicast do LWAPP para determinar para qual WLAN/SSID ele então envia esse pacote.

Figura 5 - Controlador único no modo multicast-multicast



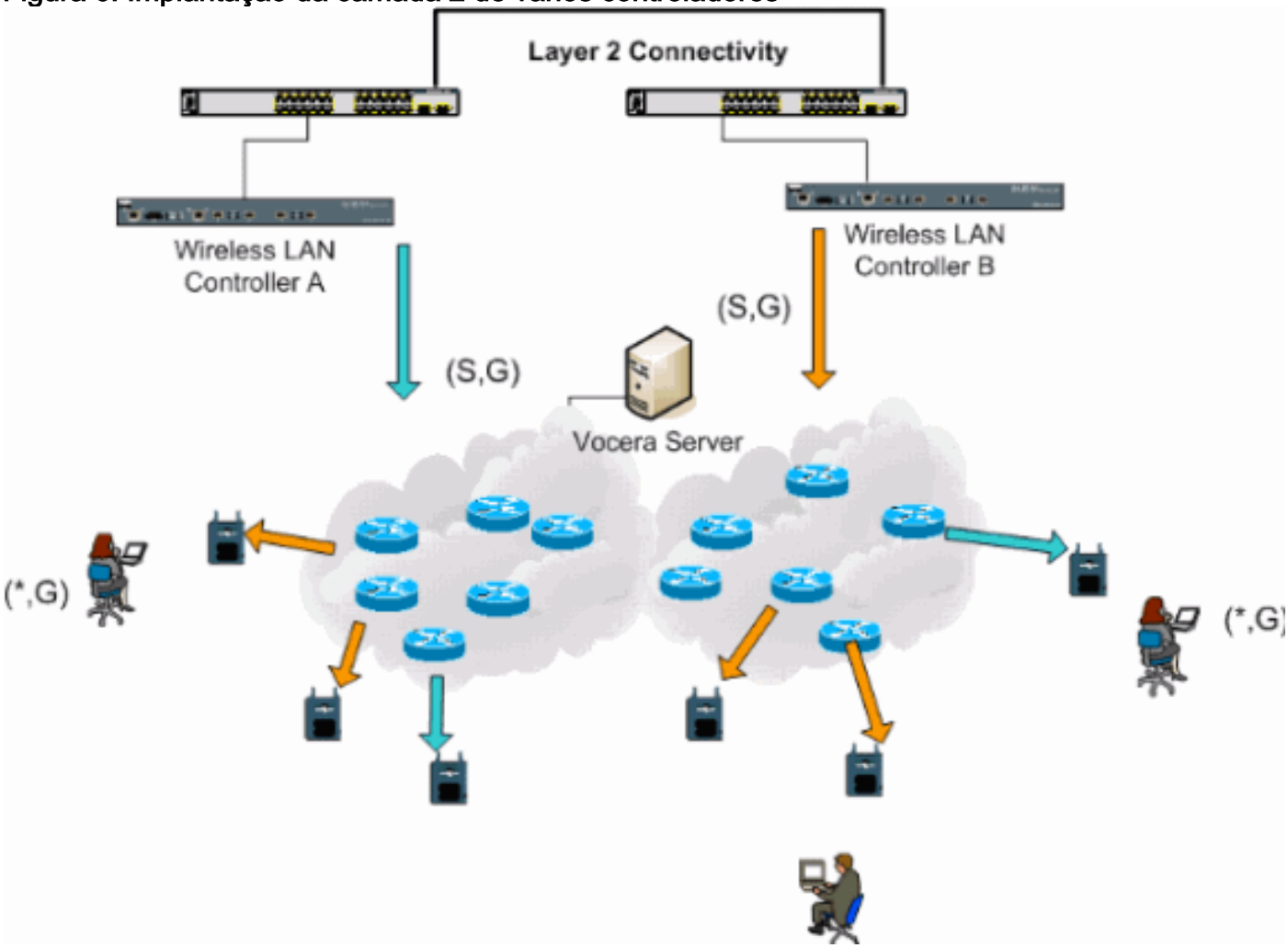
Implantação da camada 2 de vários controladores

Vários controladores devem ter conectividade entre si através do mesmo domínio de broadcast da camada 2. Ambos os controladores estão configurados para multicast como mostrado, usando os grupos de multicast de access point idênticos em cada controlador para limitar a fragmentação. Com a suposição de que esse domínio de broadcast de Camada 2 está conectado através de um switch comum ou de um conjunto comum de switches, a espionagem de CGMP/IGMP nesses switches deve ser desativada para essa única VLAN ou executar o software 4.0.206.0 ou posterior da WLC. Com a função de transmissão Vocera e um roaming de usuário de um ponto de acesso em um controlador para um ponto de acesso em um controlador diferente, não há mecanismo para que as junções IGMP sejam encaminhadas para a nova porta de Camada 2 para que o rastreamento IGMP funcione. Sem um pacote IGMP que chegasse ao CGMP de upstream ou switch compatível com IGMP, o grupo multicast especificado não é encaminhado ao controlador e, portanto, não é recebido pelo cliente. Em alguns casos, isso pode funcionar, se um cliente que faz parte do mesmo grupo de broadcast Vocera já tiver enviado esse pacote IGMP antes que o cliente de roaming faça roaming para o novo controlador Com as vantagens da versão 4.0.206.0, um cliente que faz roaming para outro controlador como um roaming de Camada 2 recebe uma consulta IGMP geral imediatamente após a autenticação. Em seguida, o cliente deve responder com os grupos interessados, e o novo controlador é ligado ao switch conectado localmente. Isso permite as vantagens do IGMP e do CGMP em seus switches upstream.

Você pode criar SSIDs de crachá adicionais e domínios de Camada 2 para redes de crachá

separadas, desde que sua rede esteja configurada para transmitir o tráfego multicast apropriadamente. Além disso, cada domínio de broadcast da Camada 2 Vocera criado deve existir em todos os lugares em que um controlador está conectado à rede para não quebrar o multicast.

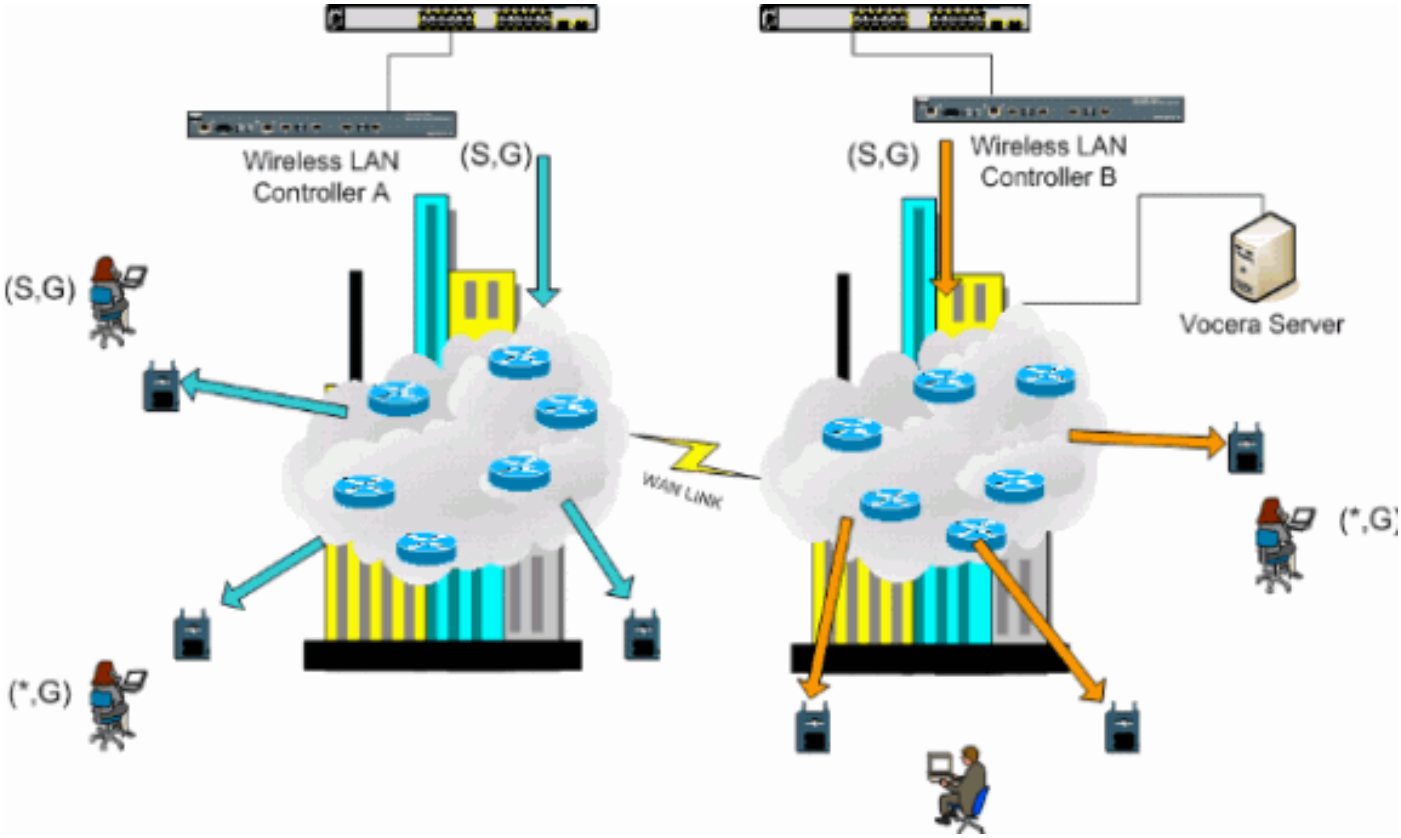
Figura 6: Implantação da camada 2 de vários controladores



Implantação da camada 3 de vários controladores

A estratégia de implantação de roaming de camada 3 deve ser usada somente com roaming de controlador para controlador com o software WLC versão 4.0.206.0 ou posterior. Se um cliente que foi conectado ao grupo de broadcast Vocera e recebe o fluxo multicast apropriado e os roaming para outro controlador como um roaming de Camada 3 com o roaming de Camada 3 do LWAPP configurado, ele será consultado para grupos de multicast interessados. O cliente, ao fazer a origem para o mesmo grupo de broadcast Vocera, tem esses pacotes entregues ao controlador de âncora através do túnel EoIP e tem esses pacotes roteados através de métodos normais de roteamento multicast.

Figura 7: Implantação da camada 3 de vários controladores



Implantações de VoWLAN: Recomendações da Cisco

As redes de telefonia IP sem fio exigem um planejamento cuidadoso de RF. Frequentemente, é necessário realizar uma pesquisa completa no local da voz para determinar os níveis adequados de cobertura sem fio e identificar as fontes de interferência. As opções de posicionamento do ponto de acesso e seleção da antena podem ser muito facilitadas com a ajuda dos resultados de uma pesquisa válida no local da voz. A consideração mais importante é a potência de transmissão do telefone sem fio. Idealmente, o telefone aprende a potência de transmissão do ponto de acesso e ajusta sua potência de transmissão para a do ponto de acesso.

Embora a maioria das redes sem fio atuais seja implantada após uma ampla pesquisa de site de RF, elas também são feitas para manter o serviço de dados em mente. Os telefones VoWLAN provavelmente têm características de roaming diferentes e requisitos de cobertura diferentes dos de um adaptador WLAN típico para um cliente móvel como um laptop. Portanto, uma pesquisa de local adicional para voz é geralmente recomendada para se preparar para os requisitos de desempenho de vários clientes de VoWLAN. Essa pesquisa adicional oferece a oportunidade de ajustar os access points para garantir que os telefones VoWLAN tenham cobertura RF e largura de banda suficientes para fornecer a qualidade de voz adequada.

Para obter informações adicionais sobre as considerações de projeto de RF, consulte o capítulo sobre Considerações de design de radiofrequência (RF) de WLAN no Guia de design de LAN sem fio da Cisco, disponível em http://cisco.com/go/srnd.

Recomendações para edifícios, hospitais e depósitos em vários andares

Considere os fatores listados nesta seção ao pesquisar edifícios, hospitais e depósitos de vários andares.

Métodos e materiais de construção

Muitos aspectos da construção do prédio são desconhecidos ou ocultos do levantamento do local, portanto, talvez seja necessário adquirir essas informações de outras fontes (como desenhos arquitetônicos). Alguns exemplos de métodos e materiais típicos de construção que afetam a área de alcance e cobertura dos pontos de acesso incluem filmes metálicos em vidros de janelas, vidros com chumbo, paredes de aço, pisos de cimento e paredes com reforço de aço, isolamento com bobinas, escadas e eixos de elevadores, encanamentos e acessórios, entre outros.

Inventário

Vários tipos de inventário podem afetar a gama de RF, especialmente aqueles com alto teor de aço ou água. Alguns itens a serem observados incluem caixas de papelão, alimentos para animais de companhia, tinta, produtos petrolíferos, peças de motores e assim por diante.

Níveis de inventário

Certifique-se de executar uma pesquisa de site nos níveis de estoque máximo ou nos momentos de maior atividade. Um depósito em um nível de estoque de 50% tem uma área de RF muito diferente do mesmo depósito em um nível de estoque de 100%.

Níveis de atividade

Da mesma forma, uma área de escritório após horas (sem pessoas) tem uma pegada de RF diferente da mesma área cheia de pessoas durante o dia. Embora muitas partes da pesquisa de site possam ser realizadas sem ocupação total, é essencial realizar a verificação da pesquisa de site e ajustar os valores-chave durante um período em que a localização é ocupada. Quanto mais altos os requisitos de utilização e a densidade dos usuários, mais importante é ter uma solução de diversidade bem projetada. Quando há mais usuários presentes, mais sinais são recebidos no dispositivo de cada usuário. Sinais adicionais causam mais contenção, mais pontos nulos e mais distorção de multipath. A diversidade no access point (antenas) ajuda a minimizar essas condições.

Edifícios em vários andares

Tenha em mente estas diretrizes ao realizar uma pesquisa de site para um edifício de escritório típico:

- Os eixos do elevador bloqueiam e refletem sinais de RF.
- Salas de fornecimento com inventário absorvem sinais.
- Os escritórios internos com paredes rígidas absorvem sinais de RF.
- Salas de descanso (cozinhas) podem produzir interferência de 2,4 GHz através do uso de fornos micro-ondas.
- Os laboratórios de teste podem produzir interferência de 2,4 GHz ou 5 GHz, criando distorção de multipath e sombras de RF.
- Os cubículos tendem a absorver e bloquear sinais.
- As salas de conferência exigem alta cobertura de access point porque são áreas de alta utilização.

Deve ser administrada precaução extra ao pesquisar instalações em vários andares. Os pontos de acesso em diferentes andares podem interferir entre si tão facilmente quanto os pontos de acesso localizados no mesmo andar. É possível usar esse comportamento a seu favor durante

uma pesquisa. Usando antenas de ganho mais alto, pode ser possível penetrar no chão e no teto e fornecer cobertura para andares acima, bem como abaixo do piso onde o ponto de acesso é montado. Tenha cuidado para não sobrepor canais entre pontos de acesso em diferentes andares ou pontos de acesso no mesmo andar. Em prédios com vários usuários, pode haver preocupações com segurança que exigem o uso de potências de transmissão mais baixas e antenas de ganho mais baixo para manter os sinais fora dos escritórios vizinhos.

Hospitais

O processo de pesquisa de um hospital é muito semelhante ao de uma empresa, mas o layout de uma instalação hospitalar tende a ser diferente das seguintes maneiras:

- Os edifícios hospitalares tendem a passar por muitos projetos de reconstrução e acréscimos. Cada construção adicional é susceptível de ter diferentes materiais de construção com diferentes níveis de atenuação.
- A penetração de sinais através de paredes e pisos nas áreas dos pacientes é normalmente mínima, o que ajuda a criar microcélulas e variações de vários caminhos.
- A necessidade de largura de banda aumenta com o uso cada vez maior de equipamentos de ultrassom WLAN e outros aplicativos portáteis de imagem. A necessidade de largura de banda aumenta com a adição de voz sem fio também.
- As células da área de saúde são pequenas e o roaming perfeito é essencial, especialmente com aplicativos de voz.
- A sobreposição de células pode ser alta e, assim, a reutilização de canais pode ser.
- Hospitais podem ter vários tipos de redes sem fio instaladas. Isso inclui equipamentos não 802.11 de 2,4 GHz. Esse equipamento pode causar contenção em outras redes de 2,4 GHz.
- Antenas de patch de diversidade montada na parede e antenas onidirecionais de diversidade montada no teto são populares, mas lembre-se de que a diversidade é necessária.

Armazéns

Os depósitos têm grandes áreas abertas que geralmente contêm racks de armazenamento alto. Muitas vezes, esses racks chegam quase ao teto, onde os access points são normalmente colocados. Esses racks de armazenamento podem limitar a área que o ponto de acesso pode cobrir. Nesses casos, considere colocar pontos de acesso em outros locais além do teto, como paredes laterais e pilares de cimento. Considere também estes fatores ao pesquisar um depósito:

- Os níveis de estoque afetam o número de pontos de acesso necessários. Teste a cobertura com dois ou três pontos de acesso em locais de posicionamento estimados.
- Sobreposições inesperadas de células são prováveis devido a variações de vários caminhos. A qualidade do sinal varia mais do que a intensidade desse sinal. Os clientes podem se associar e operar melhor com access points mais distantes do que com access points próximos.
- Durante uma pesquisa, os pontos de acesso e as antenas geralmente não têm um cabo de antena conectando-os. Mas em um ambiente de produção, o ponto de acesso e a antena podem exigir cabos de antena. Todos os cabos de antena apresentam perda de sinal. A pesquisa mais precisa inclui o tipo de antena a ser instalada e o comprimento do cabo a ser instalado. Uma boa ferramenta a ser usada para simular o cabo e sua perda é um atenuador em um kit de pesquisa.

Pesquisar uma fábrica é semelhante a pesquisar um depósito, exceto que pode haver muito mais

fontes de interferência de RF em uma fábrica. Além disso, os aplicativos em uma fábrica geralmente exigem mais largura de banda do que os de um depósito. Esses aplicativos podem incluir imagens de vídeo e voz sem fio. A distorção de multipath é provavelmente o maior problema de desempenho em uma instalação de fabricação.

Mecanismos de segurança suportados

Além do WEP estático e do Cisco LEAP para autenticação e criptografia de dados, os badges de voz também suportam WPA-PEAP (MS-CHAP v2)/WPA2-PSK.

Considerações do LEAP

O LEAP permite que os dispositivos sejam autenticados mutuamente (ponto de identificação para acesso e ponto de acesso para crachá) com base no nome de usuário e na senha. Na autenticação, uma chave dinâmica é usada entre o telefone e o ponto de acesso para criptografar o tráfego. No entanto, o ataque ao dicionário ASLEAP deve ser considerado quando você decidir usar o LEAP como sua solução de segurança:

Consulte Ataque de Dicionário na Vulnerabilidade do Cisco LEAP para obter mais informações.

Se o LEAP for usado, um servidor RADIUS compatível com LEAP, como o Cisco Access Control Server (ACS), é necessário para fornecer acesso ao banco de dados do usuário. O Cisco ACS pode armazenar localmente o banco de dados de nome de usuário e senha ou pode acessar essas informações de um diretório externo do Microsoft Windows NT. Ao usar LEAP, certifique-se de que senhas fortes sejam usadas em todos os dispositivos sem fio. As senhas fortes são definidas como tendo entre 10 e 12 caracteres e podem incluir caracteres maiúsculos e minúsculos, bem como caracteres especiais.

Como todos os emblemas usam a mesma senha e são armazenados no emblema, a Cisco recomenda que você use nomes de usuário e senhas diferentes em clientes de dados e clientes de voz sem fio. Essa prática ajuda a rastrear e solucionar problemas, bem como a segurança. Embora seja uma opção de configuração válida usar um banco de dados externo (fora do ACS) para armazenar os nomes de usuário e as senhas dos crachás, a Cisco não recomenda essa prática. Como o ACS deve ser consultado sempre que o distintivo trafegar entre os pontos de acesso, o atraso imprevisível para acessar um banco de dados fora do ACS pode causar atraso excessivo e má qualidade de voz.

Infraestrutura de rede sem fio

A rede de Telefonia IP sem fio, assim como uma rede de Telefonia IP com fio, exige um planejamento cuidadoso para configuração de VLAN, dimensionamento de rede, transporte multicast e opções de equipamento. Para redes de telefonia IP com e sem fio, VLANs de voz e dados separadas são geralmente a maneira mais eficaz de implantação sugerida para garantir largura de banda de rede suficiente e facilidade de solução de problemas.

VLANs de voz, dados e voz

As VLANs fornecem um mecanismo para segmentar redes em um ou mais domínios de broadcast. As VLANs são especialmente importantes para redes de telefonia IP, onde a recomendação típica é separar o tráfego de voz e dados em diferentes domínios da camada 2. A

Cisco recomenda que você configure VLANs separadas para os crachás Vocera de outro tráfego de voz e dados: uma VLAN nativa para o tráfego de gerenciamento do ponto de acesso, uma VLAN de dados para o tráfego de dados, uma VLAN de voz ou auxiliar para o tráfego de voz e uma VLAN para os badges da voz. Uma VLAN de voz separada permite que a rede aproveite a marcação da Camada 2 e fornece enfileiramento prioritário na porta do switch de acesso da Camada 2. Isso garante que a QoS apropriada seja fornecida para várias classes de tráfego e ajuda a resolver problemas de endereçamento IP, segurança e dimensionamento de rede. Os crachás de voz usam um recurso de broadcast que utiliza multicast para fornecer. Essa VLAN comum garante que, quando um crachá faz roaming entre os controladores, ela permanece parte do grupo multicast. Este último processo é discutido em detalhes quando o multicast é abordado posteriormente neste documento.

Dimensionamento de rede

O dimensionamento da rede de telefonia IP é essencial para garantir que a largura de banda e os recursos adequados estejam disponíveis para atender às demandas apresentadas pela presença de tráfego de voz. Além das diretrizes comuns de design de Telefonia IP para dimensionamento de componentes como portas de gateway PSTN, transcodificadores, largura de banda de WAN e assim por diante, leve em conta esses problemas do 802.11b quando você dimensiona sua rede de Telefonia IP sem fio. Os Crachás Vocera são um aplicativo especializado que estende o número de clientes com fio além de nossas recomendações de implantação típicas.

Número de dispositivos 802.11b por ponto de acesso

A Cisco recomenda que você não tenha mais de 15 a 25 dispositivos 802.11b por ponto de acesso.

Número de chamadas ativas por ponto de acesso

A Vocera usa dois codecs diferentes baseados em se for uma chamada emblema para emblema (proprietário de codec de taxa de bits baixa) ou uma chamada emblema para telefone (codec G.711). Esta tabela mostra uma porcentagem da largura de banda disponível por taxas de dados e fornece uma imagem mais clara do throughput esperado:

Processo de chamada	1 Mbps	2 Mbps	5.5 Mbps	11 Mbps
Crachá para telefone (G.711)	20.7%	11.8%	6,3% de	4.7%
Badge-to-Badge (proprietário codec de taxa de bits baixa)	9.4%	6.1%	4.2%	3.6%

Recomendações do switch

Observação: se você usar um Cisco Catalyst 4000 Series Switch como o roteador principal na rede, verifique se ele contém, no mínimo, um módulo Supervisor Engine 2+ (SUP2+) ou Supervisor Engine 3 (SUP3). O módulo SUP1 ou SUP2 pode causar atrasos de roaming, assim como os switches Cisco Catalyst 2948G, 2980G, 2980G-A, 4912 e 2948G-GE-TX.

Você pode criar um modelo de porta de switch para uso ao configurar qualquer porta de switch para conexão a um ponto de acesso. Este modelo deve adicionar todos os recursos básicos de

segurança e resiliência do modelo de desktop padrão. Além disso, ao conectar o ponto de acesso a um Switch Cisco Catalyst 3750, você pode otimizar o desempenho do ponto de acesso usando os comandos de QoS MLS (Multilayer Switching) para limitar a taxa de porta e mapear as configurações de CoS (Class of Service, Classe de Serviço) para DSCP (Differentiated Services Code Point, Ponto de Código de Serviços Diferenciados).

Qualquer tráfego não exigido por clientes WLAN não deve ser enviado a um ponto de acesso. Um modelo deve ser projetado de forma a ajudar a criar uma conexão de rede segura e resiliente com estes recursos:

- Retornar configurações de porta ao padrão — Impede conflitos de configuração limpando qualquer configuração de porta pré-existente.
- Desabilitar Dynamic Trunking Protocol (DTP) — Desabilita o entroncamento dinâmico, que não é necessário para a conexão com um ponto de acesso.
- Disable Port Aggregation Protocol (PagP) — O PagP é ativado por padrão, mas não é necessário para portas de usuário.
- Ativar Port Fast—Permite que um switch retome rapidamente o tráfego de encaminhamento se um link de spanning tree cair.
- Configurar VLAN sem fio—Cria uma VLAN sem fio exclusiva que isola o tráfego sem fio de outros dados, voz e VLANs de gerenciamento. Isso isola o tráfego e garante maior controle do tráfego.
- Habilitar qualidade de serviço (QoS); não confie na porta (marque para 0)—Garante o tratamento apropriado do tráfego de alta prioridade, incluindo softphones, e evita que os usuários consumam largura de banda excessiva reconfigurando seus PCs.

Os switches de alimentação em linha WS-C3750-48PS-S podem ser usados para fornecer energia a pontos de acesso capazes de receber energia em linha.

O Catalyst 6500 permite que você encaminhe pacotes em taxa de linha com todos os recursos descritos aqui, bem como integrando vários módulos de serviço. O Wireless Service Module (WiSM) permite que você tenha dois controladores cada um com a capacidade de controlar 150 access points cada um. Com até cinco WiSMs por chassi, você pode controlar mais de 1.500 access points que suportam 50.000 clientes em uma única arquitetura de comutação de alto desempenho.

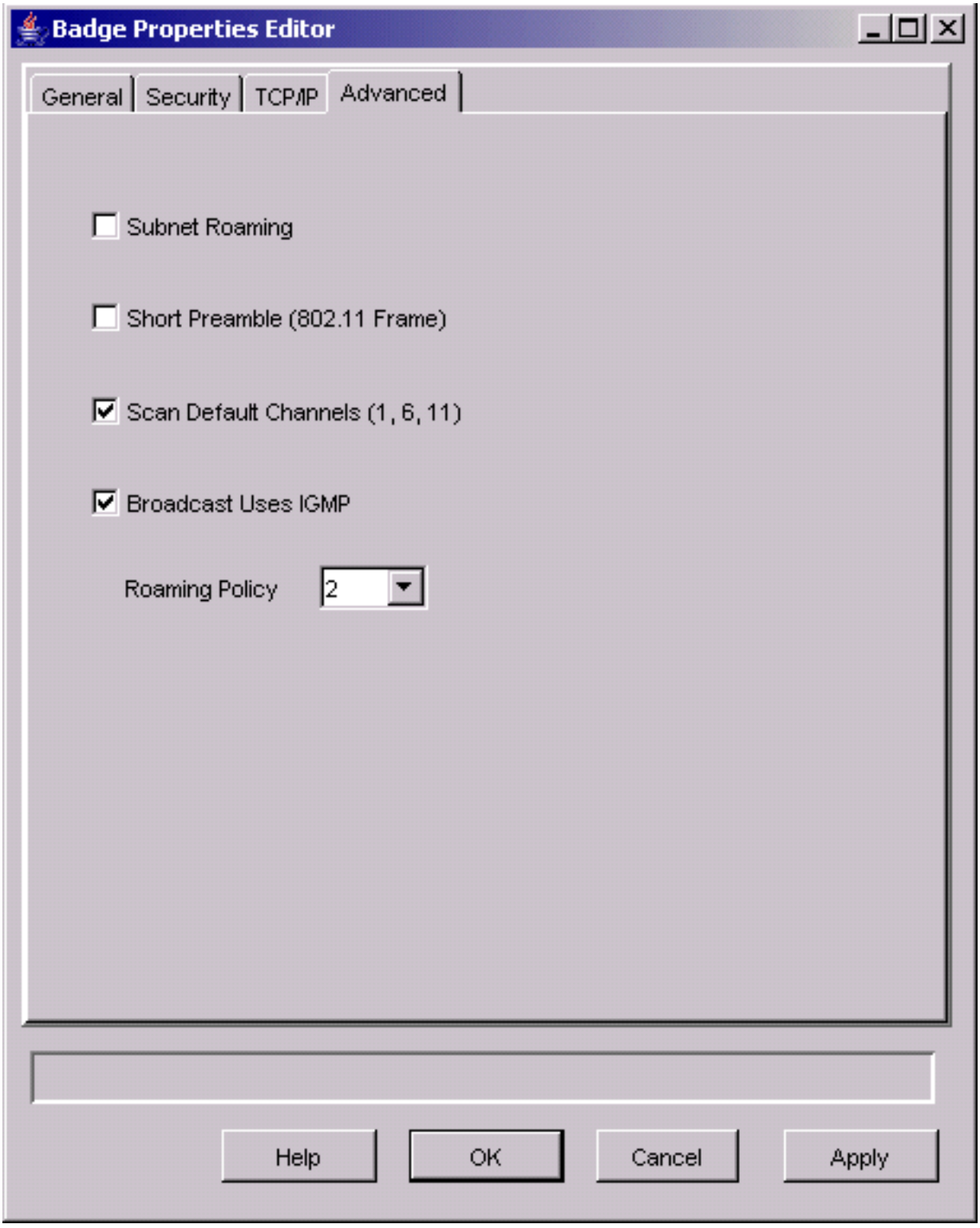
Implantações e configuração

Configuração do emblema

O utilitário de configuração de emblema de voz (BCU) e a configuração do emblema podem introduzir roaming e latência no seu ambiente se isso for feito incorretamente. Usando o BCU e o Editor de propriedades do emblema (BPE), verifique estas configurações (consulte a Figura 8):

- **O roaming de sub-rede** está desativado.
- **Scan Default Channels (1,6,11)** está marcado.
- **Broadcast Usa IGMP** está ativado.
- A política de roaming está definida como **2** ou superior.

Figura 8 - Guia Avançado do Vocera BCU



Quando o **roaming de sub-rede** é verificado, ele instrui o crachá a solicitar um novo endereço IP após cada roaming. No ambiente LWAPP, a infraestrutura ajuda a manter a conectividade do cliente na camada 3. Quando um cliente de voz deve esperar que o servidor DHCP responda antes de poder enviar ou receber pacotes, o atraso e o jitter são apresentados. Se **Scan Default Channels (1,6,11)** não estiver marcado, o crachá verificará todos os canais 802.11b quando o crachá procurar roaming. Isso evita o encaminhamento de pacotes e roaming transparente.

Ajustar AutoRF para o seu ambiente

Conforme descrito na seção Recomendações deste documento, é importante entender que cada site tem suas próprias características de RF. O AutoRF ou o Radio Resource Management (RRM)

podem precisar de ajuste, com o entendimento de que cada site é diferente e o AutoRF/RRM deve ser ajustado para o seu ambiente.

Antes de ajustar o AutoRF, consulte Gerenciamento de recursos de rádio em Redes sem fio unificadas para obter mais informações.

O RRM permite ajustar a potência de transmissão de cada ponto de acesso, ajustando a intensidade com que cada ponto de acesso ouve seu terceiro vizinho mais forte. Esse valor só pode ser ajustado da CLI usando o comando **config advanced 802.11b tx-power-threshold** conforme descrito em Tx Power Level Assignment Settings.

Antes de ajustar o AutoRF, acompanhe o local de implantação usando o crachá Vocera usado pelo usuário final e use uma ferramenta de pesquisa de site para obter um forte entendimento de como o crachá funciona e em que potência cada ponto de acesso é visto. Quando isso estiver concluído e for determinado que o ajuste desse valor é necessário, comece com um valor de -71 dBm para o algoritmo de controle de potência de transmissão. Use este parâmetro CLI:

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

Permita que a rede trabalhe com esse ajuste com no mínimo 30 minutos ou uma hora antes de observar qualquer alteração. Quando a rede receber tempo suficiente, faça o caminho do site usando a mesma ferramenta de pesquisa e os emblemas novamente. Observe as mesmas características de roaming e a mesma potência do ponto de acesso. O objetivo aqui é tentar fazer com que os distintivos façam roaming antes ou no próximo ponto de acesso para obter a melhor relação possível sinal/ruído.

- **Como saber se a energia de transmissão está muito quente ou muito fria?**Determinar se o limiar de potência de transmissão está muito alto ou muito baixo exige uma boa compreensão do seu ambiente. Se você caminhou por toda a sua área de implantação (onde espera que os seus crachás do Vocera funcionem), você deve saber onde os pontos de acesso estão localizados, bem como experimentar o comportamento de roaming do crachá.
- **O que eu faço se minha energia de transmissão estiver muito quente?**O Crachá Vocera gira apenas com base na intensidade do sinal em vez da qualidade do sinal. Se o Crachá de Vocera não girar depois de passar por vários pontos de acesso enquanto estiver engajado no tutorial de boas-vindas ou no tom de teste, o crachá será considerado pegajoso. Se esse comportamento for indicativo de toda a área de implantação do campus, o limite de potência de transmissão estará muito quente e deverá ser reduzido. Se apenas uma ou duas áreas isoladas mostrarem esse comportamento e o restante da área de implantação mostrar características de roaming mais idealistas, isso não é uma indicação de que sua rede está muito quente.
- **O que eu faço se minha potência de transmissão estiver muito fria?**O limite de transmissão padrão quase nunca deve fornecer a você uma área de implantação na qual sua rede esteja muito fria. Se o limite de potência de transmissão for ajustado para baixo, e andando pelas salas com o Crachá de Vocera fornecer um ambiente onde o crachá gira bem, mas perde a conectividade e/ou a cobertura de pontos mortos/mortos, então sua rede pode ter sido ajustada para um nível muito baixo. Se isso não for característico de toda a sua rede, mas isolado em uma ou duas áreas, então é mais indicativo de um buraco de cobertura do que de um problema em toda a rede.
- **Comportamento isolado**Se você descobrir que em uma ou duas áreas, o crachá se mantém em um ponto de acesso em vez de rodar de uma maneira idealista, examine essa área.Qual

é a diferença dessa área em relação ao restante do campus?Se essas áreas estiverem próximas a saídas de edifícios ou áreas em construção, a detecção de furos de cobertura poderia forçar esses pontos de acesso a aumentar a energia?Examine o arquivo de log do WLC e as listas de vizinhos do ponto de acesso para ajudar a determinar por que tal anomalia pode ocorrer.Se você descobrir que em uma ou mais áreas isoladas, o crachá sofre cobertura de mortos ou spotty, então você precisa examinar essas áreas separadamente.Esta área está perto de um eixo elevador, radiologia ou de uma sala de descanso?Essas áreas podem ser mais adequadas pela instalação ou melhor posicionamento de um ponto de acesso para permitir uma melhor cobertura de voz.Em ambos os casos, é sempre aconselhável entender que você está trabalhando em um espectro de rádio não licenciado e que o comportamento idealista pode nunca ser alcançável. Isso pode acontecer quando você estiver situado ao lado de uma torre ou dispositivo de transmissão de rádio, um transmissor de televisão ou, possivelmente, uma instalação de reparo de 2,4 GHz não 802.11 (telefones sem fio, e assim por diante).

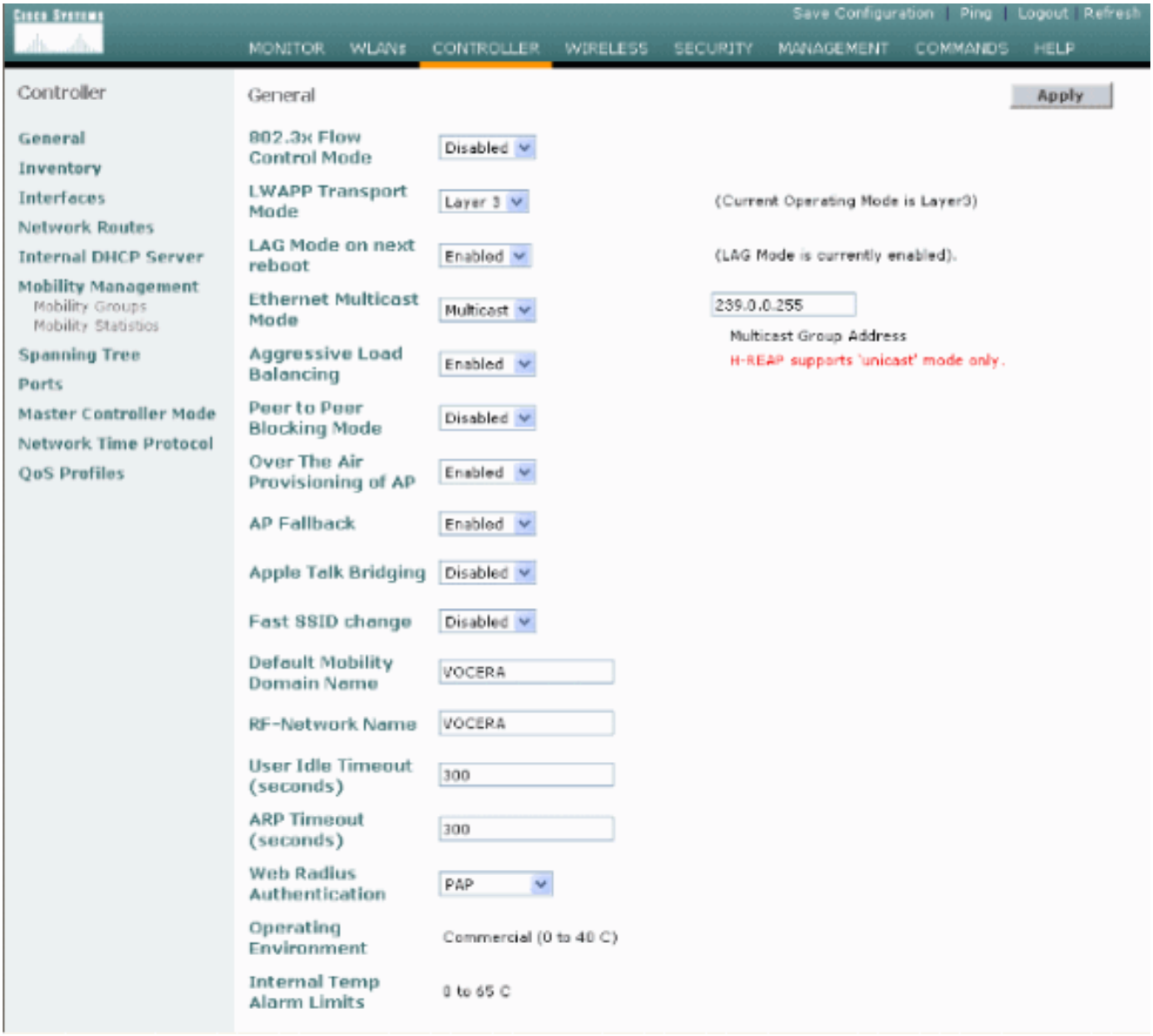
Configuração da infraestrutura de rede sem fio

O guia de projeto e implantação do Cisco Unified Wireless Network deve ser seguido para a configuração geral de suas WLCs. Esta seção fornece recomendações adicionais específicas para os emblemas de comunicação Vocera®.

Observação: as alterações não serão salvas se você não pressionar o botão **Aplicar** antes de passar para a próxima etapa.

Conclua estes passos no menu de nível superior **do controlador**:

1. Altere Ethernet Multicast Mode (Modo Multicast Ethernet) para **Multicast**.
2. Defina Multicast Group Address (Endereço do grupo multicast) como **239.0.0.255** (ou algum outro endereço de grupo multicast não utilizado).
3. Defina o Nome de domínio de mobilidade padrão e o Nome da rede RF para o projeto da rede.
4. Desative o **balanceamento de carga agressivo**.**Figura 9 — Configuração geral do WLC**

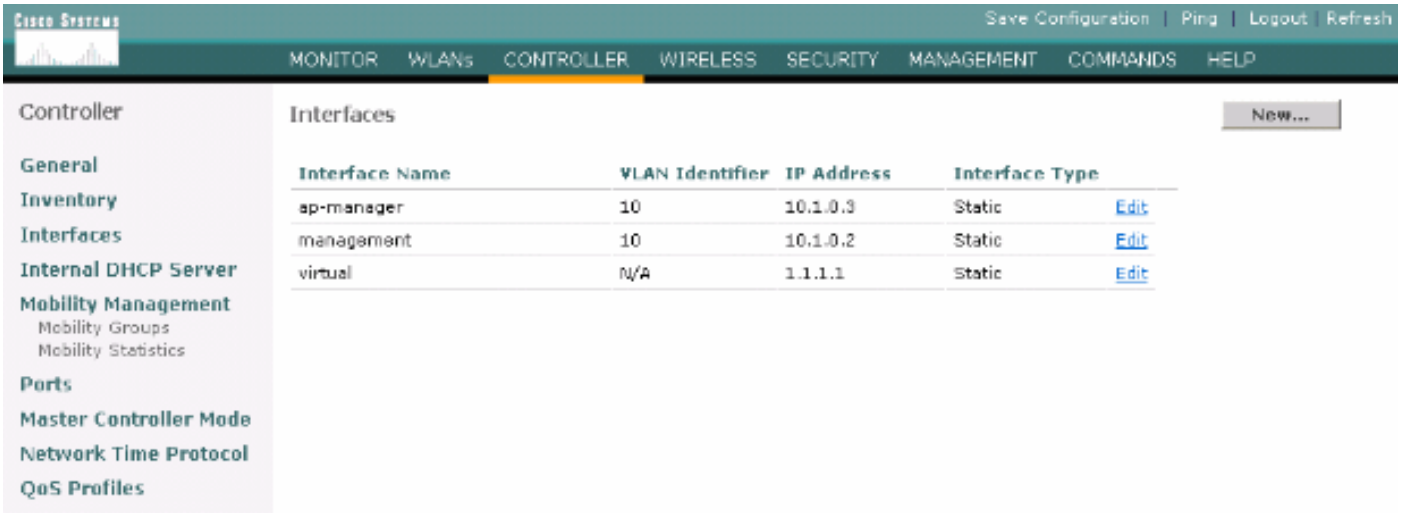


Criar interfaces

Clique em **Controller > Interfaces**.

Observação: a VLAN e o endereço IP variam. As capturas de tela aqui fornecem um endereçamento de exemplo que não deve ser seguido diretamente.

Figura 10 — Lista de interfaces WLC



Crie a interface de voz Vocera

Conclua estes passos:

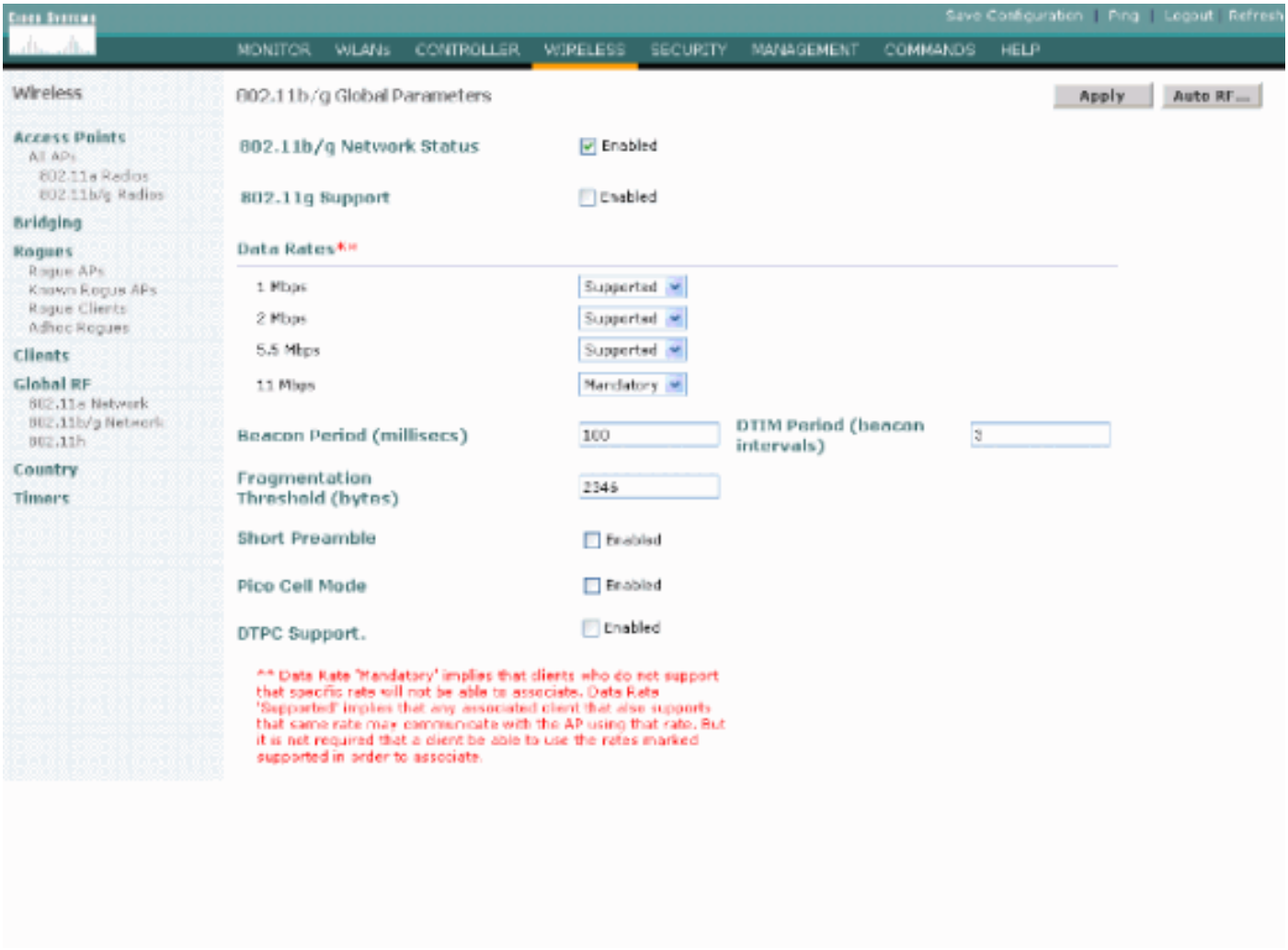
1. Clique em **New**.
2. Insira um nome de marca representativo de sua rede VoWLAN Vocera no campo Nome da interface.
3. Digite o número da VLAN dessa rede VoWLAN no campo VLAN ID.
4. Clique em **Apply** e, em seguida, clique em **Edit** para editar a interface que acabou de criar.
5. Insira o endereçamento IP para esta interface que está no intervalo da VLAN e outras informações relacionadas.
6. Clique em Apply.

Configuração específica para conexões sem fio

Para uma WLAN que tenha apenas crachás de voz, essa configuração fornece configurações de exemplo que melhor suportam o aplicativo de difusão de voz.

- O período DTIM é **1**.
- O suporte para 802.11g está desativado. Somente a taxa de dados 802.11b de **11 Mpbs** é **obrigatória**.
- O preâmbulo curto está desativado.
- O DTPC está desabilitado.

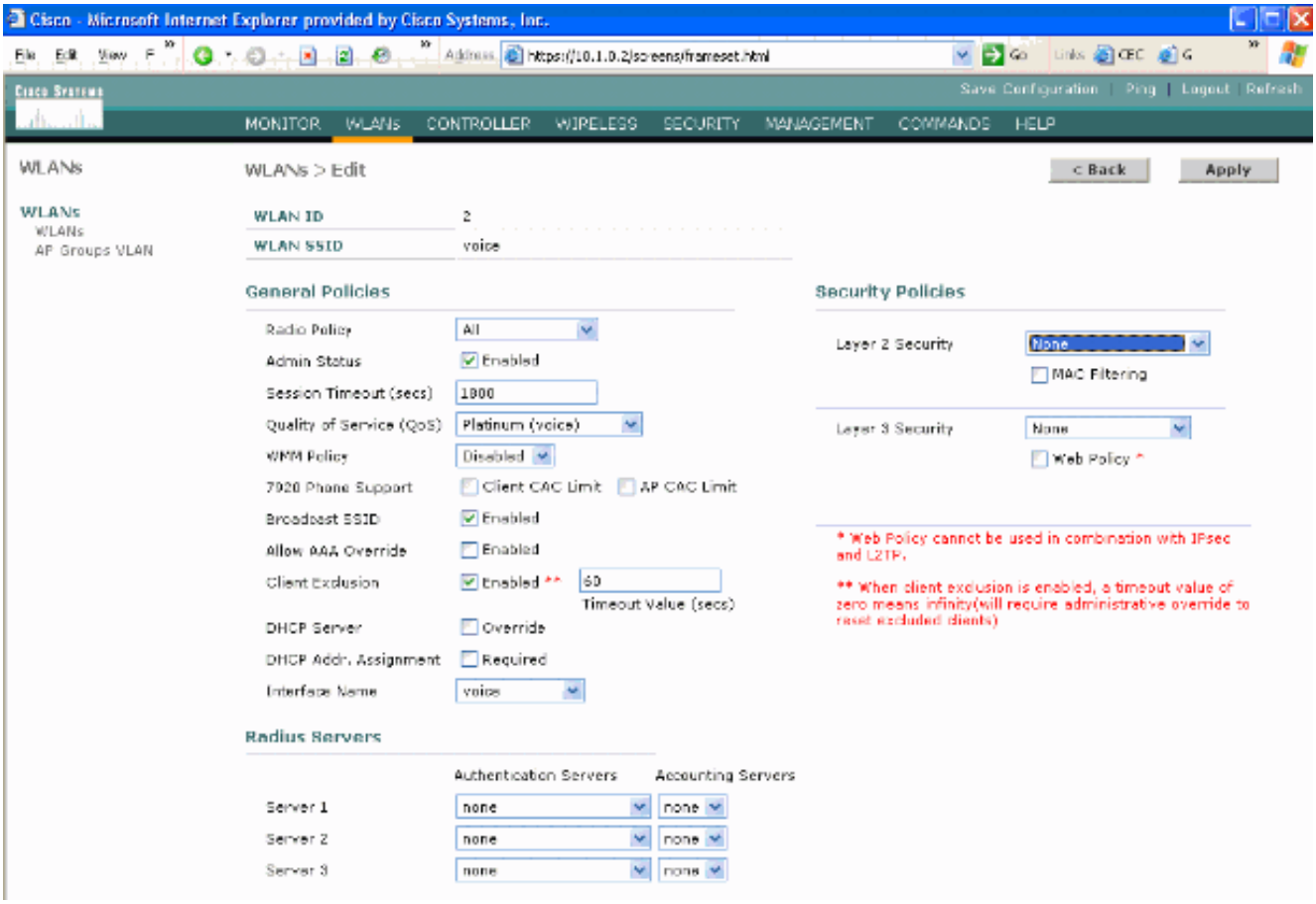
Figura 11—Configuração 802.11b/g



Configuração da WLAN

Conclua estes passos:

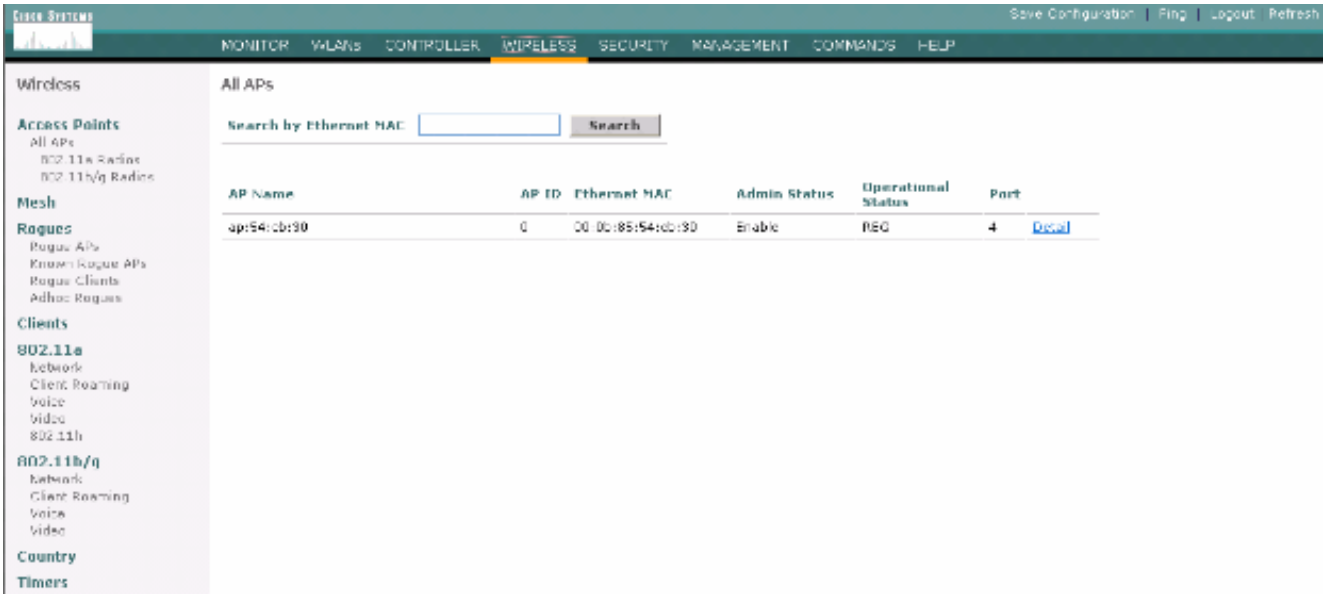
1. Atualize o campo Radio Policy (Política de rádio) para um valor que melhor se ajuste às suas necessidades.
2. Altere o Status do administrador para **Ativado**.
3. Defina Session Timeout como **1800**.
4. Defina Qualidade de Serviço como **Platinum**.
5. Defina SSID de broadcast como **Ativado**.
6. Defina o nome da interface como a interface criada para os emblemas de comunicação Vocera.
7. Defina as opções de segurança para corresponder às políticas corporativas.**Figura 12—Configuração da WLAN**



Configurar detalhes do ponto de acesso

Conclua estes passos:

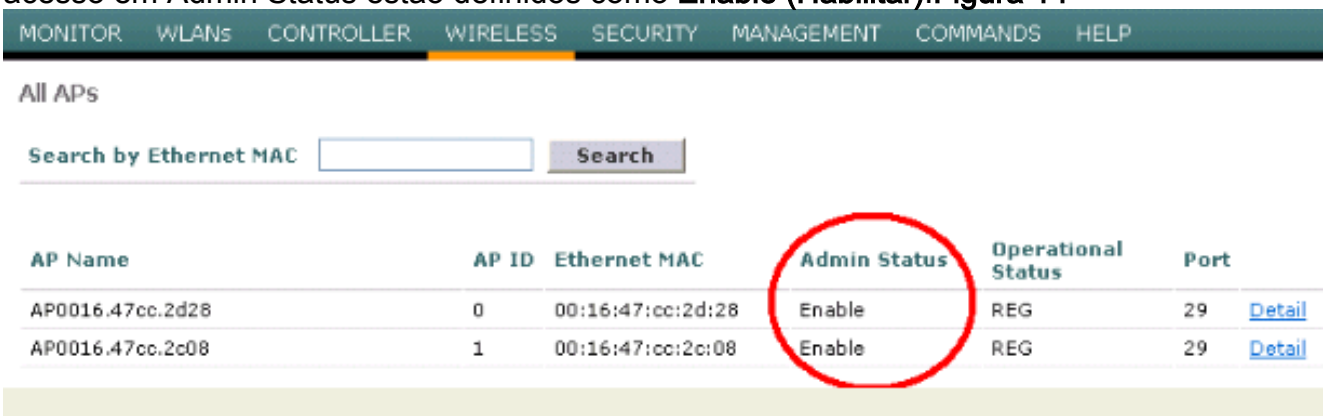
1. Clique em **Detalhes**.
2. Configure o nome do AP.
3. Verifique se o ponto de acesso está configurado para DHCP.
4. Verifique se o status Admin está **Habilitado**.
5. AP Mod" deve ser definido como **local**.
6. Digite o local do ponto de acesso.
7. Insira o nome do controlador ao qual o ponto de acesso pertence. O nome do controlador pode ser encontrado na página Monitor.
8. Clique em Apply.**Figura 13 — Detalhes do AP**



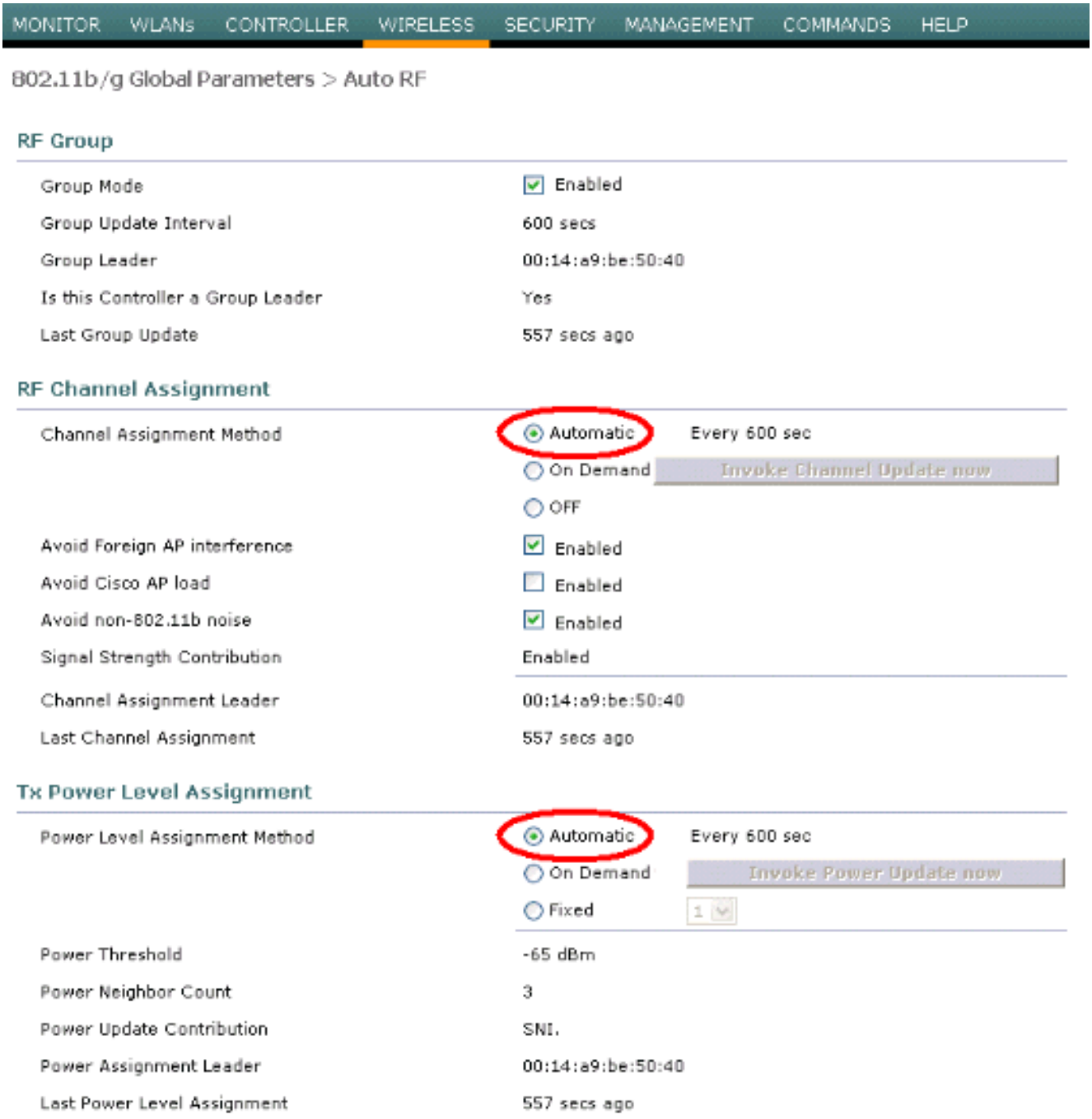
Configurar o rádio 802.11b/g

Conclua estes passos:

1. Clique em **Wireless** localizado na parte superior da WLC e verifique se todos os pontos de acesso em Admin Status estão definidos como **Enable (Habilitar)**.**Figura 14**



2. Clique em **Rede** (localizado perto de 802.11b/g).
3. Clique em **AutoRF**.
4. Use o AutoRF para criar uma cobertura completa com um canal de RF sem sobreposição e uma potência de transmissão. Para fazer isso, selecione **Automático** para Atribuição de canal RF e Atribuição de nível de potência Tx.**Figura 15**



5. Clique em Apply.
6. Clique em **Save Configuration** e consulte a seção Tune AutoRF for Your Environment deste documento.
7. Escolha **Wireless > Access Points > 802.11b/g Rádios.Figura 16**

Verificação de telefonia IP sem fio

Depois de realizar uma pesquisa de RF no local e configurar os pontos de acesso e os telefones, é fundamental realizar testes de verificação para garantir que tudo funcione conforme desejado. Esses testes devem ser realizados em todos estes locais:

- A área principal de cada célula de ponto de acesso (onde os distintivos são mais prováveis de se conectar a esse ponto de acesso específico).
- Qualquer local onde possa haver um alto volume de chamadas.
- Locais onde o uso pode ser pouco frequente, mas a cobertura ainda precisa ser certificada (por exemplo, escadas, banheiros, etc.).
- Na borda da área de cobertura do ponto de acesso.
- Estes ensaios podem ser realizados em paralelo ou em série. Se executado em paralelo, certifique-se de que os telefones estejam desligados entre os pontos de teste para testar a associação completa, a autenticação e o registro em cada local. Os ensaios de roaming e de carga devem ser os ensaios finais.

Associação, autenticação e registro

Esta seção explica como verificar se o crachá associa, autentica e se registra corretamente.

- Em vários pontos do ambiente, ligue os emblemas e verifique a associação com o access point. Se o crachá não se associar ao ponto de acesso, faça o seguinte:Verifique a configuração do distintivo para garantir o SSID correto, o tipo de autenticação e assim por diante.Verifique a configuração da WLC para garantir o SSID correto, o tipo de autenticação, os canais de rádio e assim por diante.Verifique sua pesquisa de site para garantir que o local tenha cobertura de RF adequada.
- Em vários pontos do ambiente, certifique-se de que o telefone autentica através do ponto de acesso com êxito. Se o cliente não autenticar, verifique a chave WEP ou o nome de usuário e a senha LEAP nos emblemas. Além disso, verifique o nome de usuário e a senha no servidor AAA usando um laptop sem fio com credenciais idênticas.
- Em vários pontos do ambiente, certifique-se de que os emblemas se registrem no Vocera Communication Server. Se o cliente não se registrar, faça estas verificações:Verifique se o distintivo tem o endereço IP, a máscara de sub-rede, o gateway principal, o TFTP principal, o primário/secundário e o DNS corretos.
- Chamadas de voz fixas:Em vários pontos do ambiente, enquanto você está parado, faça uma chamada para outro crachá e faça testes de voz de 60 a 120 segundos para verificar a qualidade da voz. Se a qualidade de voz for inaceitável, mova um crachá para um local melhor e teste novamente. A qualidade da voz é aceitável? Caso contrário, verifique sua cobertura sem fio.Se o servidor de telefonia estiver configurado, em vários pontos em todo o ambiente, fique parado e faça uma chamada para um telefone com fio e faça testes de voz de 60 a 120 segundos para verificar a qualidade de voz. Se a qualidade de voz for inaceitável, pergunte se você faz uma chamada usando o telefone com fio. A qualidade da voz é aceitável? Caso contrário, verifique o projeto da rede com fio em relação às diretrizes.
- Use as ferramentas de pesquisa de site para verificar se não há mais de um ponto de acesso por canal RF desse local com uma intensidade de sinal (indicador de intensidade de sinal recebido [RSSI]) maior que 35. Se houver dois pontos de acesso presentes no mesmo canal,

certifique-se de que a relação sinal/ruído (SNR) esteja o mais alta possível para minimizar a interferência. Por exemplo, se o ponto de acesso mais forte tiver um RSSI de 35, o ideal é que o ponto de acesso mais fraco tenha um RSSI inferior a 20. Para atingir esse objetivo, você pode ter que reduzir a potência de transmissão de um ponto de acesso ou mover o ponto de acesso.
- Verifique as configurações de QoS no ponto de acesso para confirmar as configurações recomendadas apropriadas.
- Chamadas de emblema de roaming:Se o servidor de telefonia não estiver disponível, inicie o Tutorial Vocera com o comando **Begin Tutorial**.OUSe o servidor de telefonia estiver disponível, inicie uma chamada com um dispositivo fixo para o crachá.Verifique continuamente a qualidade da voz enquanto atravessa a área de cobertura sem fio total. Se a qualidade de voz for insuficiente, execute estas tarefas:Ouça todas as mudanças inaceitáveis na qualidade de voz e anote os valores de localização e rádio no seu laptop e CQ do crachá.Observe e ouça o distintivo para ir até o próximo ponto de acesso.Observe os outros pontos de acesso disponíveis na pesquisa do site para verificar a cobertura e interferência.
- Faça ajustes no posicionamento e nas configurações do ponto de acesso para ajustar a WLAN e execute estas verificações para garantir a qualidade de voz:Use as ferramentas de pesquisa de site e verifique se não há mais de um ponto de acesso por canal com um valor de RSSI superior a 35 em um determinado local. Idealmente, todos os outros pontos de acesso no mesmo canal devem ter valores de RSSI o mais baixos possível (preferencialmente menos de 20). Na fronteira da área de cobertura onde o RSSI é 35, o RSSI para todos os outros pontos de acesso no mesmo canal deve ser, idealmente, inferior a 20.Use as ferramentas de pesquisa de site para verificar se há pelo menos dois pontos de acesso (total, em canais separados) visíveis em todos os locais com intensidade de sinal suficiente.Verifique se os pontos de acesso em uma determinada área de roaming estão todos em uma rede de Camada 2.

Problemas comuns de roaming

Esses problemas de roaming podem ocorrer:

- O crachá não circula quando colocado diretamente sob o ponto de acesso.
- O distintivo provavelmente não está alcançando os limites diferenciais de roaming para o indicador de intensidade do sinal recebido (RSSI) e a utilização do canal (CU). Ajuste o Limite de potência de transmissão da WLC.
- O crachá não recebe beacons ou respostas de sondagem do ponto de acesso.
- O crachá vagueia muito devagar.

O emblema perde a conexão com a rede ou o serviço de voz é perdido durante o roaming

- Verifique se há uma possível incompatibilidade WEP na autenticação.
- O emblema não envia junções IGMP ou a rede envia consultas IGMP durante um roaming. Portanto, a função de broadcast Vocera falha durante um roaming de Camada 2/Camada 3.
- O crachá é capaz apenas de roaming contínuo da camada 2 (a menos que um mecanismo de mobilidade da camada 3 esteja configurado). Certifique-se de que a nova WLC não esteja servindo uma sub-rede IP diferente.

- Verifique se o controlador/ponto de acesso associado tem conectividade IP com o servidor de comunicação Vocera.
- Verifique a intensidade do sinal RF e os valores CQ do distintivo.

O crachá perde a qualidade de voz ao roaming

- Verifique se há RSSI baixo no ponto de acesso de destino.
- A sobreposição de canais pode ser insuficiente. O distintivo deve ter tempo para desligar a chamada sem problemas antes de perder o sinal com o ponto de acesso original.
- O sinal do ponto de acesso original pode ser perdido.

Problemas de áudio

Há alguns erros comuns de configuração que podem causar alguns problemas de áudio facilmente resolvidos. Se possível, verifique os problemas de áudio em relação a um crachá fixo (referência) para ajudar a restringir o problema a um problema sem fio. Problemas comuns de áudio incluem:

- Áudio de um lado
- Áudio instável ou robótico
- Problemas de registro e autenticação

Áudio de um lado

- Esse problema pode ocorrer nas áreas marginais de um ponto de acesso, onde um sinal pode ser muito fraco no lado do distintivo ou no lado do ponto de acesso. A correspondência entre as configurações de energia no access point e o distintivo (20 mW), quando possível, pode corrigir esse problema. Esse problema é mais comum quando a variação entre a configuração do access point e a configuração do distintivo é grande (por exemplo, 100 mW no access point e 28 mW no distintivo).
- Verifique a qualidade de voz no gateway e no roteamento IP.
- Verifique se um firewall ou NAT está no caminho dos pacotes UDP proprietários. Por padrão, os firewalls e NATs causam áudio unidirecional ou sem áudio. Os NATs e firewalls do Cisco IOS® e PIX têm a capacidade de modificar essas conexões para que o áudio bidirecional possa fluir.Se você usa a mobilidade da camada 3, sua rede pode estar bloqueando o tráfego upstream com verificações do Unicast Reverse Path Forwarding (uRPF).
- O áudio unidirecional pode ocorrer se o cache ARP não estiver configurado na WLC.

Áudio instável ou robótico

- Um motivo comum para áudio cortado ou robótico é quando um micro-ondas opera nas proximidades. As micro-ondas começam no canal 9 e podem se estender dos canais 6 para 14.
- Verifique se há telefones sem fio de 2,4 GHz e outros dispositivos sem fio de chamada de enfermeira usando ferramentas como Cognio.

Problemas de registro e autenticação

Quando você encontrar problemas com a autenticação, execute estas verificações:

- Verifique os SSIDs para se certificar de que eles correspondam ao distintivo e ao ponto de acesso (ou à rede). Verifique também se a rede tem uma rota para o servidor Vocera.
- Verifique as chaves WEP para garantir que correspondam. É uma boa ideia reinseri-los no BCU (Badge Configuration Utility, Utilitário de configuração de emblema) e reprogramá-los, pois é fácil cometer um erro de digitação ao inserir uma chave ou senha WEP.

Essas mensagens ou sintomas podem ocorrer:

- Não é possível suportar todos os recursos solicitados — é muito provável que haja uma incompatibilidade de criptografia entre o access point e o cliente.
- Falha na autenticação / Nenhum AP encontrado — Verifique se os tipos de autenticação correspondem no ponto de acesso e no cliente.
- Nenhum serviço - Falha na configuração de IP—Se você usar WEP estático, verifique se as chaves estão configuradas corretamente. Verifique se outros clientes podem receber DHCP usando o mesmo SSID.
- Cancelar a autenticação de todos os clientes TKIP do AP—Este problema acontece quando o ponto de acesso detecta dois erros MIC em 60 segundos. Essa contramedida impede que todos os clientes TKIP se autentiquem novamente por 60 segundos.
- Re-autenticação / Tempo limite da sessão—Se configurado, um tempo limite de sessão ativa uma reautenticação que causa falhas no fluxo de voz (300 ms + atraso de WAN para autenticação 802.1x).

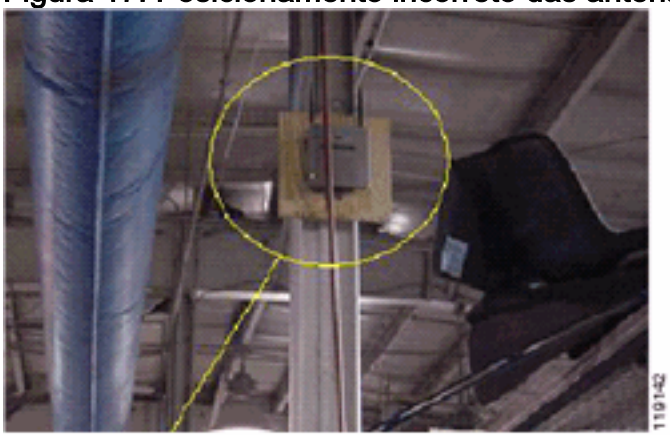
Apêndice A

Posicionamento de AP e antena

Esta seção fornece exemplos de posicionamento correto e inapropriado de pontos de acesso (APs) e antenas.

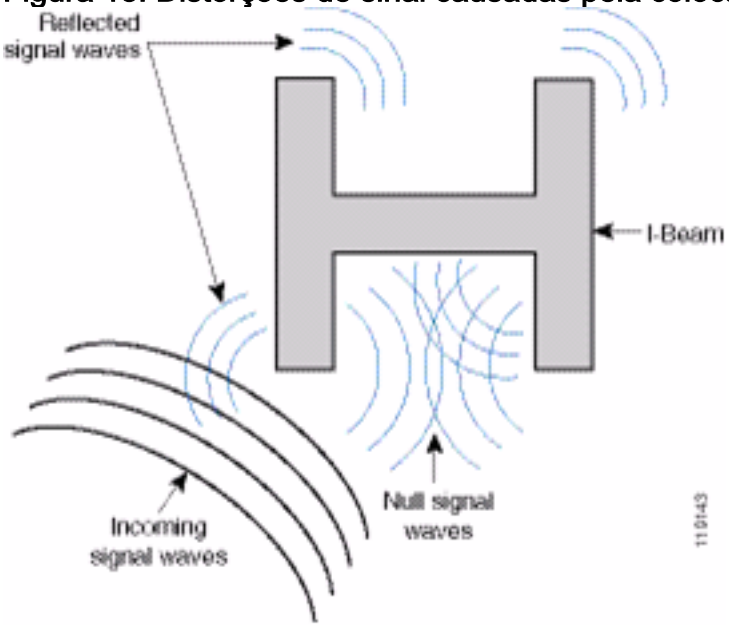
A Figura 17 mostra a posição incorreta de um ponto de acesso e antenas próximas a um feixe de I, o que cria padrões de sinal distorcidos. Um ponto nulo de RF é criado pelo cruzamento de ondas de sinal e a distorção de multipath é criada quando as ondas de sinal são refletidas. Essa colocação resulta em muito pouca cobertura atrás do access point e redução da qualidade do sinal na frente do access point.

Figura 17: Posicionamento incorreto das antenas perto de um feixe de I



A Figura 18 mostra as alterações ou distorções da propagação do sinal causadas por um feixe I. O feixe I cria muitas reflexões de pacotes recebidos e de pacotes transmitidos. Os sinais refletidos resultam em uma qualidade de sinal muito ruim devido a pontos nulos e interferência de multipath. No entanto, a intensidade do sinal é alta porque as antenas do ponto de acesso estão tão próximas do feixe de I.

Figura 18: Distorções de sinal causadas pela colocação das antenas muito perto de um feixe de I

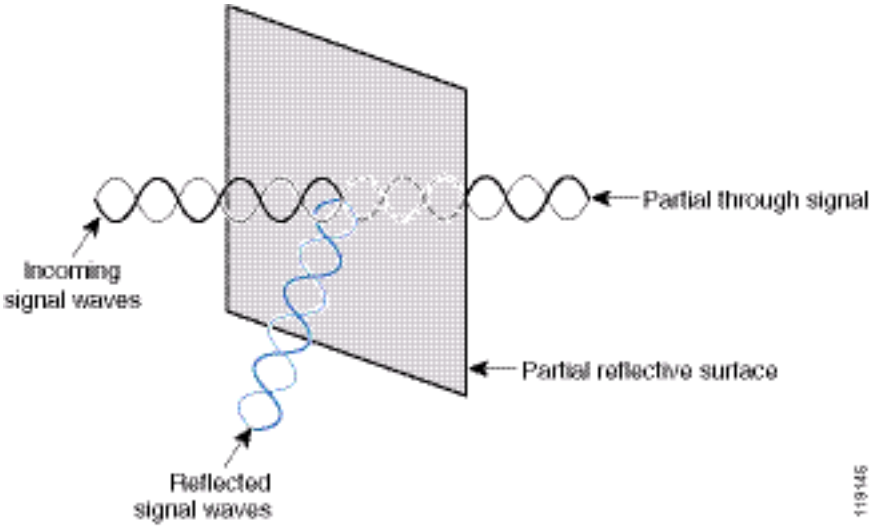


O ponto de acesso e a posição da antena na Figura 19 são melhores porque estão longe dos I-beams e há menos sinais refletidos, menos pontos nulos e menos interferência de multipath. Essa posição ainda não é perfeita, pois o cabo Ethernet não deve ser enrolado tão perto da antena. Além disso, o ponto de acesso pode ser girado com as antenas de 2,4 GHz apontadas para o chão. Isso proporciona uma melhor cobertura diretamente abaixo do ponto de acesso. Não há usuários acima do ponto de acesso.

Figura 19: Ponto de acesso e antenas montadas em uma parede, longe dos I-Beams

A Figura 20 mostra a propagação do sinal causada pela parede na qual o ponto de acesso está montado.

Figura 20—Reflexão do sinal causada por uma parede

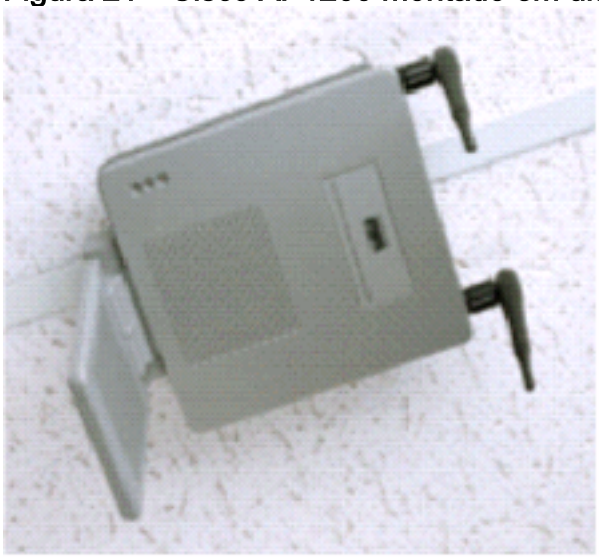


Os exemplos anteriores também se aplicam quando você coloca pontos de acesso e antenas no teto ou próximo a ele em um ambiente corporativo padrão. Se houver dutos de ar metálico, eixos de elevador ou outras barreiras físicas que podem causar reflexão de sinal ou interferência de multipath, a Cisco recomenda que você remova as antenas dessas barreiras. No caso do elevador, mova a antena alguns metros para longe para ajudar a eliminar a reflexão do sinal e a distorção. O mesmo acontece com os dutos de ar no teto.

Uma pesquisa realizada sem enviar e receber pacotes não é suficiente. O exemplo do I-feixe mostra a criação de pontos nulos que podem resultar de pacotes que têm erros de CRC. Pacotes de voz com erros de CRC são pacotes perdidos que afetam negativamente a qualidade de voz. Neste exemplo, esses pacotes podem estar acima do piso de ruído medido por uma ferramenta de pesquisa. Portanto, é muito importante que a pesquisa de site não apenas meça os níveis de sinal, mas também gere pacotes e, em seguida, informe erros de pacote.

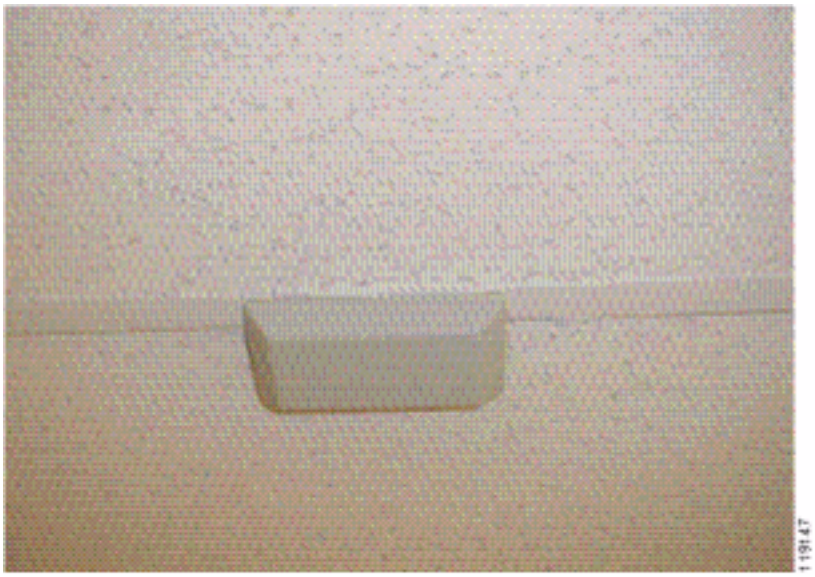
A Figura 21 mostra um Cisco AP1200 montado corretamente em uma barra em T no teto, com as antenas em uma posição omni-direcional.

Figura 21—Cisco AP1200 montado em um teto



A Figura 22 mostra uma antena de diversidade onidirecional Cisco Aironet 5959 montada corretamente em uma barra em T no teto. Nesse caso, o Cisco AP1200 é montado acima do teto.

Figura 2: Antena Cisco Aironet 5959 montada em um teto



A Figura 23 mostra um Cisco AP1200 corretamente montado em uma parede.

Figura 23—Cisco AP1200 montado em uma parede

A Figura 24 mostra a antena de correção de diversidade Cisco Aironet 2012 montada em uma parede. Nesse caso, o Cisco AP1200 é montado acima do teto.

Figura 24—Antena Cisco Aironet 2012 montada em uma parede

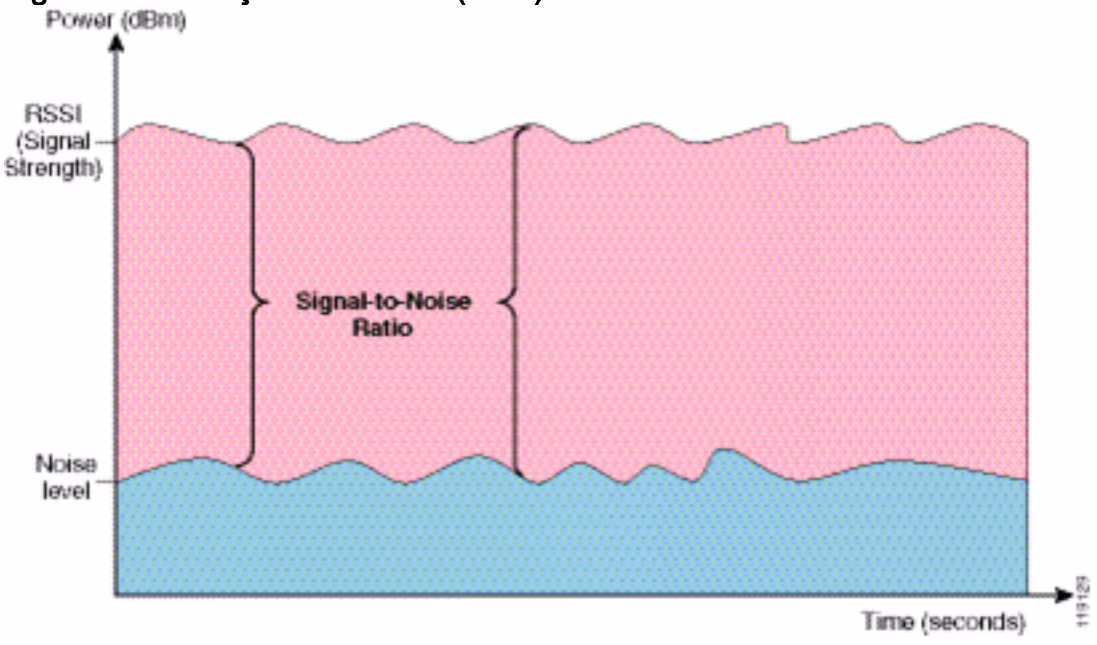
Para áreas em que o tráfego do usuário é alto (como escritórios, escolas, lojas de varejo e hospitais), a Cisco recomenda que você coloque o access point fora de vista e coloque antenas não obstrutivas abaixo do teto. A separação de antenas de não diversidade não deve exceder 18 polegadas.

Distorção de Interferência e Multipath

O desempenho de throughput da rede WLAN é afetado por sinais inutilizáveis. A interferência de WLAN pode ser gerada por fornos micro-ondas, telefones sem fio de 2,4 GHz, dispositivos Bluetooth ou outros equipamentos eletrônicos que operam na banda de 2,4 GHz. A interferência também vem normalmente de outros pontos de acesso e dispositivos clientes que pertencem à WLAN, mas que estão muito distantes para que seu sinal seja enfraquecido ou corrompido. Os pontos de acesso que não fazem parte da infraestrutura de rede também podem causar interferência de WLAN e são identificados como pontos de acesso não autorizados.

A interferência e a distorção de multipath fazem com que o sinal transmitido oscile. A interferência diminui a relação sinal/ruído (SNR) para uma taxa de dados específica. As contagens de novas tentativas de pacotes aumentam em uma área em que a interferência e/ou a distorção de multipath são altas. A interferência também é conhecida como nível de ruído ou piso de ruído. A intensidade do sinal recebido de seu ponto de acesso associado deve ser alta o suficiente acima do nível de ruído do receptor para ser decodificado corretamente. Esse nível de intensidade é conhecido como razão sinal/ruído, ou SNR. O SNR ideal para o Crachá Vocera é 25 dB. Por exemplo, se o piso do ruído for de 95 decibéis por miliwatt (dBm) e o sinal recebido no telefone for de 70 dBm, a relação sinal/ruído será de 25 dB. (Consulte a Figura 25).

Figura 25—Relação sinal-ruído (SNR)



Quando você altera o tipo e a localização da antena, ela pode reduzir a distorção e interferência de multipath. O ganho de antena é adicionado ao ganho do sistema e pode reduzir a interferência se o transmissor interferente não estiver diretamente na frente da antena direcional.

Embora as antenas direcionais possam ser de grande valor para certos aplicativos internos, a grande maioria das instalações internas usa antenas onidirecionais. A direcionalidade deve ser determinada rigorosamente por uma pesquisa de site correta e adequada. Quer você use uma antena onidirecional ou de patch, ambientes internos exigem antenas de diversidade para atenuar a distorção de multipath. Os rádios de access point Cisco Aironet Series permitem suporte à

diversidade.

Atenuação de sinal

A atenuação do sinal ou a perda de sinal ocorre mesmo quando o sinal passa pelo ar. A perda de intensidade do sinal é mais pronunciada à medida que o sinal passa por diferentes objetos. Uma potência de transmissão de 20 mW é equivalente a 13 dBm. Portanto, se a potência transmitida no ponto de entrada de uma parede de uma prancha for de 13 dBm, a intensidade do sinal será reduzida para 10 dBm ao sair dessa parede. Esta tabela mostra a provável perda na intensidade do sinal causada por vários tipos de objetos.

Atenuação de Sinal Causada por Vários Tipos de Objetos

Objeto no Caminho do Sinal	Atenuação de sinal através do objeto
Parede de placas	3 dB
Parede de vidro com armação de metal	6 dB
Garrafa	4 dB
janela do Office	3 dB
Porta de metal	6 dB
Porta metálica em parede de tijolos	12 dB
Corpo humano	3 dB

Cada site pesquisado tem diferentes níveis de distorção de multipath, perda de sinal e ruído de sinal. Os hospitais são geralmente o ambiente mais desafiador a ser pesquisado devido à alta distorção de multipath, perda de sinal e ruído de sinal. Os hospitais levam mais tempo para pesquisar, exigem uma população mais densa de access points e exigem padrões de desempenho mais altos. A indústria e o chão de fábrica são os mais difíceis de pesquisar. Esses locais geralmente têm lado metálico e muitos objetos metálicos no chão, o que resulta em sinais refletidos que recriam a distorção de multipath. Os edifícios de escritórios e os locais de hotelaria geralmente têm um sinal de alta atenuação, mas um grau menor de distorção multipath.

Informações Relacionadas

- Implantação de controladores LAN sem fio do Cisco 440X Series
- Design de rede de referência de solução
- Especificações do sistema de comunicações de voz
- Suporte Técnico e Documentação - Cisco Systems