Desenvolvimento do telefone IP de Vocera na infraestrutura de rede do Cisco Unified Wireless

Índice

Introdução

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.

Note: O apoio para o Produtos de Vocera deve ser obtido diretamente dos canais do apoio de Vocera. O Suporte técnico de Cisco não é treinado para apoiar edições Vocera-relacionadas.

Este guia é um suplemento ao guia de distribuição do controlador de LAN do Cisco Wireless e endereça somente os parâmetros de configuração que são particulares aos dispositivos de Vocera VoWLAN em uma arquitetura de pouco peso. Refira controladores de distribuição do Wireless LAN do Cisco 440X Series para mais informação.

Pré-requisitos

Requisitos

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

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

Comunicações unificadas SRND de Cisco baseadas no gerente 7.x das comunicações unificadas de Cisco — 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.

Convenções

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

Sumário executivo

Esta tabela resume as quatro funções chaves e como se comportam dentro de uma rede de Cisco Unified Wireless.

	Único controlador	Camada 2 do Controlador-à-controlador que vagueia	Camada 3 do Controlador-à-controlador que vagueia
Crachá-à-crachá	Nenhuma configuração especial	Nenhuma configuração especial	Nenhuma configuração especial
Crachá-à-telefone	Nenhuma configuração especial	Nenhuma configuração especial	Nenhuma configuração especial
Crachá-à-transmissão	Permita o Multicast do controlador	Permita o IGMP Snooping de Vocera VLAN do desabilitação do Multicast do controlador ou execute 4.0.206.0 ou mais tarde	4.0.206.0 ou mais tarde
Lugar do crachá	Nenhuma configuração especial	Nenhuma configuração especial	Nenhuma configuração especial

Vista geral do crachá de Vocera

Os crachás de uma comunicação permitem a um portador uma comunicação imediata com todo o outro portador do crachá também um seguimento do lugar da integração e do crachá do central telefônica privada (PBX). A utilização de uma rede Wireless 802.11b/g exige o uso do Multicast e a entrega de pacotes do unicast de UDP com exigências limitadas para o Qualidade de Serviço

(QoS) até à data da liberação de software do server 3.1 de Vocera (construção 1081). As capacidades da criptografia são 64/128 de Wired Equivalent Privacy (WEP) do bit, Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC), e o protocolo chave temporal da integridade de Cisco (CKIP) combinado com as capacidades da autenticação Open, da chave Acesso-PRE-compartilhada protegida Wi-fi (WPA-PSK), do protocolo extensible authentication WPA-protegido (PEAP) e do protocolo lightweight extensible authentication (PULO).

Com o impulso de um botão, o server de Vocera responde com `Vocera`, que é uma alerta para emitir comandos tais como o **registro**, **onde (am I) /is..** , **atendimento**, **jogo**, **transmissão**, **mensagens**, e assim por diante. O server de Vocera fornece os serviços e/ou a configuração de chamada necessários para terminar o pedido.

O sistema de comunicação capaz 802.11b de Vocera utiliza a compressão de voz proprietária e o uso de um intervalo de porta UDP. O software do sistema de Vocera é executado em um Windows Server que controle a configuração de chamada, a conexão de chamada e os perfis de usuário. Partnered com software do reconhecimento de discurso e do Voiceprint do nuance 8.5 a fim permitir comunicações de voz do crachá. Vocera recomenda um server das janelas separadas executar o software das soluções de telefonia de Vocera para permitir a Conectividade do serviço de telefonia tradicional (POTS) com os crachás.

Considerações da capacidade de chamada de Vocera

Veja a seção da cola da rede deste documento para uns detalhes mais adicionais.

Capacidade do Communications Server de Vocera

Refira as especificações de sistema de comunicação de Vocera para obter mais informações sobre da matriz da cola do server de Vocera.

A solução de Vocera

O crachá de Vocera utiliza o unicast e a entrega do pacote de transmissão múltipla para fornecer diversos recursos chaves que compõem esta solução completa. Estão aqui quatro dos recursos essenciais que confiam na entrega de pacotes apropriada. Igualmente é fornecida uma compreensão básica de como cada característica usa a rede subjacente para a entrega e a funcionalidade.

- Crachá às comunicações do crachá — Quando um usuário de Vocera chama um outro usuário, o crachá contacta primeiramente o server de Vocera, que olha acima o endereço IP de Um ou Mais Servidores Cisco ICM NT do crachá do callee e contacta o usuário do crachá para perguntar ao usuário se pode tomar um atendimento. Se o callee aceita o atendimento, o server de Vocera notifica o crachá de chamada do endereço IP de Um ou Mais Servidores Cisco ICM NT do crachá do callee para setup uma comunicação direta entre os crachás sem uma intervenção mais adicional do server. Toda a comunicação com o server de Vocera usa o codec de G.711 e toda a comunicação do crachá-à-crachá usa um codec do proprietário de Vocera.
- Uma comunicação da telefonia do crachá — Quando um server da telefonia de Vocera é instalado e instalação com uma conexão a um PBX, um usuário pode chamar fora extensões internas das linhas de telefone PBX ou de parte externa. Vocera permite que os usuários

façam atendimentos ou dizer os números (cinco, seis, três, dois) ou criando uma entrada de agenda telefônica no base de dados de Vocera para a pessoa ou pela função nesse número (por exemplo, farmácia, HOME, pizza) o server de Vocera determina o número que está sendo chamado, interceptando os números na extensão ou olhando o nome acima no base de dados e selecionando o número. O server de Vocera passa então essa informação ao server da telefonia de Vocera que conecta ao PBX e gerencie a Sinalização de telefonia apropriada (por exemplo, DTMF). Toda a comunicação entre o crachá e o server de Vocera e o server de Vocera e o server da telefonia de Vocera usa o codec de G.711 sobre o unicast UDP.

- Transmissão de Vocera — Um usuário do crachá de Vocera pode chamar e comunicar-se a um grupo de portadores do crachá de Vocera ao mesmo tempo usando o comando broadcast. Quando um usuário transmite a um grupo, o crachá do usuário envia o comando ao server de Vocera que olha então acima os membros de um grupo, determina que membros do grupo são ativos, atribui um endereço de multicast para usar-se para esta sessão da transmissão, e envia uma mensagem ao crachá de cada usuário ativo que instrui a para juntar-se ao grupo de transmissão múltipla com o endereço de multicast atribuído.
- Função do lugar do crachá — O server de Vocera mantém-se a par do Access point a que cada crachá ativo é associado enquanto cada crachá envia uma segundo manutenção de atividade 30 ao server com o BSSID associado. Isto permite que o sistema de Vocera calcule aproximadamente o lugar de um usuário do crachá. Esta função tem um grau de precisão relativamente baixo porque um crachá não pôde ser associado ao Access point a que é o mais próximo.

Planeamento da infraestrutura de Vocera

O guia de planejamento da infraestrutura de Vocera do whitepaper de Vocera , descreve os requisitos mínimos da análise de site que mostram que o crachá deve ter um mínimo da intensidade de sinal da recepção do dBm -65, de uma separação maior DB de 25 da razão sinal-ruído e de sobreposição e de canal do ponto de acesso apropriado. Embora os crachás usem uma antena direcional similar do omni como um caderno que seja usado para uma análise de site, não imita o comportamento do crachá muito bem, dado as influências dos portadores na intensidade de sinal. Dado este requisito exclusivo e este comportamento do dispositivo transmissor, o uso da arquitetura Cisco e a gerência de recursos do rádio são ideais a fim certificar-se que há uma falta de características incomuns do local do Radio Frequency (RF).

O crachá de Vocera é um dispositivo posto do ponto baixo, vestido ao lado do corpo com capacidades limitadas da correção de erros do sinal. As exigências de Vocera neste documento podem facilmente ser conseguidas. Contudo, pode tornar-se oprimido se há SSID demais para que processe e permita que o crachá trabalhe eficazmente.

Visão geral da arquitetura

Figura 1 — Transmissão múltipla geral dianteira e ameixa seca com o Sem fio de pouco peso do protocolo do Access point (LWAPP)

Multicast em um desenvolvimento LWAPP

Compreender o Multicast dentro de um desenvolvimento LWAPP é necessária distribuir a função

da transmissão de Vocera. Este documento cobre mais tarde as etapas essenciais para permitir o Multicast dentro da solução controlador-baseada. Há atualmente dois métodos de entrega que o controlador LWAPP se usa para entregar o Multicast aos clientes:

- Unicast-Multicast
- Multicast-Multicast

Método de entrega do Unicast-Multicast

O método de entrega do unicast-Multicast cria uma cópia de cada pacote de transmissão múltipla e para a frente ele a cada acesso-ponto. Quando um cliente envia um Multicast junte-se ao Wireless LAN, o Access point para a frente que isto se junta através do túnel LWAPP ao controlador. O controlador constrói uma ponte sobre este Multicast junta-se nele é diretamente a conexão de rede de área local conectada que é o VLAN padrão para o WLAN associado do cliente. Quando um pacote do Protocolo IP multicast chega da rede ao controlador, o controlador replicates este pacote com um cabeçalho LWAPP para cada Access point que tem um cliente dentro do domínio Wireless que se juntou a este grupo específico. Quando a fonte do Multicast é igualmente um receptor dentro do domínio Wireless, este pacote igualmente está duplicado e enviado de volta ao mesmo cliente que enviou este pacote. Para crachás de Vocera, este não é o método preferido da entrega do Multicast dentro da solução do controlador LWAPP. O método de entrega do unicast trabalha com disposições pequenas. Contudo, devido às despesas gerais consideráveis no controlador do Wireless LAN (WLC), este é nunca o método de entrega recomendado do Multicast.

Figura 2 — Multicast-unicast LWAPP

Note: Se o grupo VLAN AP está configurado, e um IGMP se junta está enviado de um cliente através do controlador, está colocado no VLAN padrão do WLAN que o cliente é sobre. Consequentemente, o cliente não pôde receber este tráfego multicast a menos que o cliente fosse um membro deste domínio de transmissão do padrão.

Método de entrega do Multicast-Multicast

O método de entrega do Multicast-Multicast não exige o controlador replicate cada pacote de transmissão múltipla recebido. O controlador é configurado para um endereço de grupo de transmissão múltipla não utilizado que cada Access point assenta bem em um membro de. Com figura 3, o grupo de transmissão múltipla definido do WLC ao Access point é 239.0.0.65. Quando um cliente envia um Multicast junte-se ao WLAN, o Access point para a frente que isto se junta através do túnel LWAPP ao controlador. O controlador para a frente este protocolo de camada de link nele é diretamente a conexão de rede de área local conectada que é o VLAN padrão para o WLAN associado do cliente. O roteador que é local ao controlador a seguir adiciona este endereço de grupo de transmissão múltipla a essa relação para enviar ((*, G)) entrada. Com figura 3, o Multicast do exemplo junta-se foi enviado ao grupo de transmissão múltipla 239.0.0.30. Quando da rede o tráfego multicast agora para a frente, o endereço de multicast de 239.0.0.30 for enviado ao controlador. O controlador encapsula então o pacote de transmissão múltipla em um pacote de transmissão múltipla LWAPP endereçado ao endereço de grupo de transmissão múltipla (o exemplo aqui é 239.0.0.65) que é configurado no controlador e enviado à rede. Cada Access point no controlador recebe este pacote como um membro do grupo de transmissão múltipla dos controladores. O Access point então para a frente os clientes/pacote de transmissão múltipla dos server (o exemplo aqui é 239.0.0.30) como uma transmissão ao WLAN/SSID identificado dentro do pacote de transmissão múltipla LWAPP.

Note: Se você configura impropriamente sua rede de transmissão múltipla, você poderia terminar

acima a recepção de pacotes de transmissão múltipla do Access point de um outro controlador. Se o primeiro controlador tem que fragmentar este pacote de transmissão múltipla, o fragmento está enviado à rede e cada Access point deve passar o tempo deixar cair este fragmento. Se você permite todo o tráfego tal como qualquer coisa da escala do Multicast 224.0.0.x, este está encapsulado igualmente e enviado subseqüentemente por cada Access point.

Figura 3 — Multicast-Multicast LWAPP

Configuração do Multicast do roteador e do interruptor

Este documento não é um manual de configuração do Multicast da rede. Refira configurar o roteamento IP Multicast para uma história completa da aplicação. Este capas de documento os princípios para permitir o Multicast dentro de seu ambiente de rede.

Permita o roteamento IP Multicast

O roteamento IP Multicast permite que o software de Cisco IOS® envie pacotes de transmissão múltipla. **O comando ip multicast-routing global configuration** é exigido permitir que o Multicast funcione em toda a rede permitida Multicast. **O comando ip multicast-routing** deve ser permitido em todo o Roteadores dentro de sua rede entre o WLC e seus Access point respectivos.

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

Permita o PIM em uma relação

Isto permite a relação do roteamento para a operação do Internet Group Management Protocol (IGMP). O modo da transmissão múltipla independente de protocolo (PIM) determina como o roteador povoa sua tabela de roteamento de transmissão múltipla. O exemplo fornecido aqui não exige o ponto de reunião (RP) ser conhecido para o grupo de transmissão múltipla e consequentemente o sparse-dense-mode é o mais desejável dado a natureza desconhecida de seu ambiente do Multicast. Esta não é uma recomendação do Multicast ser configurado para trabalhar embora a relação da camada 3 conectada diretamente a seu controlador deva ser PIM permitido para que o Multicast funcione. Todas as relações entre seu WLC e seus Access point respectivos devem ser permitidas.

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

IGMP Snooping do interruptor VLAN do desabilitação

O IGMP Snooping permite uma rede comutada com o Multicast permitido de limitar o tráfego 2 aqueles switchports que têm os usuários que querem o Multicast ser vistos ao podar os pacotes de transmissão múltipla dos switchports que não desejam ver o fluxo de transmissão múltipla. Em um desenvolvimento de Vocera, pode ser indesejável permitir mais cedo o CGMP ou o IGMP Snooping no switchport ascendente ao controlador com software release do que 4.0.206.0.

Vaguear e Multicast não são definidos com um grupo de exigências verificar que o tráfego multicast pode seguir um usuário subscrito. Embora o crachá do cliente esteja ciente que vagueou, não envia um outro IGMP junta-se para certificar-se de que a infraestrutura de rede continua a entregar o tráfego do Multicast (transmissão de Vocera) ao crachá. Ao mesmo tempo, o Access point LWAPP não envia uma pergunta da transmissão múltipla geral ao cliente

vagueado para alertar para este IGMP junta-se. Com um projeto de rede de Vocera da camada 2, desabilitar o IGMP Snooping permite que o tráfego seja enviado a todos os membros da rede de Vocera não importa onde vagueia. Isto assegura-se de que a característica da transmissão de Vocera trabalhe independentemente de onde o cliente vagueia. Desabilitar o IGMP Snooping é globalmente uma tarefa muito indesejável. Recomenda-se que o IGMP Snooping somente esteja desabilitado no Vocera VLAN que é conectado diretamente a cada WLC.

Refira configurar o IGMP Snooping para mais informação.

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

Realces do Multicast na versão 4.0.206.0 e mais tarde

Com a liberação de 4.0.206.0, Cisco introduz uma pergunta IGMP para permitir que os usuários vagueiem na camada 2 enviando uma pergunta geral IGMP quando este ocorre. O cliente responde então com o grupo de IGMP que são um membro de e este está construído uma ponte sobre à rede ligada com fio como descrito mais cedo neste documento. Quando um cliente vagueia a um controlador que não tenha Conectividade da camada 2, ou uma camada 3 vagueia, o roteamento síncrono está adicionado para pacotes do origem de transmissão múltipla. Quando um cliente, que terminasse uma camada 3 vaguear fontes um pacote de transmissão múltipla da rede Wireless, o controlador estrangeiro encapsula este pacote nos Ethernet sobre IP (EoIP) no túnel IP ao controlador da âncora. O controlador da âncora então para a frente que aos clientes Wireless localmente associou assim como constrói uma ponte sobre este de volta à rede ligada com fio onde é distribuído usando métodos de roteamento de transmissão múltipla normais.

Cenários de distribuição

Estes três cenários de distribuição cobrem melhores prática e parâmetros de projeto ajudar com um desenvolvimento bem sucedido do crachá de Vocera:

- Único desenvolvimento do controlador
- Desenvolvimento da camada 2 do controlador múltiplo
- Desenvolvimento da camada 3 do controlador múltiplo

Compreendendo como as características do crachá de Vocera interativas dentro de um ambiente rachado LWAPP MAC são essenciais. Com todos os cenários de distribuição, o Multicast deve ser permitido e o Balanceamento de carga agressivo deve ser desabilitado. Todo o crachá WLAN deve ser contido dentro do mesmo domínio de transmissão através de sua toda a rede.

Figura 4

Único desenvolvimento do controlador

Este é o cenário de distribuição o mais direto. Permite que você distribua a solução do crachá de Vocera com poucos interesses do desenvolvimento. Sua rede deve ser permitida para o roteamento IP Multicast de permitir somente que os Access point recebam os pacotes de transmissão múltipla LWAPP. Se for necessário, você pode limitar a complexidade do Multicast da rede configurando todo o Roteadores e Switches com o grupo de transmissão múltipla dos controladores.

Com o Multicast configurado globalmente no controlador, SSID apropriado, configurações de segurança, e todos os Access point registraram a solução do crachá de Vocera e todas suas funções operam-se como esperado. Com a função da transmissão de Vocera, um usuário vagueia e o tráfego multicast segue como esperado. Não há nenhuma configuração extra exigida ser configurado para permitir que esta solução funcione corretamente.

Quando um crachá de Vocera envia um mensagem de transmissão múltipla, como faz com a transmissão de Vocera, é encaminhado ao controlador. O controlador encapsula então este pacote de transmissão múltipla dentro de um pacote de transmissão múltipla LWAPP. A infraestrutura de rede encaminha este pacote a cada Access point que é conectado a este controlador. Quando o Access point recebe este pacote, olha então o encabeçamento do Multicast LWAPP para determinar que WLAN/SSID transmite então este pacote.

Figura 5 — Único controlador no modo do Multicast-Multicast

Desenvolvimento da camada 2 do controlador múltiplo

Os controladores múltiplos devem todos ter a Conectividade entre si através do mesmo domínio de transmissão da camada 2. Ambos os controladores são configurados para o Multicast como mostrado, usando os grupos de transmissão múltipla idênticos do Access point em cada controlador para limitar a fragmentação. Com a suposição que este domínio de transmissão da camada 2 está conectado através de um interruptor comum ou um grupo comum de Switches, a espião CGMP/IGMP neste Switches deve ser desabilitada para este única VLAN ou corrida 4.0.206.0 ou software WLC mais atrasado. Com a função da transmissão de Vocera e um usuário não vagueie de um Access point em um controlador a um Access point em um controlador diferente, lá é nenhum mecanismo para o IGMP junta-se para ser enviado à porta nova da camada 2 para que o IGMP Snooping trabalhe. Sem um pacote de IGMP que alcança o interruptor capaz ascendente CGMP ou IGMP, o grupo de transmissão múltipla especificado não é enviado ao controlador e consequentemente não é recebido pelo cliente. Em alguns casos isto pôde trabalhar, se um cliente que fosse parte do mesmo grupo da transmissão de Vocera tem enviado já este pacote de IGMP antes que o cliente vagueando vagueie no controlador novo com as vantagens da versão 4.0.206.0, um cliente que vagueasse a um outro controlador enquanto uma camada 2 vagueia recebe uma pergunta geral IGMP imediatamente depois da autenticação. O cliente deve então responder com os grupos interessados e o controlador novo é construído uma ponte sobre então isto localmente ao switch conectado. Isto permite as vantagens do IGMP e do CGMP em seu Switches ascendente.

Você pode criar o crachá adicional SSID e mergulhar 2 domínios para redes separadas do crachá enquanto sua rede é configurada para passar apropriadamente o tráfego multicast. Também, cada domínio de transmissão da camada 2 de Vocera criado deve existir em toda parte um controlador é conectado à rede de modo a para não quebrar o Multicast.

Figura 6 — Desenvolvimento da camada 2 do controlador múltiplo

Desenvolvimento da camada 3 do controlador múltiplo

A estratégia de distribuição vagueando da camada 3 deve somente ser usada com o controlador-à-controlador que vagueia com liberação de software WLC 4.0.206.0 ou mais tarde. Se um cliente que estivesse conectado ao grupo da transmissão de Vocera e receba o fluxo de transmissão múltipla apropriado e vagueie a um outro controlador enquanto uma camada 3 vagueia com vaguear da camada 3 LWAPP configurado, ele é perguntado para grupos de transmissão múltipla interessados. O cliente, quando fonte ao mesmo grupo da transmissão de Vocera, tiver estes pacotes entregados ao controlador da âncora através do túnel de EoIP e tiver estes pacotes distribuídos com os métodos de roteamento de transmissão múltipla normais.

Figura 7 — Desenvolvimento da camada 3 do controlador múltiplo

Disposições de VoWLAN: O Reccommendations de Cisco

As redes da Telefonia IP sem fio exigem o planeamento cuidadoso RF. Uma análise de site completa da Voz é exigida frequentemente para determinar os níveis apropriados da cobertura sem fio e para identificar origens de interferência. As escolhas da colocação e da Seleção de Antena do Access point podem extremamente ser facilitadas com a ajuda dos resultados de uma análise de site válida da Voz. A consideração a mais importante é a potência de transmissão do telefone wireless. Idealmente o telefone aprende a potência de transmissão do Access point e ajusta sua potência de transmissão àquela do Access point.

Embora a maioria das redes Wireless seja distribuída hoje após uma análise de site extensiva RF, são feitos com mantimento do serviço dos dados na mente também. Os telefones de VoWLAN são prováveis ter características vagueando diferentes e exigências diferentes da cobertura do que aquelas de um adaptador de WLAN típico para um cliente móvel tal como um portátil. Consequentemente, uma análise de site adicional para a Voz é recomendada frequentemente preparar-se para os requisitos de desempenho de clientes múltiplos de VoWLAN. Esta avaliação adicional dá a oportunidade de ajustar os Access point para assegurar-se de que os telefones de VoWLAN tenham bastante cobertura e largura de banda RF para fornecer a Qualidade de voz apropriada.

Para obter informações adicionais sobre das considerações de projeto RF, refira o capítulo em considerações de projeto do Radio Frequency (RF) WLAN no guia do projeto de LAN do Cisco Wireless, disponível em http://cisco.com/go/srnd.

Recomendações para construções, hospitais, e armazéns do Multi-assoalho

Considere os fatores alistados nesta seção quando você examina construções, hospitais, e armazéns do multi-assoalho.

Métodos e materiais da construção

Muitos aspectos da construção civil são desconhecidos ou hidden da análise de site, assim que você pôde ter que adquirir essa informação de outras fontes (tais como desenhos arquitetónicos). Alguns exemplos dos métodos e materiais típicos da construção que afetam a escala e a área de cobertura dos Access point inclui o filme metálico no vidro da janela, vidro leaded, paredes aço-enchidas, assoalhos do cimento e paredes com reforço de aço, isolação folha-suportada, vões das escadas e eixos de elevador, sondando as tubulações e os dispositivos bondes, e muitos outro.

Inventário

Os vários tipos de inventário podem afetar a escala RF, particularmente aqueles com aço alto ou conteúdo de água. Alguns artigos a olhar para incluem caixas de cartão, alimentos para animais de estimação, pintura, produtos petrolíferos, as peças de motor, e assim por diante.

Níveis do inventário

Certifique-se de você executar uma análise de site a níveis máximos do inventário ou na época da atividade a mais alta. Um armazém a nível da meia de 50% tem uma pegada muito diferente

RF do que o mesmo armazém a nível do inventário de 100%.

Níveis de atividade

Similarmente, uma área do escritório após horas (sem povos) tem uma pegada diferente RF do que a mesma área completamente dos povos durante o dia. Embora muitas partes da análise de site possam ser conduzidas sem ocupação completa, é essencial conduzir os valores chaves da verificação e da emenda da análise de site durante uma época em que o lugar for ocupado. Mais altas as exigências da utilização e a densidade dos usuários, mais importante é ter uma solução de diversidade bem-desenvolvida. Quando mais usuários estam presente, mais sinais estão recebidos no dispositivo de cada usuário. Os sinais adicionais causam mais disputa, mais pontos nulos, e mais distorção de multipath. A diversidade nas ajudas do Access point (Antenas) minimiza estas circunstâncias.

Construções do Multi-assoalho

Mantenha na mente estas diretrizes quando você conduz uma análise de site para um prédio do escritório típico:

- Os eixos de elevador obstruem e refletem sinais RF.
- As salas da fonte com inventário absorvem sinais.
- Os escritórios interiores com paredes duras absorvem sinais RF.
- As salas da ruptura (cozinhas) podem produzir 2.4 gigahertz da interferência com o uso dos fornos de micro-ondas.
- Os laboratórios de teste podem produzir uma interferência 2.4 gigahertz gigahertz ou 5, criando a distorção de multipath e as sombras RF.
- Os compartimentos tendem a absorver e sinais de bloco.
- As salas de conferência exigem a cobertura alta do Access point porque são áreas da utilização elevada.

A precaução extra deve ser administrada quando você examina facilidades do multi-assoalho. Os Access point em assoalhos diferentes podem interferir um com o otro tão facilmente quanto os Access point situados no mesmo assoalho. É possível usar este comportamento a sua vantagem durante uma avaliação. Usando antenas de ganho mais elevado, pôde ser possível penetrar assoalhos e tetos e fornecer a cobertura aos assoalhos acima assim como abaixo do assoalho onde o Access point é montado. Seja cuidadoso não sobrepor os canais entre Access point em assoalhos diferentes ou Access point no mesmo assoalho. Em construções do multi-inquilino, pôde haver os interesses de segurança que exigem o uso de umas mais baixas energias de transmissão e ganham mais baixo Antenas para manter sinais fora dos escritórios vizinhos.

Hospitais

O processo da avaliação para um hospital é muito mesmo que aquele para uma empresa, mas a disposição de uma facilidade do hospital tende a diferir nestas maneiras:

- As construções do hospital tendem a atravessar muitos projetos e adições da reconstrução. Cada construção adicional é provável ter materiais de construção diferentes com níveis diferentes da atenuação.
- A penetração do sinal através das paredes e dos assoalhos nas áreas pacientes é tipicamente mínima, que as ajudas criam micro-pilhas e variações multipath.

- A necessidade para a largura de banda aumenta com o uso crescente do equipamento do ultrassom WLAN e de outros aplicativos portáteis da imagem latente. A necessidade para aumentos da largura de banda com a adição de Voz wireless também.
- As pilhas dos cuidados médicos são pequenas, e vaguear sem emenda é essencial, especialmente com Aplicações de voz.
- A sobreposição da pilha pode ser alta, e assim que pode canalizar a reutilização.
- Os hospitais podem ter diversos tipos de redes Wireless instaladas. Isto inclui 2.4 gigahertz do equipamento non-802.11. Este equipamento pode causar a disputa com outras redes 2.4 gigahertz.
- As Antenas fixadas na parede da correção de programa da diversidade e as Antenas Omni-direcionais teto-montadas da diversidade são populares, mas mantêm-se na mente que a diversidade está exigida.

Armazéns

Os armazéns têm as grandes áreas aberta que contêm frequentemente cremalheiras altas do armazenamento. Muitas vezes, estas cremalheiras alcançam quase ao teto, onde os Access point são colocados tipicamente. Tais cremalheiras do armazenamento podem limitar a área que o Access point pode cobrir. Nesses casos, considere colocar Access point em outros lugar além do teto, tal como paredes laterais e colunas do cimento. Igualmente considere estes fatores quando você examina um armazém:

- Os níveis de inventário afetam o número de ponto de acesso necessário. Teste a cobertura com dois ou três Access point em lugar calculados da colocação.
- As sobreposições inesperadas da pilha são prováveis devido às variações multipath. A qualidade do sinal varia mais do que a força desse sinal. Os clientes puderam associar e operar-se melhor com Access point mais distante afastado do que com Access point próximos.
- Durante uma avaliação, os Access point e as Antenas geralmente não têm um cabo de antena que conecta os. Mas em um ambiente de produção, o Access point e a antena puderam exigir cabos de antena. Todos os cabos de antena introduzem a perda de sinal. A avaliação a mais exata inclui o tipo de antena a ser instalada e o comprimento do cabo a ser instalado. Uma boa ferramenta a usar-se para simular o cabo e sua perda é um atenuador em um jogo da avaliação.

Examinar uma facilidade de fabricação é similar a examinar um armazém, salvo que pôde haver muito mais fontes de interferência RF em uma facilidade de fabricação. Além, os aplicativos em uma facilidade de fabricação exigem geralmente mais largura de banda do que aquelas de um armazém. Estes aplicativos podem incluir a imagem latente video e a Voz wireless. A distorção de multipath é provável ser o grande problema de desempenho em uma facilidade de fabricação.

Mecanismos de segurança apoiados

Além do que o WEP estático e o PULO de Cisco para a autenticação e a criptografia de dados, os crachás de Vocera igualmente apoiam WPA-PEAP (MS-CHAP v2)/WPA2-PSK.

Considerações do PULO

O PULO permite que os dispositivos sejam autenticados mutuamente (ponto do crachá-à-acesso

e ponto-à-crachá do acesso) baseou em um nome de usuário e em uma senha. Em cima da autenticação, uma chave dinâmica é usada entre o telefone e o Access point para cifrar o tráfego. Contudo, o ataque do dicionário ASLEAP deve ser considerado quando você decide usar o PULO como sua solução da Segurança:

Refira o ataque do dicionário na vulnerabilidade do PULO de Cisco para mais informação.

Se o PULO é usado, um servidor Radius Pulo-complacente, tal como o Access Control Server de Cisco (ACS), está exigido para fornecer o acesso à base de dados de usuário. Cisco ACS pode ou armazenar o nome de usuário e a base de dados de senha localmente, ou pode alcançar essa informação de um diretório externo de Microsoft Windows NT. Ao usar o PULO, assegure-se de que as senhas elaboradas estejam usadas em todos os dispositivos Wireless. As senhas elaboradas são definidas como estar entre o 10 e os 12 caráteres por muito tempo e podem incluir o uppercase e os caracteres minúsculos assim como os caracteres especiais.

Porque todos os crachás usam a mesma senha e é armazenada dentro do crachá, Cisco recomenda que você usa nomes de usuário e senhas diferentes em clientes dos dados e em clientes wireless da Voz. Esta prática ajuda com seguimento e pesquisa de defeitos assim como Segurança. Embora seja uma opção de configuração válida para usar um base de dados (fora-ACS) externo para armazenar os nomes de usuário e as senhas para os crachás, Cisco não recomenda esta prática. Porque o ACS deve ser perguntado sempre que o crachá vagueia entre Access point, o atraso imprevisível para alcançar um base de dados fora-ACS poderia causar o retardo excessivo e a qualidade de voz deficiente.

Infraestrutura de rede Wireless

A rede da Telefonia IP sem fio, apenas como uma rede de telefonia do IP prendida, exige o planeamento cuidadoso para a configuração de VLAN, a cola da rede, o transporte do Multicast, e as escolhas do equipamento. Para redes prendido e da Telefonia IP sem fio, separe a Voz e os VLAN de dados são frequentemente a maioria de maneira eficaz do desenvolvimento sugerido assegurar a suficientes largura de banda de rede e facilidade do Troubleshooting.

Voz, dados e Vocera VLAN

Os VLAN fornecem um mecanismo segmentando redes em uns ou vários domínios de transmissão. Os VLAN são especialmente importantes para as redes de telefonia do IP, onde a recomendação típica é separar a voz e tráfego de dados em domínios diferentes da camada 2. Cisco recomenda que você configura VLAN separados para os crachás de Vocera da outra voz e tráfego de dados: um VLAN nativo para o tráfego de gerenciamento do Access point, VLAN de dados para o tráfego de dados, uma Voz ou um VLAN auxiliar para o tráfego de voz, e um VLAN para os crachás de Vocera. Uma Voz separada VLAN permite a rede de aproveitar-se da marcação da camada 2 e fornece filas de prioridade na porta de switch de acesso da camada 2. Isto assegura-se de que QoS apropriado esteja fornecido para várias classes de tráfego e ajuda-se a resolver casos de endereçamento tais como o endereçamento de IP, a Segurança, e o cálculo de dimensões da rede. Os crachás de Vocera usam uma característica da transmissão que utilize o Multicast para entregar. Este VLAN comum assegura aquele quando um crachá vagueia entre controladores, ele permanece parte do grupo de transmissão múltipla. Este último processo está discutido em detalhe quando o Multicast é endereçado mais tarde neste documento.

Cola da rede

A cola da rede de telefonia do IP é essencial assegurar-se de que a largura de banda adequada e os recursos estejam disponíveis para encontrar as procuras apresentadas pela presença de tráfego de voz. Além do que as diretrizes de design de telefonia IP usuais para componentes de execução sob medida tais como portas do gateway PSTN, os transcodificadores, largura de banda de WAN, e assim por diante, igualmente consideram estas edições 802.11b quando você faz sob medida sua rede da Telefonia IP sem fio. Os crachás de Vocera são um aplicativo especializado que esticam o número de clientes prendidos além de nossas recomendações da implementação típica.

Número dos dispositivos 802.11b pelo Access point

Cisco recomenda que você tem não mais de 15 a 25 dispositivos 802.11b pelo Access point.

Número de chamadas ativa pelo Access point

Vocera usa dois codecs diferentes baseados sobre se é um atendimento do crachá-à-crachá (codec proprietário da taxa baixa de bit) ou um atendimento do crachá-à-telefone (codec de G.711). Esta tabela mostra uma porcentagem da largura de banda disponível por taxas de dados e dá-lhe uma imagem mais clara da taxa de transferência prevista:

Processo de chamada	1 Mbps	2 Mbps	5.5 Mbps	11 Mbps
Crachá-à-telefone (G.711)	20.7%	11.8%	6.3%	4.7%
Crachá-à-crachá (codec proprietário da taxa baixa de bit)	9.4%	6.1%	4.2%	3.6%

Comute recomendações

Note: Se você usa um Cisco Catalyst 4000 Series Switch como o roteador principal na rede, assegure-se de que contenha, pelo menos, um módulo do Supervisor Engine 2+ (SUP2+) ou do Supervisor Engine 3 (SUP3). O módulo SUP1 ou SUP2 pode causar atrasos vagueando, como pode o Cisco catalyst 2948G, 2980G, 2980G-A, 4912, e o Switches 2948G-GE-TX.

Você pode criar um molde da porta de switch para o uso quando você configura toda a porta de switch para a conexão a um Access point. Este molde deve adicionar todas as características da segurança de linha de base e da elasticidade do molde de área de trabalho padrão. Além, quando você anexa o Access point a um Cisco Catalyst 3750 Switch, você pode aperfeiçoar o desempenho do Access point usando comandos qos do switching multicamada (MLS) limitar a taxa de porta e ao map class do serviço (CoS) aos ajustes do Differentiated Services Code Point (DSCP).

Nenhum tráfego que não for exigido por clientes de WLAN não deve ser enviado a um Access point. Um molde deve ser projetado de tal maneira que as ajudas criam uma conexão segura e de rede resistente com estas características:

- Retorne configurações de porta para optar — Impede conflitos de configuração cancelando todas as configurações de porta PRE-existentes.
- Dynamic Trunking Protocol (DTP) do desabilitação — Desabilita o entroncamento dinâmico, que não é precisado para a conexão a um Access point.

- Port Aggregation Protocol (PAgP) do desabilitação — PagP é permitido à revelia mas não precisado para portas do USER-revestimento.
- Permita a porta rapidamente — Permite que um interruptor recomece rapidamente o tráfego de encaminhamento se uma medida - o link da árvore vai para baixo.
- Configurar o VLAN sem fio — Cria um VLAN sem fio exclusivo que isole o tráfego Wireless de outros dados, Voz, e VLAN de gerenciamento. Isto isola o tráfego e assegura o maior controle do tráfego.
- Permita o Qualidade de Serviço (QoS); não confie a porta (marca para baixo a 0) — assegura o tratamento apropriado do tráfego de alta prioridade, incluindo softphones, e impede usuários da largura de banda excessiva de consumo reconfigurando seus PC.

O Switches de potência em linha WS-C3750-48PS-S pode ser usado para fornecer a potência aos Access point que são capazes de receber a potência em linha.

O Catalyst 6500 permite que você envie pacotes na linha taxa com todas as características descritas aqui assim como módulos de serviço numerosos de integração. O módulo de serviço Wireless (WiSM) permite que você tenha dois controladores cada um com a capacidade de controlar 150 Access point cada. Com até cinco WiSMs pelo chassi, isto permite que você controle sobre 1500 Access point que apoiam 50,000 clientes dentro de uma única arquitetura de switching do alto desempenho.

Disposições e configuração

Configuração do crachá

O utilitário de configuração do crachá de Vocera (BCU) e a configuração do crachá podem introduzir vaguear e latência em seu ambiente se feitos incorretamente. Usando o BCU e o editor das propriedades do crachá (BPE), verifique estes ajustes (veja figura 8):

- **A sub-rede que vagueia** é desabilitada.
- **Os canais do padrão da varredura (1,6,11)** são verificados.
- **Os usos IGMP da transmissão** são permitidos.
- A política vagueando é ajustada a **2** ou mais alto.

Figura 8 — Guia avançada de Vocera BCU

Quando a **sub-rede que vagueia** é verificada, instrui o crachá pedir um endereço IP de Um ou Mais Servidores Cisco ICM NT novo após cada um vagueia. No ambiente LWAPP, as ajudas da infraestrutura mantêm a conectividade de cliente na camada 3. Quando um cliente da Voz deve esperar o servidor DHCP para responder antes que possa enviar ou receber pacotes, o retardo e tremulação está introduzido. Se os **canais do padrão da varredura (1,6,11)** não são verificados, o crachá faz a varredura de todos os canais 802.11b quando o crachá olha para vaguear. Isto impede a transmissão dos pacotes e de vaguear sem emenda.

Acordo AutoRF para seu ambiente

Como descrito na seção das recomendações deste documento, é importante compreender que cada local o tem é possuir características RF. AutoRF ou o Radio Resource Management (RRM) puderam precisar de ser ajustado, com a compreensão que cada local é diferente e AutoRF/RRM deve ser ajustado para seu ambiente.

Antes que você ajuste AutoRF, refira a gerência de recursos de rádio sob redes Wireless unificadas para mais informação.

RRM permite que você ajuste a potência de transmissão de cada Access point, ajustando como forte cada Access point ouve seu terceiro vizinho mais forte. Este valor pode somente ser ajustado do CLI que usa o **802.11b avançado configuração TX-potência-trilha o** comando como descrito em ajustes da atribuição do nível de potência TX.

Antes que você ajuste AutoRF, anda o local do desenvolvimento usando o crachá de Vocera como vestido pelo utilizador final e usa uma ferramenta da análise de site a fim ganhar uma compreensão forte de como o crachá vagueia e em do que potência cada Access point é considerado. Uma vez que isto está completo e se determina que ajustar este valor está exigido, comece com um valor – de 71 dBm para o algoritmo de controle da potência de transmissão. Use este parâmetro CLI:

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

Permita que a rede trabalhe com este ajuste com um mínimo de 30 minutos a uma hora antes que você observe todas as mudanças. Uma vez que a rede é dada uma suficiente quantidade de tempo, anda o local usando a mesmos ferramenta e crachás da avaliação outra vez. Observe as mesmas características e potência vagueando do Access point. O objetivo aqui é tentar mandar os crachás vaguear ou antes do Access point seguinte para obter o Signal to Noise Ratio melhor possível.

- **Como eu sei se a potência de transmissão está demasiado quente ou demasiado fria?**Determinar se você tem seu ponto inicial da potência de transmissão demasiado altamente ou exige demasiado baixo uma boa compreensão de seu ambiente. Se você andou sua área inteira do desenvolvimento (onde você espera seus crachás de Vocera funcionar), você deve saber onde seus Access point são encontrados assim como experimentar o comportamento vagueando do crachá.
- **Que eu faço se minha potência de transmissão está demasiado quente?**O crachá de Vocera vagueia baseado unicamente na intensidade de sinal um pouco do que a qualidade de sinal. Se o crachá de Vocera não vagueia depois que passa diversos Access point quando contratado no tutorial bem-vindo ou o tom de teste, o crachá está considerado ser pegajoso. Se este comportamento é indicativo da área inteira do desenvolvimento do terreno, a seguir seu ponto inicial da potência de transmissão está demasiado quente e deve ser suportado para baixo. Se somente uma ou dois áreas isoladas mostram este comportamento e o resto das características vagueando mais idealistas das mostras da área do desenvolvimento esta não é uma indicação que sua rede esteja executando demasiado quente.
- **Que eu faço se minha potência de transmissão está demasiado fria?**O padrão transmite o ponto inicial deve quase nunca fornecer-lhe uma área do desenvolvimento onde sua rede execute demasiado frio. Se o ponto inicial da potência de transmissão está ajustado para baixo, e andar os salões com o crachá de Vocera o fornece um ambiente onde o crachá vagueasse bem, mas perdesse a Conectividade e/ou os mortos/cobertura manchado, a seguir sua rede pôde ter sido ajustada demasiado baixo. Se isto não é característico de sua toda a rede mas não é isolado a uma ou dois áreas, a seguir é mais indicativo de um furo da cobertura um pouco do que um problema para toda a rede.
- **Comportamento isolado**Se você encontra que em uma ou dois áreas, o crachá cola a um

Access point um pouco do que vagueando em uma maneira idealista, examine esta área.Como é esta área diferente do resto do terreno?Se esta/estas áreas é saídas ou áreas próximas da construção sob a construção, poderia a detecção do furo da cobertura forçar estes Access point para levantar a potência?Olhe as lista vizinhas do arquivo de registro e do Access point WLC para ajudar a determinar porque tal anomalia poderia ocorrer.Se você encontra que em umas ou várias áreas isoladas, nas experiências do crachá inoperantes ou na cobertura manchado, a seguir você precisa de examinar separadamente estas áreas.Está esta área perto de um eixo de elevador, da radiologia, ou de uma sala da ruptura?Estas áreas puderam melhor ser seridas pela instalação ou pela colocação melhor de um Access point para permitir a melhor cobertura da Voz.Em ambos os casos, é sempre aconselhável compreender que você está trabalhando em um espectro de rádio não-licenciado e o comportamento idealista não pôde nunca ser realizável. Isto poderia acontecer quando você é situado ao lado de uma torre ou um dispositivo da transmissão de rádio, um transmissor de televisão ou possivelmente um non-802.11 facilidade do reparo 2.4 gigahertz (telefones wireless, e assim por diante).

Configuração da infraestrutura de rede Wireless

O projeto de rede e o guia de distribuição do Cisco Unified Wireless devem ser seguidos para a configuração total de seu WLC. Esta seção fornece as recomendações adicionais específicas aos crachás de uma comunicação de Vocera®.

Note: As mudanças estão deixadas unsaved se você não pressiona o **botão Apply Button** antes que você se transporte à próxima etapa.

Termine estas etapas sob o menu de nível superior do **controlador**:

1. Mude o Modo multicast dos Ethernet ao **Multicast**.
2. Ajuste o endereço de grupo de transmissão múltipla a **239.0.0.255** (ou a algum outro endereço de grupo de transmissão múltipla não utilizado).
3. Ajuste o nome do Domain Name e da RF-rede da mobilidade do padrão a seu projeto de rede.
4. Desabilite o **Balanceamento de carga agressivo**.**Figura 9 — Configuração geral WLC**

Crie relações

Clique o **controlador > as relações**.

Note: Seus VLAN e endereço IP de Um ou Mais Servidores Cisco ICM NT variam. Os screen shots aqui fornecem o endereçamento da amostra que não deve diretamente ser seguido.

Figura 10 — Lista de relações WLC

Crie a interface de voz de Vocera

Conclua estes passos:

1. Clique em **New**.
2. Inscreva um representante do nome da etiqueta de sua rede de Vocera VoWLAN no campo

de nome da relação.
3. Inscreva o número de VLAN dessa rede de VoWLAN no campo do ID de VLAN.
4. O clique **aplica-se** e clica-se então **edita** a fim editar a relação que você apenas criou.
5. Incorpore o endereçamento de IP para esta relação que está na escala do VLAN e da outra informação relacionada.
6. Clique em Apply.

Configuração Sem fio-específica

Para um WLAN que tenha somente crachás de Vocera, esta configuração fornece exemplos de configuração que melhor apoie o aplicativo da transmissão de Vocera.

- O período DTIM é **1.**
- O apoio para 802.11g é desabilitado. Somente a taxa de dados 802.11b de **11 Mpbs** é **imperativa**.
- O preâmbulo curto é desabilitado.
- DTPC é desabilitado.

Figura 11 — configuração 802.11b/g

Configuração WLAN

Conclua estes passos:

1. Atualize o campo de rádio da política a um valor que o melhor o caiba precise.
2. Mude o status administrativo ao **permitido**.
3. Ajuste o timeout de sessão a **1800**.
4. Ajuste Qualidade de Serviço à **platina**.
5. Ajuste a transmissão SSID ao **permitido**.
6. Ajuste o nome da relação à relação criada para os crachás de uma comunicação de Vocera.
7. Ajuste as opções de segurança combinar suas políticas corporativas.**Figura 12 — Configuração WLAN**

Configurar o detalhe do Access point

Conclua estes passos:

1. Clique o **detalhe**.
2. Configurar o nome AP.
3. Assegure-se de que o Access point esteja configurado para o DHCP.
4. Assegure-se de que o status administrativo **esteja permitido**.
5. A modificação AP" deve ser ajustada ao **local**.
6. Entre no lugar do Access point.
7. Dê entrada com o nome do controlador que o Access point pertence a. O nome do controlador pode ser encontrado na página do monitor.
8. Clique em Apply.**Figura 13 — Detalhe AP**

Configurar o rádio 802.11b/g

Conclua estes passos:

1. Clique o **Sem fio** situado na parte superior do WLC e verifique que todos os Access point sob o status administrativo estão ajustados **para permitir**.**Figura 14**
2. **Rede do** clique (situada perto de 802.11b/g).
3. Clique **AutoRF**.
4. Use AutoRF para criar uma cobertura completa com a NON-sobreposição do canal RF e de uma potência de transmissão. A fim fazer isto, selecione **automático** para a atribuição do canal RF e a atribuição do nível de potência TX.**Figura 15**
5. Clique em Apply.
6. Clique a **configuração da salvaguarda** e veja o acordo AutoRF para sua seção do ambiente deste documento.
7. Escolha o **Sem fio > os Access point > os rádios 802.11b/g**.**Figura 16**

Verificação da Telefonia IP sem fio

Depois que você conduz uma análise de site RF e configura os Access point e os telefones, é crucial conduzir testes de verificação para assegurar-se de que tudo trabalhe como desejado. Estes testes devem ser executados de todo destes lugar:

- A área preliminar de cada pilha do Access point (onde os crachás são mais provável de conectar a esse Access point particular).
- Algum lugar onde pôde haver um volume de chamada alto.
- Os lugar onde o uso pôde ser raro mas a cobertura ainda têm que ser certificados (por exemplo, vões das escadas, toaletes, e assim por diante).
- Nas franjas da área de cobertura do Access point.
- • Estes testes podem ser executados paralelamente ou série. Se executado paralelamente, assegure-se de que os telefones estejam postos fora entre pontos de testes para testar a associação, a autenticação, e o registro completos em cada lugar. Os testes vaguear e de carga devem ser os testes finais.

Associação, autenticação, e registro

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

- Em pontos múltiplos durante todo o ambiente, a ligação inicial os crachás e verifica a associação com o Access point. Se o crachá não associa com o Access point, execute estas verificações:Verifique a configuração do crachá para assegurar o SSID apropriado, tipo do autenticação, e assim por diante.Verifique a configuração WLC para assegurar o SSID apropriado, tipo do autenticação, os canais de rádio, e assim por diante.Verifique sua análise de site para assegurar-se de que o lugar tenha a cobertura adequada RF.
- Em pontos múltiplos durante todo o ambiente, assegure-se de que o telefone autentique através do Access point com sucesso. Se o cliente não autentica, verifique a chave de WEP ou o nome de usuário e senha do PULO nos crachás. Também, verifique o nome de usuário e senha no servidor AAA usando um portátil wireless com as credenciais idênticas.
- Em pontos múltiplos durante todo o ambiente, assegure-se de que os crachás se registrem com o servidor de comunicação de Vocera. Se o cliente não se registra, execute estas

verificações:Verifique que o crachá tem o endereço IP de Um ou Mais Servidores Cisco ICM NT correto, a máscara de sub-rede, o gateway principal, o TFTP, preliminares preliminar/secundários e DNS.

- Chamadas de voz estacionárias:Em pontos múltiplos durante todo o ambiente, quando você estiver ainda, faça um atendimento a um outro crachá e conduza 60 aos testes da Voz 120-second para verificar a Qualidade de voz. Se a Qualidade de voz é inaceitável, mova um crachá para um lugar melhor e teste-o outra vez. É a Qualidade de voz aceitável? Se não, verifique sua cobertura sem fio.Se o server da telefonia é configurado, em pontos múltiplos durante todo o ambiente, esteja ainda e faça um atendimento a um telefone prendido e conduza 60 aos testes da Voz 120-second para verificar a Qualidade de voz. Se a Qualidade de voz é inaceitável, pergunte se você faz um atendimento usando o telefone prendido. É a Qualidade de voz aceitável? Se não, verifique o projeto de rede ligada com fio contra as diretrizes.
- Use as ferramentas da análise de site para verificar que há não mais de um Access point pelo canal RF desse lugar com uma intensidade de sinal ([RSSI] do indicador da força de sinal recebido) maior de 35. Se há dois Access point atuais no mesmo canal, assegure-se de que a razão sinal-ruído (SNR) esteja tão alta como possível minimizar a interferência. Por exemplo, se o Access point mais forte tem um RSSI de 35, idealmente o Access point mais fraco deve ter um RSSI de menos de 20. A fim conseguir este objetivo, você pôde ter que reduzir a uma potência de transmissão do Access point ou mover o Access point.
- Verifique os ajustes de QoS no Access point para confirmar configurações recomendadas apropriadas.
- Atendimentos vagueando do crachá:Se o server da telefonia não está disponível, inicie o curso de Vocera com o comando **começam o curso**.OUSe o server da telefonia está disponível, inicie um atendimento com um dispositivo estacionário ao crachá.Verifique continuamente a Qualidade de voz quando você atravessar a área total da cobertura sem fio. Se a Qualidade de voz é insuficiente, execute estas tarefas:Escute todas as mudanças inaceitáveis na Qualidade de voz e tome a nota do lugar e dos valores de rádio em seu portátil e os valores CQ do crachá.Olhe e escute o crachá para vaguear ao Access point seguinte.Note os outros Access point disponíveis na análise de site para verificar a cobertura e a interferência.
- Faça ajustes à colocação e aos ajustes do Access point para ajustar o WLAN, e execute estas verificações para assegurar a Qualidade de voz:Use as ferramentas da análise de site e verifique que há não mais de um Access point pelo canal com um valor RSSI maior de 35 em todo o lugar dado. Idealmente, todos Access point restantes no mesmo canal devem ter valores RSSI o mais baixo possível (preferivelmente menos de 20). Na beira da área de cobertura onde o RSSI é 35, o RSSI para todos Access point restantes no mesmo canal deve idealmente ser menos de 20.Use as ferramentas da análise de site para verificar que há pelo menos dois Access point (totais, nos canais separados) visíveis em todo o lugar com suficiente intensidade de sinal.Certifique-se de todos os Access point em uma área vagueando dada sejam em uma rede da camada 2.

Edições vagueando comuns

Estas edições vagueando podem ocorrer:

- O crachá não vagueia quando colocado diretamente sob o Access point.

- O crachá é mais provável não alcançando os pontos iniciais diferenciais vagueando para o indicador da força de sinal recebido (RSSI) e a utilização de canal (CU). Ajuste o formulário do ponto inicial da potência de transmissão o WLC.
- O crachá não recebe balizas nem sonda respostas do Access point.
- O crachá vagueia demasiado lentamente.

O crachá perde a conexão à rede ou o serviço de voz é perdido ao vaguear

- Verifique a autenticação para ver se há uma má combinação possível WEP.
- O crachá não manda o IGMP junta-se ou a rede envia perguntas IGMP durante vaguear. Consequentemente, a função da transmissão de Vocera falha durante uma camada 2/Layer 3 vagueia.
- O crachá é capaz da camada sem emenda 2 que vagueia somente (a menos que um mecanismo da mobilidade da camada 3 é configurado). Assegure-se de que o WLC novo não esteja servindo uma sub-rede diferente IP.
- Verifique que o Access point associado/controlador tem a conectividade IP ao servidor de comunicação de Vocera.
- Verifique os valores CQ da intensidade de sinal e do crachá RF.

O crachá perde a Qualidade de voz ao vaguear

- Verifique para ver se há o baixo RSSI no Access point do destino.
- A sobreposição do canal pôde ser insuficiente. O crachá deve ter o tempo para entregar lisamente fora do atendimento antes que perca seu sinal com o Access point original.
- O sinal do Access point original pôde ser perdido.

Problemas de áudio

Há alguns erros da configuração comum que podem causar alguns problemas de audio facilmente resolvidos. Se possível, verifique problemas de áudio contra um crachá estacionário (da referência) para ajudar o estreito o problema a uma edição wireless. Os problemas de áudio comuns incluem:

- Áudio unilateral
- Áudio agitado ou robótico
- Registro e problemas de autenticação

Áudio unilateral

- Este problema pode ocorrer nas áreas da franja de um Access point, onde um sinal possa ser demasiado fraco no lado do crachá ou no lado do Access point. Combinar as configurações de energia no Access point ao crachá (20 mW), quando possível, pode fixar este problema. Este problema é o mais comum quando a variação entre o ajuste do Access point e o ajuste do crachá é grande (por exemplo, 100 mW no Access point e 28 mW no crachá).
- Verifique o gateway e Roteamento IP para ver se há a Qualidade de voz.
- Verifique para ver se um Firewall ou um NAT estão no trajeto dos pacotes de UDP proprietários. À revelia, os Firewall e os NAT causam o áudio de sentido único ou não audio.

Cisco IOS® e PIX NAT e Firewall tem a capacidade para alterar aquelas conexões de modo que o áudio de duas vias possa fluir.Se você usa a mobilidade da camada 3, sua rede poderia obstruir o tráfego ascendente com verificações do Unicast Reverse Path Forwarding (uRPF).
- O áudio de sentido único pode ocorrer se pôr em esconderijo ARP não é configurado no WLC.

Áudio agitado ou robótico

- Um motivo comum para o áudio agitado ou robótico é quando uma micro-ondas se opera próximo. As micro-ondas começam no canal 9 e podem estender dos canais 6 a 14.
- Verifique para ver se há telefones wireless 2.4 gigahertz e outros dispositivos Wireless de atendimento da enfermeira usando ferramentas como Cognio.

Registro e problemas de autenticação

Quando você encontra problemas com autenticação, execute estas verificações:

- Verifique SSID para certificar-se que combinam no crachá e o Access point (ou rede). Igualmente seja certo que a rede tem uma rota ao server de Vocera.
- Verifique as chaves de WEP para certificar-se que combinam. É uma boa ideia reenter os no utilitário de configuração do crachá (BCU) e reprogram o crachá, porque é fácil fazer um erro de digitação quando você incorpora uma chave de WEP ou uma senha.

Estes mensagens ou sintomas podem ocorrer:

- Não pode apoiar todas as capacidades pedidas — Isto é mais provável uma má combinação da criptografia entre o Access point e o cliente.
- Autenticação falhada/nenhum AP encontrado — Assegure o fósforo dos tipos do autenticação no Access point e no cliente.
- Nenhum serviço – Configuração IP falhada — Se você usa o WEP estático, assegure-se de que as chaves estejam configuradas corretamente. Assegure-se de que outros clientes possam receber o DHCP usando o mesmo SSID.
- De-autentique todos os clientes TKIP do AP — Este problema acontece quando o Access point detecta dois erros MIC dentro de 60 segundos. Esta contramedida mantém todos os clientes TKIP de autenticar novamente por 60 segundos.
- Reautenticação/timeout de sessão — Se configurado, um timeout de sessão provoca uma reautenticação que cause diferenças no fluxo de voz (Senhora 300 + atraso MACILENTO para a autenticação do 802.1x).

Apêndice A

AP e substituição de antena

Esta seção dá exemplos da colocação apropriada e imprópria dos Access point (AP) e das Antenas.

Figura 17 mostra a colocação imprópria de um Access point e de Antenas perto de um Eu-feixe,

que crie testes padrões distorcidos do sinal. Um ponto nulo RF é criado pelo cruzamento de ondas do sinal, e a distorção de multipath é criada quando as ondas do sinal são refletidas. Esta colocação conduz à cobertura muito pequena atrás do Access point e à qualidade de sinal reduzida na frente do Access point.

Figura 17 — Colocação imprópria das Antenas perto de um Eu-feixe

Figura 18 mostra as mudanças ou as distorções da propagação do sinal causadas por um Eu-feixe. O Eu-feixe cria muitas reflexões dos pacotes recebidos e dos pacotes transmitido. Os sinais refletido conduzem à qualidade de sinal muito deficiente devido aos pontos nulos e às interferências multipath. Contudo, a intensidade de sinal é alta porque as antenas de ponto de acesso estão tão perto ao Eu-feixe.

Figura 18 — Distorções de sinal causadas colocando as Antenas demasiado perto a um Eu-feixe

O Access point e a substituição de antena em figura 19 são melhores porque é longe dos Eu-feixes e há menos sinais refletido, menos pontos nulos, e menos interferências multipath. Esta colocação não é ainda perfeita porque o cabo do Ethernet não deve ser bobinado acima tão próximo à antena. Também, o Access point podia ser girado com as Antenas 2.4GHz apontadas ao assoalho. Isto fornece a melhor cobertura diretamente abaixo do Access point. Não há nenhum usuários acima do Access point.

Figura 19 — Access point e Antenas montados em uma parede, longe dos Eu-feixes

Figura 20 mostra a propagação do sinal causada pela parede em que o Access point é montado.

Figura 20 — Reflexão do sinal causada por uma parede

Os exemplos precedentes igualmente aplicam-se quando você coloca Access point e Antenas em ou perto do teto em um ambiente de empreendimento padrão. Se há canais de ar do metal, eixos de elevador, ou outras barreiras físicas que podem causar a reflexão ou as interferências multipath do sinal, recomenda Cisco altamente que você move as Antenas longe daquelas barreiras. No caso do elevador, mova a antena alguns pés afastado a fim ajudar a eliminar a reflexão e a distorção do sinal. O mesmo é verdadeiro com os canais de ar no teto.

Uma avaliação conduzida sem enviar e receber pacotes não é suficiente. O exemplo do Eu-feixe mostra a criação dos pontos nulos que podem resultar dos pacotes que têm erros CRC. Os pacotes de voz com erros CRC são os pacotes faltados que afetam adversamente a Qualidade de voz. Neste exemplo, aqueles pacotes podiam estar acima do assoalho do ruído medido por uma ferramenta da avaliação. Consequentemente, é muito importante que as medidas dos níveis de sinal da análise de site não somente mas igualmente gerenciem pacotes e relatam então erros de pacote.

Figura 21 mostra Cisco AP1200 montado corretamente a uma T-barra do teto, com as Antenas em uma posição Omni-direcional.

Figura 21 — Cisco AP1200 montado a um teto

Figura 22 mostra uma antena de diversidade Omni-direcional do Cisco Aironet 5959 montada corretamente a uma T-barra do teto. Neste caso, Cisco AP1200 é montado acima da telha do teto.

Figura 22 — Antena do Cisco Aironet 5959 montada a um teto

Figura 23 mostra Cisco AP1200 montado corretamente a uma parede.

Figura 23 — Cisco AP1200 montado a uma parede

Figura 24 mostra a antena da correção de programa da diversidade do Cisco Aironet 2012

montada a uma parede. Neste caso, Cisco AP1200 é montado acima da telha do teto.

Figura 24 — Antena do Cisco Aironet 2012 montada a uma parede

Para as áreas onde o tráfego de usuário é alto (como os espaços do escritório, escolas, lojas de varejo, e hospitais), Cisco recomenda que você coloca o acesso indica da vista e coloca Antenas discretas abaixo do teto. A separação para Antenas da NON-diversidade não deve exceder 18 polegadas.

Interferência e distorção de multipath

O desempenho da taxa de transferência de dados da rede de WLAN é afetado por sinais inusáveis. As interferências de WLAN podem ser geradas por fornos de micro-ondas, por telefones sem fio 2.4 gigahertz, por dispositivos de Bluetooth, ou pelo outro equipamento eletrônico que opera-se na faixa 2.4 gigahertz. A interferência igualmente vem tipicamente de outros Access point e dispositivos do cliente que pertencem no WLAN mas que esteja distante o suficiente ausente de modo que seu sinal seja enfraquecido ou se torne corrompido. Os Access point que não são parte da infraestrutura de rede podem igualmente causar interferências de WLAN e são identificados como Access point desonestos.

A interferência e a distorção de multipath causam o sinal transmitido flutuar. A interferência diminui a razão sinal-ruído (SNR) para uma taxa de dados particular. Os contagens de novas tentativas do pacote vão acima em uma área onde a interferência e/ou a distorção de multipath sejam altas. A interferência é referida igualmente como o assoalho do nível de ruído ou do ruído. A força do sinal recebido de seu Access point associado deve estar altamente bastante acima do nível de ruído do receptor a ser descodificado corretamente. Este nível de força é referido como a razão sinal-ruído, ou o SNR. O SNR ideal para o crachá de Vocera é DB 25. Por exemplo, se o assoalho do ruído é 95 decibéis por miliwatt (dBm) e o sinal recebido no telefone é 70 dBm, a seguir a razão sinal-ruído é DB 25. (Veja figura 25.)

Figura 25 — Razão sinal-ruído (SNR)

Quando você muda o tipo e o lugar da antena, pode reduzir a distorção de multipath e a interferência. O ganho da antena adiciona ao ganho de sistema e pode reduzir a interferência se o transmissor de interferência não é diretamente na frente da antena direcional.

Quando as antenas direcional puderem ser de aplicativos internos do valor maior com certeza, a grande maioria das instalações internas usa Antenas Omni-direcionais. O Directionality deve restritamente ser determinado por uma análise de site correta e apropriada. Se você usa um Omni-direcional ou remenda a antena, os ambientes internos exigem antenas de diversidade abrandar a distorção de multipath. Os rádios do Access point do Cisco Aironet Series permitem o apoio da diversidade.

Atenuação de sinal

A atenuação de sinal ou a perda de sinal ocorrem mesmo enquanto o sinal passa através do ar. A força da perda de sinal é mais pronunciada porque o sinal passa através dos objetos diferentes. Uma potência de transmissão de 20 mW é equivalente a 13 dBm. Consequentemente, se a potência transmitida no ponto de entrada de uma parede da placa de gesso está em 13 dBm, a intensidade de sinal é reduzida ao dBm 10 ao retirar essa parede. Esta tabela mostra a perda provável na intensidade de sinal causada por vários tipos de objetos.

Atenuação de sinal causada por vários tipos de objetos

Objeto no trajeto do sinal	Atenuação de sinal através do objeto
Parede da placa de gesso	3dB
Parede de vidro com quadro do metal	DB 6
Parede do bloco de cinza	DB 4
Indicador do escritório	3dB
Porta do metal	DB 6
Porta do metal na parede de tijolo	DB 12
Corpo humano	3dB

Cada local examinado tem níveis diferentes da distorção de multipath, o sinal perde, e ruído do sinal. Os hospitais são tipicamente o ambiente o mais desafiante para examinar devido à distorção de multipath alta, perdas de sinal e ruído do sinal. Os hospitais tomam mais por muito tempo para examinar, exigir uma população mais densa dos Access point, e para exigir padrões de alto desempenho. A fabricação e as lojas são as seguintes o mais duramente a examinar. Estes locais têm geralmente o tapume do metal e muitos metal os objetos no assoalho, que conduzem aos sinais refletido que recreiam a distorção de multipath. Os prédios do escritório e os locais da hospitalidade têm geralmente a atenuação de sinal alta mas um grau menor de distorção de multipath.

Informações Relacionadas

- Implantação de Controladoras Wireless LAN Cisco 440X Series
- Projeto de rede da referência da solução
- Especificações de sistema de comunicação de Vocera
- Suporte Técnico e Documentação - Cisco Systems