Guia de design CX - Sem fio para grandes redes públicas

Contents

Introdução

Este documento descreve as diretrizes de projeto e configuração para grandes redes Wi-Fi públicas.

Guia de design do CX

Os guias de design do CX são escritos por especialistas do Cisco Technical Assistance Center (TAC) e do Cisco Professional Services (PS) e revisados por especialistas da Cisco; os guias são baseados nas práticas recomendadas da Cisco, bem como no conhecimento e na experiência obtidos com inúmeras implementações de clientes ao longo de muitos anos. As redes projetadas e configuradas de acordo com as recomendações neste documento ajudam a evitar armadilhas comuns e a melhorar a operação da rede.

Âmbito de aplicação e definições

Este documento fornece diretrizes de design e configuração para grandes redes sem fio públicas.

Definição: Grandes redes públicas - implantações sem fio, frequentemente em alta densidade, que fornecem conectividade de rede para milhares de dispositivos clientes desconhecidos e/ou não gerenciados.

Este documento frequentemente supõe que a rede de destino está fornecendo serviços para eventos grandes e/ou temporários. Ele também se encaixa em redes estáticas permanentes para locais que recebem muitos convidados. Por exemplo, um shopping center ou aeroporto tem semelhanças com a rede Wi-Fi de um estádio ou local de concertos - no sentido de que não há controle sobre os usuários finais e eles existem na rede normalmente apenas por algumas horas ou no máximo por dia.

A cobertura sem fio para grandes eventos ou locais tem seu próprio conjunto de requisitos, que tende a ser diferente das redes empresariais, de manufatura ou até mesmo de grandes redes educacionais. As grandes redes públicas podem ter milhares de pessoas, concentradas em apenas um ou alguns edifícios. Eles podem ter roaming de cliente muito frequente, constantemente ou durante picos, além de a rede precisar ser o mais compatível possível com qualquer coisa em termos de dispositivos de cliente sem fio, sem controle sobre a configuração ou a segurança do dispositivo de cliente.

Este guia apresenta conceitos gerais de RF para alta densidade, bem como detalhes de implementação. Muitos dos conceitos de rádio neste guia se aplicam a todas as redes de alta densidade, incluindo a Cisco Meraki. No entanto, os detalhes e as configurações da implementação estão focados no Catalyst Wireless usando o Catalyst 9800 Wireless Controller, já que esta é a solução mais comum implantada para grandes redes públicas atualmente.

Este documento usa os termos Controlador sem fio e Controlador de LAN sem fio (WLC) de forma intercambiável.

Grandes redes públicas

Grandes redes públicas e de eventos são únicas em muitos aspectos, este documento explora e fornece orientação sobre essas áreas principais.

- Grandes redes públicas são intensas; há milhares de dispositivos em um espaço reduzido de Radiofreqüência (RF) e roaming significativo à medida que as pessoas andam por aí, alguns eventos e locais podem ser mais estáticos com picos de largura de banda em horários muito específicos. A infraestrutura precisa lidar com todas essas alterações de estado da forma mais tranquila possível para os clientes que entram e se movimentam na área.
- A principal prioridade é a facilidade de integração. Um cliente associado é um cliente feliz. Isso significa que você deseja fazer a associação do cliente à rede o mais rápido possível. Um cliente que não está conectado a Wi-Fi verifica se há pontos de acesso disponíveis, o que gera energia de RF indesejada, o que se traduz em congestionamento adicional e perda de capacidade pelo ar.
- A implantação de RF precisa ser projetada com o maior cuidado possível. Um projeto de RF apropriado usando antenas direcionais é obrigatório se for necessária uma densidade muito alta ou se o local tiver grandes espaços abertos e/ou tetos altos.
- Outra unidade de design importante é a compatibilidade. Alguns recursos são padrão na especificação 802.11, enquanto outros recursos são proprietários, nem representam qualquer problema para os clientes. No entanto, a realidade é diferente e há muitos drivers de cliente mal programados que se comportam mal quando veem beacons complicados ou

recursos/configurações que não entendem.
- A solução de problemas é desafiadora devido às restrições de escala e tempo. Se algo não funcionar com um cliente específico, você não poderá trabalhar com esse usuário final para entender o problema. Os usuários podem ser difíceis de encontrar, mas também podem não cooperar devido à natureza transitória de sua visita no local.
- A segurança é um fator importante. Há menos controle devido à grande quantidade de visitantes convidados e uma superfície de ataque muito maior.

Referências externas

Nome do documento	Fonte	Local
Práticas recomendadas de configuração do Cisco Catalyst 9800 Series	Cisco	Ligação
Solucionar problemas da CPU da controladora Wireless LAN	Cisco	Ligação
Validar o rendimento do Wi-Fi: Guia de teste e monitoramento	Cisco	Ligação
Guia de implantação do ponto de acesso Cisco Catalyst CW9166D1	Cisco	Ligação
Guia de implantação da antena de estádio Catalyst 9104 (C-ANT9104)	Cisco	Ligação
Monitorar KPIs do Catalyst 9800 (Indicadores-chave de desempenho)	Cisco	Ligação
Troubleshooting de Fluxo de Problemas de Conectividade do Cliente Catalyst 9800	Cisco	Ligação
Guia de configuração de software do Cisco Catalyst 9800 Series Wireless Controller (17.12)	Cisco	Ligação
Wi-Fi 6E: o próximo grande capítulo no white paper sobre Wi-Fi	Cisco	Ligação

Ressalva

Este documento oferece recomendações com base em determinados cenários, suposições e conhecimento obtidos de várias implantações. No entanto, você, o leitor, é responsável por determinar o projeto de rede, os negócios, a conformidade regulamentar, a segurança, a

privacidade e outros requisitos, inclusive se deve seguir as orientações ou recomendações fornecidas neste guia.

Projetando a rede

Considerações de RF

Tipos de local

Este guia se concentra em grandes redes de convidados, geralmente abertas ao público e com controle limitado sobre usuários finais e tipos de dispositivos clientes. Esses tipos de redes podem ser implantados em vários locais e podem ser temporários ou permanentes. O caso de uso principal geralmente é fornecer acesso à Internet aos visitantes, embora esse raramente seja o único caso de uso.

Locais típicos:

- Estádios e arenas
- Locais de conferência
- Grandes auditórios

Do ponto de vista de RF, cada um desses tipos de localização tem seu próprio conjunto de nuances. A maioria desses exemplos são geralmente instalações permanentes, além de locais de conferência, já que podem ser permanentes ou configurados para uma feira de negócios específica em caráter temporário.

Outros locais:

- Navio de cruzeiro
- Aeroporto
- Centro de Compras / Shopping Center

Aeroportos e navios de cruzeiro também são exemplos de implantações que se encaixam na categoria de grandes redes públicas; no entanto, eles têm considerações adicionais específicas para cada caso e frequentemente fazem uso de APs onidirecionais internos.

Estratégias de cobertura

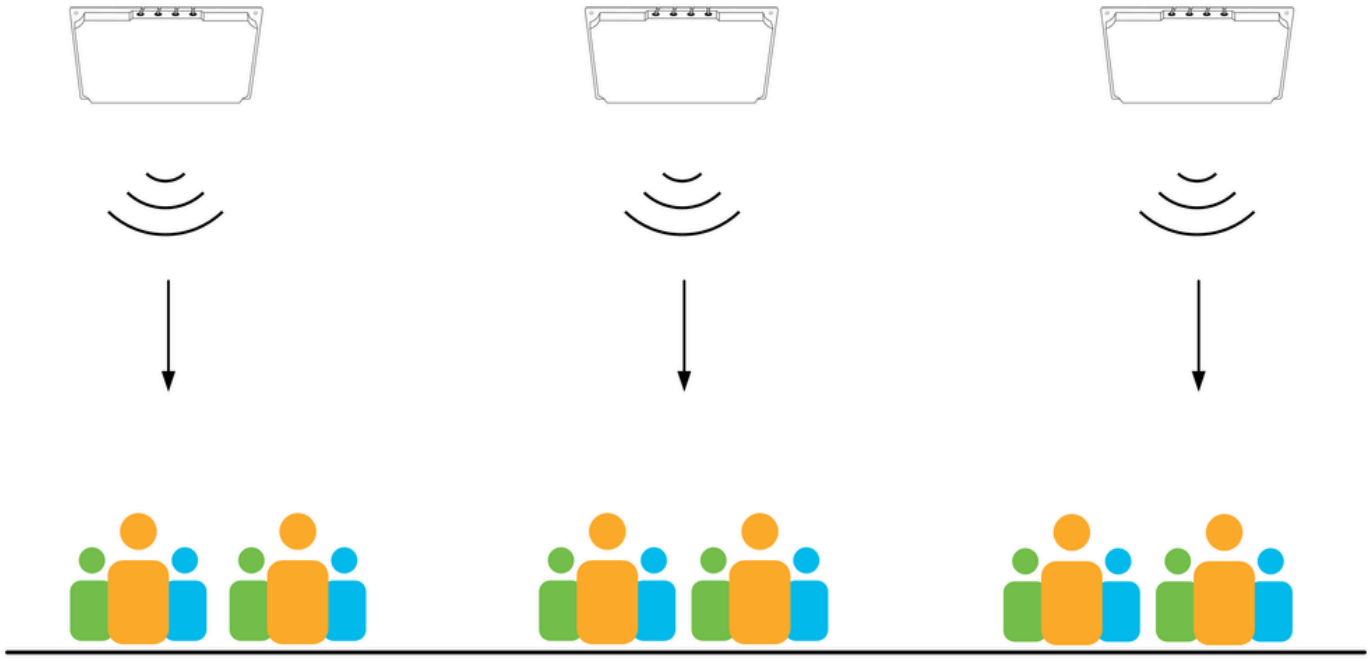
As estratégias de cobertura dependem muito do tipo de local, das antenas usadas e dos locais de montagem da antena disponíveis.

Sobrecarga

Sempre que possível, a cobertura de despesas gerais é a preferida.

As soluções de sobrecarga têm a vantagem distinta de que todos os dispositivos de cliente normalmente têm linha de visão direta para a sobrecarga da antena, mesmo em cenários sobrecarregados. As soluções de overhead que usam antenas direcionais fornecem uma área de

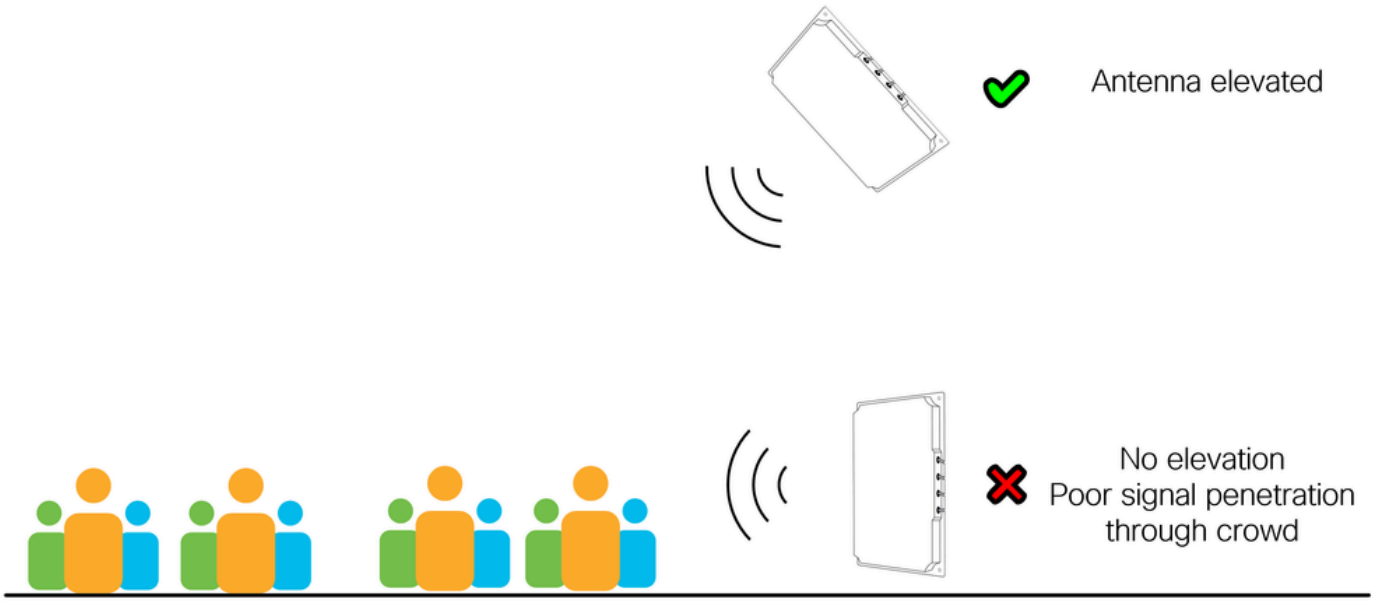
cobertura mais controlada e bem definida, tornando-as menos complicadas do ponto de vista do ajuste de rádio, enquanto fornecem balanceamento de carga superior e características de roaming de cliente. Consulte a seção Equilíbrio de Energia para obter informações adicionais.



APs acima dos clientes

Lado

As antenas direcionais montadas na lateral são uma escolha popular e funcionam bem em uma variedade de cenários, particularmente quando a montagem de sobrecarga não é possível devido à altura ou às restrições de montagem. Ao usar a montagem lateral, é importante entender o tipo de área coberta pela antena, por exemplo, é uma área externa aberta ou uma área interna densa? Se a área de cobertura for uma área de alta densidade com muitas pessoas, então a antena deve ser elevada o máximo possível, pois a propagação do sinal através de uma multidão humana é sempre fraca. Lembre-se de que a maioria dos dispositivos móveis é usada mais abaixo, na cintura, e não acima da cabeça do usuário! A altura da antena é menos significativa se a área de cobertura for uma área de menor densidade.



A elevação da antena é sempre melhor

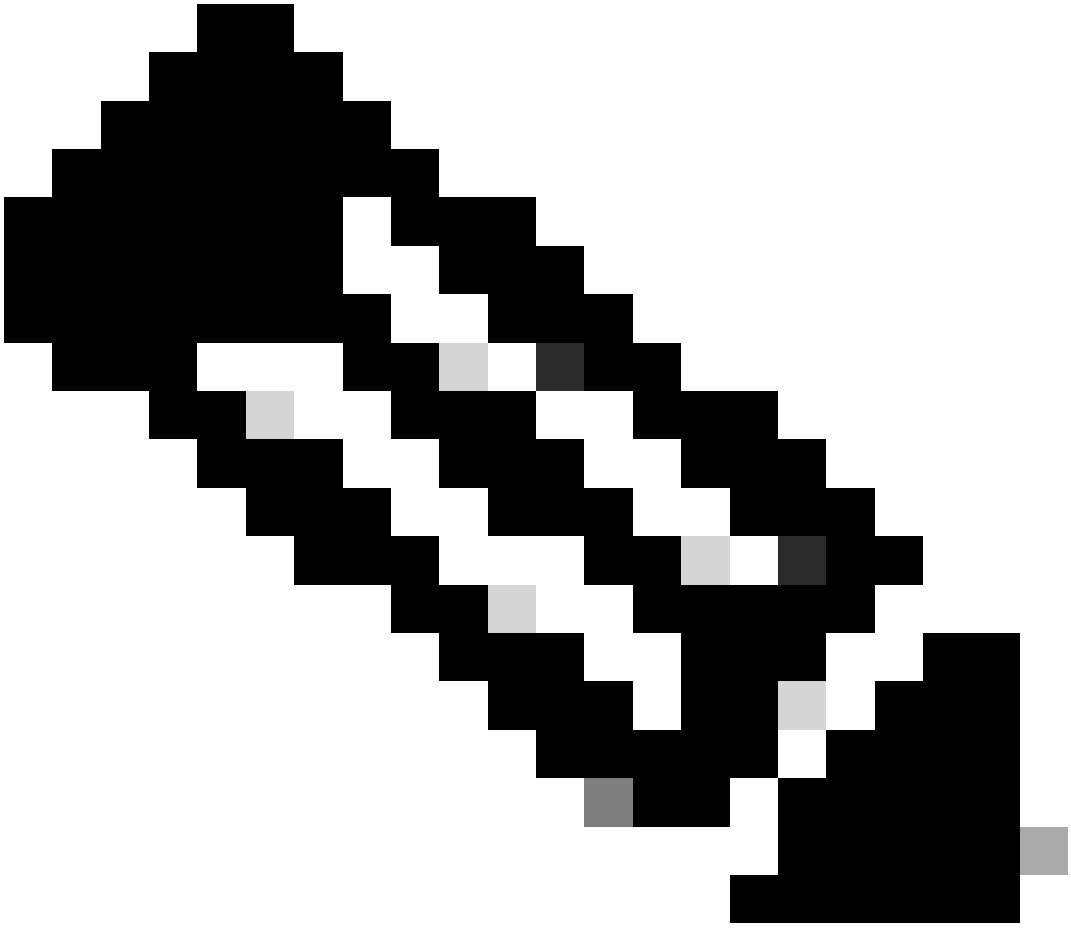
Onidirecional

O uso de antenas onidirecionais (internas ou externas) deve ser geralmente evitado em cenários de densidade muito alta, devido à área de impacto potencialmente alta para interferência de co-canal. As antenas onidirecionais não devem ser usadas a uma altura acima de 6m (não se aplica a unidades externas de alto ganho).

Sob o assento

Em algumas arenas ou estádios, pode haver situações em que não haja locais adequados para a montagem da antena. A última alternativa restante é fornecer a cobertura abaixo, posicionando os APs sob os assentos onde os usuários estão sentados. Esse tipo de solução é mais difícil de ser implantado corretamente e geralmente é mais caro, exigindo significativamente mais APs e procedimentos de instalação específicos.

O principal desafio com a implantação abaixo do local é a grande diferença na cobertura entre quando um local cheio e um local vazio. Um corpo humano é muito eficiente na atenuação do sinal de rádio, o que significa que quando há uma multidão de pessoas ao redor do AP a cobertura resultante é significativamente menor em comparação com quando essas pessoas não estão lá. Esse fator de atenuação da multidão humana permite que mais APs sejam implantados, o que pode aumentar a capacidade geral. No entanto, quando o local está vazio, não há atenuação dos corpos humanos e interferência significativa, e isso leva a complicações quando o local está parcialmente cheio.



> Observação: a implantação abaixo do local é uma solução válida, mas incomum; ela deve ser avaliada caso a caso. A implantação abaixo do local não é discutida mais neste documento.

Estética

Em algumas implantações, a questão da estética entra em cena. Essas áreas podem ter designs arquitetônicos específicos, valor histórico ou espaços onde a publicidade e/ou marca determinam onde o equipamento pode (ou não) ser montado. Soluções específicas podem ser necessárias para contornar qualquer limitação de posicionamento. Algumas dessas soluções alternativas incluem ocultar o AP/antena, pintar o AP/antena, montar o equipamento em um gabinete ou simplesmente usar um local diferente. Pintar a antena anula a garantia, se você optar por pintar a antena sempre use tinta não metálica. A Cisco geralmente não vende gabinetes para antenas, mas muitos estão facilmente disponíveis através de vários provedores.

Todas essas soluções alternativas têm um impacto no desempenho da rede. Os arquitetos sem fio sempre começam propondo posições de montagem ideais para a melhor cobertura de rádio, e

essas posições iniciais geralmente fornecem o melhor desempenho. Quaisquer mudanças nessas posições frequentemente resultam em antenas sendo movidas para longe de suas localizações ideais.

Os locais onde as antenas são montadas são frequentemente elevados, podendo ser tetos, passarelas, estruturas de telhado, vigas, passarelas e qualquer local que forneça alguma elevação sobre a área de cobertura pretendida. Esses locais são geralmente compartilhados com outras instalações, como: equipamentos de áudio, ar-condicionado, iluminação e vários detectores/sensores. Por exemplo, os equipamentos de áudio e iluminação devem ser montados em locais muito específicos - mas por que isso? Simplesmente, é porque o equipamento de áudio e de iluminação não funciona corretamente quando está escondido em uma caixa ou atrás de uma parede, e todos reconhecem isso.

O mesmo se aplica às antenas sem fio, que funcionam melhor quando há uma linha de visão para o dispositivo cliente sem fio. A priorização da estética pode (e muitas vezes tem) um efeito negativo no desempenho sem fio, diminuindo o valor do investimento em infraestrutura.

Redes invasoras

Redes Wi-Fi invasoras são redes sem fio que compartilham um espaço comum de RF, mas não são gerenciadas pelo mesmo operador. Eles podem ser temporários ou permanentes e incluem dispositivos de infraestrutura (APs) e dispositivos pessoais (como telefones celulares que compartilham um hotspot Wi-Fi). Redes Wi-Fi invasoras são uma fonte de interferência e, em alguns casos, também um risco à segurança. O impacto de invasores no desempenho sem fio não deve ser subestimado. As transmissões de Wi-Fi são limitadas a uma faixa relativamente pequena de espectro de rádio que é compartilhada entre todos os dispositivos Wi-Fi; qualquer dispositivo com comportamento inadequado nas proximidades tem o potencial de interromper o desempenho da rede para muitos usuários.

No contexto de grandes redes públicas, elas são normalmente cuidadosamente projetadas e ajustadas usando antenas especializadas. Um bom design de RF cobre apenas as áreas necessárias, geralmente usando antenas direcionais, e ajusta as características de envio e recebimento para obter eficiência máxima.

No outro extremo do espectro encontram-se os dispositivos de consumo ou os dispositivos fornecidos por fornecedores de serviços de Internet. Eles têm opções limitadas para ajuste fino de RF ou são configurados para alcance máximo e desempenho percebido, geralmente com alta potência, baixas taxas de dados e canais amplos. A introdução de tais dispositivos em uma rede de eventos de grande porte tem o potencial de criar problemas.

O que pode ser feito?

No caso dos hotspots pessoais, há muito pouco que possa ser feito, já que seria quase impossível monitorar dezenas de milhares de pessoas que entram em um local. No caso de infraestrutura, ou dispositivos semipermanentes, há algumas opções. A possível correção começa com uma educação simples, incluindo uma sinalização simples para conscientização, através de documentos assinados de políticas de rádio, terminando com aplicação ativa e análise de

espectro. Em todos os casos, deve ser tomada uma decisão de negócio sobre a proteção do espectro de rádio dentro do local dado, juntamente com medidas concretas para fazer cumprir essa decisão de negócio.

O aspecto de segurança de redes invasoras entra em ação quando dispositivos controlados por um terceiro anunciam o mesmo SSID que a rede gerenciada. Isso equivale a um ataque de porta de mel e pode ser usado como um método para roubar credenciais do usuário. É sempre recomendável criar uma regra de invasão para alertar sobre a detecção de SSIDs de infraestrutura anunciados por dispositivos não gerenciados. A seção de segurança discute os invasores com mais detalhes.

Único 5 GHz versus duplo 5 GHz

Dual 5GHz refere-se ao uso de rádios de 5GHz em APs suportados. Há uma diferença importante entre dual 5GHz usando antenas externas e dual 5GHz usando antenas internas (células micro/macro em APs onidirecionais). No caso de antenas externas, o duplo 5 GHz é frequentemente um mecanismo útil, fornecendo cobertura e capacidade adicionais ao mesmo tempo em que reduz a contagem total de APs.

Micro/Macro/Meso

Os APs internos têm ambas as antenas próximas (dentro do AP) e há restrições relacionadas à potência Tx máxima ao usar 5GHz duplo. O segundo rádio é limitado a uma baixa potência de Tx (aplicada pelo controlador sem fio), levando a um grande desequilíbrio de potência de Tx entre os rádios. Isso pode fazer com que o rádio primário (potência mais alta) atraia muitos clientes, enquanto o rádio secundário (potência mais baixa) é subutilizado. Nesse caso, o segundo rádio está adicionando energia ao ambiente sem fornecer benefício aos clientes. Se esse cenário for observado, pode ser melhor desabilitar o segundo rádio e simplesmente adicionar outro AP (único de 5 GHz) se for necessária capacidade adicional.

Diferentes modelos de AP têm diferentes opções de configuração, o segundo rádio de 5 GHz pode operar em níveis de potência mais altos em APs macro/meso mais recentes, como o 9130 e o 9136, e alguns APs Wi-Fi 6E internos, como o 9160 Series, podem até operar em macro/macro em alguns casos. Sempre verifique a capacidade do modelo de AP exato. O segundo slot de 5 GHz também é limitado em seu uso de canal, quando um slot está operando em uma banda UNII, o outro slot é restrito a uma banda UNII diferente, o que afeta o planejamento de canais e, subsequentemente, também a potência de transmissão disponível. Sempre considere a diferença de potência de transmissão entre rádios duplos de 5 GHz; isso é verdadeiro em todos os casos, incluindo APs internos.

FRA

A Atribuição flexível de rádio (FRA - Flexible Radio Assignment) foi introduzida como uma tecnologia para melhorar a cobertura de 5 GHz através da comutação de rádios adicionais de 2,4 GHz para o modo de 5 GHz, ou rádios potencialmente não utilizados de 5 GHz para o modo de monitor (para APs que a suportavam). Como este documento abrange grandes redes públicas, presume-se que as áreas de cobertura, bem como o projeto de rádio, estejam bem definidos

usando antenas direcionais, portanto, uma configuração determinística é preferível a uma configuração dinâmica. O uso de FRA não é recomendado para grandes redes públicas.

Opcionalmente, o FRA pode ser usado quando a rede estiver configurada para ajudar a determinar quais rádios devem ser convertidos em 5 GHz, mas quando você estiver satisfeito com o resultado, é aconselhável congelar o FRA.

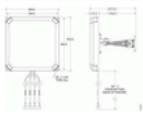
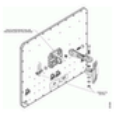
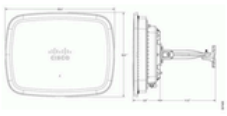
Regulamentações

Cada domínio regulatório define quais canais estão disponíveis para uso e seus níveis máximos de energia. Há também restrições sobre quais canais podem ser usados em ambientes internos em comparação com os externos. Dependendo do domínio regulatório, às vezes não é possível utilizar uma solução dupla de 5 GHz de forma eficaz. Um exemplo disso é o domínio ETSI onde 30dBm é permitido em canais UNII-2e, mas somente 23dBm em UNII1/2. Neste exemplo, se o design exigir o uso de 30 dBm (geralmente devido à maior distância até a antena), o uso de um único rádio de 5 GHz pode ser a única solução viável.

Antenas

As redes públicas grandes podem usar qualquer tipo de antena e normalmente escolhem a antena mais adequada para o trabalho. A combinação de antenas dentro da mesma área de cobertura torna o processo de projeto de rádio mais desafiador e deve ser evitado, se possível. No entanto, as grandes redes públicas geralmente têm grandes áreas de cobertura com diferentes opções de montagem, mesmo dentro da mesma área, tornando necessário misturar antenas em alguns casos. As antenas onidirecionais são bem compreendidas e funcionam da mesma forma que qualquer outra antena. Este guia discute as antenas direcionais externas.

Esta tabela lista as antenas externas mais usadas.

	C-ANT9103 Patch antenna (8x8) 6 dBi	5GHz Beamwidth 70°x70° ~33ft (10m)
	ANT2566P4W-R/S Patch antenna (4x4) 6 dBi	5GHz Beamwidth 110°x55° (120°x60°) ~33ft (10m)
	ANT2566D4M-R/S Patch antenna (4x4) 6 dBi	5GHz Beamwidth 55°x60° (60°x60°) ~33ft (10m)
	ANT2513P4M-N/S HD “Stadium” antenna 13 dBi	5GHz Beamwidth 31°x27° (30°x30°) ~66ft (20m)
	C-ANT9104 HD “Stadium” antenna Narrow 10dBi / Wide 7dBi	5GHz Beamwidth Narrow 25°x25° Wide 80°x25°

Lista de antenas

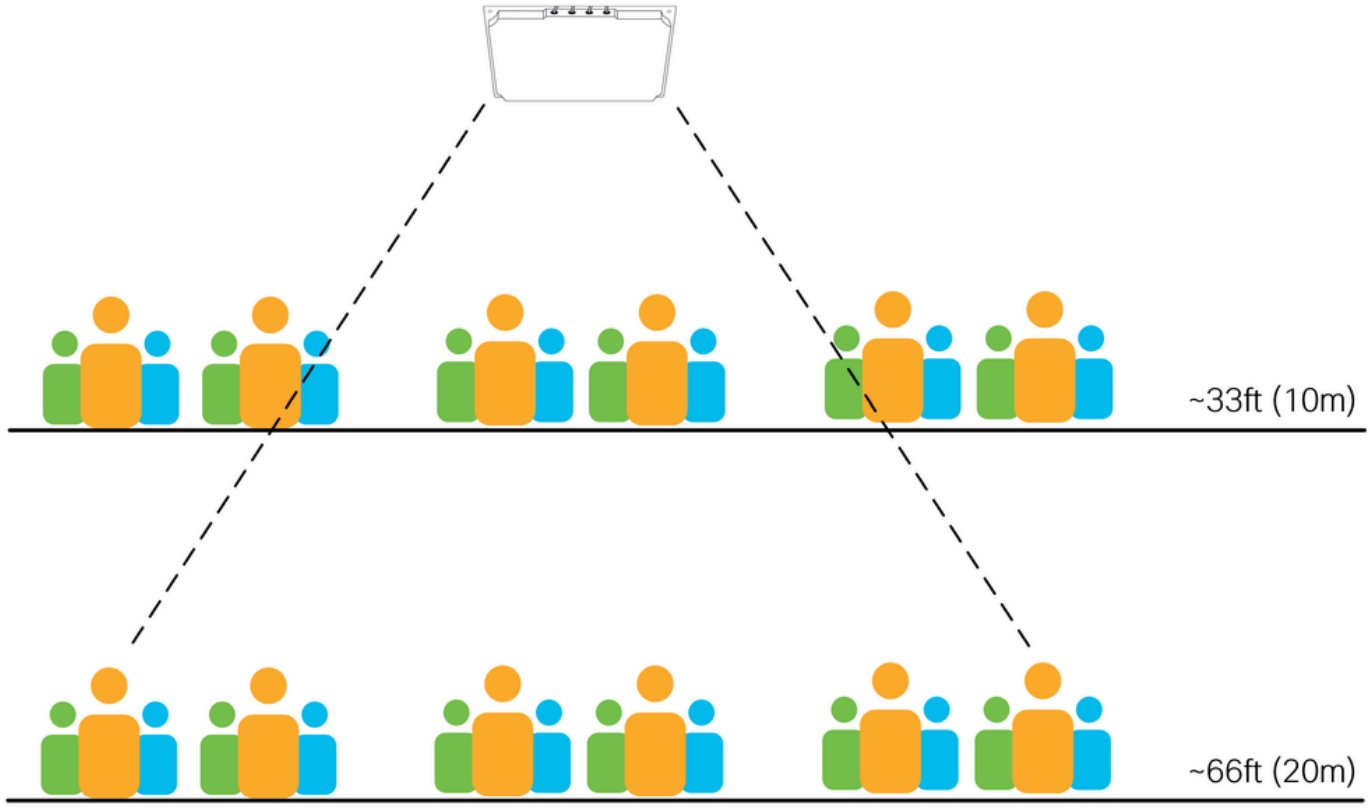
Os principais fatores a serem considerados ao escolher uma antena são a largura do feixe da

antena e a distância/altura na qual a antena está montada. A tabela mostra a largura do feixe de 5 GHz para cada uma das antenas, com os números entre colchetes mostrando valores arredondados (e mais fáceis de lembrar).

As distâncias sugeridas na tabela não são regras rígidas, apenas diretrizes baseadas na experiência. As ondas de rádio viajam na velocidade da luz e não param simplesmente depois de atingirem uma distância arbitrária. Todas as antenas funcionam além da distância sugerida, no entanto, o desempenho cai à medida que a distância aumenta. A altura da instalação é um fator importante durante o planejamento.

O diagrama abaixo mostra duas alturas de montagem possíveis para a mesma antena a ~33 pés (10 m) e ~66 pés (20 m) em uma área de alta densidade. Observe que o número de clientes que a antena pode ver (e aceitar conexões de) aumenta com a distância. A manutenção de células de tamanho menor torna-se mais desafiadora com distâncias maiores.

A regra geral é quanto maior a densidade de usuários, mais importante é usar a antena correta para a distância determinada.



Uma antena do estádio

A antena do estádio C9104 é adequada para cobrir áreas de alta densidade a grandes distâncias. Consulte o Guia de implantação da antena do estádio Catalyst 9104 (C-ANT9104) para obter mais informações.

Alterações ao longo do tempo

Alterações no ambiente físico ao longo do tempo são comuns em quase todas as instalações sem fio (por exemplo, movimento de paredes internas). Visitas regulares ao local e inspeções visuais

sempre foram uma prática recomendada. Para as redes de eventos, há a complexidade adicional de lidar com sistemas de áudio e iluminação e, em muitos casos, também com outros sistemas de comunicação (como 5G). Todos esses sistemas são frequentemente instalados em locais elevados acima dos usuários, às vezes resultando em contenção para o mesmo espaço. Um bom local para uma antena de estádio sem fio é também, muitas vezes, um bom local para uma antena 5G! Além disso, à medida que esses sistemas são atualizados com o tempo, eles podem ser realocados para locais onde obstruem e/ou interferem ativamente no seu sistema sem fio. É importante acompanhar as outras instalações e se comunicar com as equipes que as instalam para garantir que todos os sistemas sejam instalados em locais adequados sem interferir uns nos outros (física ou eletromagneticamente).

Alta densidade e 6 GHz

No momento em que este documento foi escrito, havia uma seleção limitada de antenas externas compatíveis com 6 GHz. Somente o AP/antena integrado CW9166D1 opera a 6 GHz, as especificações detalhadas da antena estão disponíveis no Guia de implantação do ponto de acesso Cisco Catalyst CW9166D1. O CW9166D1 fornece cobertura de 6 GHz com uma largura de feixe de 60°x60° e pode ser usado efetivamente para qualquer implantação que atenda às condições desse tipo de antena. Por exemplo, auditórios e depósitos são bons candidatos para a implantação do CW9166D1, pois a unidade integrada oferece funcionalidade de antena direcional para uso interno.

	CW9166D1 6GHz (4x4) or XOR 5GHz	60° x 60° 8 dBi
	5GHz (4x4)	70° x 70° 6 dBi
	2.4GHz (4x4)	70° x 70° 6 dBi

9166D1

No contexto de grandes redes públicas, muitas vezes elas têm várias áreas grandes e exigem o uso de uma combinação de antenas em várias alturas. Pode ser um desafio implantar uma rede pública grande de ponta a ponta usando apenas uma antena de 60°x60° devido a limitações de distância. Portanto, também pode ser desafiador fornecer cobertura de ponta a ponta a 6 GHz usando apenas o CW9166D1 para uma rede pública grande.

Uma abordagem possível é usar 5 GHz como a banda de cobertura primária, enquanto usa 6 GHz apenas em áreas específicas para descarregar dispositivos de cliente com capacidade para a banda mais limpa de 6 GHz. Esse tipo de abordagem utiliza antenas de apenas 5 GHz em áreas maiores, utilizando as antenas de 6 GHz onde possível e onde é necessária capacidade

adicional.

Como exemplo, considere um grande salão de eventos em uma conferência comercial, o salão principal usa antenas de estádio para fornecer cobertura primária a 5 GHz, a altura da instalação exige o uso de antenas de estádio. O CW9166D1 não pode ser usado no hall principal neste exemplo devido a limitações de distância - mas pode ser efetivamente usado em um hall VIP adjacente ou área de imprensa onde a densidade mais alta é necessária. O roaming de clientes entre bandas de 5 GHz e 6 GHz será discutido posteriormente neste documento.

Regulamentações

Como no caso de 5 GHz, a potência e os canais disponíveis para 6 GHz diferem significativamente entre os domínios regulatórios. Notavelmente, há uma grande diferença no espectro disponível entre os domínios FCC e ETSI, bem como diretrizes rígidas sobre a potência Tx disponível para uso interno e externo, Low Power Indoor (LPI) e Standard Power (SP), respectivamente. Com 6 GHz, restrições adicionais incluem limites de energia do cliente, o uso de antenas externas e inclinação de antena e (somente nos EUA por enquanto) o requisito de AFC (Automated Frequency Coordination) para implantações de SP.

Para obter mais informações sobre Wi-Fi 6E, consulte Wi-Fi 6E: The Next Great Chapter no Wi-Fi White Paper.

Radio Resource Management

O Gerenciamento de Recursos de Rádio (RRM) é um conjunto de algoritmos responsáveis pelo controle da operação de rádio. Este guia faz referência a dois algoritmos RRM chave, a saber, Dynamic Channel Assignment (DCA) e Transmit Power Control (TPC). O RRM é uma alternativa ao canal estático e à configuração de energia.

- O DCA é executado em uma programação configurável (padrão 10 minutos).
- O TPC é executado em uma programação automática (padrão de 10 minutos).

O Cisco Event Driven RRM (ED-RRM) é uma opção de DCA que permite que uma decisão de alteração de canal seja tomada fora da programação padrão de DCA, geralmente em resposta a condições graves de RF. O ED-RRM pode alterar um canal imediatamente quando níveis excessivos de interferência são detectados. Em ambientes ruidosos e/ou instáveis, a habilitação de ED-RRM apresenta um risco de alterações excessivas de canal, isso é um possível impacto negativo nos dispositivos do cliente.

O uso de RRM é incentivado e geralmente preferido em relação à configuração estática - no entanto, com certas advertências e exceções.

- O TPC deve ser limitado a uma faixa estreita de valores utilizando a configuração mín/máx do TPC, conforme necessário, e sempre alinhado ao projeto de RF.
    - Ative o TPC Channel Aware em ambientes de alta densidade.

- O ciclo DCA deve ser alterado da configuração padrão de 10 minutos.
    - Não use ED-RRM em ambientes HD.

    - Desative a opção Evitar carregamento de AP Cisco.
    - As opções de prevenção de AP invasor, como Evitar interferência de AP estrangeiro, podem resultar em um ambiente instável se houver muitos invasores. É sempre melhor remover o invasor do que tentar responder a ele.
- As decisões de RRM podem ser afetadas por APs/antenas que não ouvem uns aos outros corretamente, como no caso de antenas direcionais que apontam um para o outro.
- Algumas antenas (C9104, por exemplo) não suportam RRM e sempre exigem configuração estática.
- O RRM não corrige o design de RF ruim.

Em todos os casos, o RRM deve ser implantado com uma compreensão do resultado esperado e ajustado para operar dentro dos limites apropriados para o ambiente de RF especificado. As seções subsequentes deste documento exploram esses pontos com mais detalhes.

Configuração de RF

Canais

Em geral, quanto mais canais melhor. Em implantações de alta densidade, pode haver muito mais APs e rádios implantados do que os canais disponíveis, o que implica uma grande taxa de reutilização de canal e, junto com isso, níveis mais altos de interferência entre canais. Todos os canais disponíveis devem ser usados e, em geral, não é recomendável limitar a lista de canais disponíveis.

Pode haver casos em que um sistema sem fio específico (e separado) precise coexistir no mesmo espaço físico, e canais dedicados devem ser alocados a ele, ao mesmo tempo removendo os canais alocados da lista de DCAs do sistema primário. Esses tipos de exclusões de canais devem ser avaliados com muito cuidado e usados somente quando necessário. Um exemplo disso pode ser um link ponto-a-ponto operando em uma área aberta adjacente à rede primária ou uma área de imprensa dentro de um estádio. Se mais de um ou dois canais estiverem a ser excluídos da lista de DAC, isso é motivo para uma reavaliação da solução proposta. Em alguns casos, como em estádios de densidade muito alta, a exclusão de um único canal pode, às vezes, não ser uma opção viável.

A atribuição dinâmica de canais (DCA) pode ser usada com RRM baseado em WLC ou RRM com IA.

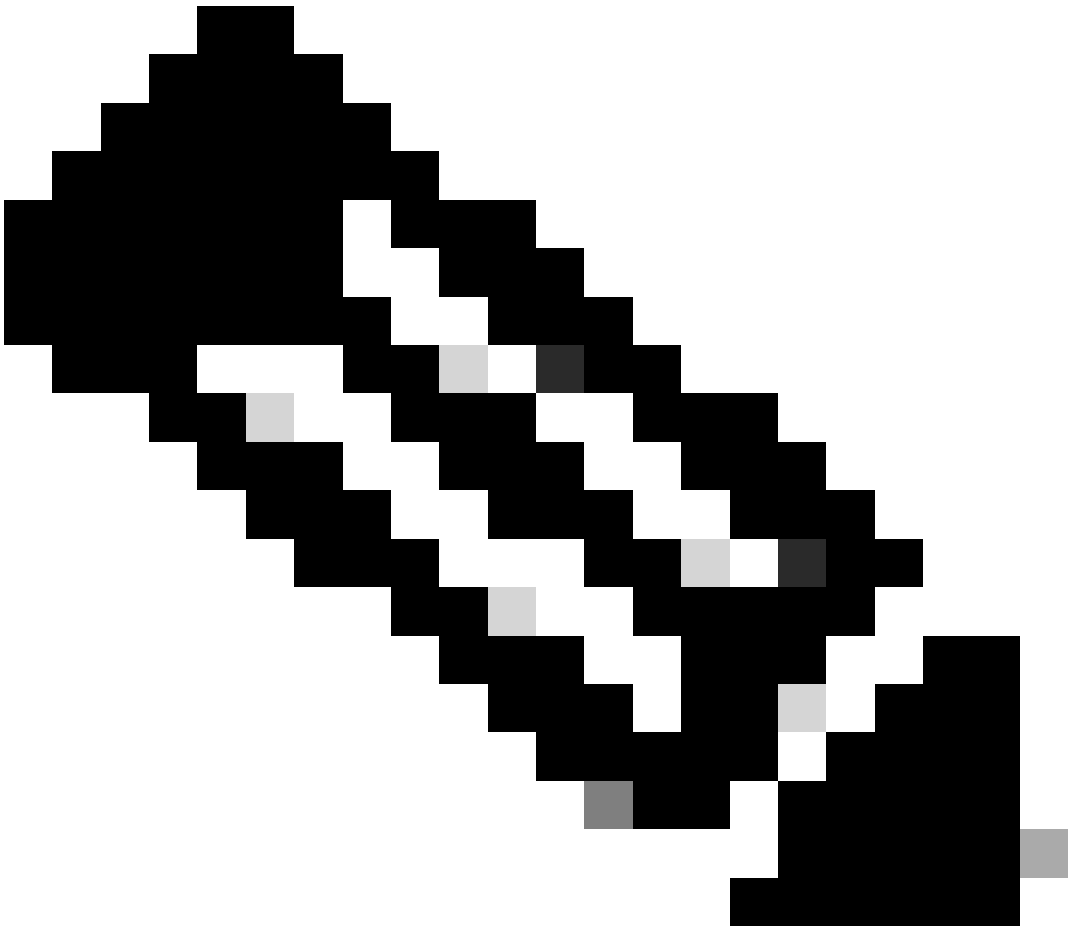
O intervalo padrão de DCA é de 10 minutos, o que pode resultar em frequentes alterações de canal em ambientes de RF instáveis. O temporizador de DCA predefinido deve ser aumentado dos 10 minutos predefinidos em todos os casos, o intervalo de DCA específico deve ser alinhado com os requisitos de operação da rede em questão. Um exemplo de configuração pode ser: intervalo de DCA de 4 horas, tempo de ancoragem de 8. Isso limita as alterações de canal a uma vez a cada 4 horas, a partir das 8h.

À medida que as interferências acontecem, a adaptação a elas de cada ciclo de DCA não necessariamente agrega valor, pois muitas dessas interferências são temporárias. Uma boa técnica é usar o DCA automático durante as primeiras horas e congelar o algoritmo e o plano de

canais quando você tiver algo estável com o qual esteja satisfeito.

Quando a WLC é reinicializada, o DCA é executado no modo agressivo por 100 minutos para encontrar um plano de canal adequado. É recomendável reiniciar o processo manualmente quando forem feitas alterações significativas no projeto de RF (por exemplo, adicionar ou remover vários APs ou alterar a largura do canal). Para iniciar esse processo manualmente, use esse comando.

```
ap dot11 [24ghz | 5ghz | 6ghz] rrm dca restart
```



Observação: as alterações de canal podem causar interrupções nos dispositivos cliente.

2,4 GHz

A banda de 2,4 GHz tem sido frequentemente criticada. Ele tem apenas três canais que não se

sobrepõem e muitas outras tecnologias além do Wi-Fi o usam, criando interferências indesejáveis. Algumas organizações insistem em fornecer serviço sobre ele, então o que é uma conclusão razoável? É um fato que a banda de 2,4 GHz não oferece uma experiência satisfatória para os usuários finais. Pior, ao tentar fornecer serviço em 2,4 GHz, você afeta outras tecnologias de 2,4 GHz, como Bluetooth. Em locais ou eventos grandes, muitas pessoas ainda esperam que seus fones de ouvido sem fio funcionem quando fazem uma chamada ou que seus equipamentos vestíveis inteligentes continuem funcionando normalmente. Se a sua rede Wi-Fi densa opera em 2,4 GHz, você está afetando os dispositivos que nem sequer estão usando a rede Wi-Fi de 2,4 GHz.

Uma coisa é certa: se você realmente precisa fornecer um serviço Wi-Fi de 2,4 GHz, é melhor fazer isso em um SSID separado (dedicá-lo a dispositivos da IoT ou chamá-lo de "legado"). Isso significa que os dispositivos de banda dupla não se conectam a 2,4 GHz involuntariamente e apenas os dispositivos de banda única de 2,4 GHz se conectam a ele.

A Cisco não aconselha ou suporta o uso de canais de 40 MHz em 2,4 GHz.

5 GHz

Implantação típica para redes sem fio de alta densidade. Use todos os canais disponíveis sempre que possível.

O número de canais varia de acordo com o domínio regulatório. Considere o impacto do radar no local específico, use os canais DFS (incluindo canais TDWR) onde possível.

A largura de canal de 20 MHz é altamente recomendada para todas as implantações de alta densidade.

Os 40 MHz podem ser usados na mesma base que os 2,4 GHz, isto é, somente quando (e onde) for absolutamente necessário.

Avaliar a necessidade e o benefício real dos canais de 40 MHz no ambiente específico. Os canais de 40 MHz exigem uma relação sinal-ruído (SNR) mais alta para obter qualquer melhoria possível no throughput, se SNR mais alta não for possível, os canais de 40 MHz não servirão para nada. As redes de alta densidade priorizam a média de todos os usuários em relação a um throughput potencialmente mais alto para qualquer usuário. É melhor colocar mais APs em canais de 20 MHz do que ter APs usando 40 MHz, pois o canal secundário é usado apenas para quadros de dados e, portanto, é usado de forma muito menos eficiente do que ter duas células de rádio diferentes, cada uma operando em 20 MHz (em termos de capacidade total, não em termos de throughput de um único cliente).

6 GHz

A banda de 6 GHz ainda não está disponível em todos os países. Além disso, alguns dispositivos têm um adaptador Wi-Fi compatível com 6 GHz, mas precisam de uma atualização do BIOS para que ele seja habilitado para o país específico onde você estiver operando o dispositivo. A forma mais popular com que os clientes descobrem rádios de 6 GHz agora é através de anúncio RNR no rádio de 5 GHz. Isso significa que 6GHz não deve operar sozinho sem um rádio de 5GHz no

mesmo AP. 6GHz está lá para descarregar clientes e tráfego do rádio de 5GHz e para fornecer normalmente uma melhor experiência para os clientes capacitados. Os canais de 6 GHz permitem usar larguras de banda maiores, mas isso depende muito do número de canais disponíveis no domínio regulatório. Com 24 canais de 6 GHz disponíveis na Europa, não é insensato escolher canais de 40 MHz para fornecer melhor throughput máximo em comparação aos 20 MHz que você provavelmente está usando em 5 GHz. Nos EUA, com quase o dobro do número de canais, o uso de 40 MHz é algo fácil e até mesmo ir para 80 MHz não é irracional para um evento de grande densidade. Larguras de banda maiores não devem ser usadas em eventos ou locais de alta densidade.

Taxas de dados

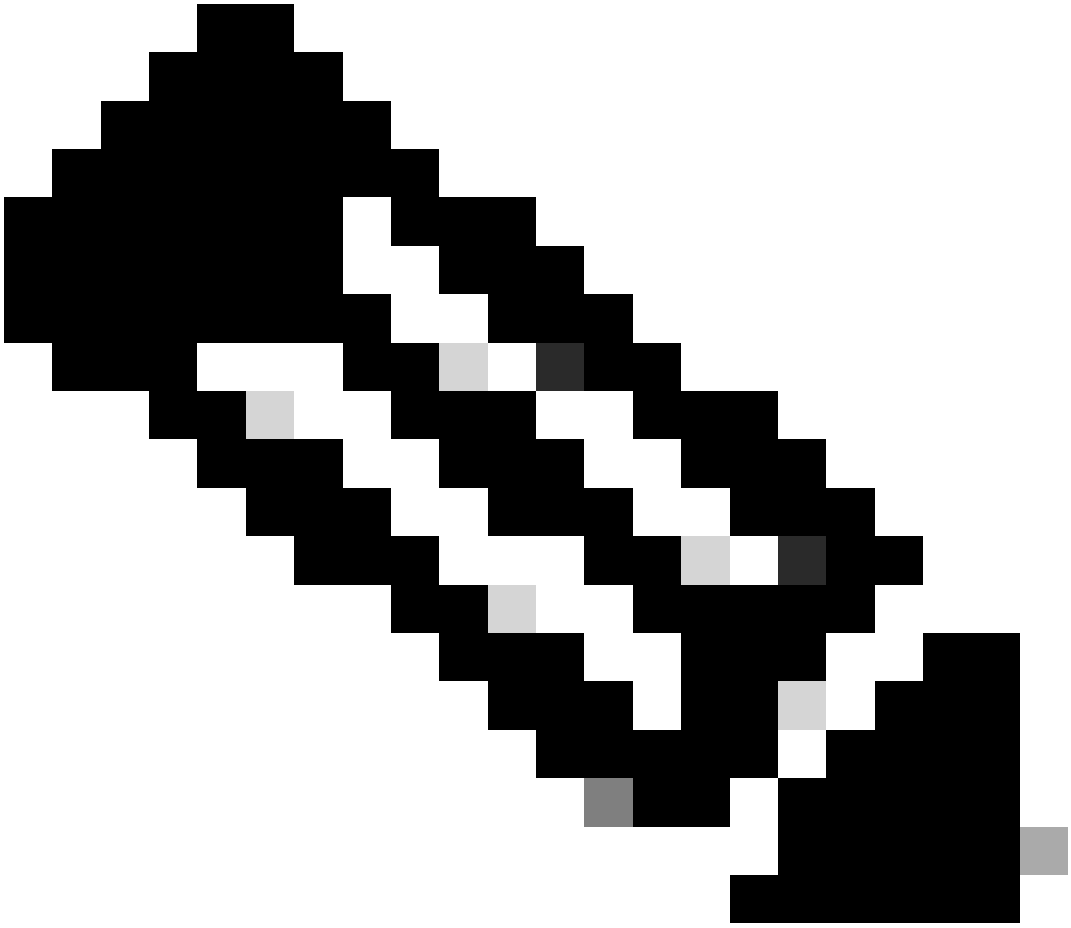
A taxa de dados que um cliente negocia com um AP é em grande parte uma função da razão sinal-ruído (SNR) dessa conexão, e o oposto também é verdadeiro, ou seja, taxas de dados mais altas exigem SNR mais alto. Na verdade, é principalmente o SNR que determina a velocidade máxima possível do link, mas por que isso é importante ao configurar as taxas de dados? É porque algumas taxas de dados têm significado especial.

As taxas de dados OFDM clássico (802.11a) podem ser configuradas em uma das três configurações: Desabilitado, Suportado ou Obrigatório. As taxas de OFDM são (em Mbps): 6, 9, 12, 18, 24, 36, 48, 54, e o cliente e o AP devem suportar uma taxa antes que ela possa ser usada.

Suportado - o AP usará a taxa

Obrigatório - o AP usará a taxa e enviará o tráfego de gerenciamento usando essa taxa

Desativado - o AP não usará a taxa, forçando o cliente a usar outra taxa



Nota: As taxas obrigatórias também são chamadas de taxas Básicas

O significado da taxa obrigatória é que todos os quadros de gerenciamento são enviados usando essa taxa, bem como quadros de broadcast e multicast. Se houver várias taxas obrigatórias configuradas, os quadros de gerenciamento usarão a menor taxa obrigatória configurada e o broadcast e o multicast usarão a maior taxa obrigatória configurada.

Os quadros de gerenciamento incluem beacons que devem ser ouvidos pelo cliente para poderem ser associados ao AP. Aumentar a taxa obrigatória também aumenta a exigência de SNR para essa transmissão, lembre-se de que taxas de dados mais altas exigem SNR mais alto, e isso geralmente significa que o cliente precisa estar mais próximo do AP para poder decodificar o beacon e se associar. Portanto, ao manipular a taxa de dados obrigatória, também manipulamos o intervalo de associação efetivo do AP, forçando os clientes a se aproximarem do AP ou em direção a uma possível decisão de roaming. Os clientes próximos ao AP usam taxas de dados mais altas, e as taxas de dados mais altas usam menos tempo de transmissão - o efeito pretendido é uma célula mais eficiente. É importante lembrar que o aumento da taxa de dados afeta apenas a taxa de transmissão de determinados quadros, não afeta a propagação de RF da

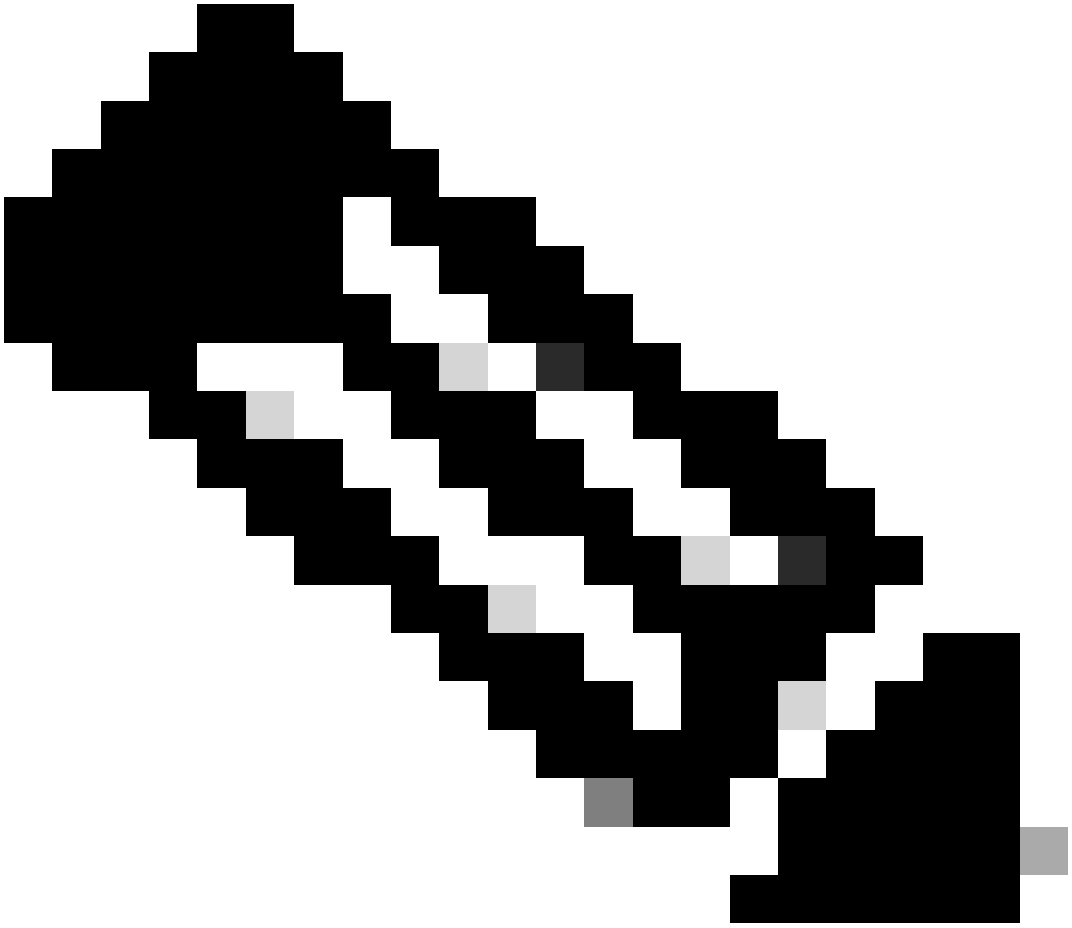
antena ou a faixa de interferência. Ainda são necessárias boas práticas de design de RF para minimizar a interferência e o ruído entre canais.

Por outro lado, deixar taxas menores como obrigatórias geralmente significa que os clientes poderão se associar a uma distância muito maior, útil em cenários de menor densidade de AP, mas com potencial para causar estragos com o roaming em cenários de maior densidade. Qualquer pessoa que tenha tentado localizar um AP invasor que esteja transmitindo um 6 Mbps saberá que você pode detectar o AP muito longe de sua localização física!

No tópico de broadcast e multicast, em alguns casos, uma segunda taxa obrigatória (mais alta) é configurada para aumentar a taxa de entrega do tráfego multicast. Isso raramente é bem-sucedido, pois o multicast nunca é reconhecido e nunca retransmitido caso os quadros sejam perdidos. Como alguma perda é inerente a todos os sistemas sem fio, é inevitável que alguns quadros multicast sejam perdidos independentemente da taxa configurada. Uma melhor abordagem para a entrega confiável de multicast são as técnicas de conversão de multicast para unicast que transmitem o multicast como um fluxo unicast, o que tem o benefício de taxas de dados mais altas e entrega confiável (confirmada).

É preferível usar apenas uma única taxa obrigatória, desabilite todas as taxas abaixo da taxa obrigatória e deixe todas as taxas acima da taxa obrigatória como suportada. A taxa específica a ser usada depende do caso de uso, já que as taxas mais baixas mencionadas são úteis em cenários de menor densidade e externos onde as distâncias entre APs são maiores. Para redes de eventos e de alta densidade, taxas baixas devem ser desativadas.

Se você não tiver certeza de onde começar, use uma taxa obrigatória de 12 Mbps para implantações de baixa densidade e 24 Mbps para implantações de alta densidade. Muitos eventos de grande escala, estádios e até mesmo implantações de escritórios empresariais de alta densidade provaram funcionar de forma confiável com uma configuração de taxa obrigatória de 24 Mbps. Recomenda-se o teste apropriado para casos de uso específicos em que as taxas abaixo de 12 Mbps ou acima de 24 Mbps são necessárias.

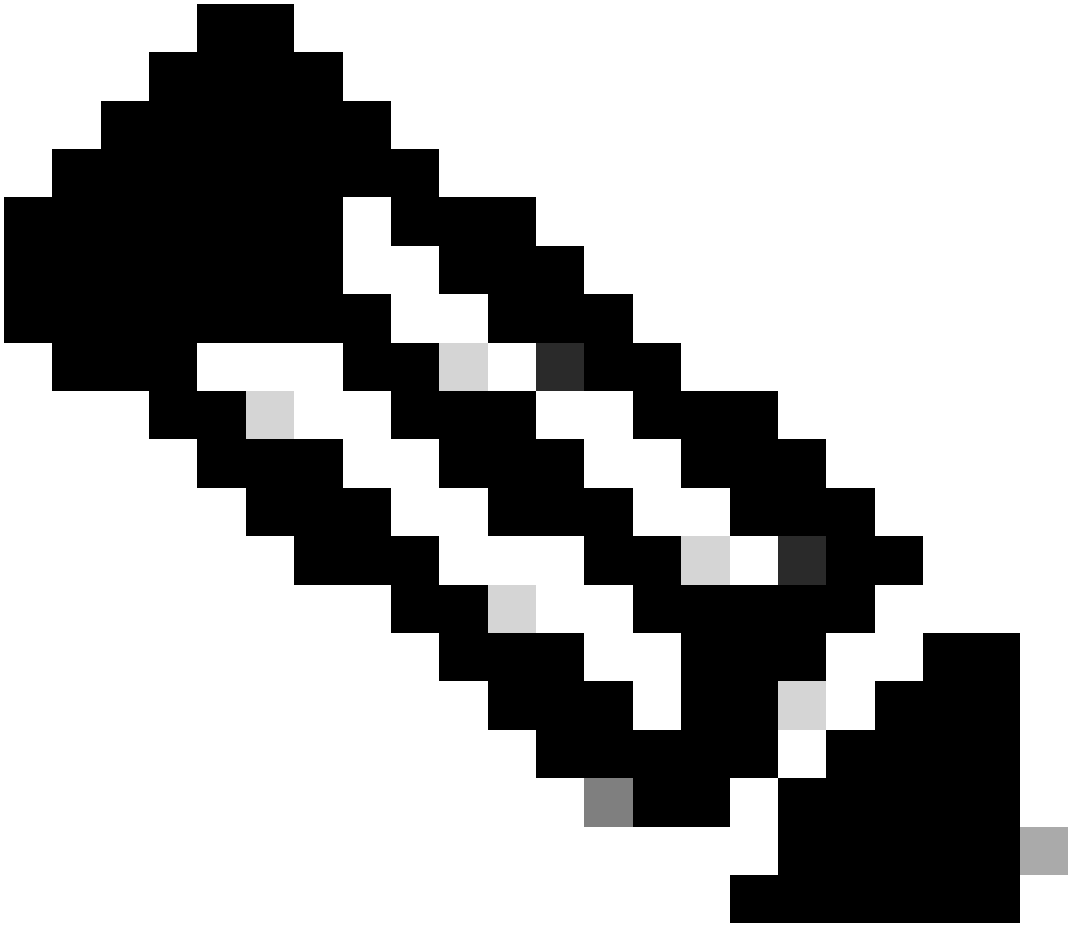


Observação: é melhor deixar todas as taxas de 802.11n/ac/ax ativadas (todas as taxas na seção Alto throughput da GUI da WLC); raramente há necessidade de desativar qualquer uma dessas taxas.

Potência de transmissão

As recomendações de potência de transmissão variam de acordo com o tipo de implantação. Aqui, diferenciamos as implantações internas usando antenas onidirecionais daquelas usando antenas direcionais. Os dois tipos de antenas podem existir em uma grande rede pública, embora eles normalmente estejam cobrindo diferentes tipos de áreas.

Para implementações onidirecionais, é comum usar o TPC (Transmit Power Control) automático com um limite mínimo estaticamente configurado e, em certos casos, também um limite máximo estaticamente configurado.



Observação: os limites de TPC referem-se à potência de transmissão por rádio e excluem o ganho da antena. Sempre verifique se o ganho da antena está configurado corretamente para o modelo de antena usado. Isso é feito automaticamente no caso de antenas internas e antenas de identificação automática.

Exemplo 1

TPC Mín.: 5 dBm, TPC Máx.: Máximo (30 dBm)

Isso resultaria no algoritmo TPC determinando a potência de transmissão automaticamente, mas nunca indo abaixo do limite mínimo configurado de 5dBm.

Exemplo 2

TPC Mín.: 2dBm, TPC Máx.: 11 dBm

Isso faria com que o algoritmo TPC determinasse a potência de transmissão automaticamente, mas sempre permanecesse entre 2dBm e 11dBm.

Uma boa abordagem é criar vários perfis de RF com limites diferentes, por exemplo baixo consumo de energia (2-5dBm), média potência (5-11dbM) e alta potência (11-17dBM), atribuindo APs onidirecionais a cada perfil de RF conforme necessário. Os valores de cada perfil de RF podem ser ajustados ao caso de uso pretendido e à área de cobertura. Isso permite que os algoritmos de RRM operem dinamicamente enquanto permanecem dentro de limites predefinidos.

A abordagem para antenas direcionais é muito semelhante, a única diferença é o nível de precisão exigido. A colocação da antena direcional deve ser projetada e verificada durante uma pesquisa de RF de pré-implantação, e os valores específicos da configuração de rádio são geralmente um resultado desse processo.

Por exemplo, se for necessária uma antena patch montada no teto para cobrir uma determinada área a partir de uma altura de ~26 pés (8 m), a pesquisa de RF deve determinar a potência Tx mínima necessária para atingir essa cobertura pretendida (isso determina o valor TPC mínimo para o perfil de RF). Da mesma forma, com a mesma pesquisa de RF, entendemos a possível sobreposição necessária entre essa antena e a próxima, ou até mesmo o ponto no qual queremos que a cobertura termine - isso forneceria o valor máximo de TPC para o perfil de RF.

Os perfis de RF para antenas direcionais são normalmente configurados com os mesmos valores de TPC mínimo e máximo ou com uma faixa estreita de valores possíveis (geralmente <= 3dBm).

Os perfis de RF são preferidos para garantir a consistência da configuração; a configuração estática de APs individuais não é recomendada. É uma boa prática nomear os perfis de RF de acordo com a área de cobertura, o tipo de antena e o caso de uso, por exemplo, RF-Auditorium-Patch-Ceiling.

A quantidade correta de potência Tx é quando o valor SNR necessário é alcançado pelo cliente mais fraco na área de cobertura pretendida, e não mais do que isso. 30dBm é um ótimo valor-alvo de SNR do cliente sob condições reais (ou seja, em um local cheio de pessoas).

CHD

A Detecção de furos de cobertura (CHD - Coverage Hole Detection) é um algoritmo separado para identificar e corrigir furos de cobertura. O CHD é configurado globalmente e por WLAN. Um possível efeito da CHD é o aumento da potência Tx para compensar os furos de cobertura (áreas com clientes consistentemente detectados com sinal fraco), esse efeito está no nível do rádio e afeta todas as WLANs, mesmo quando disparadas por uma única WLAN configurada para CHD.

As grandes redes públicas são normalmente configuradas para níveis de energia específicos usando perfis de RF, algumas podem estar em áreas abertas com clientes em roaming entrando e saindo das áreas, não há necessidade de um algoritmo para ajustar dinamicamente a potência do AP Tx em resposta a esses eventos do cliente.

O CHD deve ser desabilitado globalmente para grandes redes públicas.

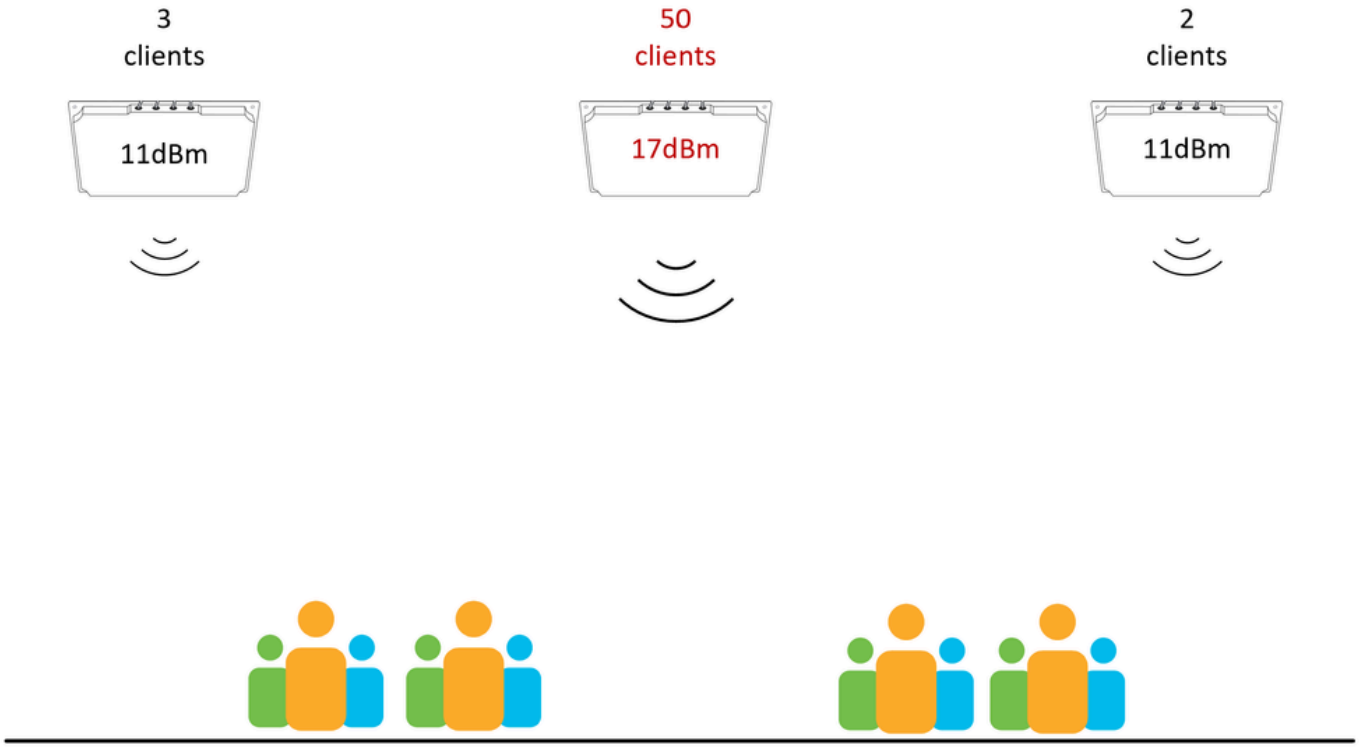
Equilíbrio de energia

A maioria dos dispositivos clientes prefere um sinal recebido mais alto ao escolher a qual AP se

associar. Devem ser evitadas situações em que um AP é configurado com uma potência de Tx significativamente maior em comparação com outros APs adjacentes. Os APs que operam com maior potência de transmissão atraem mais clientes, levando a uma distribuição desigual de clientes entre APs (por exemplo, um único AP/rádio é sobrecarregado com clientes enquanto os APs adjacentes são subutilizados). Essa situação é comum em implantações com sobreposição de cobertura grande de várias antenas e nos casos em que um AP tem várias antenas conectadas.

As antenas para estádios, como o C9104, exigem cuidado especial ao selecionar a potência Tx, pois os feixes da antena se sobrepõem por design. Consulte o Guia de implantação da antena para estádios Catalyst 9104 (C-ANT9104) para obter mais informações sobre isso.

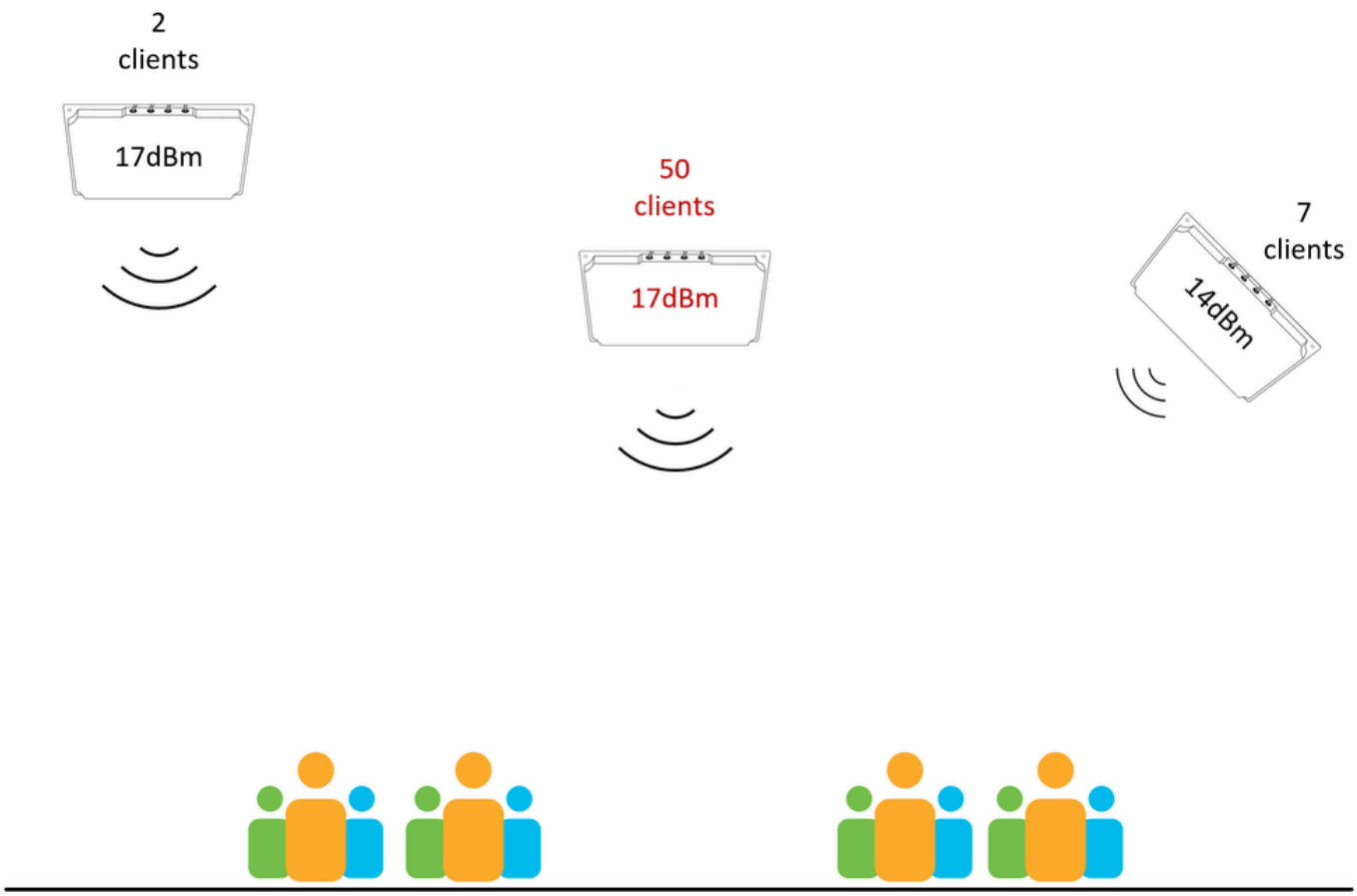
No diagrama abaixo, a antena do meio é configurada com uma potência de transmissão mais alta do que as antenas ao redor. Essa configuração provavelmente fará com que os clientes fiquem ‘presos’ à antena do meio.



Um AP com maior potência do que seus APs vizinhos atrai todos os clientes ao redor

O próximo diagrama mostra uma situação mais complicada, nem todas as antenas estão na mesma altura e nem todas as antenas estão usando a mesma inclinação/orientação. É mais complicado obter uma potência equilibrada do que simplesmente configurar todos os rádios com a mesma potência de transmissão. Em cenários como esse, uma pesquisa de site pós-implantação pode ser necessária, isso fornece uma visão da cobertura do ponto de vista do dispositivo cliente (no local). Os dados da pesquisa podem ser usados para equilibrar a configuração para melhor cobertura e distribuição ao cliente.

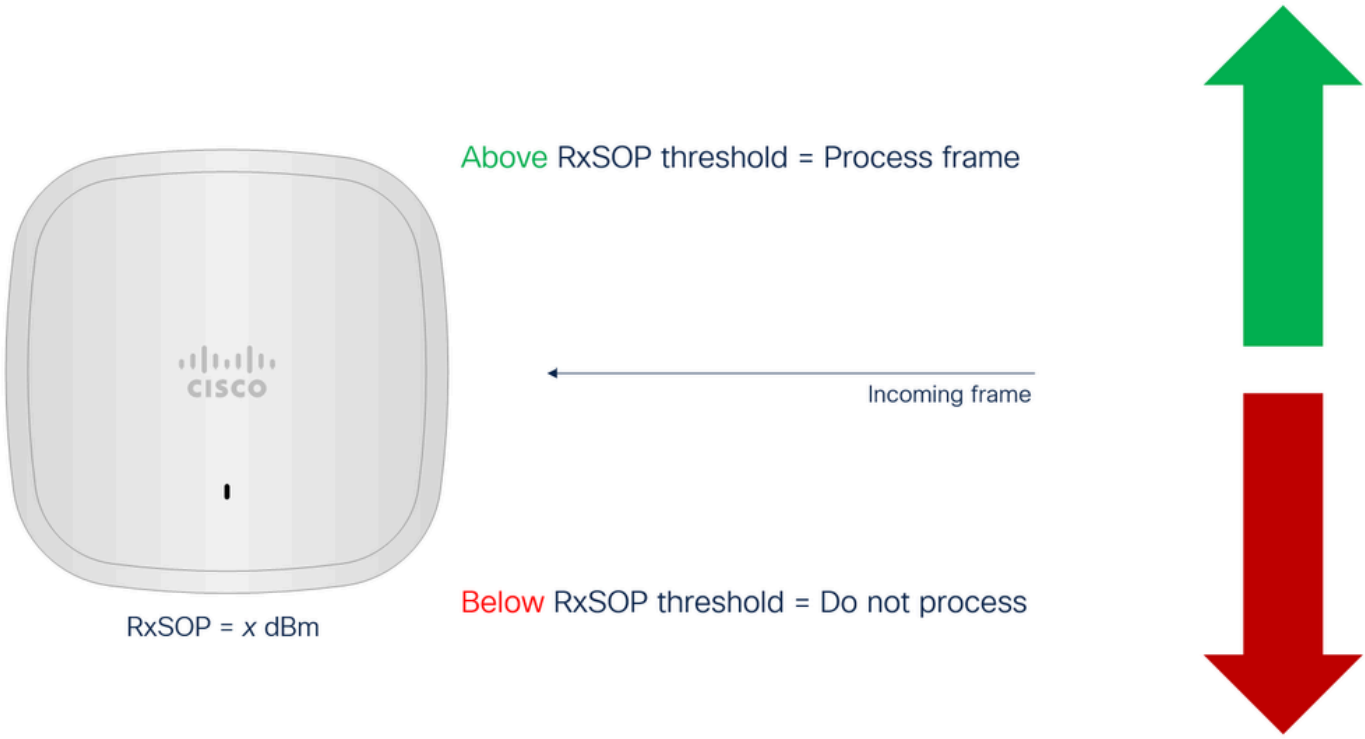
Projetar locais de posicionamento de AP uniformes que evitem situações complicadas como essa é a melhor maneira de evitar cenários de ajuste de RF desafiadores (embora às vezes não haja outra escolha!).



Um AP está atraindo todos os clientes, apesar da potência de transmissão ser semelhante, mas a altura e os ângulos desempenham um papel

RxSOP

Em contraste com mecanismos como a potência de transmissão ou taxas de dados que afetam as características da célula de transmissão, RxSOP (Detecção de início de pacote do receptor) visa influenciar o tamanho da célula de recepção. Em essência, o RxSOP pode ser entendido como um limite de ruído, na medida em que define o nível de sinal recebido abaixo do qual o AP não tenta decodificar transmissões. Quaisquer transmissões que cheguem com um nível de sinal mais fraco do que o limiar RxSOP configurado não são processadas pelo AP e são efetivamente tratadas como ruído.



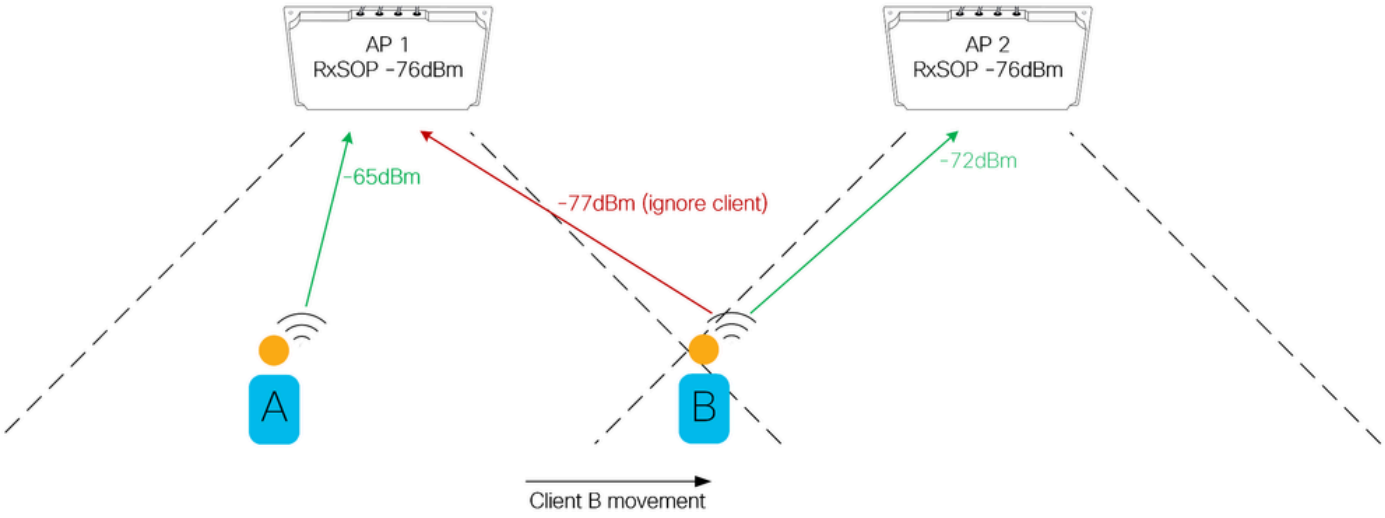
Conceito de RxSOP explicado

O significado do RxSOP

O RxSOP tem vários usos. Ele pode ser usado para melhorar a capacidade dos APs de transmitir em ambientes ruidosos, para controlar a distribuição de clientes entre antenas, bem como otimizar para clientes mais fracos e aderentes.

No caso de ambientes ruidosos, lembre-se de que, antes de transmitir um quadro 802.11, a estação transmissora (o AP, neste caso) precisa primeiro avaliar a disponibilidade do meio, parte desse processo é ouvir primeiro as transmissões que já estão ocorrendo. Em ambientes Wi-Fi densos, é comum que muitos APs coexistam em um espaço relativamente limitado, frequentemente usando os mesmos canais. Em tais ambientes ocupados, o AP pode relatar a utilização do canal dos APs vizinhos (incluindo reflexões) e atrasar sua própria transmissão. Ao definir o limiar RxSOP apropriado, o AP pode ignorar essas transmissões mais fracas (redução na utilização percebida do canal), levando a oportunidades de transmissão mais frequentes e melhor desempenho. Os ambientes em que os APs relatam uma utilização significativa do canal (por exemplo, > 10%) sem nenhuma carga de cliente (por exemplo, um local vazio) são bons candidatos para o ajuste RxSOP.

Para otimização de cliente usando RxSOP, considere este diagrama.



Roaming de cliente afetado por rxsop

Neste exemplo, há dois APs/antenas com áreas de cobertura bem definidas. O cliente B está mudando da área de cobertura do AP1 para a área de cobertura do AP2. Há um ponto de cruzamento no qual o AP2 ouve o cliente melhor que o AP1, mas o cliente ainda não fez roaming para o AP2. Este é um bom exemplo de como a definição do limite RxSOP pode aplicar o limite da área de cobertura. Garantir que os clientes estejam sempre conectados ao AP mais próximo melhora o desempenho, eliminando conexões de clientes distantes e/ou fracas atendidas a taxas de dados mais baixas. Configurar os limiares de RxSOP dessa forma exige um entendimento completo de onde a área de cobertura esperada de cada AP começa e termina.

Os perigos do RxSOP.

Definir o limite de RxSOP de forma muito agressiva resulta em falhas de cobertura, pois o AP não está decodificando transmissões válidas de dispositivos cliente válidos. Isso pode ter consequências adversas para o cliente, pois o AP não responde; afinal, se a transmissão do cliente não foi ouvida, não há motivo para responder. O ajuste dos limiares de RxSOP deve ser feito com cuidado, sempre garantindo que os valores configurados não excluam clientes válidos dentro da área de cobertura. Observe que alguns clientes podem não responder bem a serem ignorados dessa forma, configurações muito agressivas de RxSOP não dão ao cliente uma chance de fazer roaming naturalmente, forçando efetivamente o cliente a encontrar outro AP. Um cliente que pode decodificar um beacon de um AP supõe que ele é capaz de transmitir para esse AP, portanto, a intenção do ajuste RxSOP é corresponder o tamanho da célula de recepção ao intervalo de beacon do AP. Tenha em mente que um dispositivo cliente (válido) nem sempre tem linha de visão direta para o AP, o sinal é frequentemente atenuado pelos usuários voltados para longe da antena ou carregando seus dispositivos em bolsas ou bolsos.

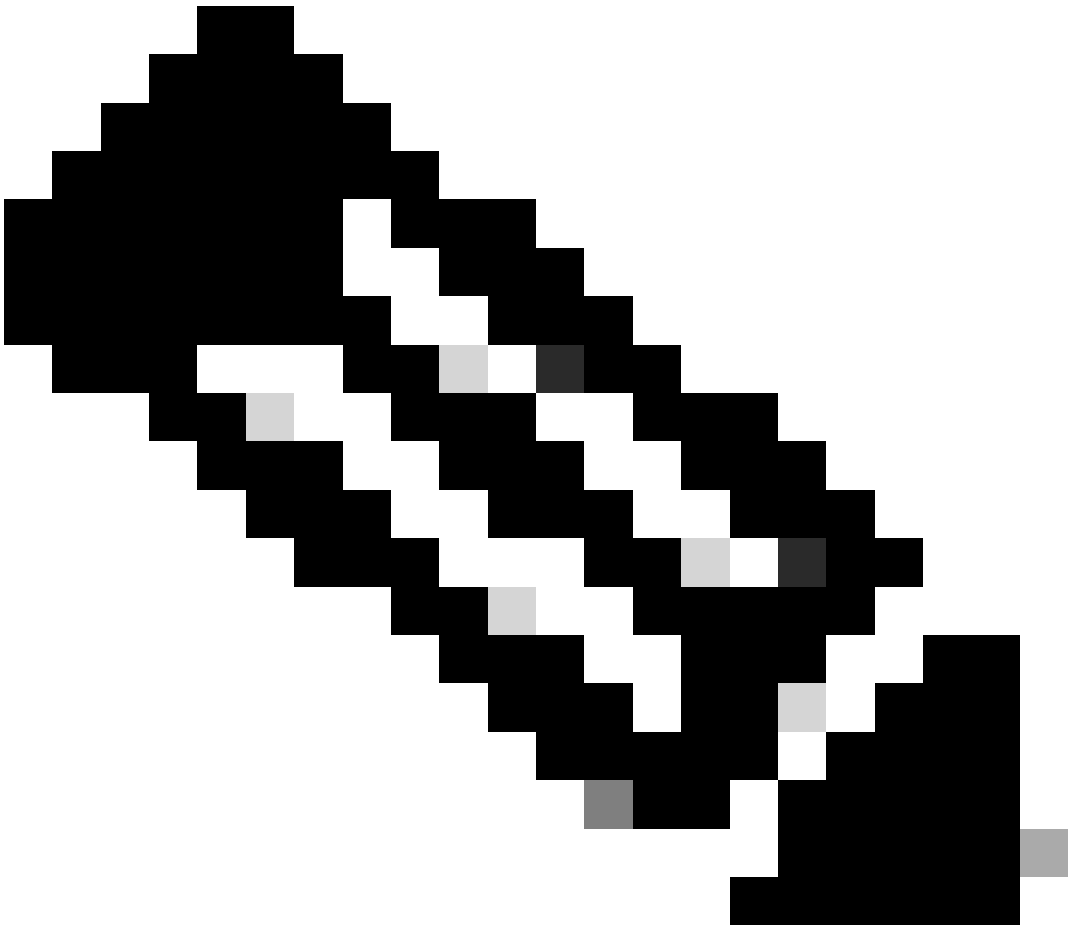
Configuração de RxSOP

O RxSOP é configurado por perfil de RF.

Para cada banda, há limites predefinidos (Baixo/Médio/Alto) que definem um valor de dBm predefinido. A recomendação aqui é sempre usar valores personalizados, mesmo que o valor pretendido seja das predefinições disponíveis, isso torna a configuração mais legível.

Setting	Value
Auto	Not configured
Low	-80dBm
Medium	-78dBm
High	-76dBm
Custom	-60dBm to -85dBm

Tabela de configurações de RxSop



Observação: as alterações de RxSOP não exigem uma reinicialização por rádio e podem

ser feitas instantaneamente.

Dimensionamento da rede

Em geral, usar um dispositivo até o máximo de seus recursos documentados é uma má ideia. As fichas técnicas relatam a verdade, mas os números mencionados podem estar em condições específicas de atividade. As controladoras sem fio são testadas e certificadas para suportar um determinado número de clientes e APs e um certo rendimento, mas isso não pressupõe que os clientes estejam em roaming a cada segundo, que você pode ter configurado ACLs exclusivas extremamente longas para cada cliente ou habilitado todos os recursos de rastreamento disponíveis. Portanto, é importante considerar todos os aspectos cuidadosamente para garantir que a rede seja dimensionada durante as horas de pico e também para manter uma margem de segurança para crescimento futuro.

Número de APs

Uma das primeiras tarefas na implantação de qualquer rede é orçar e solicitar a quantidade certa de equipamentos, e o maior fator variável é o número e o tipo de pontos de acesso e antenas. As soluções sem fio sempre devem ser baseadas em um projeto de radiofrequência, no entanto (e infelizmente), muitas vezes esse é o segundo passo no ciclo de vida do projeto. No caso de implantações corporativas internas simples, há várias técnicas de estimativa que podem, com um nível razoável de certeza, prever quantos APs podem ser necessários antes mesmo de um arquiteto sem fio olhar as plantas baixas. Modelos preditivos também podem ser muito úteis neste caso.

Para instalações mais desafiadoras, como as industriais, externas, grandes redes públicas ou em qualquer lugar onde as antenas externas sejam necessárias, as técnicas de estimativa simples são frequentemente inadequadas. É necessário algum nível de experiência em instalações anteriores semelhantes para estimar adequadamente o tipo e a quantidade de equipamento necessário. Uma visita ao local por um arquiteto de tecnologia sem fio é o mínimo para se entender o layout de um local ou instalação complexa.

Esta seção fornece diretrizes sobre como determinar o número mínimo de APs e antenas para a implementação especificada. As quantidades finais e os locais de montagem específicos sempre serão determinados por meio de um processo de análise de requisitos e projeto de rádio.

A lista de materiais inicial deve ser baseada em dois fatores: tipo de antenas e quantidade de antenas.

Tipo de antenas

Não há atalhos aqui. O tipo de antena é determinado pela área que precisa ser coberta e pelas opções de montagem disponíveis nessa área. Não é possível determinar isso sem um entendimento do espaço físico, o que significa que uma visita ao local é necessária para alguém com um entendimento das antenas e seus padrões de cobertura.

Quantidade de antenas

A quantidade de equipamentos necessários pode ser obtida a partir da compreensão da quantidade esperada de conexões de clientes.

Dispositivos por pessoa

O número de usuários humanos pode ser determinado pela capacidade de assentos de um local, pelo número de ingressos vendidos ou pelo número esperado de visitantes com base em estatísticas históricas. Cada usuário humano pode transportar vários dispositivos e é comum assumir mais de um dispositivo por usuário, embora a capacidade de um usuário humano de usar ativamente vários dispositivos ao mesmo tempo seja questionável. O número de visitantes que se conectam ativamente à rede também depende do tipo de evento e/ou implantação.

Exemplo 1: é normal que um estádio de 80.000 lugares não tenha 80.000 dispositivos conectados, essa porcentagem é geralmente significativamente menor. Taxas de usuários conectados de 20% não são incomuns durante eventos esportivos, isso significa que, para o exemplo de estádio com 80.000 lugares, o número esperado de dispositivos conectados pode ser 16.000 (80.000 x 20% = 16.000). Esse número também depende do mecanismo de integração usado. Se o usuário for solicitado a executar alguma ação (como clicar em um portal da Web), os números serão menores do que quando a integração do dispositivo for automática. A integração automática pode ser tão simples quanto uma PSK que foi lembrada de um evento anterior, ou algo mais avançado como o uso do OpenRoaming que integra dispositivos sem interação do usuário. As redes OpenRoaming podem fazer com que o usuário obtenha taxas bem acima de 50%, o que pode ter um impacto significativo no planejamento da capacidade.

Exemplo 2: é razoável esperar que uma conferência de tecnologia tenha uma alta taxa de conexão de usuário. Os participantes da conferência passam mais tempo conectados à rede e esperam poder acessar seus emails e executar tarefas diárias durante o dia. Também é mais provável que esse tipo de usuário conecte mais de um dispositivo à rede, embora sua capacidade de usar vários dispositivos simultaneamente permaneça questionável. Para conferências de tecnologia, presume-se que 100% dos visitantes se conectam à rede, esse número pode ser menor dependendo do tipo de conferência.

Em ambos os exemplos, a chave é entender o número esperado de dispositivos conectados e não há uma solução única para cada grande rede pública. Em ambos os casos, uma antena é conectada a um rádio e são os dispositivos clientes (não usuários humanos) que se conectam a esse rádio. Portanto, os dispositivos de cliente por rádio são uma métrica utilizável.

Dispositivos por rádio

Os APs Cisco têm uma contagem máxima de 200 dispositivos conectados por rádio para APs Wi-Fi 6 e 400 dispositivos por rádio para APs Wi-Fi 6E. No entanto, não é aconselhável projetar para a contagem máxima de clientes. Para fins de planejamento, é recomendável manter a contagem de clientes por rádio bem abaixo de 50% da capacidade máxima do AP. Além disso, o número de rádios depende do tipo de AP e da antena usada, a seção sobre 5 GHz único versus duplo explora isso com mais detalhes.

Neste estágio, é uma boa ideia dividir a rede em áreas distintas, com a contagem de dispositivos esperada por área. Lembre-se, esta seção tem como objetivo estimar um número mínimo de APs e antenas.

Considere um exemplo de três áreas de cobertura distintas, a contagem esperada de clientes é fornecida para cada área e um valor (íntegro) de 75 clientes por rádio é usado para estimar o número de rádios necessários.

Area	Expected Devices	Devices / Radio	Radios
Area 1	1000	75	14
Area 2	2000	75	27
Area 3	2500	75	34
Total			75

Contagem esperada de rádios/clientes por área

Esses números iniciais agora precisam ser combinados com a compreensão de que tipos de APs e antenas são implantados em cada área e se um ou dois 5 GHz são usados. Os cálculos de 6 GHz seguem a mesma lógica de 5 GHz. 2,4 GHz não é considerado neste exemplo.

Vamos supor que cada uma das três áreas use uma combinação de antena patch de 2566P e antena do estádio 9104, com uma combinação de único e duplo 5GHz - este cenário é usado para fins de ilustração.

Area	Total Radios	2566P (Dual 5GHz)	2566P (Single 5GHz)	9104 (Dual 5GHz)
Area 1	14	0	6	4
Area 2	27	6	3	6
Area 3	34	7	0	10
Total Antennas		26	9	20
Total APs		13	9	0 (integrated)

Antenas por área

Cada área lista os tipos de antenas e APs necessários. Observe que, no caso de 5 GHz duplo, a relação é de duas antenas para um AP.

Esta seção demonstra uma abordagem para estimar um número inicial de antenas e APs necessários para uma implantação. A estimativa requer uma compreensão das áreas físicas, possíveis opções de montagem em cada área, o tipo de antenas a ser usado em cada área e o número de dispositivos de cliente esperados.

Cada implantação é diferente e equipamentos adicionais são frequentemente necessários para cobrir áreas específicas ou desafiadoras, esse tipo de estimativa considera apenas a capacidade do cliente (não cobertura) e serve para delinear a escala do investimento necessário. Os locais finais de posicionamento do AP/antena e os totais de equipamentos estão sempre sujeitos a um entendimento completo do caso de uso e verificação no local por um profissional sem fio experiente.

Rendimento esperado

Cada canal sem fio pode oferecer uma quantidade de capacidade disponível que é normalmente traduzida em throughput. Essa capacidade é compartilhada entre todos os dispositivos conectados ao rádio, o que significa que o desempenho de cada usuário diminui à medida que mais conexões de usuário são adicionadas ao rádio. Essa queda no desempenho não é linear e também depende da combinação exata de clientes conectados.

As capacidades do cliente diferem entre os dispositivos, dependendo do chipset do cliente e do número de fluxos espaciais que o cliente suporta. As taxas máximas de dados do cliente para cada número de fluxos espaciais com suporte estão listadas na tabela abaixo.

Client Capability	20MHz channel Wi-Fi 5 (802.11ac)	20MHz channel Wi-Fi 6 (802.11ax)
1 Spatial Stream(s)	86.7Mbps	121.9Mbps
2 Spatial Stream(s)	173.3Mbps	243.8Mbps
3 Spatial Stream(s)	288.9Mbps	365.6Mbps
4 Spatial Stream(s)	346.7Mbps	487.5Mbps

Throughput real máximo esperado para cada tipo de cliente

As taxas listadas são taxas MCS (Modulation and Coding Scheme - Esquema de modulação e codificação) teóricas máximas derivadas do padrão 802.11 e presumem uma razão sinal/ruído (SNR) >30dBm. O principal objetivo do projeto de redes sem fio de bom desempenho é alcançar esse nível de SNR para todos os clientes em todos os locais, mas isso raramente acontece. As

redes sem fio são dinâmicas por natureza e usam frequências não licenciadas, várias interferências não controladas têm um impacto no SNR do cliente, além das capacidades do cliente.

Mesmo nos casos em que o nível exigido de SNR é atingido, as taxas listadas anteriormente não consideram a sobrecarga de protocolo e, portanto, não mapeiam diretamente para o throughput real (medido por várias ferramentas de teste de velocidade). O mundo real é sempre inferior à taxa MCS.

Para todas as redes sem fio (incluindo grandes redes públicas), o throughput do cliente sempre depende de:

- Recursos do cliente.
- Relação sinal/ruído do cliente nesse momento específico.
- Número de outros clientes conectados naquele momento específico.
- Recursos de outros clientes em um momento específico.
- Atividade de outros clientes nesse momento específico.
- Interferência em um momento específico.

Com base na variabilidade desses fatores, não é possível garantir um mínimo por cliente em todas as redes sem fio, independentemente do fornecedor do equipamento.

Para obter mais informações, consulte o Validate Wi-Fi Throughput: Testing and Monitoring Guide.

Plataforma WLC

Escolher sua plataforma WLC pode parecer fácil. A primeira coisa em que você pode pensar é observar a contagem estimada de APs e clientes que você pretende gerenciar. A folha de dados de cada plataforma WLC contém todos os objetos máximos suportados na plataforma: ACLs, contagem de clientes, marcas de site e assim por diante. Esses são números máximos literais e muitas vezes há uma aplicação difícil. Você não pode unir os APs 6001 a um 9800-80 que suporte somente 6000 APs, por exemplo. Mas será sensato visar o máximo em toda a parte?

Os controladores sem fio da Cisco são testados para atingir esses máximos, mas não podem necessariamente atingir todos os máximos documentados em todas as condições ao mesmo tempo. Vamos pegar o exemplo de throughput, um 9800-80 pode alcançar até 80 Gbps de encaminhamento de dados do cliente, mas esse é o caso em que cada pacote do cliente é o tamanho máximo e ideal de 1500 bytes. Com uma combinação de tamanhos de pacote, o throughput máximo efetivo é menor. Se você habilitar a criptografia DTLS, o throughput será reduzido ainda mais, o mesmo acontecendo com a visibilidade do aplicativo. É otimista esperar mais de 40 Gbps de um 9800-80 em condições realistas em uma rede grande com muitos recursos ativados. Como isso varia muito dependendo dos recursos em uso e do tipo de atividade de rede, a única maneira de obter uma ideia real da capacidade é medir a utilização do caminho de dados usando esse comando. Foco na métrica de carga, que é uma porcentagem do throughput máximo que o controlador pode encaminhar.

```
WLC#show platform hardware chassis active qfp datapath utilization summary

  CPP 0:                      5 secs        1 min        5 min       60 min

Input:     Total (pps)            9            5            5            8

                  (bps)        17776         7632         9024        10568

Output:    Total (pps)            5            3            3            6

                  (bps)        11136        11640        11440        41448

Processing: Load (pct)            0            0            0            0


WLC#
```

Da mesma forma, o 9800-80 pode perfeitamente lidar com 6.000 APs com atividade regular. No entanto, 6.000 APs em um local público, como um estádio ou um aeroporto, não contam como atividade regular. Considerando a quantidade de roaming de clientes e sondagem de ambiente, grandes redes públicas em escala máxima podem causar maior utilização da CPU em uma única WLC. Se você adicionar monitoramento e interceptações SNMP (traps) a serem enviadas toda vez que os clientes se movimentam, a carga pode rapidamente se tornar excessiva. Um dos principais aspectos específicos de um grande local público ou grande evento é que há muito mais eventos de integração de clientes à medida que as pessoas se movimentam e constantemente se associam/desassociam, o que causa pressão extra na CPU e no plano de controle.

Várias implantações mostraram que um único par (HA) de 9800-80 controladores sem fio pode lidar com uma implantação em um grande estádio com bem mais de 1000 APs. Também é comum distribuir os APs em dois ou mais pares de controladores para eventos críticos onde o tempo de atividade e a disponibilidade são as principais preocupações. Quando grandes redes são distribuídas em várias WLCs, há a complexidade adicional do roaming entre controladores, o roaming de clientes deve ser considerado cuidadosamente em espaços confinados, como um estádio.

Consulte também a seção Marca do site neste documento.

Alta disponibilidade da WLC

Recomenda-se o uso de um par de HA SSO (High-Availability Stateful Switch Over), que fornece redundância de hardware, mas também protege contra falhas de software. Usando HA SSO, um travamento de software em um dispositivo é transparente para os usuários finais à medida que o WLC secundário assume perfeitamente. Outra vantagem de um par HA SSO são as atualizações sem interrupções oferecidas pelo recurso In-Service Software Upgrade (ISSU).

Se a rede for grande o suficiente, também é aconselhável usar um controlador extra (N+1). Ele pode servir a várias finalidades que o HA SSO não pode cumprir. Você pode testar uma nova versão de software nesta WLC antes de atualizar o par de produção (e migrar apenas alguns APs de teste para ela para testar uma seção específica da rede). Algumas condições raras podem

afetar ambas as WLCs em um par HA (quando o problema é replicado para o standby) e aqui o N+1 permite ter uma WLC segura em um cenário ativo-ativo no qual você poderia migrar progressivamente APs de e para. Ele também pode servir como um controlador de provisionamento para configurar novos APs.

As 9800-CLs são muito escaláveis e eficientes. Deve-se observar que eles têm uma capacidade de encaminhamento de dados muito menor (de 2 Gbps a 4 Gbps para a imagem SR-IOV), o que tende a restringi-los aos cenários de switching local FlexConnect (e possivelmente a um pequeno número de APs no switching central). No entanto, eles podem ser úteis como dispositivos N+1 quando você precisa de controladores extras durante uma janela de manutenção ou ao solucionar um problema.

Sistemas externos

Embora este documento se concentre principalmente no componente sem fio de redes de eventos grandes, também há vários sistemas de suporte que exigem consideração durante a fase de dimensionamento e projeto, alguns deles são discutidos aqui.

Rede de núcleo

Redes sem fio grandes são normalmente implantadas no modo de switching central e com sub-redes grandes. Isso implica que um número muito grande de endereços MAC do cliente e entradas ARP são enviadas para a infraestrutura com fio adjacente. É fundamental que os sistemas adjacentes dedicados às várias funções L2 e L3 possuam os recursos adequados para lidar com essa carga. No caso de switches L2, uma configuração comum é o ajuste do modelo Switch Device Manager (SDM), que é responsável pela alocação de recursos do sistema, balanceando entre recursos L2 e L3, dependendo da função do dispositivo na rede. É importante garantir que os dispositivos L2 do núcleo possam suportar o número de entradas de endereço MAC esperado.

NAT de gateway

O caso de uso mais comum de redes públicas é fornecer acesso à Internet aos visitantes. Em algum lugar no caminho de dados deve haver um dispositivo responsável pela conversão de NAT/PAT. Os gateways de Internet devem possuir os recursos de hardware necessários e a configuração do pool IP para lidar com a carga. Lembre-se de que um único dispositivo cliente sem fio pode ser responsável por várias conversões NAT/PAT.

DNS/DHCP

Esses dois sistemas são fundamentais para garantir uma boa experiência ao cliente. Os serviços DNS e DHCP exigem não apenas o dimensionamento apropriado para lidar com a carga, mas também consideração com relação ao posicionamento na rede. Sistemas rápidos e ágeis, colocados no mesmo local da WLC, garantem a melhor experiência e evitam longos tempos de integração do cliente.

Portal AAA/Web

Ninguém gosta de uma página da Web lenta, escolher um sistema apropriado e bem dimensionado para autenticação da Web externa é importante para uma boa experiência de integração do cliente. Da mesma forma para AAA, os servidores de autenticação RADIUS devem ser capazes de lidar com as demandas do sistema sem fio. Tenha em mente que em alguns casos a carga pode aumentar durante momentos-chave, por exemplo, meio período durante uma partida de futebol, o que pode gerar alta carga de autenticação em uma pequena quantidade de tempo. O dimensionamento do sistema para uma carga simultânea adequada é fundamental. Deve-se ter cuidado específico ao usar recursos como contabilidade AAA. Evite a contabilidade baseada em tempo a todo custo e, se você usar a contabilidade, tente desativar a contabilidade provisória. Outro item importante a ser considerado é o uso de balanceadores de carga, onde os mecanismos de pino de sessão devem ser usados para garantir fluxos de autenticação completos. Certifique-se de manter o tempo limite do RADIUS em 5 segundos ou mais.

Se estiver usando um SSID 802.1X com uma grande contagem de clientes (por exemplo, com OpenRoaming), certifique-se de habilitar a Transição Rápida (FT) 802.11r, caso contrário os clientes poderão causar uma tempestade de autenticação sempre que fizerem roaming.

DNS/DHCP

Algumas recomendações para o DHCP:

- Verifique se o pool DHCP é pelo menos três vezes o número de clientes esperado. Os IPs permanecem atribuídos por algum tempo mesmo depois que o cliente é desconectado, portanto, dependendo do tempo de permanência dos convidados, isso pode consumir mais endereços IP. Tente corresponder o tempo de aluguel à duração esperada da visita do usuário ao local. Não há motivo para alocar um endereço IP por uma semana. Se uma visita típica tiver duas horas, isso ajudará a eliminar os aluguéis obsoletos.
- O uso de uma única sub-rede grande para clientes é recomendado, a WLC tem um recurso de proxy ARP e não encaminha broadcasts por padrão (além do DHCP). Usar uma sub-rede de cliente grande (por exemplo, /16) para seus clientes não representa um problema. Uma única VLAN grande é mais simples se comparada a um grupo de VLANs com muitas VLANs. A configuração de muitas sub-redes menores (por exemplo, /24) e grupos de VLANs não influencia o domínio de broadcast e resulta apenas em uma configuração mais complicada, resultando em problemas como VLANs sujas e tendo que rastrear vários pools de DHCP que não podem ser usados uniformemente.
- Mantenha o DHCP no modo de Bridging no controlador sem fio com a funcionalidade de retransmissão de DHCP tratada pelo gateway de Camada 3 da sub-rede. Isso permite o máximo de eficiência e simplicidade. A ideia é não envolver o controlador sem fio no processo DHCP.
- Use o DHCP necessário em qualquer WLAN pública, independentemente do método de autenticação. Embora isso possa acionar uma pequena porcentagem de associações de clientes com falha, pode evitar problemas de segurança significativos, seja por clientes que tentam atribuir a si mesmos endereços IP estáticos ou por clientes que se comportam mal e tentam reutilizar um endereço IP anterior sem permissão.

Operando a rede

A configuração certa

É tentador permitir que muitas opções se beneficiem de todos os recursos mais recentes do Wi-Fi moderno. No entanto, certos recursos funcionam bem em ambientes pequenos, mas têm um grande impacto em ambientes grandes e densos. Da mesma forma, certos recursos podem apresentar problemas de compatibilidade. Embora os equipamentos da Cisco respeitem todos os padrões e ofereçam compatibilidade com uma grande variedade de clientes testados, o mundo está repleto de dispositivos de cliente exclusivos que às vezes têm versões de software de driver com bugs ou incompatibilidade com determinados recursos.

Dependendo do nível de controle que você tem sobre os clientes, você deve ser conservador. Por exemplo, se você implantar o Wi-Fi para a grande reunião anual da sua empresa, saberá que a maioria dos clientes são dispositivos da empresa e poderá planejar o conjunto de recursos para ativá-lo de acordo. Por outro lado, se você opera um Wi-Fi de aeroporto, seu nível de satisfação do convidado está diretamente relacionado à capacidade de se conectar à sua rede, e você não tem nenhum controle sobre os dispositivos clientes que as pessoas podem usar.

SSID

Quantos SSIDs?

A recomendação sempre foi usar o menor número possível de SSIDs. Isso é exacerbado em redes de alta densidade, já que a possibilidade de ter vários APs no mesmo canal é quase garantida. Geralmente, muitas implantações usam muitos SSIDs, reconhecem que têm muitos SSIDs, mas declaram que não podem usar menos. Você deve realizar um estudo comercial e técnico para cada SSID para entender as semelhanças entre os SSIDs e as opções para recolher vários SSIDs em um.

Vamos analisar alguns tipos de segurança/SSID e seu uso.

WPA2/3 pessoal

Um SSID de chave pré-compartilhada é imensamente popular devido à sua simplicidade. Você pode imprimir a chave em algum lugar em crachás ou em papel ou placas ou comunicá-la de alguma forma aos visitantes. Às vezes, um SSID de chave pré-compartilhada é preferido até mesmo para um SSID de convidado (desde que a chave seja bem conhecida por todos os participantes). Ele pode ajudar a evitar o esgotamento do pool de DHCP devido à natureza deliberada da conexão. Os dispositivos que passam não se conectam automaticamente à rede, portanto, não podem consumir um endereço IP do pool DHCP.

A WPA2 PSK não fornece privacidade, pois o tráfego pode ser facilmente descriptografado, já que todos usam a mesma chave. Ao contrário, o WPA3 SAE fornece privacidade e, mesmo que todos tenham a chave mestra, não é possível derivar a chave de criptografia usada por outros clientes.

O WPA3 SAE é a melhor opção para segurança e muitos smartphones, laptops e sistemas operacionais oferecem suporte a ela. Alguns dispositivos da IoT ou wearables inteligentes ainda

podem ter suporte limitado e os clientes mais antigos em geral são susceptíveis a problemas se não receberem atualizações recentes de drivers ou firmware.

Pode ser tentador considerar um modo de transição WPA2 PSK-WPA3 SAE SSID para simplificar as coisas, mas isso foi mostrado no campo para causar alguns problemas de compatibilidade. Clientes mal programados não esperam dois tipos de métodos de chave compartilhada no mesmo SSID. Se você quiser oferecer as opções WPA2 e WPA3, é aconselhável configurar SSIDs separados.

WPA2/3 empresarial

A WPA3 Enterprise (usando a criptografia AES de 128 bits) é tecnicamente o mesmo método de segurança (pelo menos, como anunciado nos beacons SSID) que a WPA2 Enterprise, que fornece compatibilidade máxima.

Para 802.1X, um SSID de modo de transição é aconselhado, pois problemas de compatibilidade não são vistos com dispositivos recentes (problemas foram relatados com o Android 8 ou versões antigas do Apple IOS). O IOS XE 17.12 e versões posteriores permitem ter um único SSID corporativo de transição, onde somente a WPA3 é usada e anunciada em 6 GHz, enquanto a WPA2 é oferecida como uma opção na banda de 5 GHz. Recomendamos habilitar a WPA3 em SSIDs corporativos assim que possível.

Os SSIDs WPA Enterprise podem ser usados para usuários-chave para os quais existe um banco de dados de provedor de identidade que permite retornar parâmetros AAA (como VLANs ou ACLs) dependendo da identidade do usuário. Esses tipos de SSIDs podem incluir eduroam ou OpenRoaming, que combinam os benefícios dos SSIDs convidados (permitindo que os visitantes se conectem facilmente sem inserir credenciais) com a segurança de um SSID corporativo. Eles reduzem muito a complexidade da integração normalmente associada ao 802.1X, pois os clientes não precisam fazer nada para participar do eudroam ou do SSID do OpenRoaming, desde que tenham um perfil no telefone (que pode ser facilmente fornecido através de um aplicativo de evento)

SSIDs convidados

Um SSID convidado é geralmente sinônimo de autenticação aberta. Você pode adicionar um portal da Web (ou não) atrás dele (dependendo da simpatia desejada ou dos requisitos locais) em suas várias formas: autenticação da Web externa, local ou central, mas o conceito permanece o mesmo. Ao usar um portal para convidados, a escalabilidade pode rapidamente se tornar um problema em grandes ambientes. Consulte a seção Configuração da Escalabilidade para obter mais informações sobre isso.

As operações de 6 GHz exigem que seu SSID convidado use a Abertura aprimorada em vez de apenas Aberta. Isso ainda permite que qualquer pessoa se conecte, mas fornece privacidade (uma privacidade melhor do que WPA2-PSK) e criptografia, tudo sem fornecer nenhuma chave ou credenciais ao se conectar no SSID. Os principais fornecedores de smartphones e sistemas operacionais agora suportam o Enhanced Open, mas o suporte ainda não está difundido na base de clientes sem fio. O modo de transição Aberto Aprimorado fornece uma boa opção de

compatibilidade na qual os dispositivos capazes se conectam ao SSID convidado criptografado (usando o Aberto Aprimorado), e os dispositivos que não são capazes ainda usam o SSID como simplesmente aberto como antes. Embora apenas um único SSID seja percebido pelos usuários finais, lembre-se de que esse modo de transição envia dois SSIDs em seus beacons (embora apenas um esteja visível).

Em grandes eventos e locais, é geralmente aconselhável configurar uma PSK no SSID convidado, em vez de deixá-lo puramente aberto (o modo Enhance Open Transition seria melhor, mas isso cria dois SSIDs e a compatibilidade com o cliente ainda deve ser amplamente comprovada). Embora isso torne a integração um pouco mais complicada (você deve imprimir a PSK em crachás ou bilhetes das pessoas ou anunciá-la de alguma forma), evita que clientes casuais se conectem à rede automaticamente sem que o usuário final tenha qualquer intenção de usar a rede. Mais e mais fornecedores de sistemas operacionais móveis também despriorizam redes abertas e mostram um aviso de segurança. Em outras situações, você pode querer um número máximo de transeuntes para se conectar e, portanto, abrir é a melhor opção.

Conclusão sobre o número de SSIDs

Não pode haver uma resposta satisfatória para a questão de a quantos SSIDs você deve se ater. O efeito depende da taxa de dados mínima configurada, do número de SSIDs e do número de APs que transmitem no mesmo canal. Em um grande evento da Cisco, a infraestrutura sem fio usou 5 SSIDs: o WPA2 PSK principal, um WPA 3 SAE SSID para segurança e cobertura de 6 GHz, um Eduroam SSID corporativo para facilidade de acesso para participantes educacionais, um OpenRoaming SSID para receber com segurança qualquer pessoa que tenha configurado o Wi-Fi no aplicativo do evento e um 802.1X SSID separado para a equipe e o acesso à rede administrativa. Isso já era quase demais, mas o efeito se manteve razoável graças ao grande número de canais disponíveis e às antenas direcionais usadas para reduzir ao máximo a sobreposição de canais.

Os conceitos de SSID antigo versus SSID principal

Por um certo período, foi recomendado restringir o serviço de 2,4 GHz a um SSID separado "Herdado" anunciado apenas em 2,4 GHz. Isso está ficando menos popular à medida que as pessoas param de fornecer serviço de 2,4 GHz. No entanto, a ideia pode e deve persistir, mas com outros conceitos. Você quer implementar o WPA3 SAE, mas o modo de transição está lhe dando problemas de compatibilidade com seus clientes? Tenha um SSID WPA2 "herdado" e um SSID WPA3 SAE principal. Nomeando o SSID de menor desempenho como "antigo", ele não atrai clientes e você pode ver facilmente quantos clientes ainda enfrentam problemas de compatibilidade com o seu SSID principal e exigem esse antigo.

Mas por que parar por aí? Você ouviu rumores de que o 802.11v causou problemas com alguns clientes mais antigos ou que alguns drivers de cliente não gostam de ver a Análise de Dispositivo habilitada no SSID? Ative todos esses recursos úteis no SSID principal avançado e deixe-os desativados no SSID herdado/de compatibilidade. Isso permite que você teste a distribuição de novos recursos no SSID principal e ainda forneça um SSID de compatibilidade máxima para o qual os clientes possam recorrer. Esse sistema só funciona dessa maneira. Se você usar o nome

oposto de seu SSID orientado por compatibilidade como principal e nomear seu SSID avançado com algo como "<name>-WPA3", perceberá que as pessoas se agarram ao SSID antigo a que estavam acostumadas e que a adoção permanece pequena por muitos anos em seu "novo" SSID. A implantação de novas configurações ou recursos tem resultados inconclusivos devido ao menor número de clientes que se conectam a ele.

Recursos de SSID

- É melhor manter as extensões Aironet desabilitadas. Eles são particularmente úteis para pesquisas de site e operações WGB, mas às vezes causam problemas com alguns clientes legados. O Aironet IE também anuncia o nome de host do AP que é indesejado em implantações de segurança consciente.
- O CCKM é um protocolo preterido (em favor do FT) e deve ser desabilitado.
- Neste momento, é melhor usar a criptografia AES-128, mesmo em WPA3 devido ao baixo suporte do cliente de criptografias mais altas (a menos que você possa pagar um SSID específico mais seguro e restritivo)
- A detecção de furos de cobertura é melhor desativada (para todos os SSIDs). Implantações grandes normalmente usam antenas direcionais, exigindo uma pesquisa de site completa. Os níveis de potência de cada antena seriam um resultado do processo de projeto de RF e normalmente configurados para níveis específicos.
- A FT adaptativa deve ser desabilitada, pois alguns clientes podem ter problemas quando a FT não está totalmente anunciada, mas presente em alguns atributos. Desabilite totalmente a FT (para compatibilidade máxima) ou use a FT+802.1X para a qual a maioria dos clientes (a menos que sejam antigos ou mais orientados à IoT) oferece suporte. Ao configurar o FT+802.1X, até mesmo os clientes não-FT podem se associar ao SSID. O único problema possível é com alguns clientes que não tolerariam ver duas opções de segurança no mesmo SSID.
- Desabilite o MIMO de MU 802.11ac. Ela aumenta a complexidade e tem um benefício muito baixo em 802.11ac.
- Desabilite o Tempo de Ativação do Destino BSS. Atualmente, a adoção do produto é baixa no lado do cliente.
- Desative o balanceamento de carga agressivo e a Seleção de banda. A seleção de banda não é necessária se você não anunciar o SSID em 2,4 GHz (ou se ele estiver em um SSID dedicado) e o balanceamento de carga agressivo atrasa a associação do cliente, rejeitando-o algumas vezes antes de finalmente aceitá-lo, se ele insistir em se conectar a um AP carregado. Você carregou APs de qualquer forma em um ambiente ocupado e isso é negativo para a experiência do cliente.
- Desative o Fastlane+.
- Desabilite o Universal Admin, esse recurso era para 3700 AP e somente no domínio -UX. Deixá-lo em folhas abre um vetor de ataque desnecessário.
- Manter OKC (Cache de Chave Oportunista) habilitado. Ele serve como um mecanismo de roaming rápido para clientes que não suportam FT.
- Mantenha a WMM permitida. Desativá-la levaria sua rede de volta à era 802.11g e exigi-la não traz nenhuma vantagem para a plataforma 9800.
- Ative o IP Source Guard.
- Desative a criação de perfil RADIUS. Em um ambiente muito ocupado, isso pode enviar

mensagens de contabilização RADIUS excessivas (sempre que os clientes executam DHCP ou enviam pacotes HTTP) e tem um potencial muito real de sobrecarregar o servidor RADIUS.
- Evite usar SSIDs ocultos. Isso não serve a nenhum propósito de segurança, o nome SSID ainda pode ser facilmente descoberto com aplicativos simples ou por uma captura de farejador. Ocultar o SSID reduz a velocidade de roaming de todos os clientes, pois eles não se beneficiam mais da varredura passiva de beacon e devem confiar na varredura ativa para obter informações de AP vizinhos.
- Tente não usar mais do que quatro WLANs por rádio, pois isso tem um impacto significativo na utilização de RF. Não é um limite rígido, o uso de cinco WLANs pode funcionar, mas tenha muito cuidado com o tempo de transmissão desperdiçado ao usar cada vez mais WLANs.
- 802.11v e 802.11k são padrões que são cada vez mais suportados por tipos populares de clientes. Normalmente, não representam um problema com relação à conexão do cliente. Os benefícios que eles trazem dependem muito de como os clientes utilizam esses protocolos e podem, às vezes (no caso do 802.11k) causar um uso de CPU ligeiramente maior. Você pode mantê-los fora da IoT ou do SSID herdado, mas eles devem ser ativados, se possível, no SSID de produção.

Marca Site

As marcas de site são um item de configuração que permite agrupar pontos de acesso que compartilham as mesmas configurações do FlexConnect, bem como as configurações de perfil de ingresso no AP (como credenciais, detalhes de SSH e código de país). Por que as marcas de site são importantes? As marcas de site também definem como os APs são tratados pelo processo WNCD dentro do Catalyst 9800. Vamos dar alguns exemplos para ilustrar:

- Se você configurar quatro marcas de site em um 9800-80 que tenha oito processos WNCD, cada marca de site será atribuída a um processo WNCD diferente (executando cada uma em um núcleo de CPU separado) e quatro processos WNCD não farão nada. Isso significa que você não está utilizando todas as CPUs do seu 9800-80 e não seria recomendável carregá-lo com o máximo de 6000 APs suportados.

Site tag 1	Site tag 2	Site tag 3	Site tag 4	-	-	-	-
WNCD 1	WNCD 2	WNCD 3	WNCD 4	WNCD 5	WNCD 6	WNCD 7	WNCD 8
CPU	CPU	CPU	CPU	CPU	CPU	CPU	CPU

Primeiro exemplo de balanceamento de tag de site

- Se você configurar 10 tags laterais em um 9800-80 que tenha oito processos WNCD, dois processos WNCD tratarão de duas tags de site cada, enquanto os seis restantes tratarão de uma tag de site cada.

Site tag 1 Site tag 9	Site tag 2 Site tag 10	Site tag 3	Site tag 4	Site tag 5	Site tag 6	Site tag 7	Site tag 8
WNCD 1	WNCD 2	WNCD 3	WNCD 4	WNCD 5	WNCD 6	WNCD 7	WNCD 8
CPU	CPU	CPU	CPU	CPU	CPU	CPU	CPU

Segundo exemplo de balanceamento de tag de site

Para implantações geograficamente grandes com muitos sites e muitas marcas de site, o número de marcas de site é recomendado para ser um múltiplo do número de processos WNCD na plataforma que você está usando.

No entanto, para redes de eventos que geralmente estão sob um telhado, ou vários prédios no mesmo local, a recomendação é corresponder o número de identificadores de site ao número exato de WNCDs na plataforma em questão. O objetivo final é que cada processo WNCD (e, portanto, cada núcleo de CPU alocado para tarefas sem fio) lide com um número aproximadamente similar de eventos de roaming de clientes para que a carga seja balanceada em todos os núcleos de CPU.

Platform type	Number of WNCD processes
9800-CL small OVA	1
9800-CL medium OVA	3
9800-CL large OVA	7
9800-L	1
9800-40/CW9800-M	5
9800-80/CW9800-H	8

Número de processos WNCD para cada tipo de plataforma

No núcleo, o que realmente importa é agrupar os APs que estão na mesma vizinhança física na mesma tag de site, para que os eventos frequentes de roaming de clientes entre esses APs permaneçam no mesmo processo de CPU. Isso significa que, mesmo se você tiver um único local grande, é recomendável dividir o local em várias marcas de site (quantos processos WNCD estiverem manipulando o local) e agrupar APs o mais logicamente possível nesses grupos para formar grupos de vizinhança RF lógicos que também estejam distribuídos uniformemente entre as marcas de site.

Iniciando o IOS XE 17.12, um algoritmo de balanceamento de carga pode ser habilitado de modo que a WLC agrupe os APs com base em sua proximidade de RF. Isso tira a carga de suas mãos e cria uma propagação equilibrada dos APs no processo WNCD. Isso pode ser útil se você não

conseguir desenhar facilmente grupos de APs vizinhos para serem colocados na quantidade correta de tags de site. Uma especificidade desse algoritmo é que ele atribui APs ao processo WNCD, independentemente de sua atribuição de marca de site, o que significa que ele não altera a atribuição de marca de site do AP. Você pode atribuir tags de site puramente básicas em uma lógica de configuração e deixar que o algoritmo equilibre os APs nas CPUs da maneira mais ideal.

O recurso de Balanceamento de Carga de AP Automático baseado em RF está documentado no Guia de Configuração de Software do Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Dublin 17.12.x.

O uso da CPU dos processos WNCD deve ser monitorado durante eventos grandes. Se um ou mais processos WNCD mostrarem alta utilização, pode ser que o WNCD esteja lidando com muitos APs ou clientes, ou que os APs ou clientes que ele lida estejam mais ocupados que a média (se todos eles estiverem constantemente em roaming, como em um aeroporto, por exemplo).

Perfil da política

- Ative o ARP e o Proxy de Detecção de Endereço Duplicado (DAD - Duplicate Address Detection); isso permite que a WLC responda em nome dos clientes sem fio quando um dispositivo está tentando aprender o endereço MAC de um dispositivo sem fio. Isso também economiza baterias de clientes sem fio.
- Não habilite recursos WGB a menos que seja necessário.
- Ative o DHCP necessário para evitar clientes com endereços IP estáticos.
- Keep idle-timeout short (300 segundos). Alguns administradores demoram para evitar que os clientes precisem reautenticar, mas o tempo limite ocioso longo resulta em entradas de clientes fantasma (afetando os relatórios) à medida que a contagem de clientes é atrasada em tempo real. É melhor manter o timeout de ociosidade menor que o temporizador de rotação de chave de grupo para evitar inundações de contabilização quando os clientes são excluídos. O intervalo de rotação de chave de grupo pode ser configurado na interface do usuário da Web em Configuration > Security > Advanced EAP como "EAP-Broadcast Key Interval"
- Faça com que o tempo limite da sessão seja de 86400 segundos para evitar desconexões e reautenticações desnecessárias.

Perfil de ingresso no AP

- Certifique-se de que o ajuste de MSS do TCP esteja habilitado.
- Habilite Trust DSCP upstream. Muitos clientes sem fio não fazem a marcação UP WMM 802.11e infelizmente, confiar no campo DSCP é uma maneira segura de fornecer a prioridade correta para aplicativos de voz.
- Ative o Syslog para seus pontos de acesso. A configuração de um IP de servidor Syslog faz com que os APs unicast seus registros de console nele. Não só é útil solucionar problemas de APs, mas também é melhor para a rede do que a configuração padrão que faz com que os APs transmitam seu Syslog na VLAN local. O registro de AP pode gerar uma carga significativa de mensagens, mesmo nos casos em que o Syslog de AP não é monitorado,

ainda é uma boa ideia limitar o número de eventos definindo a gravidade da mensagem apropriada e/ou configurando um endereço IP de Syslog fictício (por exemplo, 0.0.0.0) para evitar que as mensagens sejam transmitidas.
- Maximize as tentativas de CAPWAP e o tempo limite. Os problemas são detectados menos rapidamente, mas a rede é mais resistente a quedas de pacotes transientes menores.
- Habilite o SSH e configure as credenciais. Desative o console do AP.
- Ative o monitor AP se necessário, mas não o monitor de rádio.
- Ative a detecção de invasor e configure um limite de RSSI de -70 dBm.

Monitorando a rede

Quando a rede estiver em funcionamento, você terá que monitorá-la atentamente em busca de problemas. Em um ambiente de escritório padrão, os usuários conhecem a rede e podem ajudar uns aos outros em caso de problemas ou abrir um ticket interno de helpdesk. Em um local maior, com muitos visitantes, você deve se concentrar nos maiores problemas, em vez de em indivíduos específicos que podem ter uma configuração incorreta, para que você precise ter a estratégia de monitoramento certa.

É possível monitorar a rede a partir da CLI ou da GUI do Catalyst 9800, mas essa não é a melhor ferramenta para monitorar diariamente. É o mais direto quando você já tem suspeitas e/ou dados sobre o problema e deseja executar comandos específicos em tempo real. As principais opções de monitoramento são o Cisco Catalyst Center ou, possivelmente, um painel de telemetria personalizado. É possível usar ferramentas de monitoramento de terceiros, mas quando elas usam o SNMP como um protocolo, os dados estão longe do tempo real e as ferramentas de monitoramento usuais de terceiros não são suficientemente granulares com todas as especificidades de fornecedores sem fio. Se você escolher o protocolo SNMP, certifique-se de usar o SNMPv3, pois o SNMPv2 tem segurança desatualizada.

O Cisco Catalyst Center é a melhor opção, pois permite que você gerencie sua rede além de monitorá-la. Mais do que monitorar, ele também permite solucionar problemas ao vivo e corrigir muitas situações.

Um painel de telemetria personalizado pode ser útil se você quiser exibir métricas e widgets muito específicos em uma tela de forma sempre ativa para um NOC ou SOC. Se houver áreas muito específicas da sua rede que você deseja vigiar, você pode criar widgets dedicados para mostrar as métricas de rede nessas áreas da maneira que você escolher.

Para redes de eventos, é uma boa ideia monitorar estatísticas de RF em todo o sistema, em particular a utilização de canal e o número de clientes por AP. Isso pode ser feito a partir do CLI, mas fornece apenas um instantâneo em um momento específico, a utilização do canal tende a ser dinâmica e é mais adequada para monitoramento ao longo do tempo. Para esse tipo de monitoramento, um painel personalizado é geralmente uma boa abordagem. Outras métricas que são mais valiosas quando monitoradas ao longo do tempo podem incluir a utilização de WNCD, o número de clientes e seus estados e métricas específicas do local. Um exemplo de métricas específicas do local seria monitorar o uso e/ou a carga de uma área ou local específico, por exemplo, o hall X no caso de um centro de conferências, ou a área de assentos Y no caso de um local de evento.

Para o monitoramento personalizado, tanto a telemetria de fluxo NETCONF RPC (pull) quanto a telemetria de fluxo NETCONF (push) são abordagens válidas, embora o uso de telemetria de fluxo personalizado em conjunto com o Catalyst Center exija alguma diligência, pois há um limite para o número de assinaturas de telemetria que podem ser configuradas na WLC e o Catalyst Center pré-preenche (e utiliza) muitas dessas.

Ao usar o NETCONF RPC, alguns testes são necessários para garantir que o WLC não fique sobrecarregado com solicitações do NETCONF, particularmente importante lembrar que são taxas de atualização para alguns dos pontos de dados e o tempo necessário para que os dados sejam retornados. Por exemplo, a utilização do canal AP é atualizada (de AP para WLC) a cada 60 segundos, e a coleta de métricas de RF para 1.000 APs (de WLC) pode levar vários segundos. Neste exemplo, fazer polling na WLC a cada 5 segundos não seria útil; uma melhor abordagem seria coletar métricas de RF em todo o sistema a cada 3 minutos.

NETCONF é sempre o preferido em relação ao SNMP.

Por fim, o monitoramento dos componentes da rede central não pode ser ignorado, incluindo a utilização do pool de DHCP, o número de entradas NAT nos roteadores centrais e assim por diante. Como a falha de qualquer um desses pode ser facilmente a causa de uma interrupção sem fio.

Quanto mais você monitora, mais você pode causar seus próprios problemas

Há alguns cenários clássicos em que um excesso de monitoramento cria problemas:

- Os sensores sem fio que atuam como clientes podem ser úteis para medir o throughput e a conectividade em locais específicos da rede, mas lembre-se de que definir uma alta frequência de testes significa que o sensor passará muito tempo fazendo grandes transferências de dados e, portanto, deixando o canal e a rede realmente ocupados, mesmo que não fosse de outra forma. Este é o primeiro exemplo de "quanto mais você monitora, pior sua aparência de métricas".
- O SNMP, como já mencionado, é um protocolo legado que tem um alto impacto na CPU. Fazer um grande polling SNMP pode saturar facilmente a CPU da rede sem fio com solicitações assim que você monitora com frequência todos os seus clientes sem fio ou APs quando você tem um grande número deles. Sempre considere a quantidade de objetos que você está fazendo polling antes de definir um intervalo de polling agressivo. O daemon SNMP está dentro do processo IOSd no IOS-XE, portanto, quando ele está em uma CPU alta, pode afetar o restante das funcionalidades do IOS.
- Mesmo que a telemetria seja mais eficiente que o SNMP, grandes redes sem fio podem ter uma quantidade muito grande de clientes, APs, mas também interferências e dispositivos invasores. Se a sua configuração de telemetria estiver definida de forma muito agressiva e a WLC tiver que reportar qualquer alteração no sinal de qualquer dispositivo invasor constantemente, isso também poderá saturar facilmente qualquer dispositivo do controlador. Fique atento ao processo de "publicação" que é responsável pela telemetria e certifique-se de que ele não esteja em alta utilização da CPU. Em caso afirmativo, reconsidere seus limites e certifique-se de seguir as melhores práticas do 9800.

Problemas específicos de redes grandes

Se você tiver um SSID usando autenticação da Web, um problema pode ser que os clientes se conectam a esse SSID e obtêm um endereço IP, mas nunca se autenticam porque o usuário final não está tentando se conectar ativamente (o dispositivo se conectou automaticamente). O controlador deve interceptar cada pacote HTTP enviado por esses clientes que estão no estado chamado autenticação da Web pendente e que usa recursos WLC. Quando a rede estiver em execução, verifique periodicamente o número de clientes que estão no estado de autenticação da Web pendente em um determinado momento para ver como ele se compara aos números da linha de base. A mesma coisa para clientes no estado IP Learn. Você sempre tem clientes nesse estado quando eles estão executando o processo DHCP, mas saber qual é o número de trabalho adequado para sua rede ajuda a definir uma linha de base e identificar momentos em que esse número pode ser muito alto e indicar um problema maior.

Para locais grandes, não é raro ver ~10% dos clientes no estado Autenticação da Web Pendente.

Monitoramento do dia 2: Como acompanhar a satisfação do usuário

Uma vez que a rede está funcionando, há dois tipos típicos de reclamações do usuário final: eles não podem se conectar ou têm dificuldade para se conectar (desconexões), ou o Wi-Fi está operando mais lentamente do que o esperado. Este último é muito difícil de identificar, pois primeiro depende das expectativas de velocidade, bem como da densidade em tempo real de uma determinada área. Vamos abordar alguns recursos que podem ser úteis no monitoramento diário de uma grande rede de instalações públicas.

Validar o rendimento do Wi-Fi: Guia de teste e monitoramento. Este documento cisco.com aborda como monitorar uma rede para detectar problemas de throughput. Ele analisa a quantidade de throughput que os clientes podem esperar razoavelmente em sua rede quando as coisas estão quietas e calcula o quanto essas estimativas ficam inativas à medida que a quantidade de clientes e a carga aumentam. Isso é essencial para avaliar se uma reclamação do usuário final sobre o throughput é legítima de um ponto de vista técnico ou não, e se você precisa reprojetar essa área para a carga que ela enfrenta potencialmente.

Quando os clientes relatam problemas de conectividade, depois que isso foi isolado e esclarecido com o Catalyst Center, examine Troubleshooting do Catalyst 9800 Client Connectivity Issues Flow.

Por fim, como uma boa prática geral, fique de olho nas principais métricas gerais da WLC com a ajuda dos KPIs de Monitoramento do Catalyst 9800 (Indicadores-Chave de Desempenho).

Configuração para escalabilidade

SVIs e interfaces no 9800

Evite criar SVIs para VLANs clientes na WLC. Os administradores costumavam ter o reflexo de criar uma interface de camada 3 para cada VLAN cliente, mas isso raramente é necessário. As interfaces aumentam o vetor de ataque do plano de controle e podem exigir mais ACLs com

entradas mais complexas. A WLC pode ser acessada, por padrão, em qualquer uma de suas interfaces, mais trabalho é necessário para proteger uma WLC com mais interfaces. Isso também complica o roteamento, portanto, é melhor evitá-lo.

A partir do IOS XE 17.9, as interfaces SVI não são mais necessárias para os cenários de snooping de mDNS ou de retransmissão de DHCP. Portanto, há muito poucas razões para configurar uma interface SVI em uma VLAN cliente.

Resposta de sondagem agregada

Para redes públicas grandes, é aconselhável modificar o intervalo de sondagem agregado padrão enviado por pontos de acesso. Por padrão, os APs atualizam a WLC a cada 500 ms sobre as sondas enviadas pelos clientes. Essas informações são usadas pelos recursos de balanceamento de carga, seleção de banda, localização e 802.11k. Se houver muitos clientes e pontos de acesso, é aconselhável modificar o intervalo de atualização para evitar problemas de desempenho do plano de controle na WLC. A configuração recomendada é 50 respostas de sonda agregadas a cada 64 segundos. Além disso, certifique-se de que os seus APs não estejam relatando sondas de endereços MAC administrados localmente, pois não há razão para rastrear aqueles que consideram um único cliente poderiam estar usando muitos MACs administrados localmente ao fazer a varredura para evitar o rastreamento propositalmente.

```
wireless probe limit 50 64000

no wireless probe localy-administered-mac
```

IPv6

Muitos administradores de rede ainda negam o IPv6. Há apenas duas opções aceitáveis com o IPv6: ou você o suporta e deve implantar a configuração adequada em todos os lugares, ou não o faz, e você deve bloqueá-lo. Não é aceitável não se importar com o IPV6 e deixá-lo habilitado em alguns lugares sem a configuração adequada. Isso deixaria todo o mundo IP ao qual a segurança da sua rede seria indiferente.

Se você habilitar o IPv6, será obrigatório configurar um endereço IPv6 virtual no intervalo 2001:DB8::/32 (que é uma etapa frequentemente esquecida).

É importante observar que, embora o IPv6 dependa muito do multicast para suas operações básicas, ele ainda pode operar se você desabilitar o encaminhamento multicast na WLC. O encaminhamento multicast se refere ao encaminhamento de dados multicast do cliente e não à descoberta de vizinhos, às solicitações de roteador e a outros protocolos necessários para operar o IPv6.

Se sua conexão com a Internet ou o provedor de serviços de Internet fornecer endereços IPv6, você poderá optar por permitir o IPv6 para seus clientes. Essa é uma decisão diferente da habilitação do IPv6 em sua infraestrutura. Seus APs podem continuar operando somente no IPv4,

mas ainda transportar o tráfego de dados do cliente IPv6 dentro de seus pacotes CAPWAP. Habilitar o IPv6 em sua infraestrutura também exige que você pense em proteger o acesso do cliente a seus APs, WLC e sub-rede de gerenciamento.

Verifique a frequência de RA dos gateways do cliente. A WLC oferece uma política de otimização de RA que limita o número de RAs encaminhadas aos clientes, já que eles podem ficar conversando algumas vezes.

mDNS

Em geral, é melhor manter o mDNS completamente desabilitado em uma implantação de local grande.

O mDNS Bridging se refere ao conceito de permitir que os pacotes mDNS sejam enviados como um multicast de Camada 2 (portanto, para toda a sub-rede do cliente). O mDNS se tornou popular em cenários de home office e pequenos escritórios, onde é muito prático descobrir serviços em sua sub-rede. No entanto, em uma rede grande, isso significa enviar o pacote para todos os clientes na sub-rede, o que é problemático do ponto de vista do tráfego em uma rede pública grande. Por outro lado, o bridging não causa nenhuma sobrecarga na CPU do AP ou da WLC, pois é considerado como tráfego de dados regular. O Proxy mDNS ou gateway mDNS se refere ao conceito de usar a WLC como um diretório para todos os serviços na rede. Isso permite oferecer serviços mDNS através dos limites da Camada 2 de maneira eficiente e também reduzir o tráfego geral. Com o gateway mDNS, uma impressora, por exemplo, envia seu anúncio de serviço periódico via mDNS com um multicast de Camada 2 de mesma sub-rede, mas a WLC não o encaminha a todos os outros clientes sem fio. Em vez disso, ele toma nota do serviço oferecido e o registra em seu diretório de serviços. Sempre que qualquer cliente solicita serviços de um determinado tipo disponíveis, a WLC responde em nome da impressora com o anúncio. Isso evita que todos os outros clientes sem fio ouçam sobre solicitações e ofertas de serviço desnecessárias e obtenham uma resposta apenas quando perguntarem quais serviços estão por perto. Embora melhore muito a eficiência do tráfego, ele causa uma sobrecarga na WLC (ou no AP, se você confia em AP mDNS em cenários FlexConnect) devido à espionagem de tráfego mDNS. Se estiver usando o gateway mDNS, é essencial ficar de olho no uso da CPU.

Fazê-lo em ponte leva a uma tempestade de multicast em sua sub-rede grande e rastreá-lo (com o recurso de gateway mDNS) causa muita utilização da CPU. Desabilite-o globalmente e em cada WLAN.

Alguns administradores habilitam o mDNS porque alguns serviços precisam dele em locais específicos, mas é importante entender o volume de tráfego indesejado que isso adiciona. Os dispositivos Apple muitas vezes estão se autoproclamando, bem como constantemente procurando por serviços, causando um ruído de fundo de consultas mDNS, mesmo quando ninguém está fazendo um uso específico de qualquer serviço. Se você precisar permitir o mDNS devido a um determinado requisito comercial, habilite-o globalmente e, em seguida, habilite-o apenas na WLAN onde for necessário e tente restringir o escopo onde o mDNS é permitido.

Fortalecendo a rede

Security

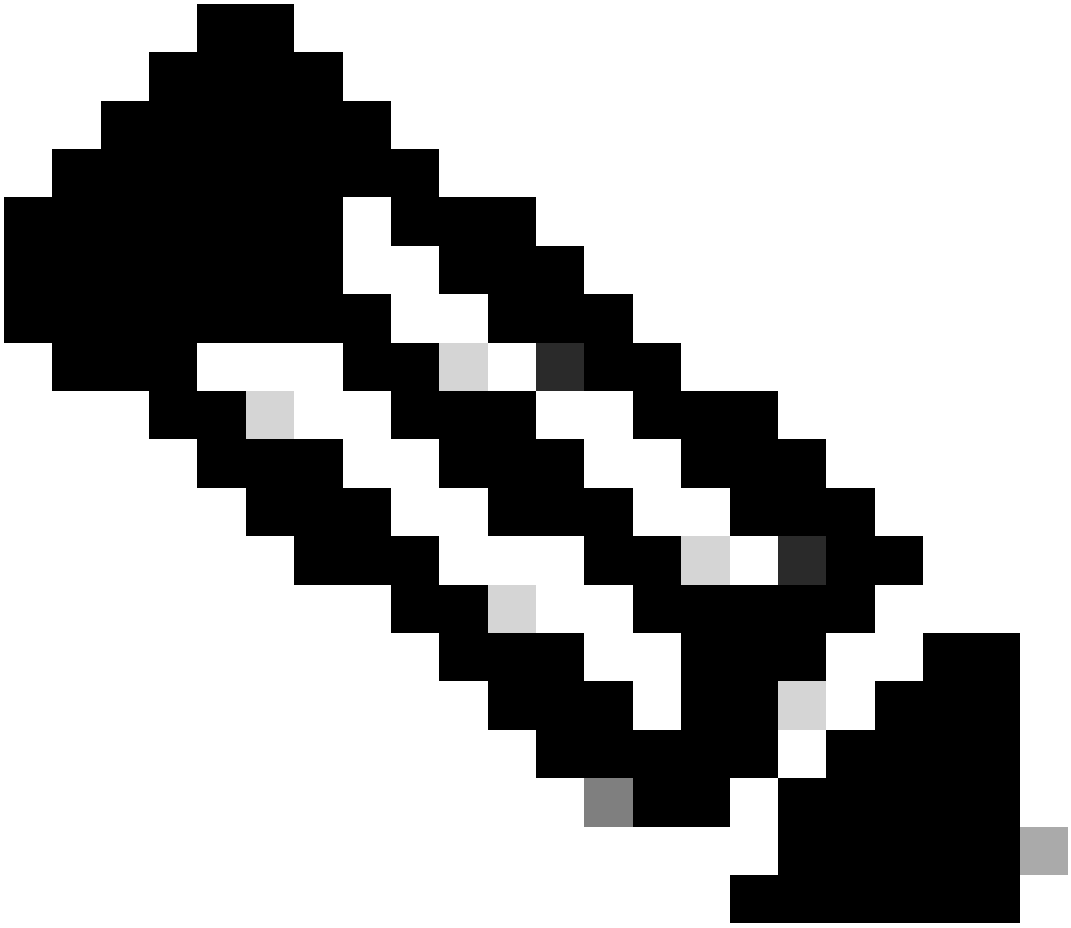
Em grandes redes públicas, muitas coisas podem estar acontecendo sem que o administrador saiba. As pessoas pedem cabos em lugares aleatórios ou ligam um switch doméstico em um local para ter mais portas para seus shenanigans, ... Normalmente eles tentam essas coisas sem antes pedir permissão. Isso significa que, mesmo sem um agente ruim entrar em cena, a segurança já pode ser comprometida por clientes e/ou funcionários que desejam bem-estar. Assim, fica muito fácil para um ator ruim simplesmente andar e encontrar um cabo para conectar e ver qual acesso à rede ele obtém a partir daí. Configurar a autenticação 802.1X em todas as portas de switch é quase um requisito para manter uma segurança decente em uma rede grande. O Catalyst Center pode ajudá-lo a automatizar essa implementação, e exceções podem ser feitas para dispositivos específicos que não suportam a autenticação 802.1X, mas tentam confiar o mínimo possível na autenticação baseada em MAC, já que isso não é (sinceramente) segurança real.

Pontos de acesso invasores

Sua estratégia para combater invasores depende de alguns fatores. Muitos administradores instintivamente optam por regras muito rígidas, mas as principais perguntas são:

- Quando você recebe centenas (se não milhares) de alertas falsos, você tem os recursos humanos para examiná-los e tomar medidas em relação a todos eles?
- Seu objetivo é remover fisicamente os invasores para manter um espectro de RF limpo? Nesse caso, você precisa de muitas pessoas para conduzir essa operação. Ou talvez seu objetivo seja apenas ficar de olho no fator de segurança e apenas garantir que os invasores não representem nenhum perigo? Isso tem um custo de trabalho humano muito mais gerenciável.
- Ativar a detecção de invasores pode ter um impacto no tempo de transmissão e a contenção de invasores normalmente tem um impacto ainda maior. Você analisou esse impacto e o levou em conta?

No que diz respeito ao impacto da detecção de invasor, os 9120 e 9130s têm um chip CleanAir dedicado que cuida da verificação fora do canal (e, portanto, da detecção de invasor), tornando o impacto no rádio de atendimento ao cliente quase nulo. Os APs da série 9160 com seu chip CleanAir Pro têm um recurso de verificação sem impacto semelhante, mas outros APs que não têm o chip CleanAir precisam tirar o rádio de atendimento ao cliente do canal para verificar se há invasores ou para fazer a contenção. O modelo de AP que você está usando, portanto, desempenha um papel na decisão de usar APs dedicados no modo de monitor para detecção e contenção de invasores ou não.

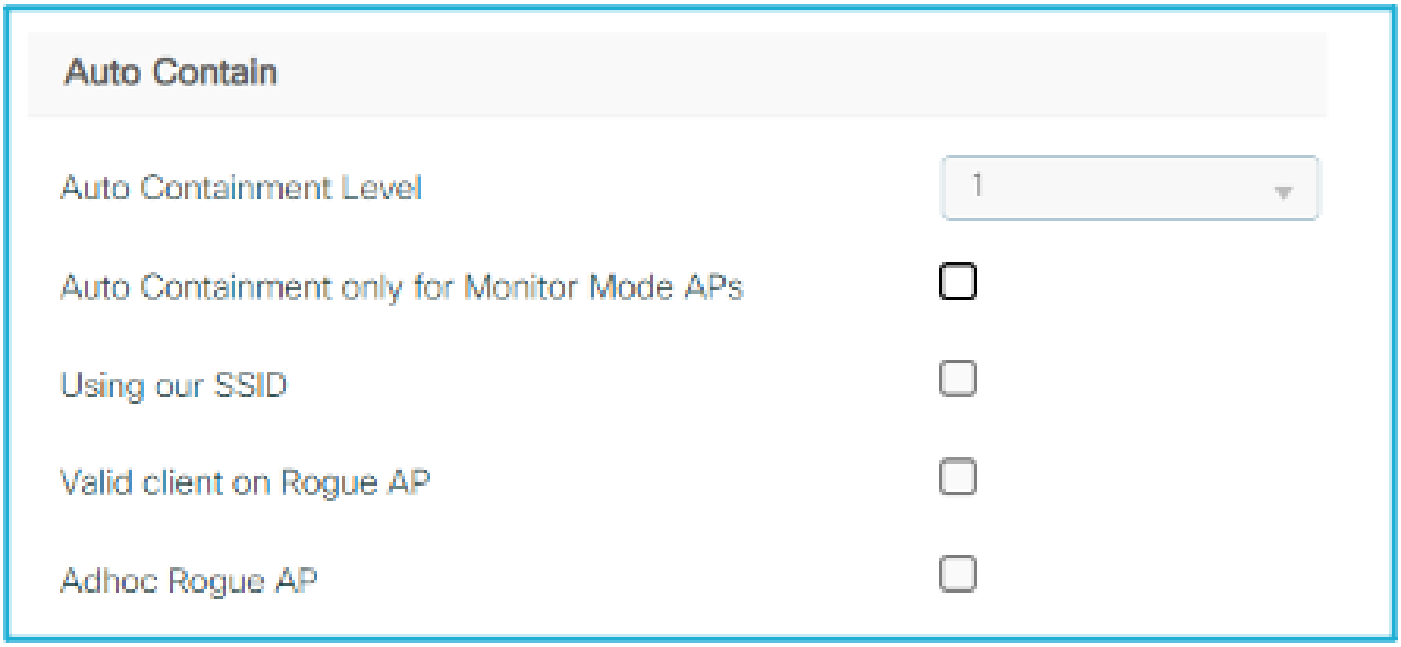


Observação: os telefones celulares que compartilham um hotspot Wi-Fi operam no modo de ‘infraestrutura’, assim como os APs tradicionais, o modo ‘ad-hoc’ se refere a uma conexão direta entre dispositivos móveis e é menos comum.

A contenção desonesta é geralmente proibida por regras regulatórias, por isso é essencial que você verifique com sua autoridade local antes de habilitá-la. Conter um invasor não significa desligar o invasor remotamente, mas enviar spam para os clientes que tentam se conectar ao ponto de acesso invasor com quadros de desautenticação para que eles não se conectem. Isso só pode funcionar no SSID de segurança herdado (não funciona no WPA3 ou quando o PMF está habilitado no WPA2) porque seus pontos de acesso não podem assinar corretamente os quadros de desautenticação. A contenção tem um impacto negativo no desempenho de RF no canal de destino, pois seus APs estão preenchendo o tempo de transmissão com quadros de desautenticação. Portanto, ela deve ser considerada apenas como uma medida de segurança para impedir que seus próprios clientes legítimos se associem a um access point invasor por engano. Por todos os motivos mencionados, é recomendável não fazer nenhuma contenção, pois isso não resolve completamente o problema do invasor e causa mais problemas de RF. Se você precisar usar contenção, só faz sentido ativá-la para invasores que falsificam um de seus SSID

gerenciados, já que é um ataque de "ponto de mel" óbvio.

Você pode configurar a contenção automática com a opção "usando nossos SSIDs":



Configurações de contenção automática

Você também pode configurar regras de invasor para classificá-las como pontos de acesso mal-intencionados de acordo com seus próprios critérios. Não se esqueça de digitar o nome de seus SSIDs vizinhos e aprovados como invasores amigáveis para removê-los de sua lista de alarmes.

Ative a autenticação de AP ou PMF para proteger seus APs contra representação.

Um invasor com fio é um ponto de acesso invasor conectado à sua rede com fio, o que, obviamente, é uma ameaça à segurança cada vez maior. A detecção de invasores com fio é mais complicada, pois o endereço MAC Ethernet de um invasor geralmente difere do endereço MAC de rádio. O Cisco Catalyst Center tem algoritmos que ainda tentam detectar se um invasor está conectado com fio e procura por MACs de clientes invasores que são ouvidos e vistos na infraestrutura com fio. A melhor solução para evitar invasores com fio é proteger todas as suas portas de switch com autenticação 802.1X.

Se você vai agir fisicamente em um ponto de acesso invasor, aproveitar o Cisco Spaces é a chave para ter uma localização precisa do invasor. Você provavelmente ainda precisa pesquisar uma vez no local, pois as pessoas tendem a ocultar APs invasores às vezes, mas reduzir a área de pesquisa para alguns metros torna isso uma tarefa muito viável. Sem Espaços, o invasor é mostrado no mapa ao lado do AP, detectando-o o mais alto, o que faz com que uma área de pesquisa muito grande. Existem muitas ferramentas e dispositivos sem fio que mostram o sinal do ponto de acesso invasor em tempo real para ajudá-lo a localizar o invasor fisicamente.

Não está exatamente relacionado a invasores, mas como o CleanAir acabou de ser coberto, é importante observar que a ativação do CleanAir não tem um impacto negativo perceptível nos desempenhos, exceto na detecção de beacon BLE, pois isso afeta o desempenho de 2,4 GHz. Você pode configurar sua rede sem fio para ignorar totalmente as interferência Bluetooth, pois

elas são onipresentes no mundo de hoje, e você não pode impedir que seus clientes ativem seu Bluetooth.

WiPS

O WiPS abrange vetores de ataque mais avançados do que apenas detectar a presença de um dispositivo invasor não autorizado. Além desses ataques, às vezes ele também fornece um PCAP do evento para análise forense.

Embora esse seja um recurso de segurança muito útil para a empresa, uma rede voltada para o público deve enfrentar a eterna pergunta: o que fazer contra isso?

Com a dificuldade de gerenciar muitos clientes que você não controla, é possível dividir os alarmes em duas categorias. Os alarmes que você pode decidir ignorar no Cisco Catalyst Center se vir muitos deles são:

- 10001 : DoS: Alarme de Inundação de Autenticação
- 10002: DoS: Alarme de Solicitação de Associação
- 10003: DoS: Alarme de inundação de sonda de difusão
- 10004: DoS: Alarme de Inundação de Desassociação
- 10005: DoS: Alarme de Desassociação de Broadcast
- 10006: DoS: Alarme de inundação de desautenticação
- 10007: DOS: Alarme de desautenticação de transmissão
- 10008: DOS: Alarme de ataque EAPOL-Logoff
- 10009: Alarme de inundação CTS
- 10010 : Alarme de Solicitação de Associação RTS
- 10011 : Inundação de Desautenticação por Par
- 10021: Airdrop Session (esta geralmente ocorre em qualquer rede e simplesmente descreve a atividade regular entre dispositivos Apple)
- 10022: Solicitação de Associação Malformada
- 10023: Inundação de Falhas de Autenticação por Assinatura
- 10024: MAC OUI inválido por assinatura
- 10025: Autenticação Malformada

Esses alarmes podem ser potencialmente causados por um cliente que se comporta mal. Não é possível impedir automaticamente um ataque de negação de serviço, pois, essencialmente, você não pode impedir que um cliente com defeito mantenha o tempo de transmissão ocupado. Mesmo que a infraestrutura ignore o cliente, ainda assim seria capaz de usar o meio e o tempo de transmissão, afetando, portanto, o desempenho dos clientes ao seu redor.

Os outros alarmes são tão específicos que muito provavelmente representam um ataque mal-intencionado real e dificilmente podem acontecer devido a drivers de clientes ruins. É melhor continuar monitorando estes alarmes:

- 10012: Sinal luminoso
- 10013: Solicitação de Sondagem Confundida
- 10014: Resposta de Sonda Confundida

- 10015: Inundação de Votação PS por Assinatura
- 10016: Inundação de V1 Inicial EAPOL por Assinatura
- 10017: Inundação de Solicitação de Reassociação por Destino
- 10018: Inundação de Beacons por Assinatura
- 10019: Inundação de Resposta de Sondagem por Destino
- 10020: Bloquear Inundação de Confirmações por Assinatura
- 10026/10027: Ataque de Detecção de Portadora Virtual RTS e CTS

Às vezes, a infraestrutura sem fio pode tomar medidas de mitigação, como bloquear a listagem do dispositivo ofensivo, mas a única ação real para se livrar de tal ataque é ir fisicamente até lá e remover o dispositivo ofensivo.

Recomenda-se ativar todas as formas de exclusão de clientes para economizar o tempo de transmissão desperdiçado ao interagir com clientes defeituosos.

Restringindo o acesso do cliente

É aconselhável ativar o bloqueio ponto-a-ponto em todas as suas WLANs (a menos que você tenha um requisito difícil para a comunicação cliente-cliente - mas isso precisa ser cuidadosamente considerado e possivelmente limitado). Este recurso impede que os clientes na mesma WLAN entrem em contato uns com os outros. Essa não é uma solução perfeita, pois clientes em WLANs diferentes ainda podem entrar em contato entre si e clientes pertencentes a WLCs diferentes no grupo de mobilidade também podem ignorar essa restrição. Mas ele funciona como uma primeira camada de segurança e otimização fácil e eficiente. Uma outra vantagem desse recurso de bloqueio ponto-a-ponto é que ele também impede o ARP cliente-cliente, que impede que os aplicativos descubram outros dispositivos na rede local. Sem o bloqueio ponto-a-ponto, a instalação de um aplicativo simples no cliente poderia mostrar todos os outros clientes conectados na sub-rede com possivelmente seus endereços IP e nomes de host.

Além disso, é recomendável aplicar uma ACL IPv4 e IPv6 (se você estiver usando IPv6 na rede) nas WLANs para impedir a comunicação cliente-cliente. A aplicação de uma ACL que bloqueia a comunicação cliente-cliente no nível da WLAN funciona independentemente de você ter SVIs cliente ou não.

A outra etapa obrigatória é impedir o acesso de clientes sem fio a qualquer forma de gerenciamento do controlador sem fio.

Exemplo:

```
ip access-list extended ACL_DENY_CLIENT_VLANS

 10 deny ip any 10.131.0.0 0.0.255.255

 20 deny ip 10.131.0.0 0.0.255.255 any

 30 deny ip any 10.132.0.0 0.0.255.255

 40 deny ip 10.132.0.0 0.0.255.255 any
```

```
 50 deny ip any 10.133.0.0 0.0.255.255

 60 deny ip 10.133.0.0 0.0.255.255 any

 70 deny ip any 10.134.0.0 0.0.255.255

 80 deny ip 10.134.0.0 0.0.255.255 any

 90 deny ip any 10.135.0.0 0.0.255.255

 100 deny ip 10.135.0.0 0.0.255.255 any

 110 deny ip any 10.136.0.0 0.0.255.255

 120 deny ip 10.136.0.0 0.0.255.255 any

 130 deny ip any 10.137.0.0 0.0.255.255

 140 deny ip 10.137.0.0 0.0.255.255 any

 150 permit ip any any
```

Essa ACL pode ser aplicada na interface de gerenciamento SVI:

```
interface Vlan130

 ip access-group ACL_DENY_CLIENT_VLANS in
```

Isso é feito em uma WLC com VLANs clientes de 131 a 137 criadas no banco de dados de VLAN da camada 2, mas sem nenhuma SVI correspondente, e existe apenas uma SVI para a VLAN 130, que é como a WLC é gerenciada. Essa ACL impede que todos os clientes sem fio enviem qualquer tráfego para os planos de gerenciamento e controle da WLC completamente. Não se esqueça de que o gerenciamento de SSH ou de IU da Web não é a única coisa que você precisa permitir, pois uma conexão CAPWAP para todos os APs também é necessária para ser permitida. É por isso que essa ACL tem uma permissão padrão, mas bloqueia os intervalos de cliente sem fio, em vez de confiar em uma ação deny all padrão, que exigiria a especificação de todos os intervalos de sub-rede de AP permitidos e intervalos de gerenciamento.

Da mesma forma, você pode criar outra ACL que especifique todas as sub-redes de gerenciamento possíveis:

```
ip access-list standard ACL_MGMT

 10 permit 10.128.0.0 0.0.255.255

 20 permit 10.127.0.0 0.0.255.255

 30 permit 10.100.0.0 0.0.255.255

 40 permit 10.121.0.0 0.0.255.255
```

```
 50 permit 10.141.0.0 0.0.255.255
```

Em seguida, você pode aplicar esta ACL para acesso CLI:

```
line vty 0 50
 access-class ACL_MGMT in
 exec-timeout 180 0
 ipv6 access-class ACL_IPV6_MGMT in
 logging synchronous
 length 0
 transport preferred none
 transport input ssh
 transport output ssh
```

A mesma ACL também pode ser aplicada para acesso de administrador da Web.

Proteção contra tempestades de tráfego

Multicasts e broadcasts são usados mais intensamente por alguns aplicativos do que por outros. Ao considerar uma rede somente com fio, a proteção contra tempestade de broadcast é geralmente a única precaução tomada. No entanto, um multicast é tão problemático quanto um broadcast quando enviado pelo ar e é importante entender o porquê. Primeiro, imagine um pacote enviado (via broadcast ou multicast) para todos os seus clientes sem fio, que rapidamente se soma a vários destinos. Cada AP precisa então transmitir esse quadro pelo ar da maneira mais confiável possível (embora não seja garantido como confiável) e isso é obtido usando uma taxa de dados obrigatória (às vezes a mais baixa, às vezes configurável). Em termos leigos, isso significa que o quadro é enviado usando uma taxa de dados OFDM (802.11a/g), o que claramente não é ótimo.

Em uma rede pública grande, não é aconselhável confiar em multicast para preservar o tempo de transmissão. No entanto, em uma rede corporativa de grande porte, você pode ter um requisito para manter o multicast habilitado para um aplicativo específico, embora seja necessário controlá-lo o máximo possível para limitar seu impacto. É uma boa ideia documentar os detalhes do aplicativo, o IP multicast e certificar-se de bloquear outras formas de multicast. Habilitar o encaminhamento Multicast não é um requisito para habilitar o IPv6, como explicado anteriormente. O encaminhamento de broadcast é melhor mantido completamente desabilitado. Os broadcasts são às vezes usados por aplicativos para descobrir outros dispositivos na mesma sub-rede, o que é claramente uma preocupação de segurança em uma rede grande.

Se você habilitar o encaminhamento multicast global, certifique-se de usar a configuração de CAPWAP AP AP multicast-multicast. Com isso habilitado, quando a WLC recebe um pacote multicast da infraestrutura com fio, ela o envia a todos os APs interessados com um único pacote multicast, economizando em muita duplicação de pacotes. Certifique-se de definir um IP multicast CAPWAP diferente para cada uma de suas WLCs, caso contrário os APs recebem tráfego multicast de outras WLCs, o que não é desejado.

Se os seus APs estiverem em outras sub-redes da sua interface de gerenciamento sem fio da WLC (provavelmente em uma rede grande), você deverá ativar o roteamento multicast na sua infraestrutura com fio. Você pode verificar se todos os seus APs estão recebendo corretamente o tráfego multicast com o comando:

```
show ap multicast mom
```

O multicast IGMP (para IPv4) e o multicast MLD (para IPv6) também são recomendados para serem habilitados em todos os casos se você precisar confiar no multicast. Eles permitem que somente os clientes sem fio interessados (e, portanto, somente APs que têm clientes interessados) recebam o tráfego multicast. A WLC faz o proxy do registro para o tráfego multicast e cuida de manter o registro ativo, descarregando assim os clientes.

Conclusão

As grandes redes públicas são complexas, cada uma delas é única, com requisitos e resultados específicos.

Respeitar as diretrizes neste documento é um ótimo ponto de partida e ajuda a obter sucesso com sua implantação, evitando os problemas mais comuns. No entanto, as diretrizes são apenas diretrizes e podem precisar ser interpretadas ou ajustadas no contexto do local específico.

O Cisco CX tem equipes de profissionais sem fio dedicadas a grandes implantações sem fio, com experiência em vários eventos grandes, incluindo eventos esportivos e conferências. Entre em contato com a equipe da sua conta para obter assistência adicional.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.