Paulo César Bento Farias

Treinamento Profissional em

Redes Wireless

Diretor Editorial
Luis Matos

Assistência Editorial
Monalisa Neves
Erika Sá

Preparação dos originais
Luciana Salgado G. Moreira

Revisão
Sirlene Farias

Projeto Gráfico
Daniele Fátima

Diagramação
Rogério Chagas

Capa
Laboratório do Livro

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

F224 t Farias, Paulo César Bento.

Treinamento Profissional em Redes Wireless / Paulo César Bento Farias. –– São Paulo : Digerati Books, 2006.
128 p.

ISBN 85-60480-06-4

1. Sistemas de comunicação sem fio. 2. Redes de computadores. 3. Wireless. I. Paulo César Bento Farias. II Título.

CDD 621.382

Universo dos Livros Editora Ltda.
Rua Tito, 1.609
CEP 05051-001 • São Paulo/SP
www.universodoslivros.com.br
e-mail: editor@universodoslivros.com.br

Conselho Administrativo: Alessandro Gerardi, Alessio Fon Melozo, Luis Afonso G. Neira, Luis Matos e William Nakamura.

Sumário

Capítulo 1

Introdução

As redes sem fio ou wireless (WLANs) surgiram da mesma forma que muitas outras tecnologias; no meio militar. Havia a necessidade de implementação de um método simples e seguro para troca de informações em ambiente de combate. O tempo passou e a tecnologia evoluiu, deixando de ser restrita ao meio militar e se tornando acessível a empresas, faculdades e ao usuário doméstico. Nos dias de hoje, podemos pensar em redes wireless como uma alternativa bastante interessante em relação às redes cabeadas, embora ainda com custo elevado. Suas aplicações são muitas e variadas e o fato de ter a mobilidade como principal característica tem facilitado sua aceitação, principalmente nas empresas.

A evolução dos padrões, oferecendo taxas de transmissão comparáveis à Fast Ethernet, por exemplo, torna as redes wireless uma realidade cada vez mais presente.

WLANs usam ondas de rádio para transmissão de dados. Comumente podem transmitir na faixa de freqüência 2.4 GHz (não licenciada) ou 5 GHz.

Padrões

Como WLANs usam o mesmo método de transmissão das ondas de rádio AM/FM, as leis que as regem são as mesmas destes. O FCC (Federal Comunications Comission) regula o uso dos dispositivos WLAN. O IEEE (Institute of Eletrical and Eletronic Engineers) é responsável pela criação e adoção dos padrões operacionais. Citamos os mais conhecidos:

IEEE 802.11	• Criado em 1994, foi o padrão original. • Oferecia taxas de transmissão de 2 Mbps. • Caiu em desuso com o surgimento de novos padrões.
IEEE 802.11b	• Taxas de transmissão de 11 Mbps. • Largamente utilizada hoje em dia. • Opera em 2.4 GHz. • Alcance de até 100 m indoor e 300 m outdoor. • Mais voltado para aplicações indoor. • Tende a cair em desuso com a popularização do 802.11 g.

IEEE 802.11a	• Taxas de transmissão de 54 Mbps. • Alcance menor do que a 802.11b. • Opera em 5 GHz. • Alcance de até 60 m indoor e 100 m outdoor. • Mais voltado para aplicações indoor. • Seu maior problema é a não compatibilidade com dispositivos do padrão b, o que prejudicou, e muito, sua aceitação no mercado.
IEEE 802.11g	• Taxas de transmissão de 54 Mbps, podendo chegar, em alguns casos, a 108 Mbps. • Opera em 2.4 GHz. • Mais voltado para aplicações indoor. • Reúne o melhor dos mundos a e b. (alcance x taxa).
IEEE 802.16a	• Criado em 2003. • Popularmente conhecido como Wi-Max. • Voltado exclusivamente para aplicações outdoor. • Alcance de até 50 km. • Taxas de transmissão de até 280 Mbps.

Tabela 1.1.

Técnicas de Transmissão

WLANs usam uma técnica de transmissão conhecida como difusão de espectro (Spread Spectrum). Essa técnica se caracteriza por largura ampla de banda e baixa potência de sinal. São sinais difíceis de detectar e mesmo interceptar sem o equipamento adequado. Existem dois tipos de tecnologia de Spread Spectrum regulamentadas pelo FCC: Direct Sequence Spread Spectrum (DSSS) e Frequency Hopping Spread Spectrum (FHSS).

DSSS	• Menos resistente à interferência. • Compatibilidade com equipamentos de padrões anteriores. • Taxa de transmissão de 11 Mbps. • Menor segurança. • Possui 11 canais, mas destes somente três são não-interferentes e efetivamente usados para transmissão (canais 1, 6 e 11).
FHSS	• Mais resistente à interferência. • Não possui compatibilidade com equipamentos de padrões anteriores. • Taxa de transmissão de 2 Mbps. • Maior segurança. • 79 canais disponíveis para transmissão.

Tabela 1.2.

Observação: no mundo das WLANs, o DSSS é a tecnologia utilizada.

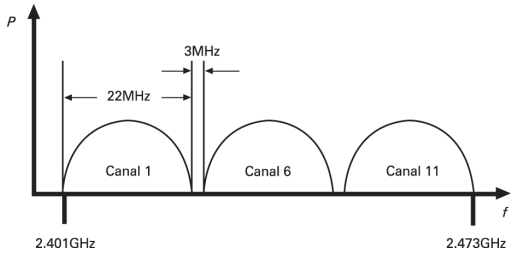

Figura 1.1: Canais não-interferentes no DSSS.

Elementos de Hardware

Na tabela a seguir, descrevemos os componentes de uma WLAN:

PC Card	• Usado somente em notebooks. • Serve para conectar o notebook à rede wireless. • Possui antena interna embutida.
Placas PCI	• Usadas somente em desktops. • Servem para conectar o desktop à rede wireless. • Possuem antena externa acoplada à saída da placa.
Adaptadores USB	• Podem ser usados em notebooks ou desktops. • Servem para conectar o notebook ou desktop à rede wireless. • Possuem antena interna embutida.

Pontos de Acesso	• Concentram todo o tráfego da rede wireless, além das conexões oriundas dos clientes. • Possuem um identificador para rede chamado SSID. • Funcionam como interface entre a rede wireless e a rede cabeada por possuír porta UTP 10 ou 100 Mbps. • Possuem antena interna embutida. • Suportam a conexão de antenas externas, na maioria dos casos.
Pontes Wireless Workgroup	• Agrupam vários clientes LAN e transformam essa LAN em único cliente WLAN. • Recomendadas em situações em que um pequeno grupo de usuários necessita de acesso à rede principal. • O número máximo de estações que podem ser conectadas está compreendido entre 8 e 128, dependendo do fabricante.
Pontes Wireless	• Conectam duas ou mais redes. • Compreendem quatro modos de operação: Root, Non-Root, Access Point e Repeater. • Possuem a capacidade de formação de backbone wireless através de dois PC Cards.
Gateways	• Conectam um pequeno número de dispositivos wireless à Internet ou outra rede. • Possuem uma porta WAN e várias portas LAN. Geralmente têm um hub ou switch embutido e possuem as funcionalidades de um Ponto de Acesso.
Antenas	• Podem ser conectadas a pontos de acesso ou a máquinas clientes para aumentar o ganho do sinal e assim melhorar a transmissão de dados. • Podem ser direcionais ou omni-direcionais.

Tabela 1.3.

Tipos de WLAN

Uma WLAN pode ser utilizada tanto na forma indoor como na forma outdoor.

Indoor

Dizemos que uma WLAN é indoor quando o sinal é transmitido em ambiente fechado, normalmente na presença de muitos obstáculos; um escritório é um bom exemplo.

Não há necessidade de visada direta entre as antenas para que haja comunicação. Possui um alcance pequeno, em torno de até 300 m. Podem ter a presença de um Ponto de Acesso ou não.

ADHOC	• Não existem Pontos de Acesso (AP). • Comunicação feita cliente – cliente. • Não existe canalização do tráfego. • Performance diminui à medida que novos clientes são acrescentados. • Suporta no máximo cinco clientes para uma performance aceitável com tráfego leve.
Infra-estrutura	• Necessidade de um Ponto de Acesso (AP). • Comunicação cliente – cliente não é permitida. Toda a comunicação é feita com o AP. • Centralização do tráfego. Todo o tráfego da rede passa pelo AP. • Compreende dois modos de operação: BSS (Basic Service Set), ESS (Extended Service Set).

Tabela 1.4.

• BSS: consiste de um Ponto de Acesso ligado à rede cabeada e um ou mais clientes wireless. Quando um cliente quer se comunicar com outro ou com algum dispositivo na rede cabeada deve usar o Ponto de Acesso para isso. O BSS compreende uma simples célula ou área de RF e tem somente um identificador (SSID). Para que um cliente possa fazer parte da célula ele deve estar configurado para usar o SSID do Ponto de Acesso.

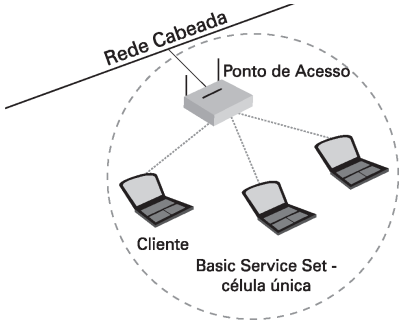

Figura 1.2: Sistema BSS.

• ESSS: são dois sistemas BSS conectados por um sistema de distribuição, seja ele LAN, WAN, Wireless ou qualquer outro. Necessita, portanto, de dois Pontos de Acesso. Permite roaming entre as células. Não necessita do mesmo SSID em ambos os BSS.

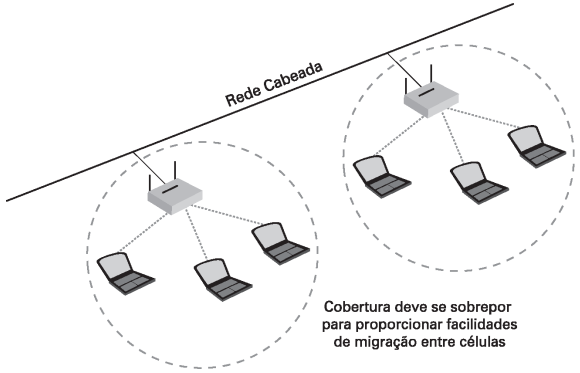

Figura 1.3: Sistema ESS.

Outdoor

Dizemos que uma WLAN é outdoor quando o sinal é transmitido ao ar livre; uma comunicação entre dois prédios é um bom exemplo. As antenas ficam nos topos dos prédios e, para que haja comunicação, é necessário haver visada direta entre elas. Possui longo alcance, que pode chegar a vários quilômetros.

Capítulo 2

Aplicações

Hoje em dia, a utilização das WLANs deixou de estar restrita a grandes empresas ou faculdades. Com os preços dos equipamentos mais acessíveis, elas atraíram a atenção do usuário comum devido à ampla gama de possibilidades de utilização. Vejamos as mais comuns.

Expansão da Rede Cabeada

Pode haver casos em que a expansão de uma rede seja inviável devido ao custo proibitivo da estrutura necessária para o cabeamento adicional (cabos, contratação de instaladores e eletricistas), ou casos em que a distância pode ser muito grande (acima de 100 m) para se usar cabos CAT5, como em uma loja de departamentos, por exemplo. Em tais casos, as WLANs certamente serão uma alternativa de baixo custo e de fácil implementação.

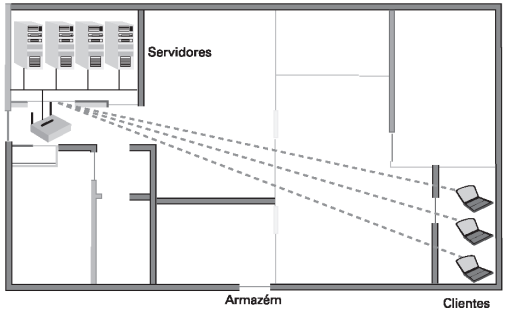

Figura 2.1.

Conexão entre Prédios

É muito comum uma empresa ter escritórios em prédios diferentes que necessitam estar conectados à mesma infra-estrutura de rede. O que era comum para atingir esse objetivo era alugar linhas privadas de uma companhia de telefonia ou utilizar passagens subterrâneas para a infra-estrutura de cabos. Esses métodos eram dispendiosos e demorados para implementar. WLANs surgem como uma alternativa de rápida implementação e de baixo custo comparadas aos métodos tradicionais. A comunicação entre os prédios se torna possível graças às antenas e aos equipamentos wireless de cada um deles.

A comunicação pode ser realizada, basicamente, de duas formas no que se refere à conectividade prédio a prédio:

• PTP: Ponto a Ponto. São conexões wireless entre dois prédios que usam antenas direcionais de alto ganho em cada um deles.

Figura 2.2: Comunicação ponto a ponto.

• PTMP: Ponto-Multiponto. São conexões wireless entre três ou mais prédios, sendo que um atua como central. No prédio central, usa-se uma antena omni-direcional e, nos outros, antenas direcionais.

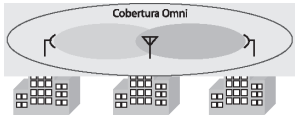

Figura 2.3: Comunicação ponto-multiponto.

Observação: em ambos os tipos de comunicação é fundamental haver visada direta entre as antenas.

Serviços de Última Milha

Esse tipo de serviço é largamente utilizado por provedores de Internet para levar o acesso a uma localidade remota que não dispõe dos meios tradicionais em banda larga (xDSL e cable modem).

A grande vantagem é que os custos de instalação são bem menores se comparados aos métodos tradicionais, mas sempre deve ser levada em conta a situação e a relação custo x benefício. Da mesma forma que provedores xDSL têm problemas com distâncias grandes a partir do escritório central, e provedores de cabos têm problemas com o meio compartilhado pelos usuários, provedores wireless têm problemas com telhados, árvores, montanhas, torres e muitos outros obstáculos.

Embora provedores wireless não tenham uma solução à prova de falhas, eles podem levar seus serviços até onde os outros, de tecnologias tradicionais, não conseguem.

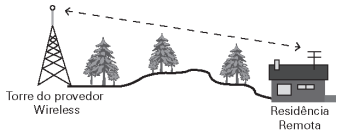

Figura 2.4: Serviço de última milha.

Mobilidade

Uma das principais características da tecnologia wireless é a mobilidade que, por sua vez, pode acarretar um aumento real de produtividade em determinados casos, como em uma loja de departamentos.

Em uma loja de departamentos, os funcionários responsáveis por catalogar os produtos podem estar munidos de scanners de mão wireless e estes, por sua vez, estarem conectados a um computador central por meio de uma rede wireless. Existe uma economia de tempo brutal nesse caso e um conseqüente aumento de produtividade por não haver necessidade da entrada de dados manual através de um terminal ligado ao computador central por meio de cabos. Os dados são transferidos automaticamente.

Escritórios Móveis

Imagine que você tem uma empresa de treinamento e gostaria de divulgar seus serviços ao público em geral. Sua empresa possui um trailer e seu desejo é usá-lo como uma sala de aula móvel com acesso à Internet e também divulgar serviços oferecidos pela sua empresa. Uma boa maneira de viabilizar isso seria com a tecnologia wireless. Para tal, é necessária uma antena omni-direcional posicionada no topo do prédio de sua empresa e outra direcional de alto ganho colocada no alto do veículo, além dos computadores e mais alguns equipamentos. Lembrando que a sua mobilidade estará restrita à área de cobertura da antena omni-direcional.

Hotspots

São pontos de acesso wireless que permitem ao usuário conectar-se à Internet em locais públicos como aeroportos, shoppings, hotéis, cafeterias e outros.

Bastam um laptop com um PCCard e uma conta de acesso do provedor do serviço para navegar na Internet nesses locais, sem esquecer que o usuário é cobrado pelo uso do serviço.

Uso doméstico

Na sua casa você pode ter mais de um computador que necessite de acesso à Internet. Normalmente, você precisaria levar cabos para esses computadores adicionais a partir do hub em que também está conectado o computador que acessa a Internet.

Com a tecnologia wireless, a passagem de cabos se torna desnecessária (o que muitas vezes pode resultar em significativa economia de tempo) e, se você tiver um notebook, ganha mobilidade. Imagine poder acessar a Internet do seu notebook em qualquer cômodo da casa? Ou ainda, no caso do computador, mudá-lo do quarto para a sala, se houver necessidade, sem se preocupar em passar cabos?

No que se refere ao custo, instalar uma rede wireless ainda é bem mais caro que uma rede cabeada, mas os benefícios compensam. A tabela seguinte ilustra a diferença de custo (preços médios) para dois computadores (um notebook e um desktop), distantes 15 m do hub ou switch. O notebook e o desktop já possuem placa de rede.

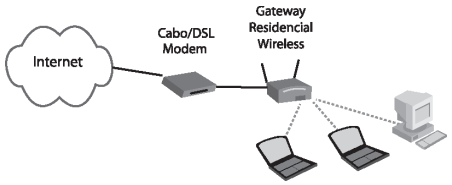

Figura 2.5: Rede doméstica wireless com acesso à Internet.

Usando cabos	
Item	**Preço**
30 m de Cabo UTP CAT 5	R$ 24,00
Canaletas	R$ 20,00
Quatro Conectores RJ45 machos	R$ 2,80
Switch 5 portas	R$ 90,00
TOTAL	**R$ 136,80**

Tabela 2.1.

Usando Wireless 802.11g	
Item	**Preço**
PC Card 802.11g para o notebook	R$ 153,00
Placa PCI Wireless 802.11g para o desktop	R$ 156,00
Residencial Gateway	R$ 350,00
TOTAL	**R$ 659,00**

Tabela 2.2.

Capítulo 3

Fundamentos de RF

Toda a transmissão e recepção de sinais no mundo wireless se baseia em radiofreqüência (RF). O comportamento da RF pode afetar a performance de uma WLAN. Logo, um bom entendimento dos conceitos de RF será de grande utilidade na implantação, expansão, manutenção e troubleshooting de redes wireless.

Introdução

Sinais de RF são sinais de alta freqüência que se propagam por um condutor de cobre e são irradiados no ar através de uma antena. Na prática, uma antena converte um sinal cabeado em um sinal wireless e vice-versa. Esses sinais são, então, irradiados ao ar livre na forma de ondas de rádio, que se propagam em linha reta e em todas as direções.

Você pode imaginar essas ondas como círculos concêntricos que vão aumentando seu raio à medida que se afastam da antena. Mas não é preciso ter uma antena para visualizar o formato dessas ondas. Basta pegar uma pedra e atirar em um lago, por exemplo, que o efeito é o mesmo.

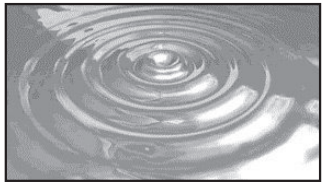

Figura 3.1: Ondas de RF.

Ganho de Potência

Todo sinal elétrico que se propaga em um meio, independentemente de qual seja esse meio, sofre uma perda na sua amplitude, ou seja, perde potência. Porém, essa perda de potência pode ser compensada com uso de equipamentos, tais como amplificadores de RF que amplificam o sinal. Veja a **Figura 3.2**:

Figura 3.2: Sinal de RF visto por um osciloscópio.

Observe que o sinal original está representado pelo traço pontilhado, e o sinal amplificado, pelo traço cheio.

O uso de fontes de potência externas para amplificar o sinal é um processo ativo.

Ganho de potência também pode ser obtido por processos passivos, tais como reflexão do sinal. Quando o sinal se propaga em um meio, pode haver sua reflexão, e essa reflexão pode ser entendida como um desdobramento do sinal original, em sinais de menor amplitude que se somam ao sinal original aumentando seu ganho. Porém essas reflexões nem sempre se somam ao sinal original. Não há como ter controle sobre esse processo.

Perdas

Conforme dito, todo sinal que se propaga em um meio sofre uma perda na sua amplitude à medida que o percorre, seja este meio um cabo ou o ar livre. Portanto, quanto maior a distância percorrida pelo sinal, menor a amplitude, a potência. Normalmente essa redução na amplitude é causada pelas resistências de cabos e conectores. O não casamento de impedâncias entre cabos e conectores pode fazer com que parte da potência do sinal seja refletida de volta para a fonte, causando, assim, degradação do sinal. Objetos que estejam no meio do caminho de um sinal de RF podem refletir ou absorver esse sinal, tudo vai depender do material de que é composto esse objeto.

Calcular a perda de RF entre um transmissor (antena) e um receptor (rádio) é muito importante. Todo rádio tem uma sensibilidade de recepção, através da qual se distingue um sinal de um ruído. Logo, é preciso garantir que o sinal chegue ao receptor em um nível de potência que esteja dentro desse parâmetro (sensibilidade) para que ele possa ser reconhecido e haja comunicação. Uma forma de compensar essa perda é utilizar amplificação no transmissor ou direcionar o sinal de forma que não passe pelos objetos que estão causando a perda.

Reflexão

Refexão ocorre quando um sinal de RF incide sobre um objeto que tem dimensões muito largas quando comparado ao comprimento de onda do sinal. Prédios, paredes e muitos outros obstáculos podem causar reflexões. Dependendo da superfície do obstáculo, o sinal refletido pode permanecer intacto ou sofrer perda devido à absorção de parte do sinal.

Reflexões podem causar muitos problemas em WLANs, tais como degradação ou cancelamento do sinal original ou buracos em uma área de cobertura. À reflexão do sinal original em uma área de transmissão damos o nome de multipath.

Reflexões dessa magnitude nunca são desejáveis e requerem um mecanismo especial para compensá-las.

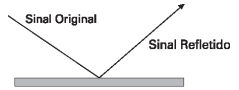

Figura 3.3: Reflexão de sinal.

Refração

Refração é o desvio que uma onda de rádio sofre ao passar através de um meio de densidade diferente, conforme ilustrado na **Figura 3.4**. Na realidade, quando uma onda de rádio atravessa um meio de densidade diferente, parte da onda é refletida e parte sofre um desvio em outra direção.

Refração pode se tornar um problema para links RF de longa distância. Como as condições atmosféricas estão sujeitas a variações, refração pode fazer com que o sinal sofra um desvio acentuado, de forma que não chegue ao receptor.

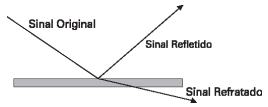

Figura 3.4: Reflexão e refração.

Difração

A difração ocorre quando o caminho entre o transmissor e o receptor é obstruído por uma superfície com bordas de tamanhos irregulares. Nesse caso, parte do sinal sofre um desvio de direção passando a circundar a superfície, como mostra a **Figura 3.5**.

Parte do sinal que circunda a superfície sofre um retardo na velocidade de propagação, enquanto a outra parte mantém a velocidade de propagação original.

Dependendo do tamanho do objeto, o sinal pode até ser inteiramente bloqueado.

Difração é comumente confundida com refração. Mas a principal diferença é que difração ocorre quando um sinal incide sobre um objeto, e a reflexão ocorre quando um sinal atravessa um meio.

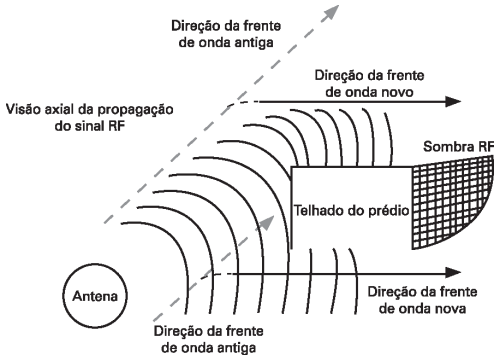

Figura 3.5: Como ocorre a difração.

Espalhamento

O espalhamento ocorre quando o sinal atravessa um meio que consiste de objetos com dimensões pequenas se comparadas ao comprimento de onda do sinal, e o número de obstáculos por unidade de volume é grande. Telhados, pequenos objetos e outras pequenas irregularidades no caminho do sinal podem causar seu espalhamento.

O espalhamento pode provocar sérios prejuízos em uma área de transmissão. Dependendo da superfície atingida, o sinal é refletido em muitas direções simultaneamente, com amplitudes menores interferindo significativamente no sinal original, podendo causar degradação substancial ou mesmo perda completa do sinal.

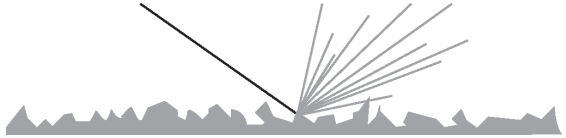

Figura 3.6: Espalhamento de sinal.

Capítulo 4

VSWF

VSWR (Voltage Standing Wave Radio) pode ser definido como um indicador da quantidade de sinal refletida de volta ao transmissor em um circuito RF. Para que toda potência transmitida chegue à antena, a impedância de cabos e conectores deve ser a mesma (casamento de impedância), do contrário teremos parte do sinal transmitido sendo refletido na linha, no ponto onde não há esse casamento.

Essa parte do sinal que é refletida contribui para a variação no nível do sinal que está sendo transmitido.

VSWR é expresso como uma relação entre dois números. Esses dois números confrontam uma situação de não casamento de impedância e uma outra situação, em que há o casamento de impedância perfeito. Um valor típico de VWSR é 1.5:1. O segundo número é sempre 1. Quanto menor o valor do primeiro número (mais próximo de 1), melhor o casamento de impedância do seu sistema, e, conseqüentemente, menos sinal refletido na linha. Logo, um circuito RF com VSWR de 1.4:1 é melhor do que outro com 1.5:1. Um VSWR com 1.1:1 significa casamento de impedância perfeito e a garantia de que não há sinal refletido de volta para o transmissor.

Um VSWR excessivo poderia causar sérios problemas em um circuito RF, além dos já citados. Pode haver, inclusive, queima de componentes eletrônicos, porque os dispositivos não têm nenhuma proteção contra esse sinal refletido que volta para o transmissor. Algumas medidas podem ser tomadas para evitar os efeitos negativos da VSWR:

- O uso de dispositivos de alta qualidade;
- Conexões bem apertadas entre cabos e conectores;
- Cabos, conectores e todos os dispositivos do transmissor, até a antena devem possuir impedâncias próximas uma das outras quanto possível, ou seja, nunca usar cabos de 75 Ohms com dispositivos de 50 Ohms.

O VSWR em um circuito RF pode ser medido com instrumentação adequada.

Antenas

Antenas são um dos principais elementos presentes em um circuito RF. É por meio delas que os sinais de RF são transmitidos e recebidos. Existem dois pontos fundamentais que precisamos saber sobre antenas.

- Convertem sinais elétricos em sinais de RF e vice-versa;
- As dimensões físicas de uma antena estão diretamente relacionadas à freqüência na qual a antena pode propagar e receber ondas de RF.

As antenas podem ser classificadas em omni-direcionais e direcionais. As omni-direcionais irradiam em todas as direções enquanto as direcionais, apenas em uma determinada direção.

Visada Direta

Para que haja comunicação entre transmissor e receptor em um circuito RF, é preciso haver visada direta entre as antenas dos dois lados. Por esse motivo, elas devem estar posicionadas nos lugares mais altos (normalmente no topo dos prédios) e livres de obstáculos, para que não ocorram os já citados fatores de reflexão, difração e espalhamento. Podemos fazer uma analogia com um tubo e duas pessoas, uma em cada extremidade, com lanternas. Uma pessoa pode ver perfeitamente a luz da lanterna da outra se não houver nenhum obstáculo entre elas. Porém, dependendo do tamanho do obstáculo, a quantidade de luz que pode ser vista em cada extremidade é prejudicada ou pode até ser bloqueada inteiramente. Traduzindo para o caso de ondas RF, o link poderia ser seriamente afetado ou mesmo interrompido.

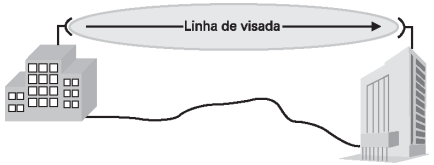

Figura 4.1: Visada direta entre duas antenas.

Zona de Fresnel

A Zona de Fresnel é um aspecto de suma importância no planejamento e troubleshooting de um link RF.

Pode ser definida como uma série de elipses concêntricas em torno da linha de visada. Ela é importante para a integridade do link porque determina uma área em torno da linha de visada, que pode introduzir interferência no sinal caso ele seja bloqueado.

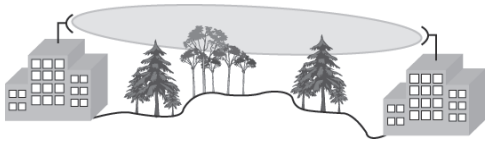

Figura 4.2: Zona de Fresnel.

Objetos na Zona de Fresnel, tais como árvores, prédios entre outros, podem produzir reflexão, difração, absorção ou espalhamento do sinal, causando degradação ou perda completa do sinal.

O raio da Zona de Fresnel mais distante pode ser calculado pela seguinte fórmula:

$$r = 43.3x\sqrt{\frac{d}{4f}}$$

Onde d é a distância do link em milhas, f é a freqüência em GHz e r é expresso em pés.

Assim, para um link de duas milhas na freqüência de 2.4GHz, teríamos:

r = 39.52 pés

e passando para quilômetros:

r = 1204.57 metros (1.2 km)

Levando em conta a importância de uma Zona de Fresnel desobstruída, é importante quantificar até que grau a Zona de Fresnel pode ser bloqueada sem que haja perda completa do sinal. Normalmente, um bloqueio em torno de 20% introduz pouca ou nenhuma interferência no link.

Se a Zona de Fresnel do link proposto for bloqueada em mais de 20%, elevar as antenas aliviará o problema.

Ganho

Um elemento de antena, sem amplificadores e filtros associados a ela, é um dispositivo passivo. Não há nenhuma manipulação ou am-

plificação do sinal pelo elemento de antena. Uma antena pode criar um efeito de amplificação focando a radiação em um lóbulo estreito, da mesma forma de uma lanterna que emite luz a uma grande distância. O foco da radiação é medido pelos lóbulos em grau horizontal e vertical. Por exemplo, uma antena omni-direcional tem um lóbulo de 360 graus. Se estreitarmos esse lóbulo para algo em torno de 30 graus, podemos levar essa mesma radiação a uma distância maior. As **Figuras 4.3** e **4.4** ilustram bem esse efeito; observe que há um achatamento dos lóbulos. O ganho é expresso em dB (decibéis). Quanto maior for o ganho da antena, mais estreito será seu lóbulo principal.

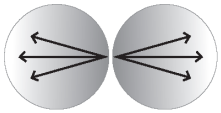

Figura 4.3: Lóbulos de um elemento de antena, sem ganho.

Figura 4.4: Lóbulos de uma antena com ganho.

Gerador de RF

Conforme definido pelo FCC, um gerador é um dispositivo de RF especificamente projetado para gerar sinais RF. Em termos de hardware, o gerador de RF incluiria o dispositivo RF e todos os conectores e cabeamento envolvidos, com exceção da antena, conforme mostrado na **Figura 4.5**.

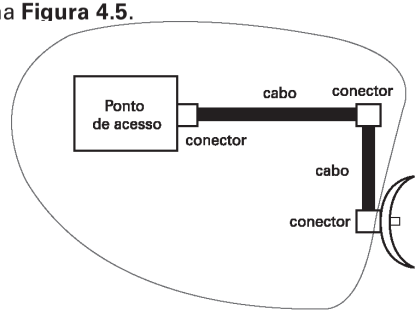

Figura 4.5: Gerador de RF.

EIRP

EIRP (Equivalent Isotropic Irradiated Power) é a potência atualmente irradiada pelo elemento de antena.

Este conceito é importante porque é regulado pelo FCC e porque é usado no cálculo para avaliar a viabilidade de um link wireless. O ganho da antena também é levado em conta.

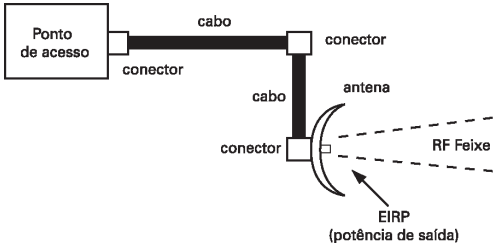

Figura 4.6: Ilustrando o EIRP.

Se uma estação de transmissão usar uma antena de 10 dBi, amplifica o sinal de entrada em dez vezes, e se tivermos um sinal de 100 mW na entrada, o EIRP será de 1.000 mW ou 1 watt.

Capítulo 5

Cálculos de potência

Depois de conhecermos vários conceitos de RF e sua importância em uma WLAN, torna-se necessário avaliar através de cálculos a viabilidade de um link wireless, sem infringir as regras do FCC no que se refere a limitações de potência. São quatro os aspectos importantes no cálculo de potência:

- Potência do dispositivo de transmissão;
- Perda e ganho entre o dispositivo de transmissão e a antena causados por conectores, cabos, amplificadores e atenuadores;
- Potência no último conector, antes do sinal RF entrar na antena;
- Potência no elemento de antena (EIRP).

Unidades de Medida

Watt (W)

Unidade básica de potência. É definido como 1 ampére (A) de corrente em 1 volt (V), logo: potência = volt x ampere (P=VA). O FCC permite no máximo 4 watts de potência a ser radiado de uma antena em uma WLAN ponto multiponto sobre a freqüência de 2.4 GHz. Pode não parecer muita potência, mas é o suficiente para enviar sinais RF claros por quilômetros.

Miliwatt (mW)

Em WLANs, níveis de potência são comumente expressos em miliwatts (mW), ou seja (1/1.000 W). Em um segmento WLAN típico indoor, os níveis de potência raramente ultrapassam 100 mW, o que é suficiente para se comunicar na faixa de 500 m ou mais em condições ótimas. Os pontos de acesso normalmente irradiam o sinal entre 30-100 mW, dependendo do fabricante.

Decibéis (dB)

Usado para expressar sinais da ordem de 0.000000001 watts. Normalmente, um receptor muito sensível a sinais RF deve ser capaz de captar sinais dessa ordem. O decibel é usado como uma forma mais inteligível de expressar esses sinais.

Decibéis estão relacionados a watts por uma expressão logarítmica com base dez. Assim, se nós temos 1.000 e queremos encontrar o log, teríamos como resposta três, porque $1.000 = 10^3$. Observe que, na realidade, o logaritmo nada mais é que o expoente.

Observação: tanto dB como mW são padrões utilizados pela indústria para medidas de potência.

Unidades de Medida para Perda e Ganho

Perda e ganho de potência em um circuito são medidos em decibéis e não em watts. Isso se explica pelo fato de que perda e ganho são conceitos relativos e decibel é uma medida relativa. Perder metade da potência em um sistema corresponde à perda de três decibéis. Se um sistema perde metade da sua potência (-3 dB) e logo após perde a metade novamente, isso equivale à perda de ¾ da potência original. (½ da primeira mais ½ da segunda). Como referência rápida, existem números relacionados a ganho e perda com os quais nos devemos familiarizar:

- -3 dB = Metade da potência em mW;
- +3 dB = Dobro da potência em mW;
- -10 dB = Um décimo da potência em mW;
- +10 dB = Dez vezes a potência em mW.

Esses valores facilitam o cálculo da perda e ganho em um circuito RF sem o uso de uma calculadora. Para os casos em que esse método não é utilizável, há fórmulas de conversão:

- Convertendo mW para dBm:

$$P_{dbm} = 10\log_{PmW}$$

- Convertendo dBm para mW:

$$Pmw = \log^{-1}\left(\frac{P_{dbm}}{10}\right)$$

Observe que log $^{-1}$ é, na verdade, o logaritmo inverso.

dBm

O ponto de referência que relaciona a escala logarítmica dB com a escala linear watts é:

1 mW = 0 dBm

O m em dBm nada mais é que uma referência em relação a um mW e, logo, uma medida em dBm é uma medida de potência absoluta.

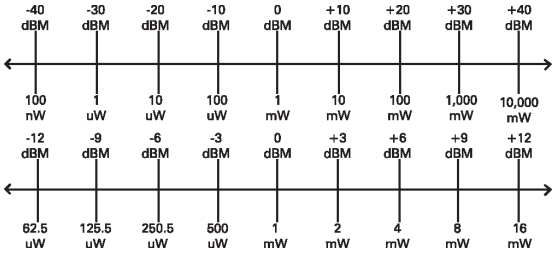

Figura 5.1: Diagrama de nível de potência.

Observe no diagrama anterior que o ponto de referência é sempre o mesmo, mas os níveis de potência podem se mover em qualquer direção do ponto de referência se representarem perda ou ganho.

Podemos, inclusive, usar esse diagrama como uma tabela de conversão.

Exemplo 1

Converter +43 dBm em mW

Observe que se formos expressar 43 em dez e três teríamos:

43 = 10 + 10 + 10 + 10 + 3.

Olhando para o diagrama da **Figura 5.1**, partindo do ponto de referência e seguindo para a direita, deveríamos multiplicar quatro vezes o fator de dez mais uma vez o fator de dois.

- 1 mW x **10** = 10 mW;
- 10 mW x **10** = 100 mW;
- 100 mW x **10** = 1.000 mW;
- 1.000 mW x **10** = 10.000 mW;
- 10.000 mW x **2** = 20.000 mW = 20 W.

Ou seja, +43 dBm é igual a 20 watts.

Exemplo 2

Converter -26 dBm em uW

Expressando -26 em dez e três:

-26 = -10 -10 -3 -3

Olhando para o diagrama da **Figura 5.1**, partindo do ponto de referência e seguindo para a esquerda, deveríamos dividir duas vezes o fator de dez mais duas vezes o fator de dois.

- 1 mW /**10** = 100 uW;
- 100 uW /**10** = 10 uW;
- 10 uW /**2** = 5 uW;
- 5 uW / **2** = 2,5 uW.

Ou seja, -26 dBm é igual a 2,5 microwatts.

dBi

Ao quantificarmos o ganho de uma antena, comumente usamos a expressamos em dBi, que é uma medida relativa. O i se refere apenas a uma antena isotrópica. Conforme já vimos, uma antena isotrópica é teoricamente um transmissor ideal que irradia sinal em todas as direções com a mesma intensidade, com 100% de eficiência em três dimensões. dBi é usado em RF da mesma maneira que dB.

Considere uma antena de dez dBi com dez miliwatts de potência aplicada:

10 mW + 10 dBi (acréscimo de 10 vezes) = 100 mW

Antenas não degradam o sinal, salvo se estiverem danificadas. O valor em dBi é sempre positivo.

Como dB, dBi é uma unidade de medida relativa e pode ser adicionada ou subtraída de outras unidades decibel. Por exemplo, se um sinal RF sofre uma perda de dois dB antes de chegar a uma antena com ganho de oito dBi, o sinal resultante tem um ganho de seis dB.

Exemplo 3

Dado o circuito RF seguinte, calcular o sinal resultante irradiado pela antena, levando em conta os dados mostrados na tabela:

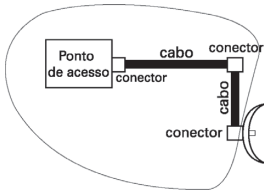

Figura 5.2.

Potência de saída do Access Point	100 mW
Ganho da antena	12 dBi
Perdas	
Primeiro conector	- 3 dB
Segundo conector	- 3 dB
Terceiro conector	- 3 dB

Tabela 5.1.

Para designar o nível de potência em vários pontos do circuito, faremos:

- P1: potência de saída do Access point;
- P2: potência irradiada pela antena;
- P3: potência do sinal antes de chegar à antena.

Primeiro vamos transformar a potência de saída do Access Point para facilitar o cálculo:

P (dBm) = 10 log 100

P1 = 10 x 2 = **20 dBm**

Agora calculamos o sinal resultante computando as perdas causadas pelos conectores e o ganho da antena.

P2 = Potência do AP – perdas dos conectores + ganho da antena

P2 = 20 – 3 – 3 – 3 + 12 = **23 dBm = 200 mW**

Observe que o ganho real foi de três dB (o dobro) em relação ao sinal que sai do AP.

Para calcularmos o sinal que chega à antena, fazemos:

P3 = Potência do AP – perdas dos conectores

P3 = 11 dBm.

Capítulo 6

Técnicas de transmissão

Conforme mencionado anteriormente, WLANs utilizam uma técnica de transmissão conhecida como difusão de espectro (Spread Spectrum). Essa técnica se caracteriza por ampla largura de banda e baixa potência de sinal. Possui uma série de vantagens em relação à sua antecessora (banda estreita) por constituir sinais difíceis de detectar ou mesmo interceptar sem o equipamento adequado. São menos suscetíveis a interferências do que os sinais de banda estreita (Narrow Band). Por todas essas razões tem sido a técnica preferida do meio militar. Existem dois tipos de tecnologias de Spread Spectrum regulamentadas pelo FCC: Direct Sequence Spread Spectrum (DSSS) e Frequency Hopping Spread Spectrum (FHSS). Mas, antes, vamos falar um pouco sobre transmissão em banda estreita.

Banda Estreita (Narrow Band)

A transmissão em banda estreita é uma tecnologia que se caracteriza pela alta potência do sinal e pelo uso do espectro de freqüência suficiente para carregar o sinal de dados e nada mais. Quanto menor a faixa de freqüência utilizada, maior deverá ser a potência para transmitir o sinal. Para que esses sinais sejam recebidos, eles devem estar acima (de forma significativa) de um nível de ruído conhecido como noise floor. Devido ao fato de sua banda ser muito estreita, um alto pico de potência garante uma recepção livre de erros. Uma das grandes desvantagens dessa técnica é a sua suscetibilidade à interferência, aliada ao fato de que é simples evitar que o sinal original seja recebido, transmitindo sinais indesejáveis na mesma banda com potência maior do que a do sinal original.

Difusão de Espectro (Spread Spectrum)

Diferentemente da transmissão em banda estreita, a difusão de espectro utiliza uma faixa de freqüência muito maior do que a necessária para carregar a informação. São menos suscetíveis à interferência e usam menos potência para transmitir um sinal do que a que seria necessária para transmitir o mesmo sinal na banda estreita. Veja a **Figura 6.1**:

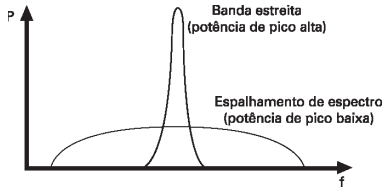

Figura 6.1: Comparação entre transmissão em Narrow Band e Spread Spectrum.

Para exemplificar, usaríamos 1 MHz em 10 watts com Narrow Band e 20 MHz em 100 mW com Spread Spectrum.

As principais características de um sinal Spread Spectrum (grande largura de banda e baixa potência) faz com que ele se assemelhe a um sinal de ruído. Como receptores não irão interceptar nem decodificar um sinal de ruído, isso cria uma espécie de canal de comunicação seguro.

Essa segurança foi o que encorajou o meio militar nos anos 1950 e 1960 a usar a tecnologia. Obviamente essa segurança deixava de ser válida se mais alguém usasse a tecnologia.

Nos anos 1980, o FCC criou uma série de regras que tornava disponível a tecnologia para o público, encorajando sua pesquisa e comercialização. Essa atitude não influenciou o meio militar porque as bandas e as técnicas de modulação usadas pelo público eram diferentes.

Desde então a tecnologia tem sido usada em telefones sem fio, GPS, telefones celulares e mais recentemente em WLANs.

Embora haja muitas implementações da tecnologia, somente dois tipos são regulamentados pelo FCC: o FHSS (Frequency Hope Spread Spectrum) e o DSSS (Direct Sequence Spread Spectrum).

FHSS (Frequency Hope Spread Spectrum)

FHSS é uma técnica que usa a agilidade de freqüência para espalhar os dados. Essa agilidade pode ser entendida como a mudança repentina da freqüência de transmissão dentro da faixa de RF utilizável. No caso das WLANs, a banda utilizável dentro da 2.4 GHz ISM é a de 83.5 MHz, segundo regulamentado FCC e do IEEE 802.11.

A portadora muda a freqüência de acordo com uma seqüência pseudo-randômica. Essa seqüência nada mais é que uma lista de freqüências que a portadora deve pular em intervalos de tempo especificados. O transmissor usa essa seqüência para selecionar suas freqüências de transmissão. A portadora permanecerá em uma freqüência por um determinado período de tempo e depois pulará para a próxima. Quando a lista de freqüências chegar ao final, o transmissor repetirá a seqüência. A **Figura 6.2** ilustra um sistema de FHSS usando uma seqüência de cinco freqüências: 2.449 GHz, 2.452 GHz, 2.448 GHz, 2.450 GHz, 2.451 GHz.

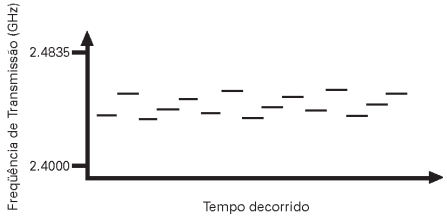

Figura 6.2: Sistema FHSS.

Uma vez que a informação tenha sido transmitida na portadora 2.451 GHz, a seqüência é repetida iniciando em 2.449 GHz. O processo de repetição continuará até que a informação tenha sido recebida completamente.

O rádio receptor, por sua vez, é sincronizado na seqüência do transmissor para receber a freqüência correta no tempo certo e, por fim, o sinal é demodulado.

Efeitos da Interferência

Similarmente a todas as tecnologias de Spread Spectrum, sistemas FHSS são resistentes, mas não imunes à interferência.

Se um sinal viesse a interferir no nosso sinal ilustrado na **Figura 6.2**, na freqüência de 2.451 GHz, aquela porção do sinal estaria perdida e teria de ser retransmitida, mas o resto do sinal permaneceria intacto.

Na realidade, um sinal interferente de banda estreita ocuparia vários megahertz da largura de banda. Como a banda do FHSS tem largura maior que 83 MHz, um sinal interferente em banda estreita seria incapaz de causar uma degradação muito significativa do sinal.

Sistemas FHSS

O IEEE 802.11 especifica taxa de dados de 1 Mbps e 2 Mbps para sistemas FHSS. Para que eles sejam compatíveis com o padrão 802.11, devem operar na banda 2.4 GHz ISM.

No máximo 79 rádios sincronizados podem ser usados, mas o fato de cada rádio necessitar de sincronização precisa com os outros sem causar interferência torna o custo desses sistemas proibitivo e geralmente não é considerado como uma opção.

Se forem usados rádios não-sincronizados, o limite cai para 26, levando-se em conta uma WLAN de médio tráfego. O aumento significativo do tráfego ou a transferência de grandes arquivos faz com que esse limite caia ainda mais, chegando a 15.

Se esse limite não for respeitado, haverá interferência entre os sistemas, aumentando o número de colisões e reduzindo drasticamente o throughput da WLAN.

DSSS (Direct Sequence Spread Spectrum)

DSSS é o método de envio de dados em que os sistemas de transmissão e recepção são ambos um set de freqüências de 22 MHz de largura, sendo a mais conhecida e mais utilizada das tecnologias de espalhamento.

Combina um sinal de dados na transmissão com uma alta taxa de seqüência de bit rate, conhecida como chipping code ou ganho de processamento. Quanto maior for o ganho de processamento, maior será a resistência do sinal a interferências. Embora o FCC estipule como um mínimo um ganho de processamento de dez, muitos fabricantes trabalham com um ganho de processamento da ordem de vinte.

O processo de Direct Sequence, que são as duas primeiras iniciais do DSSS, começa com uma portadora sendo modulada em uma seqüência de código. O número de "chips" no código vai determinar como ocorrerá o espalhamento; e o número de chips por bit e a velocidade da codificação em chips por segundo vão determinar qual será a taxa de dados.

Sua popularidade, principalmente em relação ao FHSS, está baseada na facilidade de implementação e nas altas taxas de transmissão, devido à largura do canal. A maioria dos equipamentos WLAN, hoje em dia, usa essa técnica de transmissão.

Sistemas DSSS

Na banda não licenciada de 2.4 GHz, o IEEE especifica o uso do DSSS na taxa de dados de 1 Mbps e 2 Mbps no padrão 802.11. No padrão 802.11b, a taxa de dados é de 5 Mbps e 11 Mbps. Dispositivos 802.11b são capazes de operar com dispositivos 802.11, devido à compatibilidade. Logo, não seria necessário fazer upgrade de uma rede 802.11 inteira para 802.11b para usufruir os benefícios, preservando assim o investimento anterior.

Já o 802.11a com taxas atrativas de 54 Mbps não possui essa compatibilidade com os padrões anteriores pelo fato de usar a banda de 5 GHz, fazendo com que usuários do 802.11 e 802.11b investissem no upgrade de toda a rede para usufruir essas altas taxas de dados.

O 802.11g é uma alternativa ao 802.11a, apresentando os mesmos benefícios da taxa de dados de 54 MHz do 802.11a e compatibilidade com os padrões 802.11 e 802.11b, por operar na faixa de 2.4 GHz. Com a popularização do padrão 802.11g, o 802.11a tende a ter seu uso cada vez mais restrito. Existem fabricantes, como a Dlink, que fabricam equipamentos para operar com uma taxa de 128 Mbps, também chamada de turbo.

Canais

Diferentemente do FHSS, que usa seqüências de pulo para definir os canais, o DSSS usa uma definição de canais mais convencional. Cada canal é uma banda contígua de freqüências com largura de 22 MHz e portadoras de 1 MHz, como no FHSS. Por exemplo, o canal um opera de 2.401 GHz a 2.423 GHz (2.412 GHz +/- 11 MHz). Veja a **Figura 6.3**:

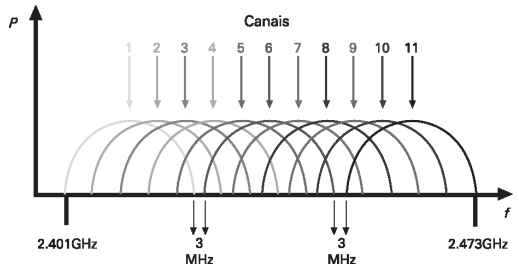

Figura 6.3: Canais DSSS e relacionamento espectral.

Observe que os canais um e dois se entrelaçam de maneira significativa. Cada uma das freqüências mostradas é considerada freqüência central. A partir dela somamos e subtraímos 11 MHz para obter o canal utilizável de 22 MHz. Veja a tabela seguinte:

Canal	Freqüência estipulada pelo FCC (GHz)
1	2.412
2	2.417
3	2.422
4	2.427
5	2.432
6	2.437
7	2.442
8	2.447
9	2.452
10	2.457
11	2.462

Tabela 6.1.

O uso de rádios DSSS com canais entrelaçados (um e dois, por exemplo), no mesmo espaço físico pode causar interferência entre eles, reduzindo drasticamente o throughput de toda a rede. Para usar rádios DSSS no mesmo espaço físico, eles deveriam usar canais que não se entrelaçam (canais um e seis, por exemplo). Como as freqüências centrais estão distantes de 5 MHz e os canais têm 22 MHz de largura, é possível colocar no máximo três sistemas DSSS no mesmo espaço físico, em teoria os canais um, seis e onze não se entrelaçam. Veja a **Figura 6.4**:

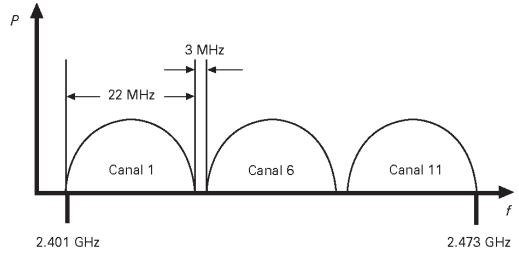

Figura 6.4: Três canais que não se entrelaçam.

Capítulo 7

A banda de 5 GHz

Na realidade a banda de 5 GHz se divide em três:

- U-NII 1: estende-se de 5.15 a 5.25 GHz;
- U-NII 2: estende-se de 5.25 a 5.35 GHz;
- U-NII 3: estende-se de 5.725 a 5.825 GHz.

A numeração de canal inicia em 5 GHz, com incrementos de 5 MHz.

Nas bandas U-NII 1 e 2, a freqüência central está distante 30 MHz das bordas, enquanto na U-NII 3 essa distância é de 20 MHz, conforme mostram as **Figuras 7.1 e 7.2**.

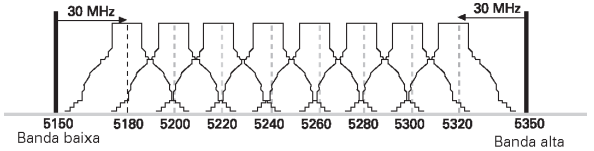

Figura 7.1: Canais na U-NII 1 e 2.

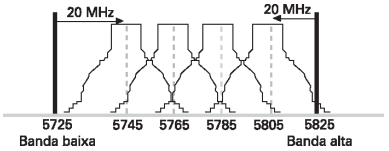

Figura 7.2: Canais na U-NII 3.

As três bandas têm diferentes limites no que se refere à potência de transmissão. A banda U-NII 1 é voltada para uso indoor somente, em níveis baixos de potência; a banda U-NII 3 é voltada para uso outdoor e aplicações de longa distância em níveis mais altos de potência.

- Na banda U-NII 1, pode-se usar um transmissor de até 40 mW (16 dBm), com uma antena de ganho de 6 dBi, produzindo uma EIRP máxima de 22 dBm. Para cada ganho adicional acima dos 6 dBi, deve-se reduzir a potência no transmissor de 1 dB;
- Na banda U-NII 2, pode-se usar um transmissor de até 200 mW (23 dBm), com uma antena de ganho de 6 dBi, produzindo uma EIRP máxima de 29 dBm. Para cada ganho adicional acima dos 6 dBi, deve-se reduzir a potência no transmissor de 1 dB;
- Na banda U-NII 3, pode-se usar um transmissor de até 800 mW (29 dBm), com uma antena de ganho de 6 dBi, produzindo uma EIRP máxima de 35 dBm. Para cada ganho adicional acima dos 6 dBi, deve-se reduzir a potência no transmissor de 1 dB.

Operações na banda U-NII 3 permitem o uso de antenas de 23 dBi sem uma redução na potência de transmissão em links ponto a ponto. Essa configuração resulta em uma EIRP máxima de 52 dBm.

Efeitos de Interferência

Da mesma forma que no FHSS, sistemas DSSS são resistentes à interferência de banda estreita devido a características do seu espectro, mas são mais suscetíveis a ela em comparação aos sistemas FHSS, em virtude da sua pequena largura de banda (22 MHz em vez dos 79 MHz do FHSS) e pelo fato de a informação ser transmitida ao longo da banda inteira simultaneamente, em vez de uma freqüência em um dado momento.

Regras do FCC que Afetam o DSSS

O FCC determina que sistemas DSSS usem no máximo 1 watt de potência na transmissão para topologias ponto-multiponto. A potência de saída máxima é a mesma, qualquer que seja o canal utilizado. Essas regras se aplicam tanto para a banda não licenciada de 2.4 GHz como para a banda de 5 GHz.

Comparação entre DSSS e FHSS

Ambas as tecnologias têm vantagens e desvantagens, e cabe ao administrador de uma WLAN escolher qual usar e em que situação usá-la ao implementar uma WLAN. Veremos a seguir alguns dos fatores que deveriam ser levados em conta quando da escolha de qual tecnologia é a mais apropriada para determinada situação.

Interferência de Banda Estreita

Uma das grandes vantagens do FHSS é a grande resistência à interferência. O DSSS é muito mais suscetível à interferência de banda estreita devido às bandas contíguas de pequena largura (22 MHz). Esse fato deve ter um peso grande na decisão, em ambientes em que essa interferência está presente.

Custo

O custo de implementação de um sistema DSSS é muito menor se comparado à implementação de um sistema FHSS. Isso se deve muito ao fato de que equipamentos DSSS são facilmente encontrados no mercado e sua rápida adoção tem ajudado a baixar os custos. Nos dias de hoje, um bom PC Card DSSS 802.11b pode ser comprado por algo em torno de R$ 100,00, enquanto um cartão FHSS compatível com 802.11 pode ser adquirido por algo em torno de R$ 150,00 a R$ 350,00, dependendo do fabricante e do padrão.

Coexistência no Mesmo Ambiente Físico

Uma vantagem do FHSS sobre o DSSS é poder ter em um mesmo ambiente físico um número maior de rádios. Como vimos anteriormente, como o FHSS usa 79 canais discretos, podemos ter até 79 rádios contra apenas três do DSSS.

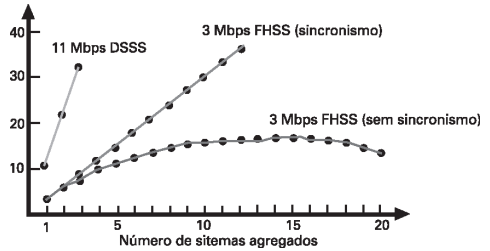

Figura 7.3: Comparação de coexistência.

Porém, quando levamos em consideração o custo de hardware de um sistema FHSS para obter o mesmo throughput de um DSSS, a vantagem desaparece rapidamente.

Para um sistema DSSS, podemos ter no máximo três rádios, o que nos daria um throughput máximo de:

3 x 11 Mbps = 33 Mbps

O throughput real seria portanto: 33 / 2 = **16,5 Mbps**

Para obtermos o mesmo throughput usando FHSS, teríamos:

16 x 2 Mbps = 32 Mbps

Sendo o throughput real igual a **16 Mbps.**

Ou seja, precisaríamos de 16 rádios. Além disso, teríamos o gasto adicional com cabos, conectores e antenas.

Se os objetivos é baixo custo e o alto throughput, escolha o DSSS.

Se o objetivo é manter usuários segmentados por diferentes rádios em um ambiente de coexistência mais denso, escolha o FHSS.

Compatibilidade e Disponibilidade

A Wireless Ethernet Compatibility Alliance (WECA) criou um padrão de compatibilidade que garante que um dispositivo DSSS 802.11b de um fabricante opere e interaja com o dispositivo 802.11b de outro fabricante sem maiores problemas. Esse padrão foi chamado de Wireless Fidelity ou simplesmente Wi-Fi. Dispositivos que passam nos testes de interoperabilidade levam um selo Wi-Fi, significando que o mesmo tem capacidade de interagir com outros dispositivos Wi-Fi.

Não acontece o mesmo com equipamentos FHSS. Existem padrões, como 802.11 e Openair, mas não há nenhum órgão que faça o mesmo teste de compatibilidade que o WECA faz para o DSSS.

Devido à sua imensa popularidade, é muito mais fácil encontrar dispositivos DSSS. Como se isso não bastasse, a demanda para dispositivos DSSS tem crescido continuamente, enquanto a demanda para dispositivos FHSS tem permanecido estacionada nos últimos anos.

Taxa de Dados e Throughput

Os últimos sistemas FHSS são muito mais lentos que os últimos sistemas DSSS, devido à sua taxa de dados ser de apenas 2 Mbps. Existem alguns sistemas FHSS que operam com 3 Mbps ou mais, mas eles não são compatíveis com o padrão 802.11 e não devem operar com outros sistemas FHSS no mesmo ambiente. O HomeRF 2.0 é um bom exemplo disso, pois consegue alcançar uma taxa de dados de 10 Mbps. Porém o HomeRF 2.0 tem a potência de saída limitada em 125 mW.

Tanto sistemas DSSS como FHSS têm um throughput (dados sendo enviados) de apenas metade da taxa de dados.

Na realização de testes de uma nova WLAN, são comuns throughput de 5 ou 6 Mbps para uma taxa de dados de 11 Mpbs.

Quando frames wireless são transmitidos, há pausas entre data frames para sinais de controle e outras tarefas. Nos sistemas FHSS, esse espaçamento entre frames é mais longo do que nos sistemas DSSS, causando uma lentidão na taxa em que os dados são enviados (throughput). Além disso, quando o sistema FHSS está no processamento de mudança de freqüência, nenhum dado é enviado e com isso há maior perda no throughput.

Alguns sistemas WLAN, na tentativa de alcançar maiores throughput, usam protocolos proprietários na camada física e chegam a obter até 80% da taxa de dados. Porém essa medida sacrifica a interoperabilidade com outros dispositivos.

Segurança

Pela forma de implementação dos padrões, poderíamos ser levados a acreditar que o FHSS é mais seguro que o DSSS, afinal, somente a descoberta da seqüência do pulo da freqüência poderia comprometer um sistema FHSS. Mas há dois fatores que provam que isso não é tão difícil assim.

O primeiro deles é que rádios FHSS são produzidos por um número pequeno de fabricantes e todos eles aderem aos padrões 802.11 ou Openair para vender seus produtos. Segundo, cada um dos fabricantes usa um set padrão de seqüências para o pulo da freqüência, o qual geralmente vem ao encontro de uma lista predeterminada, produzida pelos padrões (IEEE ou WLIF). Esses dois fatores tornam a quebra da seqüência do pulo da freqüência relativamente simples.

Outra razão é que o número do canal é transmitido em texto puro em cada beacon. Além disso, o endereço MAC do rádio que está transmitindo pode ser visto em cada beacon (o que indica o fabricante do rádio).

Alguns fabricantes permitem ao administrador definir a seqüência, porém essa funcionalidade não adiciona nenhum nível de segurança porque alguns dispositivos, tais como um analisador de espectro, juntamente com um laptop, podem ser usados para rastrear a seqüência de pulos da freqüência em questão de segundos.

Capítulo 8

Infra-estrutura de uma WLAN

Existem diversos dispositivos que compõem a infra-estrutura de uma WLAN. Podemos dividi-los em duas categorias, conforme ilustrado na tabela seguinte:

Equipamentos de conectividade	• Pontos de Acesso • Pontes • Roteadores • Gateways
Dispositivos Clientes	• Cartões PCMCIA • Adaptadores ISA/PCI • Dispositivos USB

Tabela 8.1: Infra-estrutura de uma WLAN.

Pontos de Acesso (AP)

Pontos de Acesso, como o próprio nome sugere, funcionam como pontos de entrada de uma rede para um cliente. É um dispositivo half-duplex com funcionalidades similares aos switches Ethernet modernos, com a diferença de ser sem fio.

É composto por uma ou duas antenas de ganho baixo (normalmente 5 dBi no máximo) que na maioria dos casos pode ser removida para a conexão de antenas com ganho maior, e uma porta Ethernet para conectar com a rede cabeada. São considerados portais pelo fato de conectarem clientes de uma rede 802.11 (WLAN) a uma rede 802.3 (Ethernet) ou 802.5 (Token Ring). Em uma rede com AP, todo o fluxo de dados passa por ele. Normalmente são utilizados para aplicações indoor.

Figura 8.1: Ponto de Acesso.

Figura 8.2: Ponto de Acesso (vista traseira).

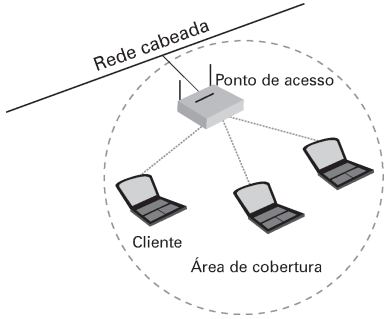

Figura 8.3: Ponto de Acesso instalado em uma rede típica.

Modos de operação

Pontos de Acesso podem se comunicar com seus clientes wireless, com a rede Ethernet e com outros pontos de acesso. Existem três modos de operação:

- Modo root;
- Modo Repetidor;
- Modo Ponte.

Modo Root

É utilizado quando o AP é conectado a um backbone Ethernet. Esse é o modo de operação padrão. Neste modo, APs que estão conectados ao mesmo segmento Ethernet podem se comunicar por meio deste. APs se comunicam para coordenar funcionalidades de roaming, tais como reassociação. Clientes Wireless localizados em células diferentes podem se comunicar por meio de seus respectivos APs, através do segmento Ethernet.

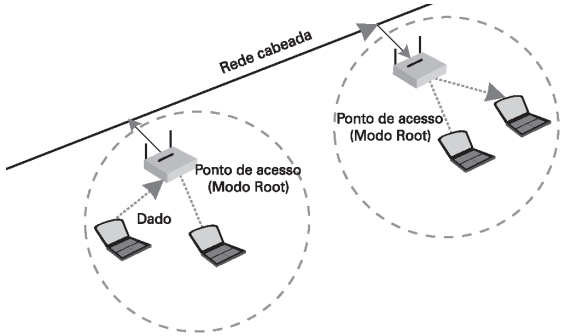

Figura 8.4: Pontos de Acesso operando em modo root.

Modo Ponte

Nesse modo, o AP atua como se fosse uma ponte wireless ligando dois segmentos Ethernet. A finalidade de uma ponte é isolar dois segmentos de rede e, dessa forma, impedir que o tráfego não endereçado a máquinas de um determinado segmento o atinja, e com isso evitar a sobrecarga desse segmento. Nesse modo, os APs fazem o mesmo, só que a ligação entre eles é sem fio. Existem poucos APs no mercado com essa funcionalidade, devido ao fato de que essa característica aumenta substancialmente o custo do equipamento.

Diferentemente do modo root, nesse modo os clientes não se associam ao AP.

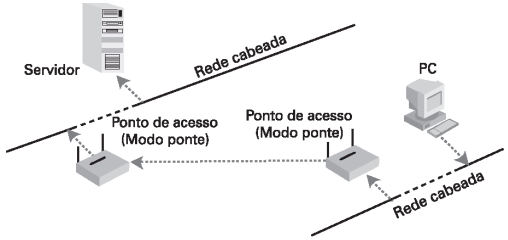

Figura 8.5: APs operando em modo ponte.

Modo Repetidor

Neste modo, um AP atua no modo root enquanto o outro atua como repetidor. Os clientes se associam ao AP repetidor, que por sua vez é um cliente do AP root. A ligação entre eles forma um link wireless dentro de uma estrutura cabeada. Este modo não é muito utilizado porque existem algumas desvantagens:

• Os clientes ligados ao AP repetidor experimentam baixo throughput e um grande período de latência nessa configuração, devido ao fato de que ambos os APs se comunicam com os clientes através do mesmo link wireless;

• O alcance no qual os clientes podem se associar ao AP repetidor é reduzido drasticamente.

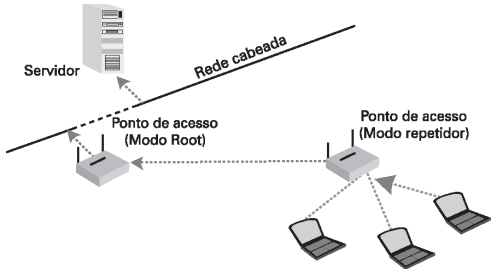

Figura 8.6: AP no modo repetidor.

Características comuns

Embora haja diversos fabricantes de APs, existem características que são comuns à maioria eles. Abordaremos as principais.

Antenas fixas ou removíveis

Dependendo da necessidade, você deve escolher entre ter um AP com antenas fixas ou removíveis. A grande vantagem de ter um AP com antena removível reside na flexibilidade de usar uma antena com qualquer comprimento de cabo que você necessite. Imagine que você tenha clientes outdoor que necessitam ter acesso à sua rede Ethernet. Nesse caso, o AP deve ser montado em um lugar protegido dentro do prédio, e uma antena outdoor de alto ganho ser acoplada a ele por meio de um cabo e conectores.

Filtragem avançada

Um AP pode controlar quem tem permissão de se associar a ele ou não. Para evitar associação de clientes não-autorizados, o AP possui uma tabela de endereços MAC (endereços físicos) dos clientes que podem se associar a ele. A máquina que tiver um endereço MAC que não faz parte da tabela não conseguirá se associar. Também é possível explicitamente permitir ou negar a associação de um determinado MAC.

Uma outra característica interessante é a filtragem de protocolos. Por meio dela, somente os protocolos permitidos pelo administrador podem trafegar no link wireless.

Cartões PCMCIA removíveis

Existem APs que possuem dois slots para cartões PCMCIA. Essa configuração tem uma série de benefícios:

• Cada cartão pode ser configurado para operar em modos diferentes. Um pode atuar em modo root e outro em modo ponte, por exemplo (em muitos casos, um backbone wireless);

• Cada cartão pode ser tratado como dois APs independentes, suportando o dobro de usuários no mesmo espaço físico sem necessidade de compra de um AP adicional e, dessa forma, reduzir os custos. Lembre que os cartões devem ser configurados para operar em canais diferentes ligados à mesma antena.

• Cada cartão pode operar com tecnologia diferente, conectado a uma antena diferente. Por exemplo, um cartão pode ser 802.11a e outro, 802.11b, conectados a uma antena de 5 GHz e outra de 2.4 GHz, respectivamente.

SSID

O SSID é o identificador de uma determinada célula. Para que haja associação com um AP, o cliente deve saber o SSID daquela célula. O cliente pode fazer isso de duas formas:

• O AP divulga o SSID, dessa forma o cliente se conecta ao AP de modo automático, bastando apenas operar no mesmo canal do AP;

• O AP não divulga o SSID. Nesse caso, a associação só ocorre se o cliente estiver configurado com o SSID do AP. Essa é uma medida de segurança. Nem todos os APs têm essa característica.

Capítulo 9

Potência de saída variável

Essa característica permite controlar a potência com que o AP transmite os dados. Controlar a potência de saída se torna necessário quando nós distantes não conseguem localizar o AP. Também permite controlar a área de cobertura do AP. À medida que os clientes se movem para longe do AP, eles não perdem a conectividade.

A maior vantagem é poder controlar o tamanho das células, evitando assim que invasores consigam conectar a rede fora do prédio e aumentando a segurança. Com APs que não dispõem dessa funcionalidade, temos que lançar mão de outros mecanismos para controlar a potência, tais como amplificadores, atenuadores, cabos de grande comprimento e antenas de alto ganho.

Vários Tipos de Conectividade para Rede Cabeada

As opções de conectividade para rede cabeada de um AP podem incluir 10 Base Tx, 10/100 Base Tx, 100 Base Tx, 100 Base Fx, token ring e outros.

Como um AP é um dispositivo com o qual clientes wireless se comunicam com a rede cabeada, o entendimento de como conectar o AP à rede cabeada é importante, evitando assim que o AP venha a se tornar um gargalo na rede.

Criptografia

Em uma rede wireless, levando-se em conta o aspecto da segurança, é muito perigoso que os dados trafeguem sem nenhum tipo de proteção entre o AP e os clientes. Alguém mal intencionado que conseguir se associar ao AP pode usar um sniffer e ver o que está trafegando pela rede. Para evitar que isso ocorra, é possível criptografar os dados. O protocolo WEP é responsável por essa tarefa. Ativando o protocolo WEP, os dados estarão criptografados, o que aumentará a segurança. Porém, o uso do WEP aumenta significativamente a carga de processamento no AP.

Configuração e Gerenciamento

Existem várias formas de configurar um AP, mas nem todos dispõem de todas elas. As mais comuns são: console, telnet e Web.

Devemos ter em mente que, quanto mais funcionalidades um AP tiver, mais caro ele será. Existem dois tipos de APs: os que são volta-

dos para uso doméstico e os que são voltados para uso empresarial. Os APs de uso doméstico são menos robustos e resistentes e, por isso, mais baratos. Já os de uso empresarial, que incorporam uma série de funcionalidades, são mais robustos, têm maior poder de processamento e são mais caros.

Tipos	Funcionalidades
Uso doméstico	• Filtros MAC • WEP (64 ou 128 bits) • USB ou console para configuração • Configuração via Web
Uso empresarial	• Filtros MAC • WEP (64 ou 128 bits) • USB ou console para configuração • Configuração via Web • Acesso Telnet • Cliente Radius • 802.1x/EAP • Gerenciamento SNMP • VPN • Roteamento (estático e dinâmico) • Funções de repetidor • Funções de ponte

Tabela 9.1: Tipos de Pontos de Acesso.

Alguns APs empresariais permitem gerenciamento por meio de SNMP. SNMP é um protocolo de gerenciamento usado para gerenciar dispositivos em uma rede. Um software de gerenciamento coleta informações dos dispositivos que fazem parte da rede e os mostra em um console de gerenciamento. Quando há alguma condição de anormalidade com um cliente ou com a rede, o software de gerenciamento toma conhecimento por meio dos alertas que ele recebe.

Pontes Wireless

Pontes wireless são dispositivos que permitem a interligação de dois segmentos LAN. Operam em half-duplex e são dispositivos de camada dois somente. São usados em configurações ponto a ponto e ponto-multiponto.

Figura 9.1: Ponte wireless.

Modos de operação

As pontes se comunicam entre si segundo quatro modos de operação:

- Modo root;
- Modo não-root;
- Modo AP;
- Modo repetidor.

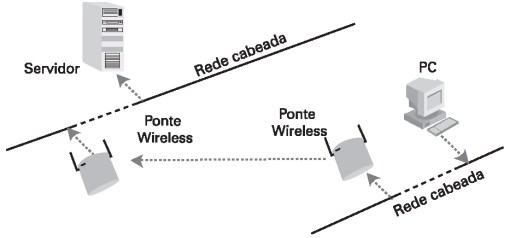

Figura 9.2: Pontes wireless em uma configuração ponto a ponto.

Modo root

Nesse modo de operação uma ponte deve ser eleita como root. Uma ponte root só pode se comunicar com pontes que não são root ou com dispositivos clientes e não podem se associar com outra ponte root.

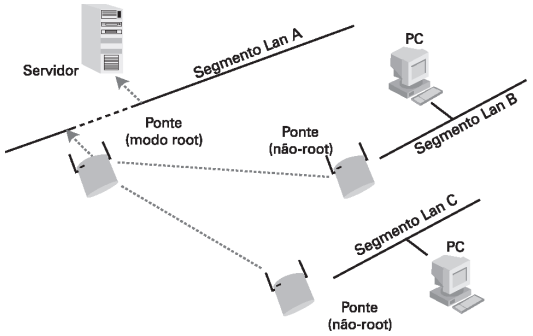

Figura 9.3: Ponte root se comunicando com outras pontes.

Modo não root

Nesse modo, a ponte se comunica com outras pontes root via wireless. Alguns fabricantes permitem que a ponte, operando nesse modo, aceite conectividade com dispositivos clientes, atuando dessa forma como ponte e como Ponto de Acesso simultaneamente.

Modo AP

Alguns fabricantes permitem que clientes se conectem às pontes, o que nada mais é do que adicionar à ponte uma funcionalidade de AP. Em muitos casos, a ponte tem um modo AP que a converte para esse modo.

Modo repetidor

Nesse modo, a ponte pode ser posicionada entre duas outras pontes, com o propósito de estender o comprimento do segmento wireless. Apesar de essa configuração ter a vantagem de estender o link, existe uma grande desvantagem, que é a redução do throughput devido à necessidade de repetir a transmissão de todos os frames por um mesmo rádio. Esse modo é utilizado por pontes não root e, muitas vezes, a porta LAN estará desabilitada.

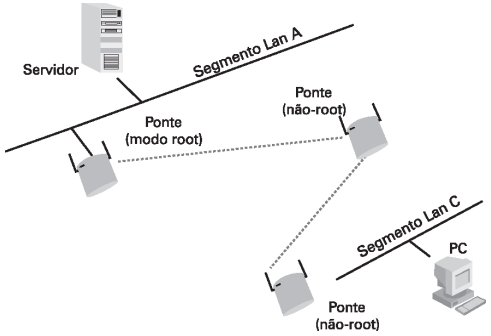

Figura 9.4: Ponte atuando no modo repetidor.

Características comuns

As características das pontes são as mesmas já descritas para os Pontos de Acesso. Mas existem duas muito interessantes que poderíamos citar: balanceamento de carga e integridade de link.

Capítulo 10

Pontes wireless de workgroup

Pontes de workgroup operam de maneira similar e são muitas vezes confundidas com as pontes wireless. A principal diferença é que pontes de workgroup são dispositivos clientes. Elas são capazes de agrupar vários clientes LAN em um único cliente wireless. Na tabela MAC do AP, podemos ver a ponte de workgroup com um simples cliente wireless. Os endereços MAC dos clientes que estão por trás da ponte não serão vistos pelo AP.

Pontes de workgroup são muito úteis quando há a necessidade de um pequeno grupo de usuários acessar uma rede principal, tal como em salas de aula e escritórios móveis.

Em ambientes indoor, em que um grupo de usuários está isolado da rede principal de usuários, uma ponte de workgroup pode ser a solução para conectar esse grupo à rede principal via wireless.

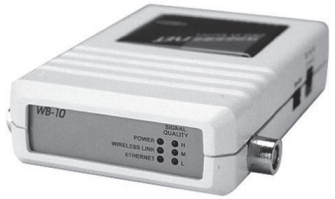

Figura 10.1: Ponte de workgroup.

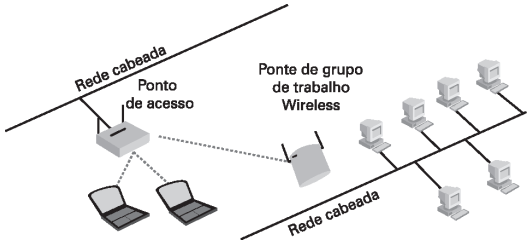

Figura 10.2: Ponte de workgroup interligada a uma rede.

Opções comuns

Praticamente todas as opções encontradas nas pontes wireless podem ser encontradas nas pontes de workgroup. Porém, as pontes de workgroup têm um limite de usuários no segmento LAN, variando de 8 a 128, dependendo do fabricante. O uso de mais de 30 clientes no link wireless já é suficiente para causar impacto na velocidade com que cada um executa suas tarefas.

Dispositivos Clientes

Clientes WLAN nada mais são do que os equipamentos dos usuários finais, tais como desktops, laptops ou PDAs, que necessitam de conectividade wireless dentro de uma infra-estrutura. Os dispositivos clientes que veremos a seguir fornecem esse tipo de conectividade para clientes WLAN.

PCMCIA e Flash Cards

O componente mais comum em qualquer rede wireless é o cartão PCMCIA ou PC Card. Esses dispositivos são usados em notebooks e PDAs para conexão à rede WLAN. PC Cards são comumente usados como rádios modulares em APs, pontes, dispositivos USB, adaptadores ISA e PCI e servidores de impressão. As antenas no PC Card variam de fabricante para fabricante. Enquanto umas são embutidas, outras são externas e podem ser conectadas ao PC Card por um cabo fino.

Flash Cards são similares aos PC Cards, mas são menores e mais compactos, tipicamente usados em PDAs. Consomem menos energia e têm baixa potência de saída em comparação aos PC Cards.

Figura 10.3: PC Card.

Figura 10.4: Flash Card.

Conversores

WLAN e Seriais

Conversores seriais são usados com qualquer dispositivo que tenha Ethernet e um conector serial DB9 com o propósito de converter conexões LAN em WLAN. Quando usamos um conversor WLAN, estamos externamente conectando um rádio WLAN a um dispositivo com cabo CAT5. Um uso comum desses conversores é a conexão de um servidor de impressão baseado em Ethernet em uma rede WLAN.

Esse dispositivo raramente inclui um rádio. Você deve adquirir o PC Card separadamente e instalá-lo no slot PCMCIA do conversor.

Conversores Ethernet normalmente permitem a conversão de um grande número de clientes LAN em WLAN em um curto espaço de tempo.

A configuração normalmente é feita via console através da entrada serial DB9 do conversor.

Figura 10.5: Conversor WLAN.

Ethernet – WLAN

Esse tipo conecta diretamente um simples dispositivo Ethernet a um AP, fornecendo uma conectividade wireless. Esse tipo de conexão oferece uma alternativa ao uso de PC Cards, tornando-se útil quando um dispositivo como um PC ou um console de videogame tem uma porta Ethernet e não possui nenhum rádio.

Adaptadores USB

Um adaptador USB nada mais é do que um invólucro que possui um PC Card e uma saída USB para ligar ao computador ou ao laptop. A questão do PC Card varia de fabricante para fabricante. Enquanto uns possuem um PC Card removível, outros possuem um PC Card embutido. No segundo caso não há como remover o PC Card sem abrir o invólucro. Uns são maiores e possuem um cabo USB, já outros são menores e mais compactos, idênticos a um pen drive, e são conectados diretamente à porta USB do computador.

Ao comprar um adaptador, USB é muito importante certificar se este possui ou não rádio embutido. Se não possuir, é altamente recomendável que o PC Card seja do mesmo fabricante do adaptador USB.

Figura 10.6: Adaptador USB com cabo.

Figura 10.7: Adaptador USB estilo pen drive.

Adaptadores ISA e PCI

Da mesma forma que um adaptador USB, um adaptador ISA ou PCI também usa um PC Card, porém o que muda é a forma de conexão: esses adaptadores são para instalação dentro do computador através de slots ISA ou PCI.

Existem adaptadores que já vêm com o PC Card embutido, enquanto outros não incluem um PC Card. No segundo caso, é altamente recomendável que se use um PC Card do mesmo fabricante do adaptador.

Adaptadores ISA ou PCI necessitam de configuração manual de software para operar adequadamente.

Figura 10.8: Adaptador PCI.

Servidores de impressão

Os servidores de impressão servem para conectar uma impressora USB a uma rede wireless, eliminando a necessidade de deixar um PC dedicado a essa tarefa. Um outro benefício é evitar a sobrecarga no PC devido aos jobs de impressão. Como o servidor de impressão é wireless, podemos deixar a impressora em qualquer ponto que desejarmos.

Figura 10.9: Servidor de impressão.

Utilitários

Alguns fabricantes fornecem um pacote de utilitários enquanto outros, apenas os meios básicos para conectividade. Um bom pacote de utilitários deve incluir:

- Site Survey;
- Software analisador de espectro;
- Monitoração de potência e velocidade;
- Configuração de perfil;
- Monitor do estado do link.

Site Survey

Site Survey pode incluir diferentes itens que permitem ao usuário encontrar redes, identificar endereços MAC de APs, medir os níveis da potência do sinal de ruído e ver a relação sinal – ruído.

Capítulo 11

Analisador de espectro

Software de analisador de espectro pode ser usado para identificar fontes de ruído e canais interferentes em áreas próximas à rede.

Monitoração de Potência e Velocidade

A monitoração da potência de saída e a velocidade da conexão pode ser útil para saber o que um link wireless é capaz de fazer em um dado momento. Um bom exemplo é um usuário que quer transferir uma grande quantidade de dados do servidor para o laptop. O usuário não deve iniciar a transferência até que a conexão da rede esteja em 11 Mbps, em vez de 1 Mbps.

Configuração de Perfil

A configuração de perfil facilita enormemente a tarefa de mudar de uma rede wireless para outra. Em vez de reconfigurar todos os parâmetros para a nova rede, o usuário cria um perfil com as configurações adequadas para redes distintas. Assim, basta ativar o perfil correspondente à rede que ele quer conectar.

Monitor do Estado do Link

Esse utilitário permite ver erros de pacote, transmissões bem-sucedidas, velocidade, viabilidade do link e outros parâmetros.

A finalidade é fazer testes do estado do link em tempo real.

Funcionalidades Comuns

Utilitários de fabricantes variam muito na funcionalidade, mas compartilham um set de parâmetros configuráveis, tais como:

- Modo de Infra-estrutura/Modo Ad-hoc;
- SSID;
- Canal;
- Chaves WEP;
- Tipo de autenticação.

Gateways

Gateways são comumente chamados de roteadores wireless.

Esses equipamentos têm como função principal a transferência de pacotes entre duas redes e a escolha do melhor caminho para realizar essa transferência. Eles usam o protocolo IP, cabeçalhos dos pacotes e as tabelas de roteamento para escolher o melhor caminho para envio de pacotes de uma rede a outra.

Os gateways podem ser divididos em duas classes: os residenciais e os empresariais.

A grande diferença entre as classes está na aplicação e na robustez do equipamento no que se refere às funcionalidades.

Gateways residenciais

Gateways residenciais são dispositivos projetados para conectar um pequeno número de clientes WLAN ou LAN à Internet. Eles possuem um hub ou switch embutido, além de um AP totalmente configurável. A porta WAN do gateway é o lado da Internet, e essa porta pode ser usada com uma das seguintes tecnologias, dependendo do modelo:

- xDSL;
- Cable modem;
- Modem analógico;
- Modem de satélite.

Figura 11.1: Gateway residencial.

Figura 11.2: Gateway residencial (vista traseira).

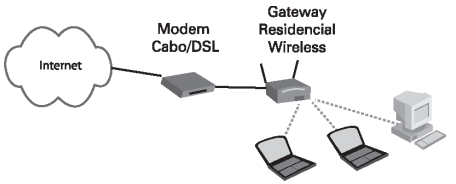

Figura 11.3: Gateway residencial conectado a uma pequena rede.

Opções comuns

Devido ao crescimento da popularidade do uso de gateways residenciais em residências e pequenos escritórios, os fabricantes decidiram adicionar novas características a esses dispositivos com o intuito de aumentar a produtividade e a segurança, tais como:

- PPOE;
- NAT;
- PAT;
- Ethernet Switching;
- Servidores virtuais;
- Serviços de impressão;
- VPNs;
- DHCP;
- Firewall.

A diversidade de funcionalidades permite que usuários domésticos ou de pequenos negócios possam ter uma solução relativamente robusta e de fácil configuração que vá ao encontro das necessidades dos negócios.

Gateways residenciais possuem todas as características de um AP já discutidas anteriormente, tais como: WEP, SSID, seleção de canal e outras.

Configuração e gerenciamento

Tanto a configuração como o gerenciamento de um gateway residencial normalmente são feitos via browser por uma de suas portas Ethernet, embora alguns modelos disponham também de console, telnet ou conectividade via USB. Normalmente o que se configuram são os parâmetros do ISP, LAN ou VPN.

Capítulo 12

Gateways empresariais

Gateways empresariais são dispositivos apropriados para uso em ambientes WLAN de larga escala, fornecendo serviços de gerenciamento WLAN, tais como: limite de banda, Qos e gerenciamento de perfil. É de suma importância que um gateway empresarial tenha um alto poder de processamento e interfaces fast ethernet, porque ele deve suportar muitos APs, todos enviando e recebendo uma grande quantidade de tráfego através dele. Gateways empresariais suportam gerenciamento por SNMP e permitem atualizações simultâneas dos perfis dos usuários por toda a rede. Eles podem ser configurados para tolerância a falhas (quando instalados em pares), suportam autenticação RADIUS, LDAP e criptografia usando túneis VPN.

Figura 12.1: Gateway empresarial.

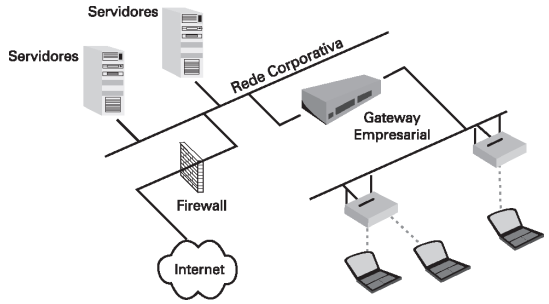

Figura 12.2: Gateway empresarial conectado a uma rede.

As tecnologias de autenticação incorporadas aos gateways empresariais são concebidas em um nível mais alto que as dos APs. VPN e 802.11x/EAP são suportados em muitos APs. Mas os gateways empresariais possuem características que não são encontradas em nenhum AP. Um bom exemplo disso é o RBAC (Controle de acesso baseado em função).

RBAC

RBAC permite a um administrador designar um determinado nível de acesso à rede wireless baseado na função de um funcionário

dentro da companhia. Por exemplo, se um funcionário tem determinados direitos de acesso à rede e é substituído, o novo funcionário adquire os mesmos direitos que o anterior possuía.

Classe de Serviço

A classe de serviço pode ser usada por um administrador para designar níveis de serviço para um usuário particular ou a função. Por exemplo, uma conta convidada poderia usar somente 500 Kbps da rede wireless enquanto o administrador poderia usar 2 Mbps.

Mobilidade IP

Um administrador também pode determinar para quais células um usuário poderá se mover, e isso deve ser definido como parte da política. Alguns gateways possuem até controle de data e hora para determinar os horários que o usuário pode usar a rede.

Gateways empresariais se tornam uma boa solução de alto custo *versus* benefício em situações em que é necessário o uso de um grande número de APs e a segurança é um ponto chave.

Configuração e gerenciamento

A configuração pode ser feita por meio de um browser (http ou https), console (CLI) ou telnet. O gerenciamento centralizado através de poucos dispositivos é a grande vantagem do uso desses equipamentos. Um administrador pode gerenciar uma grande rede por meio de poucos dispositivos centrais em vez de gerenciar um grande número de APs.

Gateways empresariais são atualizados através de TFTP, da mesma maneira que muitos roteadores e switches de hoje em dia.

Antenas e Acessórios

Uma antena RF é um dispositivo que converte os sinais de alta freqüência (RF) em um meio de transmissão (um cabo, por exemplo), em ondas eletromagnéticas que se propagam através do ar. Os campos elétricos emitidos das antenas são chamados lóbulos e podemos dividir as antenas em três categorias:

- Omni-direcional;

- Altamente direcional;
- Semi-direcional.

Cada categoria possui vários tipos de antenas, com diferentes características e várias aplicações. À medida que o ganho da antena aumenta, a área coberta fica cada vez mais estreita, de modo que antenas direcionais de alto ganho são capazes de propagar o sinal a distâncias maiores do que antenas de baixo ganho com a mesma potência de entrada.

Omni-direcionais (dipolo)

A antena mais comum é a antena dipolo. Simples de projetar, essa antena está presente na maioria dos APs. A antena dipolo é uma antena omni-direcional, porque irradia a energia igualmente em todas as direções em torno do seu eixo. Antenas dipolo usadas em WLAN são muito pequenas, porque as freqüências em uma WLAN estão no espectro de 2.4 GHz, e à medida que a freqüência aumenta, o comprimento de onda e as antenas se tornam menores.

Uma antena omini-direcional irradia o sinal em um feixe horizontal de 360 graus. Se uma antena irradia em todas as direções igualmente, formando uma esfera, ela é de irradiador isotrópico.

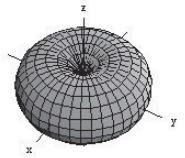

Figura 12.3: Irradiação em 3D de uma antena omni-direcional.

O sol é um bom exemplo disso. Porém, um irradiador isotrópico, quando nos referimos a antenas, só existe na teoria. Na prática, toda antena tem algum tipo de ganho em relação a um radiador isotrópico. À medida que aumentamos o ganho de uma antena, é como se achatássemos o seu lóbulo de radiação, transformando-o de uma esfera para uma elipse cada vez mais estreita. Embora um dipolo irradie uniformemente em todas as direções em torno do seu eixo, ele não irradia ao longo do comprimento do seu próprio fio.

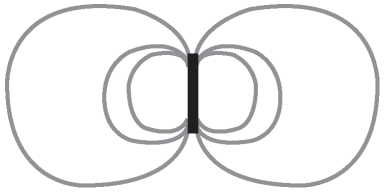

Figura 12.4: Irradiação em 2D de uma antena dipolo.

Se um dipolo é colocado no centro de um andar de um prédio, grande parte da energia será irradiada ao longo do andar, com uma fração significativa enviada para os andares acima e abaixo do Ponto de Acesso.

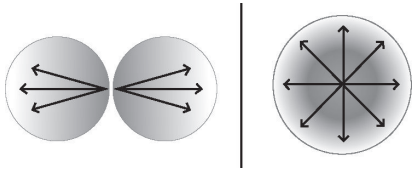

Figura 12.5: Vista lateral e superior do diagrama de irradiação de uma antena omni-direcional.

Antenas omni-direcionais de alto ganho oferecem maior área de cobertura horizontal, mas a área de cobertura vertical sofre uma redução. Essa característica se torna uma consideração importante quando a antena está localizada no teto de uma sala, por exemplo. Se o teto for muito alto, a área de cobertura não alcançará o chão, onde os usuários estão localizados.

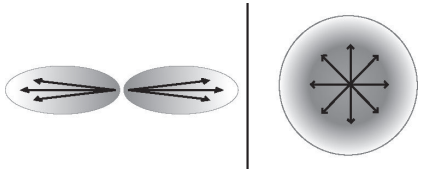

Figura 12.6: Vista lateral e superior do diagrama de irradiação de uma antena omni-direcional de alto ganho.

Aplicação

Antenas omni-direcionais são usadas quando a cobertura em todas as direções em torno do seu eixo horizontal é necessária. São mais úteis onde grandes áreas de cobertura em torno de um ponto central não são necessárias. Por exemplo, colocar uma antena omni no meio de uma grande sala proporcionará boa cobertura. Quando forem usadas externamente, deverão ser colocadas no topo de uma estrutura (um prédio, por exemplo), no centro da área de cobertura. Quando forem usadas internamente, deverão ser colocadas no teto e no meio de uma sala, por exemplo. São também comumente usadas em projetos ponto-multiponto.

Capítulo 13

Antenas semi-direcionais

Essas antenas concentram de forma significativa a energia do transmissor em uma determinada direção. Diferentemente das antenas omni, que possuem um diagrama de radiação circular e uniforme em várias direções, as antenas semi-direcionais possuem um diagrama de irradiação na forma hemisférica ou cilíndrica.

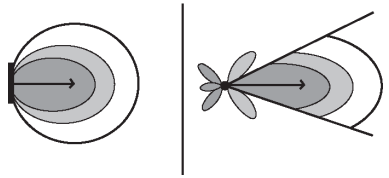

Figura 13.1: Diagrama de irradiação horizontal e vertical de uma antena semi-direcional.

Existem vários tipos de antenas semi-direcionais, mas os freqüentemente mais usados em WLAN são: Patch, Painel e Yagi. Todas essas antenas são planas, possuem diferentes características e são projetadas para montagem em superfícies planas, como paredes ou muros.

Figura 13.2: Tipos de antenas semi-direcionais, da esquerda para direita: Yagi, Patch e Painel

Aplicação

Antenas semi-direcionais são ideais em situações em que desejamos interligar duas redes distintas, localizadas em prédios diferentes separados por uma curta distância em um link ponto a ponto.

Muitas vezes, em um site survey indoor, é comum avaliar qual o melhor local para colocar antenas omni-direcionais em um prédio, por exemplo. Porém, em alguns casos, antenas semi-direcionais podem se tornar uma solução de melhor custo-benefício, eliminando a necessidade de um número alto de Pontos de Acesso se comparados com a solução de usar antenas omni-direcionais. Normalmente elas possuem lóbulos laterais e traseiros que, se usados de forma efetiva, podem reduzir ainda mais a necessidade de Pontos de Acesso adicionais.

Figura 13.3: Link ponto a ponto usando antenas semi-direcionais.

Antenas Altamente Direcionais

Essas antenas, como o próprio nome diz, emitem o cone mais estreito de irradiação de todas as antenas, além de possuir o ganho mais alto de todos os três grupos.

São tipicamente côncavas e alguns modelos se assemelham a antenas de satélite, porém menores. Outros modelos são chamados de grade, devido a seu design perfurado para resistir a ventos fortes.

Figura 13.4: Antena parabólica.

Figura 13.5: Antena grade.

Aplicação

Em virtude do seu estreito cone de irradiação, essas antenas não possuem uma área de cobertura que possa ser usada por usuários, em vez disso, são ideais para links de comunicação ponto a ponto de longa distância e podem transmitir a uma distância de até 20 km. Devem ser cuidadosamente alinhadas uma com a outra para que haja boa recepção de sinal devido a seu feixe estreito. Seu uso potencial é na conexão de dois prédios separados por quiilômetros, sem nenhuma obstrução no caminho do feixe de irradiação. Como o feixe é extremamente estreito, a probabilidade da existência de

um obstáculo que possa interferir de forma significativa no sinal é bem menor se comparada com os outros tipos de antenas. Essas antenas ainda podem ser apontadas uma para outra dentro de um prédio com o intuito de passar por obstruções, conctando lugares que não podem ser cabeados e onde redes wireless comuns não são capazes de operar.

Figura 13.6: Feixe de irradiação de uma antena altamente direcional.

Conceitos de RF

Existem diversos conceitos cujo entendimento é essencial para implementação de soluções que necessitam de uma antena de RF. São eles:

- Polarização;
- Ganho;
- Largura de feixe (BW);
- Perda em espaço livre.

Esses conceitos não são todos os existentes, mas são essenciais para entendermos como um equipamento WLAN funciona em um meio wireless.

Saber onde colocar as antenas, como posicioná-las, qual a potência que elas vão irradiar, a distância que essa potência irradiada vai percorrer e quanto dessa potência chegará até o receptor é a parte mais complexa, porém necessária, no projeto.

Polarização

Uma onda de rádio possui dois campos: um elétrico e outro magnético. Esses campos estão em planos perpendiculares um ao outro. À soma dos dois campos chamamos de campo elétrico-magnético; e a energia é transferida continuamente entre os dois campos em um processo conhecido como oscilação. O plano paralelo ao elemento da antena é chamado Plano-E, enquanto o plano perpendicular ao elemento é chamado Plano-H.

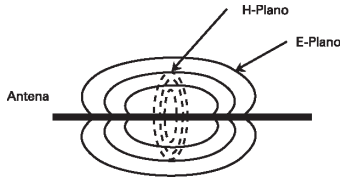

Figura 13.7: Campos elétrico e magnético de um dipolo.

Nós estamos interessados no campo elétrico, uma vez que sua posição e direção em relação à superfície da terra determinam a polarização da onda.

Polarização nada mais é que a orientação do campo elétrico de uma onda de rádio em relação à terra ou à direção de propagação. É determinada pela estrutura física da antena e por sua orientação. O campo elétrico é paralelo ao elemento de radiação de forma que, se a antena for vertical, a polarização será vertical. Na polarização vertical o campo elétrico está perpendicular à terra e, na polarização horizontal, o campo elétrico está paralelo à terra.

A polarização vertical é a mais usada em WLANs. Para que não haja perda significativa de sinal, as antenas transmissora e receptora devem ser polarizadas da mesma forma, isto é, ambas verticalmente ou ambas horizontalmente. A polarização normalmente é elíptica, significando que a antena varia conforme a polarização da onda de rádio que transmite ao longo do tempo.

As polarizações vertical e a horizontal são tipos de polarização linear. Na polarização linear, a elipse mencionada se situa ao longo de uma linha. Existe um outro tipo de polarização menos utilizado, chamado de polarização circular. Nesse tipo de antena, a orientação do campo elétrico varia continuamente em relação à terra.

Ganho

O ganho de uma antena é expresso em dBi, que significa decibéis em relação a um irradiador isotrópico. Como vimos anteriormente, um irradiador isotrópico é uma esfera que irradia igual potência em todas as direções ao mesmo tempo, mas na prática não pode ser implementado. Por outro lado, existem as antenas omni-direcionais,

que irradiam potência em 360 graus horizontalmente, mas não irradiam 360 graus verticalmente. Dessa forma, a radiação RF apresenta o formato de uma rosca. Quanto mais apertamos essa rosca, mais ela se assemelha a uma panqueca. Esse é o efeito do aumento do ganho na radiação da antena.

Quanto maior o ganho da antena, mais estreito é o feixe de radiação e mais longe conseguiremos levar o sinal, de forma que mais potência é entregue ao destino em longas distâncias.

Largura de feixe (BW)

Como discutimos anteriormente, o estreitamento do feixe de irradiação da antena aumenta o seu ganho. Largura de feixe, como o próprio nome diz, nada mais é que a largura do feixe do sinal RF que a antena transmite.

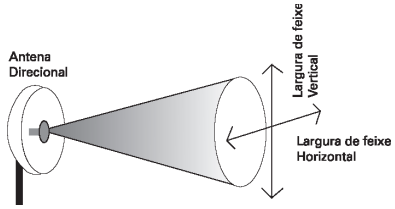

Figura 13.8: Largura de feixe horizontal e vertical de uma antena direcional.

Há dois fatores a se considerar quando falamos de largura de feixe. Tanto a largura de feixe vertical, perpendicular à terra, como a largura de feixe horizontal, paralela à terra, são medidas em graus. Isso é importante para entendermos as diferentes larguras de feixe de vários tipos de antenas. Veja a tabela seguinte:

Tipo de Antena	BW Horizontal (graus)	BW Vertical (graus)
Omni-direcional	360	7 – 80
Patch/ Painel	30-180	6 – 90
Yagi	30-78	14 – 64
Parabólica	4-25	4 – 21

Tabela 13.1.

Selecionar uma antena com largura de feixe apropriada é essencial para implementação da área de cobertura desejada. Por exemplo, imagine um longo corredor em um hospital. Há diversas salas em ambos os lados do corredor e, em vez de usar diversos APs com antenas omni, você decide usar um único AP com uma antena semi-direcional, uma antena Patch.

O AP e a antena são colocados no final do corredor. Para uma cobertura completa imediatamente acima e abaixo desse andar, uma antena Patch poderia ser escolhida, já que possui um BW vertical bem larga, em torno de 60 a 90 graus. Após alguns testes, verificamos que uma antena Patch com 80 graus fará bem o trabalho.

Para decidirmos sobre o BW horizontal, devido ao comprimento do corredor, um estudo revela que uma antena Patch de alto ganho será necessária para fazer o sinal chegar ao lado oposto. Porém, antenas de alto ganho possuem uma largura de feixe muito estreita, de forma que os quartos de ambos os lados do corredor não terão cobertura adequada. Além disso, antenas de alto ganho não terão BW vertical com largura suficiente para cobrir os andares superior e inferior. Logo, a melhor solução será usar duas antenas Patch de baixo ganho em ambas as extremidades do corredor, com dois Pontos de Acesso. Dessa forma os quartos de ambos os lados do corredor terão cobertura adequada, assim como os andares acima e abaixo.

Por esse pequeno exemplo pode-se perceber claramente a importância do BW na determinação do número de APs necessários para uma instalação.

Capítulo 14

Perda em espaço livre

Perda em espaço livre, ou simplesmente perda no meio, refere-se à perda incutida a um sinal RF devido à dispersão do sinal, o que é um fenômeno natural.

À medida que o sinal transmitido atravessa a atmosfera, o nível de potência diminui em uma razão inversamente proporcional à distância percorrida, e proporcional ao comprimento de onda do sinal. O nível de potência se torna portanto um fator muito importante quando analisamos a viabilidade de um link.

A equação de perda no meio é essencial ao cálculo de orçamento de link. Representa a maior fonte de perda em um sistema wireless.

$$PathLoss = 20LOG_{10}\left[\frac{4\pi d}{\lambda}\right]\{dB\}$$

A análise da equação anterior pode ser traduzida em uma relação muito útil quando lidamos com orçamentos de link. Cada aumento de 6 dB na EIRP é igual ao dobro da distância. Cada redução de 6 dB na EIRP resulta na redução da distância pela metade. A tabela seguinte oferece uma estimativa da perda do meio para determinadas distâncias entre transmissor e receptor em 2.4 GHz:

Distância (m)	Perda (dB)
100	80.23
200	86.25
500	94.21
1000	100.23
2000	106.25
5000	114.21
10000	120.23

Tabela 14.1.

Dispositivos POE

Power over Internet (POE) é um método utilizado para entregar voltagem DC a APs ou bridges através de cabo UTP CAT5. O cabo UTP, nesse caso, transporta tanto dados como a voltagem DC para energizar o dispositivo. POE é muito útil em situações em que no local em que o dispositivo está instalado não há tomadas de eletricidade para alimentá-lo.

Considere uma situação em que é necessário instalar um Ponto de Acesso no teto de um prédio e não há tomadas de AC disponíveis. O custo de instalar tomadas AC no teto só para o propósito de energizar o Ponto de Acesso seria dispendioso, e a contratação de um eletricista para fazer esse tipo de trabalho sairia caro e consumiria muito tempo. Nunca é demais lembrar que cabos UTP CAT5 só são capazes de transportar dados de forma confiável a uma distância máxima de 100 metros. Logo, essa é uma limitação para o uso do POE.

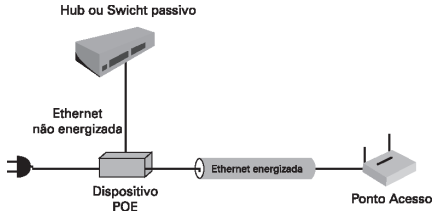

Figura 14.1: Modo de ligação de um dispositivo POE.

Existem diversos tipos de dispositivos POE:

- Injetores de porta única;
- Injetores multiporta;
- Switches Ethernet projetados para injetar voltagem DC em cada porta de um dado par de pinos.

Embora não haja qualquer necessidade de configuração e gerenciamento de um dispositivo POE, há alguns fatores que devem ser levados em consideração e que são de suma importância:

- Não há um padrão na indústria para dispositivos POE. Ou seja, cada fabricante tem a sua própria implementação, o que forçosamente nos leva a usar um POE e um AP do mesmo fabricante para evitar que tenhamos problemas;
- A tensão de saída usada para alimentar o dispositivo WLAN varia de fabricante para fabricante, o que é mais um motivo para usarmos AP e POE do mesmo fabricante;
- Os pinos não usados para carregar a voltagem DC também variam de fabricante para fabricante. Enquanto uns usam os pinos quatro e cinco para isso, outros usam os pinos sete e oito. Se conectarmos um cabo que carregue voltagem DC nos pinos quatro e cinco a um AP que não aceita voltagem DC nesses pinos, este não ligará.

Existem dispositivos que são compatíveis com POE e outros que não são. Os que são permitem receber voltagem DC através da sua porta RJ45, e podem ser ligados diretamente ao injetor. Os que não são precisam de um conversor DC (normalmente chamados de splitters) para serem ligados ao injetor.

Logo, para usar POE é necessário:

(injetor) + (dispositivo compatível POE);

ou

(injetor) + (dispositivo não compatível com POE) + (conversor).

Esse conversor leva a voltagem DC inserida no CAT5 ao equipamento por meio de uma tomada comum; ele pode ser de dois tipos: passivo e regulado.

O passivo simplesmente leva a voltagem do cabo CAT5 ao equipamento por meio de uma conexão direta. Se 48 VDC for injetado pelo injetor, 48 VDC será produzido na saída do conversor.

O regulador converte a voltagem do cabo CAT5 em outra voltagem. Dessa forma, diversos dispositivos não compatíveis com POE podem ser alimentados.

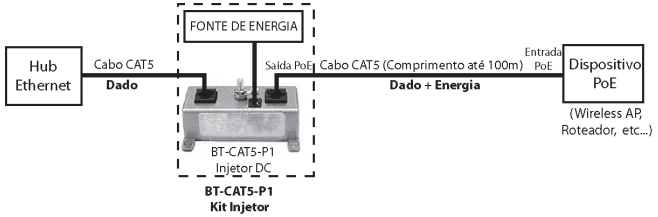

Figura 14.2: Modo de ligação de um injetor DC a um dispositivo POE.

Injetores de porta única

APs e bridges incluem um injetor de voltagem DC porta única através da sua porta RJ45 para energizar a unidade. Esses injetores são comumente usados com um pequeno número de dispositivos WLAN, mas se tornam um desordenado conjunto de fiação quando usados em redes WLAN maiores.

Figura 14.3: Injetor de porta única.

Injetores multiporta

Esses injetores são mais econômicos e convenientes para instalações maiores, em que vários dispositivos WLAN precisam ser energizados através de CAT5, originando um conjunto simples de fiação. Eles operam da mesma maneira que os de porta única e se assemelham a switches Ethernet. São mais apropriados para redes wireless de tamanho médio, com até 50 Pontos de Acesso.

Diversos fabricantes oferecem injetores multiportas, incluindo modelos de 4, 6 e 12 portas.

Figura 14.4: Injetor multiporta.

Switches Ethernet Ativos

Para implementação de APs em larga escala é necessário um switch Ethernet ativo. Esses dispositivos incorporam a injeção de voltagem DC dentro do próprio switch, permitindo a conexão de um grande número de dispositivos POE sem necessidade de hardware adicional.

Diversos fabricantes oferecem esses switches com diferentes configurações (número de portas). Em muitos switches ativos, os clientes POE podem ser detectados na rede. Se o switch não detecta o dispositivo POE, ele desliga a voltagem DC para aquela porta. Olhando externamente para um switch ativo, não difere de um switch comum. A única diferença é o acréscimo da funcionalidade interna, que fornece voltagem DC em cada porta.

Figura 14.5: Switch Ethernet ativo.

Tolerância a Falhas

O propósito principal de proteção a falhas é proteger o cabo, o equipamento e a fonte de energia em situações de falha ou curto-circuito. Em situações normais, uma falha nunca deve ocorrer em um cabo CAT5, porém há diversas formas de uma falha ser introduzida em um cabo CAT5, incluindo os seguintes exemplos:

- O dispositivo é compatível com POE e tem uma conexão defeituosa, que causa curto-circuito nas entradas POE. Até o momento, muitos dispositivos que não são compatíveis com POE não têm conexão nos pinos POE;
- Crimpagem do cabo CAT5 incorreto. Situações em que o isolamento em um ou mais condutores entra em contato com os demais.

Durante qualquer condição de falha, o circuito de proteção corta a voltagem DC injetada no cabo. A operação desses circuitos varia de modelo para modelo. Alguns modelos monitoram constantemente o cabo e restauram a energia quando a condição de falha é removida. Alguns modelos devem ser reiniciados com o botão Reset.

Capítulo 15

Acessórios WLAN

Quando chegar a hora de conectar todos os dispositivos de sua WLAN, será necessário comprar os cabos e assessórios que vão maximizar a performance, reduzir a perda de sinal e permitir fazer as conexões de forma correta. Discutiremos a seguir os acessórios que normalmente fazem parte de uma WLAN bem-sucedida e como eles se encaixam em um projeto. Alguns itens são obrigatórios, outros, opcionais. É bem provável que seja necessário instalar e usar todos esses itens mais de uma vez em uma WLAN.

- Amplificadores RF;
- Atenuadores RF;
- Centelhadores;
- Conectores RF;
- Cabos RF;
- Splitters RF;
- Filtros RF.

Amplificadores RF

Como o próprio nome indica, amplificadores são usados para amplificar (aumentar a amplitude) de um sinal RF, para compensar as perdas sofridas por ele, quer pela longa distância entre as antenas quer pelo comprimento do cabo RF, até chegar à antena. Normalmente esses amplificadores são energizados através de um sinal DC gerado por um injetor DC, que geralmente fica próximo ao Ponto de Acesso, e esse injetor, por sua vez, é energizado com a tensão AC de uma tomada comum. O cabo RF é responsável por transportar tanto esse sinal DC até o ponto de acesso como o sinal RF.

Figura 15.1: Amplificador RF típico.

Figura 15.2: Amplificador RF montado entre o Ponto de Acesso e a antena.

Existem dois tipos de amplificadores: os unidirecionais e os bidirecionais.

Os unidirecionais amplificam o sinal da transmissão antes de ele chegar até a antena, compensando as perdas causadas pelo comprimento do cabo RF.

Os bidirecionais amplificam o sinal na recepção antes de ele chegar ao dispositivo WLAN, compensando dessa forma as perdas causadas pela distância entre as antenas e aumentando a sensibilidade do sinal recebido pelo cliente.

Os amplificadores podem ser ainda indoors e outdoors.

Os indoors são projetados para ficar em um local fechado, próximos ao Ponto de Acesso, já os outdoors são projetados para ficar expostos ao tempo e são de material muito resistente. Eles são montados no mastro da antena e precisam de um injetor DC.

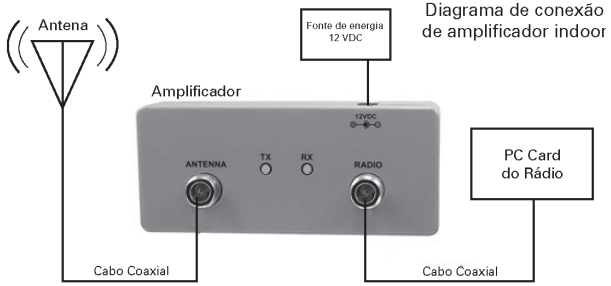

Figura 15.3: Esquema de ligação de um amplificador indoor.

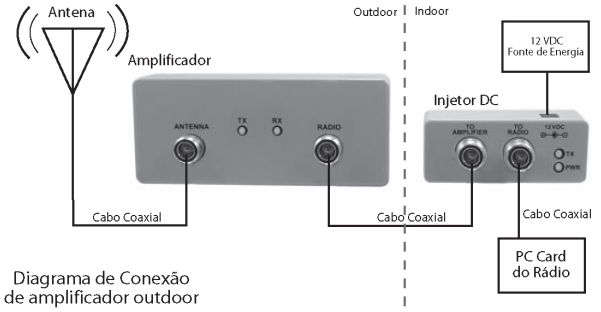

Figura 15.4: Esquema de ligação de um amplificador outdoor. Observe a presença de um injetor DC.

Opções comuns

Dentro de cada tipo, os amplificadores se dividem ainda em ganho fixo e ganho variável. Os de ganho fixo oferecem uma quantidade fixa de ganho para o sinal RF, enquanto os de ganho variável permitem ter seu ganho ajustado manualmente conforme as necessidades. Para escolher qual amplificador comprar para a sua WLAN, existem algumas variáveis que o ajudarão a decidir.

Antes de mais nada, é preciso saber as especificações do amplificador. Uma vez conhecidas as especificações de impedância (Ohms), ganho (dB), freqüência de operação (GHz), VSWR, entrada (mW ou dBm) e saída (mw ou dBm), estaremos prontos para escolher o amplificador.

- A freqüência de operação é o primeiro critério a escolher. Se a WLAN opera na faixa de 2.4 GHz, um amplificador de 5 GHz não funcionará;
- É preciso calcular quanto de potência de entrada, de saída e de ganho será necessária;
- O amplificador deve ter uma impedância igual a todos os demais componentes de hardware WLAN entre o transmissor e a antena para evitar as perdas oriundas do não casamento de impedâncias;
- Os conectores que vão conectar o amplificador ao restante da rede devem ser do mesmo tipo que os conectores dos cabos e da antena. Normalmente, amplificadores usam conectores SMA e tipo N.

Configuração e gerenciamento

Amplificadores RF normalmente são instalados em série entre o Ponto de Acesso e a antena. A configuração de um amplificador só é necessária caso ele seja de ganho variável. Nesse caso, o amplificador deve ser configurado com a quantidade de ganho necessária, de acordo com os cálculos matemáticos de RF. O manual do fabricante vai explicar como fazer essa configuração.

Apesar de a possibilidade de ajustar manualmente o ganho de um amplificador RF ser uma vantagem devido à flexibilidade, amplificadores de ganho variável não são recomendados. Isso porque os parâmetros podem ser alterados devido a problemas no amplificador, por exemplo, danificando a antena ou violando as regras do FCC no que diz respeito à potência de saída para as bandas ISM ou UNII. Amplificadores de ganho fixo são mais recomendados, e

os cálculos de RF devem ser feitos para garantir que o sinal esteja dentro dos limites permitidos pelo FCC. Somente após os cálculos estarem completos e a quantidade de amplificação ser conhecida, o amplificador pode ser comprado.

Os amplificadores devem vir com um certificado e relatório de calibração. Devem, inclusive, ser calibrados uma vez por ano para garantir sua performance e operação.

O problema da relação sinal–ruído (S/N)

A amplificação introduzida em um sinal RF é a grande razão de ser de um amplificador RF, porém essa amplificação não é de graça. Existe um grande ônus na utilização de amplificadores, que é o aumento de ruído do sinal original. Vimos anteriormente que todo sinal RF tem uma quantidade de ruído, seja qual for. O amplificador portanto amplificará o sinal e também o ruído que faz parte dele, além de introduzir mais uma parcela de ruído ao sinal RF original.

Amplificadores POE

Existem amplificadores que são compatíveis com POE. Eles possuem uma interface POE embutida, o que permite ao amplificador ser energizado através de um cabo CAT5. Essa característica simplifica muito a instalação. A figura seguinte mostra um esquema de ligação típico:

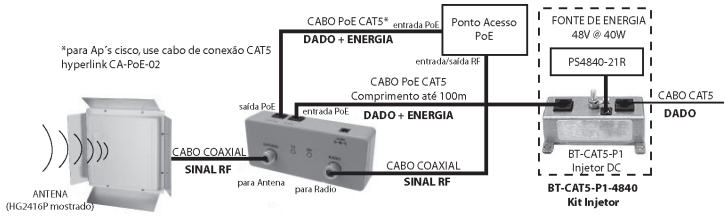

Figura 15.5: Esquema de ligação de um amplificador POE.

Atenuadores RF

Um atenuador é um dispositivo usado para reduzir a amplitude de um sinal RF. Se a função de um amplificador é amplificar o sinal, a do atenuador é reduzir o sinal. É utilizado em situações em que é necessário reduzir o sinal para não violar as regras do FCC. Imagine que temos um AP com uma potência de saída de 100 mW e uma antena com ganho de 20 dBi. O uso desses equipamentos juntos violaria as regras do FCC; portanto, precisaríamos de um atenuador para reduzir o sinal para 30 mW antes de este chegar à antena, ficando assim dentro das regras do FCC.

Os atenuadores podem ser de perda fixa ou perda variável. As figuras a seguir ilustram os dois tipos:

Figura 15.6: Atenuador de perda fixa com conector BNC.

Figura 15.7: Atenuador de perda fixa com conector SMA.

Figura 15.8: Atenuador de perda variável.

Da mesma forma que os amplificadores, atenuadores de perda variável permitem o ajuste manual da perda e, pelos mesmos motivos dos amplificadores de ganho variável, não são recomendados.

Para escolha dos atenuadores, devemos considerar os mesmos fatores abordados quando falamos de amplificadores.

Atenuadores coaxiais são conectados diretamente entre dois pontos de conexão quaisquer que estejam entre o transmissor e a antena.

A configuração de atenuadores RF só é necessária para o caso de uso de atenuadores de perda variável.

Da mesma forma que os amplificadores, os atenuadores devem vir com um certificado e relatório de calibração. Devem também ser calibrados uma vez por ano para garantir a performance e a operação.

Capítulo 16

Centelhadores e splitters

Centelhadores

Um centelhador tem a finalidade de desviar a corrente transiente, causada por raios, para a terra. Dessa forma, eles protegem os equipamentos WLAN que estão ligados ao cabo coaxial. Cabos coaxiais são suscetíveis a surtos causados por descargas em objetos próximos. É um erro pensar que centelhadores são instalados para proteger contra descargas diretas. Se um raio atingir a antena com o melhor centelhador do mercado instalado, a antena será destruída e provavelmente a WLAN será seriamente danificada.

Um centelhador pode redirecionar correntes de até 5.000 ampéres em no máximo 50 volts.

Eis como o protetor funciona:

1. Um raio atinge um objeto próximo.

2. Correntes transientes são induzidas na antena ou na linha de transmissão RF.

3. O protetor detecta essas correntes e imediatamente ioniza os gases manipulados internamente para causar um curto (um meio de quase nenhuma resistência) diretamente para a terra.

A **Figura 16.1** mostra um centelhador instalado em uma rede. Quando um objeto próximo é atingido por um raio, um campo elétrico é formado em torno desse objeto por alguns instantes. Quando a ação do raio cessa, o campo elétrico sofre um colapso, o que por sua vez induz altas correntes em objetos próximos, que no caso ilustrado representa a antena ou a linha de transmissão.

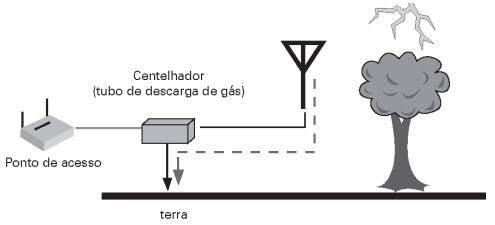

Figura 16.1: Centelhador instalado em uma WLAN.

Há poucas opções em um centelhador e o custo gira em torno de R$ 50,00 a R$ 100,00. Porém, há algumas características que devem ser consideradas para qualquer centelhador:

- Deve estar de acordo com as especificações do IEEE, com tempo menor de oito microssegundos;
- Reutilizável;
- Tensão limiar;
- Tipos de conector;
- Resposta de freqüência;
- Impedância;
- Perda de inserção;
- VSWR;
- Garantia.

Padrões IEEE

Muitos centelhadores são capazes de fechar um curto para a terra em um tempo abaixo de dois microssegundos, mas o IEEE especifica que esse processo deve ocorrer em um tempo menor de oito microssegundos. Resumindo, é muito importante que o centelhador escolhido esteja de acordo com as especificações do IEEE.

Reutilização

Alguns centelhadores são reutilizáveis enquanto outros não são. Os reutilizáveis têm uma relação custo *versus* benefício favorável porque podem ser usados várias vezes. Basta reaplicar os elementos do tubo de gás, solução mais barata do que comprar outro centelhador novo. Outra vantagem dos reutilizáveis é que o gás pode ser substituído sem precisar parar a rede.

Tensão limiar

Determinados centelhadores suportam a passagem de tensão DC para energizar os amplificadores DC. O limiar da tensão do tubo de gás (a tensão na qual o centelhador começa a desviar corrente para a terra) deve ser maior do que a tensão necessária para operar os amplificadores. É altamente recomendado que o centelhador seja

colocado como o último componente na linha de transmissão RF antes da antena, de modo que amplificadores e atenuadores, além dos Pontos de Acesso e pontes, sejam protegidos.

Tipos de conector

Os conectores devem ser do mesmo tipo daqueles usados no cabo, do contrário será necessário o uso de adaptadores, e mais perda será inserida no circuito por conta disso.

A resposta de freqüência deve ser maior que a freqüência mais alta da WLAN. Se a WLAN opera a 2.4 GHz, um centelhador de 3 GHz está de bom tamanho.

Impedância

A impedância deve se igualar à utilizada por todos os dispositivos na WLAN entre o transmissor e a antena. Normalmente essa impedância é 50 Ohms.

Perda de inserção

A perda de inserção é a perda causada pelo próprio centelhador quando o sinal passa por ele; não deve ser maior que 0.1 dB.

Taxa VSWR

A taxa de VWSR de um centelhador de qualidade está em torno de 1.1:1, embora alguns tenham 1.5:1. Quanto menor a taxa do dispositivo, melhor; isso evita que reflexões no cabo degradem significativamente o sinal RF.

Garantia

Independentemente da qualidade de um centelhador, ele não está livre de sofrer problemas. Procure os que oferecem uma boa garantia.

Splitters RF

Um splitter é um dispositivo que possui uma entrada e várias saídas e sua finalidade é dividir o sinal principal em vários sinais inde-

pendentes, atuando dessa forma como um divisor de potência. Uma situação que ilustra bem o uso de splitters é quando se deseja uma cobertura bidirecional em uma determinada área. Para isso, usamos duas antenas painel, uma de 120 graus e outra de 90 graus, apontando em direções opostas, montadas no mesmo mastro com um splitter e com o mesmo comprimento de cabo para ambas. O ônus dessa configuração é a perda do ganho resultante para algo em torno de 3 a 4 dB. Ao adquirir um splitter o que vai diferenciar um do outro é o número de vias (saídas) que ele possui.

Figura 16.2: Um splitter típico de três vias.

Figura 16.3: Splitter instalado em uma WLAN com antenas Painel.

Figura 16.4: Splitter visto em detalhes.

Como todos os outros acessórios, existem diversos fatores a se considerar quando da aquisição de um splitter. Vejamos apenas os mais importantes.

Perda de inserção

Baixa perda de inserção (perda incutida dentro do circuito pela inserção do item) é necessária porque um splitter pode causar uma redução significativa na amplitude de um sinal RF. Uma perda de inserção menor ou igual a 0.5 dB é considerada boa para um splitter.

Taxa VSWR

Da mesma forma que outros dispositivos, a taxa VSWR de um splitter deve ser a mais próxima possível de 1.1:1. Normalmente, a taxa VSWR de um splitter é menor que 1.5:1. Esse parâmetro é muito crítico para um splitter, porque a potência pode ser refletida em várias direções, afetando o splitter, o sinal de entrada e todos os sinais de saída.

Alta impedância

A alta impedância de isolamento entre as portas de um splitter é muito importante, por causa das seguintes razões:

- A carga em uma das portas de saída não afeta a potência de saída nas outras portas;
- O sinal de recepção em uma porta de saída deve ser direcionado para a porta de entrada em vez de ser direcionado para outra porta de saída.

Tudo isso só é possível por causa da impedância de isolamento existente entre os conectores de um splitter. Um isolamento típico fica em torno de 20 dB ou mais entre as portas.

Alguns modelos possuem uma característica conhecida como isolamento de porta reversa. Isso permite que as portas de saída sejam usadas como entradas. Usar o splitter dessa forma permite a conexão de dois ou três Pontos de Acesso ou pontes alimentando uma única antena, e dessa forma economiza dinheiro na compra e instalação de antenas adicionais.

Taxas de potência

Splitters são categorizados pela potência máxima de entrada que pode ser aplicada sobre eles. Exceder a especificação do fabricante resultará na queima do splitter.

Tipos de conector

Splitters geralmente possuem conector tipo N ou SMA. É de suma importância comprar um splitter com o mesmo tipo de conector dos cabos utilizados, uma vez que splitters reduzem a amplitude do sinal RF.

Passagem de voltagem DC

Alguns splitters têm a opção de passagem de voltagem DC para todas as portas de saída em paralelo. Essa característica é útil quando há amplificadores RF que energizam os circuitos internos com voltagem DC, originada de um injetor DC localizado na saída de cada porta de saída do splitter.

Observação: se algumas saídas do splitter não forem utilizadas, terminadores de 50 Ohms devem ser usados nessas saídas.

Capítulo 17

Filtros, conectores e cabos

Filtros RF

Um caso muito comum em WLANs é a interferência causada por outras fontes de transmissão próximas ao canal que se está transmitindo. Isso reduz a performance e confunde o receptor. Para evitar que isso aconteça existe o filtro RF. Ele permite a passagem apenas do canal que se está transmitindo ou recebendo, reduzindo assim a interferência dos sinais fora do seu canal. Essa característica do filtro RF favorece o uso de equipamentos próximos em uma mesma célula, por exemplo, o uso de três Pontos de Acesso.

Porém ele não reduz a interferência no canal causada por outros sinais e por usuários transmitindo no mesmo canal.

Opções comuns

Os filtros RF são classificados por pólos, podem ser indoor ou outdoor, e podem operar como canal fixo ou banda cheia.

Cada pólo representa um circuito de filtragem, assim, quanto mais pólos possuir o filtro, mais filtragem ele fará nos sinais interferentes. Existem modelos de quatro pólos, recomendados para filtrar sinais interferentes fracos, e os modelos de oito pólos, recomendados para zonas mais densas, com sinais RF fortes.

Podem ser indoor, para serem instalados em caixas fechadas, ou outdoor, próprios para ficarem expostos ao tempo e serem montados no mastro da antena.

Filtros RF de canal fixo filtram um canal específico e atuam dentro da banda; já os de banda cheia reduzem a interferência apenas de canais fora da banda.

Figura 17.1: Filtro indoor.

Figura 17.2: Filtro outdoor.

Ao adquirir um filtro RF, o que vai determinar a escolha por um de canal fixo ou um de banda cheia é onde queremos atuar. Se desejamos filtrar canais dentro da banda, devemos optar por um de canal fixo; se, por outro lado, desejamos filtrar canais fora da banda, devemos optar por um de banda cheia. Devemos estar atentos também às especificações de perda de inserção e impedância.

Conectores RF

Conectores são usados para conectar cabos a dispositivos ou dispositivos a dispositivos. Tradicionalmente, os tipos N, F, SMA, BNC e TNC têm sido usados em WLANs. Em 1994, o FCC e o DOC determinaram que os conectores para uso em WLANs devem ser proprietários, e por essa razão existem muitas variações de cada tipo, tais como: Tipo N, Tipo N polaridade reversa, Tipo N polaridade direta.

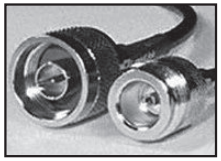

Figura 17.3: Conector N.

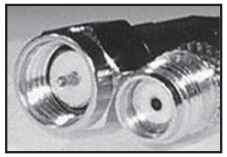

Figura 17.4: Conector SMA.

Há diversos fatores a serem considerados quando da compra de um conector:

- O conector deve ser de impedância igual a todos os demais dispositivos da WLAN;
- Saber qual a perda de inserção causada pelo conector;
- Saber qual a freqüência mais alta (resposta de freqüência).

Isso é muito importante hoje em dia, uma vez que as WLANs de 5 GHz se tornam cada vez mais comuns. Conectores projetados para operar no máximo com 3 GHz funcionarão bem com WLANs de 2.4 GHz e não funcionarão com WLANs de 5 GHz;

- Ficar atento à qualidade do conector, optando sempre por fabricantes conhecidos. Isso ajuda a evitar problemas conhecidos como VWSR, sinais espúrios e más conexões;
- Certifique-se de qual tipo de conector você precisa e se ele é macho ou fêmea.

Cabos RF

O mesmo critério utilizado na escolha de cabos para um backbone de 10 Gpbs deve ser usado na escolha de um cabo para conectar uma antena a um Ponto de Acesso.

Figura 17.5: Cabo de antena com conectores SMA reverso e tipo N.

- Cabos introduzem perda em uma WLAN, portanto, procure usar cabos que tenham o comprimento estritamente necessário;
- Procure comprar cabos curtos com conectores já crimpados. Isso minimiza o problema de má conexão entre o conector e o cabo. Cabos crimpados por profissionais são, em geral, melhores do que aqueles feitos por indivíduos não treinados;
- Procure por cabos que tenham baixa perda. A perda é expressa por dB/100 metros. Quanto menor a perda, mais caro é o cabo. A tabela seguinte mostra um exemplo para vários tipos de cabo coaxial:

Cabo LMR	9.14	15.24	45.72	67.05	137.16	274.32	457.2	548.64	609.6
100 a	3.9	5.1	8.9	10.9	15.8	22.8	30.1	33.2	35.2
195	2.0	2.6	4.4	5.4	7.8	11.1	14.5	16	16.9
200	1.8	2.3	4	4.8	7	9.9	12.9	14.2	15
240	1.3	1.7	3	3.7	5.3	7.6	9.9	10.9	11.5
300	1.1	1.4	2.4	2.9	4.2	6.1	7.9	8.7	9.2

Tabela 17.1: Taxa de atenuação de cabo coaxial (em dB/metro).

• Compre cabos que tenham a mesma impedância que os demais dispositivos da WLAN (geralmente 50 Ohms);

• A freqüência de resposta do cabo deve ser o fator principal na decisão para aquisição. Com WLANs de 2.4 GHz, um cabo de 2.5 GHz deve ser usado.

Andrew Heliax cable, Times Microwave's LMR e Belden RF series são os cabos mais utilizados em WLANs e são muito populares. Hoje em dia, LMR é sinônimo de cabo, da mesma que Xerox é sinônimo de cópia.

Cabos Pigtail

Cabos Pigtail são usados para conectar cabos com conectores-padrão da indústria a equipamentos de fabricantes WLAN. Adaptam conectores proprietários a conectores padrão tais como tipo N e SMA. Um lado do cabo possui um conector proprietário e o outro lado, um conector-padrão da indústria.

Figura 17.6: Cabo Pigtail.

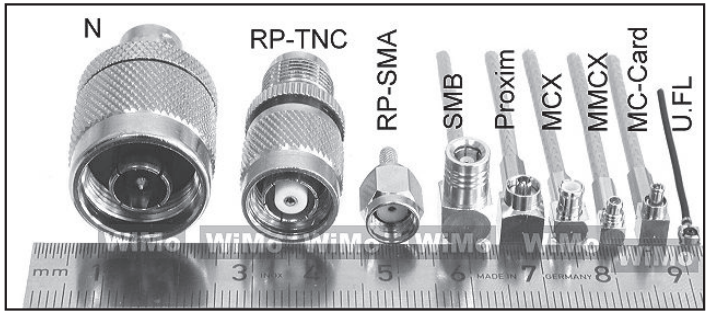

Figura 17.7: Os conectores de ambas as extremidades em detalhes.

Em 23 de junho 1994, o FCC e o DOC regulamentaram que conectores fabricados após essa data devem ser fabricados como conectores de antenas proprietárias. A intenção dessa regulamentação tem dois objetivos:

• Desencorajar o uso de amplificadores, antenas de alto ganho ou qualquer outro dispositivo que possa contribuir para o aumento significativo da radiação RF;

• Desencorajar o uso de sistemas instalados por usuários inexperientes, os quais acidentalmente ou não infringiam as regras do FCC no uso da banda ISM.

Desde então, clientes têm adquirido conectores proprietários dos fabricantes para usar com conectores-padrão da indústria.

Capítulo 18

Organizações e padrões

Muitos hardwares relacionados a computadores e tecnologias são baseados em padrões, e WLANs não são uma exceção a essa regra. Existem organizações que definem e suportam os padrões que permitem a interoperabilidade entre hardware de diferentes fabricantes.

Pelo entendimento das leis e padrões que governam e guiam a tecnologia WLAN, podemos assegurar que qualquer sistema wireless implementado terá interoperabilidade e estará de acordo com as regras.

Federal Communications Commission (FCC)

O FCC é uma agência governamental independente nos Estados Unidos. É responsável por criar as regras dentro das quais dispositivos WLAN devem operar. Determina em que parte do espectro de radiofreqüência as WLANs podem operar e em que potência, usando quais tecnologias de transmissão e como e onde várias peças do hardware podem ser utilizadas.

Para mais detalhes sobre o FCC, acesse: http://www.fcc.gov.

Bandas ISM e UNII

O FCC estabelece regras limitando quais freqüências as WLANs podem usar e a potência de saída em cada uma dessas bandas. O FCC especificou que WLANs podem usar as bandas ISM (industrial, científica e médica), que são bandas não licenciadas.

As bandas ISM estão localizadas começando em 902 MHz, 2.4 GHz e 5.8 GHz e variam na largura em torno de 26 a 150 MHz.

Além das bandas ISM, o FCC especificou três bandas UNII. Cada uma dessas bandas UNII está na faixa dos 5 GHz e tem largura de 100 MHz.

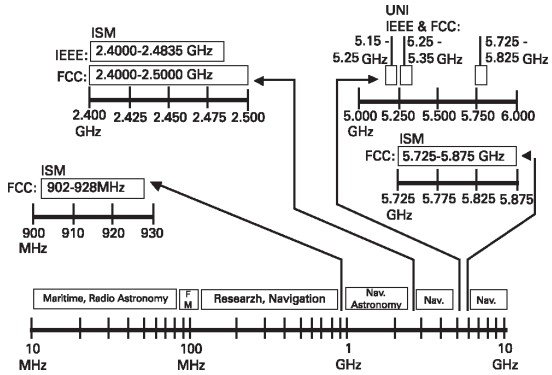

Figura 18.1: Bandas ISM e UNII.

Vantagens e desvantagens das bandas não licenciadas

Na implementação de um sistema wireless não licenciado, não há necessidade de requisição ao FCC no que tange à largura de banda e à necessidade de potência para começar a operar, embora ainda haja limites para a potência de transmissão. Logo, a maior vantagem é a inexistência do custo com licenciamento, o que permite a pequenos negócios implementarem uma WLAN e crescerem de acordo com a necessidade, fomentando ainda mais o crescimento do mercado wireless.

Por outro lado, o fato de a banda ser não licenciada possui também uma desvantagem, já que vários sistemas wireless podem competir na mesma banda e interferirem entre si.

Suponha que você resolva instalar um segmento WLAN na sua casa. Se o seu vizinho resolver fazer o mesmo em sua casa, o sistema dele deve interferir em outros e vice-versa. Se ele usar um sistema de alta potência, isso será suficiente para prejudicar o tráfego do

seu sistema wireless. Os dois sistemas competidores não têm estar necessariamente no mesmo canal, nem tão pouco usar a mesma tecnologia para que isso ocorra.

Bandas ISM

Conforme dito anteriormente, existem três bandas ISM não licenciadas, regulamentadas pelo FCC, que as WLANs podem usar. São as bandas de 900 MHz, 2.4 GHz e 5.8 GHz.

Banda de 900 MHz

É definida na faixa de freqüências de 902 a 928 MHz, com largura de 26 MHz. Embora essa banda tenha sido usada por WLANs, ela tem sido preterida pelas bandas de freqüência mais alta, que possuem maior largura de banda e melhor throughput. Alguns dos dispositivos que usam essa banda são telefones sem fio e câmeras wireless. Organizações que ainda usam essa banda sofrem com o alto custo de reposição (em torno de $800,00) para equipamentos defeituosos e são capazes de transmitir apenas em velocidade de 1 Mbps, enquanto equipamentos 802.11b custam em torno de $100,00 e operam a velocidades de 11 Mbps.

Banda de 2.4 GHz

Essa banda é usada por todos os dispositivos compatíveis com 802.11, 802.11b e 802.11g e é a mais popular das três bandas descritas. A banda é definida na faixa de freqüência de 2.4 a 2.5 GHz, com largura de 100 MHz. Desses 100 MHz entre 2.4 e 2.5 GHz, somente a faixa de 2.4 a 2.485 GHz tem sido usada por dispositivos WLAN. A principal razão para isso é que o FCC especificou potência de saída apenas para essa faixa de freqüências.

Banda de 5.8 GHz

Essa banda é freqüentemente chamada de banda 5 GHz ISM. É definida na faixa de freqüência de 5.725 a 5.875 GHz, com largura de banda de 150 MHz; não é especificada para uso com dispositivos WLAN, o que tende a fazer alguma confusão. Essa banda sobrepõe parte de uma outra banda não licenciada, a 5 GHz UNII, e esta sim é utilizada pelos dispositivos WLAN.

Bandas UNII

As bandas 5 GHz UNII podem ser divididas em três bandas com largura de 100 MHz e são usadas por dispositivos compatíveis com 802.11a. Dentro de cada uma das três bandas há quatro canais DSSS não coincidentes, cada qual separado por 5 MHz. As bandas são as seguintes: inferior, central e superior. O FCC determinou que a banda inferior deve ser usada somente para aplicações indoor, a banda central para uso indoor ou outdoor, e a banda superior somente para uso outdoor.

Como Pontos de Acesso são comumente usados indoor, as bandas de 5 GHz UNII permitem o uso de oito APs indoors em canais não coincidentes, usando as bandas inferior e central.

Banda inferior

A banda inferior vai de 5.15 a 5.25 GHz, e de acordo com o FCC, e pode ter uma potência de saída máxima de 50 mW. Na implementação de dispositivos 802.11a, o IEEE especificou a potência de saída máxima para rádios 802.11a em 40 mW (80%), reservando a banda inferior para uso indoor somente.

Banda central

A banda central vai de 5.25 a 5.35 GHz, de acordo com o FCC, e pode ter uma potência de saída máxima de 250 mW. O IEEE especificou 200 mW para potência de saída. Esse limite de potência permite seu uso tanto para aplicações indoor como outdoor. Normalmente é usado para enlaces outdoor de curta distância envolvendo dois prédios. Para casos de instalações domésticas, tal configuração pode envolver um link de RF entre uma casa e a garagem ou entre duas casas vizinhas. Devido à alta potência de saída e sua flexibilidade quanto ao uso, produtos que operam nessa banda podem ter grande aceitação no futuro.

Banda superior

A banda superior vai de 5.725 a 5.875 GHz e às vezes é confundida com a banda ISM de 5.8 GHz. O FCC limita a potência de saída em 1 W; o IEEE especificou 800 mW para a potência de saída. Seu uso está restrito para aplicações outdoor, exceto em casos de link RF de grande distância.

Regras para a Potência de Saída

O FCC reforça certas regras no que se refere à potência irradiada pela antena, dependendo se a implementação for ponto a ponto (PtP) ou ponto-multiponto (PtMP). O termo usado pela potência irradiada pela antena é o EIRP.

Ponto-Multiponto (PtMP)

Links PtMP possuem um ponto central de conexão e dois ou mais pontos não-centrais, e são tipicamente configurados em uma topologia de hub. O ponto central pode ser ou não uma antena omni-direcional, enquanto os pontos não-centrais normalmente são antenas direcionais. Quando uma antena omni-direcional é usada, o FCC automaticamente considera o link como sendo PtMP. Nesse caso, o FCC limita a EIRP em 4 W nas bandas 2.4 GHz ISM e 5 GHz UNII superior. Além disso, o limite de potência permitido para o dispositivo que transmite o sinal RF, ou seja, o rádio, em cada uma dessas bandas é 1 W. Se a transmissão nos dispositivos WLAN puder ser ajustada quanto à sua potência de saída, então o sistema pode ser customizado para as necessidades do usuário.

Suponha que um rádio com potência de saída de 1 W (+30 dBm) seja conectado a uma antena omni de 12 dBi. Isso resulta em uma EIRP de 16 W ou 42 dBm, o que está muito acima do permitido, que é 4 W ou 36 dBm. O FCC determina que para cada 3 dBi, acima de um ganho inicial da antena de 6 dBi, a potência no rádio deve ser reduzida em 3 dB. Logo, em nosso caso deveríamos reduzir a potência de saída no rádio de 6 dB, já que 42 - 6 = 36, o que resultaria em uma potência de saída de 24 dbm ou 250 mW, e uma EIRP de 4 W ou (24 + 12 = 36 dBm).

A conclusão final a que chegamos é que para estar de acordo com as regras do FCC, que determina uma EIRP máxima de 4 W para links PtMP, o rádio não poderá ter potência de saída superior a 1 W. Também devemos estar atentos à combinação potência que chega na antena *versus* ganho da antena, para não infrigirmos as regras do FCC. Lembrando que a potência que chega até a antena envolve a potência de saída do rádio e as perdas oriundas de conectores, cabos e similares. A tabela seguinte ilustra bem isso:

Potência na antena (dBm)	Ganho da antena (dBi)	EIRP (dBm)	EIRP (W)
30	6	36	4
27	9	36	4
24	12	36	4
21	15	36	4
18	18	36	4
15	21	36	4
12	24	36	4

Tabela 18.1.

Quando antenas omni-direcionais são usadas, essas regras devem ser seguidas, independentemente do link ser PtP ou PtMP.

Ponto a ponto (PtP)

Links Ptp envolvem uma única antena de transmissão direcional e uma única antena de recepção, também direcional. Essas conexões incluem conectividade entre dois prédios ou links similares. Na instalação de um link Ptp, o limite de 4 W desaparece em favor de uma regra bem flexível para o limite de potência. O FCC nesse caso determina que para cada 3 dBi acima do ganho inicial da antena de 6 dBi a potência no rádio deve ser reduzida de 1 dB abaixo da potência inicial de 30 dBm. Voltando ao caso anterior descrito no PtMP, ainda temos uma EIRP de 16 W, mas agora a potência no rádio deve ser reduzida em 2 dB e não mais em 6 dB, como no caso do PtMP. Essa redução resulta em uma potência de saída de 28 dBm (30 – 2 = 28) ou 630 mW, e uma EIRP de 40 dBm (28 + 12 = 40) ou 10 W. Em links Ptp, a potência de saída do rádio ainda é limitada em 1 W, mas o limite da EIRP aumenta com o ganho da antena. Veja a tabela seguinte:

Potência na antena (dBm)	Ganho da antena (dBi)	EIRP (dBm)	EIRP (W)
30	6	36	4
29	9	38	6.3
28	12	40	10
27	15	42	16
26	18	44	25
25	21	46	39.8
24	24	48	63
23	27	50	100
22	30	52	158

Tabela 18.2.

Capítulo 19

IEEE e outras organizações

Institute of Electrical and Eletronics Engineers (IEEE)

O IEEE é o criador de padrões para muitas coisas relacionadas à tecnologia nos Estados Unidos. Ele cria seus padrões dentro das leis criadas pelo FCC e especifica muitos padrões da tecnologia tais como: Ethernet (IEEE 802.3), criptografia com chave pública (IEEE 1363) e WLANs (IEEE 802.11).

Uma de suas missões é desenvolver padrões para operações em WLAN dentro das regras e regulamentações do FCC.

Os quatro padrões principais para WLANs que estão em uso ou na forma rascunho são: 802.11, 802.11b, 802.11a, 802.11g.

Para mais informações, acesse http://www.ieee.org.

IEEE 802.11

O padrão 802.11 foi o primeiro a descrever a operação das WLANs. Ele continha todas as tecnologias de transmissão disponíveis, incluindo DSSS, FHSS e infravermelho (IR).

Esse padrão descreve sistemas DSSS operando a 1 Mbps e 2 Mbps. Logo, um sistema que tenha uma taxa de dados de 1 Mbps, 2 Mbps e 11 Mbps pode ser compatível com um sistema 802.11. Por outro lado, um sistema proprietário que opere em outras taxas de dados, apesar da sua habilidade em operar em 1 e 2 Mbps, não será compatível com um sistema 802.11.

O IEEE 802.11 é um dos dois padrões que descrevem a operação de sistemas FHSS operando em 1 e 2 Mbps. Se um administrador WLAN se depara com um sistema FHSS, ele pode ser tanto compatível com 802.11 como compatível com sistemas Openair.

Existem muitos sistemas FHSS proprietários no mercado, que estendem essa funcionalidade para operar de 3 a-10Mbps. Mas, do mesmo modo que os sistemas DSSS, se um sistema FHSS operar em outras taxas que não sejam 1 e 2 Mbps, ele não conseguirá se comunicar automaticamente com outros dispositivos compatíveis com 802.11.

Produtos compatíveis com 802.11 operam estritamente na banda 2.4 GHz ISM, entre 2.4 e 2.4835 GHz.

IEEE 802.11b

Apesar do sucesso do padrão 802.11, que permitiu a operação de sistemas FHSS e DSSS, a tecnologia evoluiu rapidamente a ponto de superar o padrão criado. Logo após a aprovação e implementação do 802.11, as WLANs estavam trocando dados a 11 Mbps, porém sem um padrão definido para guiar a operação de tais dispositivos, facilitando, portanto, o surgimento de problemas de interoperabilidade e implementação. Como os fabricantes ignoraram muitos dos problemas de implementação, coube ao IEEE criar um novo padrão que satisfizesse a operação de dispositivos WLAN que estavam no mercado.

O IEEE 802.11b é referenciado como possuindo alta taxa de dados e Wi-Fi (wireless fidelity), e especifica sistemas DSSS operando a 1, 2, 5.5 e 11 Mbps. Esse padrão não faz referência a qualquer sistema FHSS. Ele é compatível, por padrão, com sistemas 802.11, o que é muito importante na questão custo *versus* benefício, em casos em que é preciso fazer um upgrade gradativo do hardware 802.11 existente.

Essa característica de baixo custo, juntamente com a alta taxa de dados, fez com que dispositivos 802.11b se tornassem muito populares.

A alta taxa de dados do 802.11b é resultado da substituição da técnica de codificação Barker Code pela CCK, juntamente com uma nova forma de modulação da informação, o QPSK. Isso permitiu enviar grande quantidade de informação no mesmo frame.

Produtos 802.11b operam somente na banda 2.4 GHz ISM.

IEEE 802.11a

O padrão 802.11a descreve a operação de dispositivos WLAN na banda de 5 GHz UNII. Nessa banda, taxas de dados da ordem de 6, 9, 12, 18, 24, 36, 48 e 54 Mbps podem ser alcançadas. A operação dos dispositivos nessa banda os torna automaticamente incompatíveis com os outros dispositivos da série 802.11, pelo simples fato de que sistemas operando na faixa de 5 GHz não podem se comunicar com sistemas operando em 2.4 GHz. Dispositivos usando tecnologia proprietária podem alcançar até mesmo taxas de 108 Mbps, em uma técnica conhecida como dobro de taxa. Mas essas taxas não estão

especificadas no padrão, que prevê apenas taxas de 6, 12 e 24 Mbps. Um dispositivo WLAN deve pelo menos suportar tais taxas na banda UNII para ser compatível com o 802.11a. A grande desvantagem do 802.11a é que, por não ser compatível com os demais padrões anteriores a ele, o custo de upgrade de uma rede baseada no 802.11b, por exemplo, é muito elevado, já que não havia possibilidade de ser feito de forma gradativa e de preservar o custo de investimento inicial. O 802.11a teve uma pequena aceitação no mercado se comparado com o 802.11b, e tende a ser superado em popularidade pelo 802.11g.

IEEE 802.11g

Esse padrão é o mais aceito atualmente no mercado e surgiu da necessidade de juntar o melhor dos dois mundos, as altas taxas do 802.11a com a compatibilidade e o melhor custo *versus* benefício do 802.11b. Operando na banda de 2.4 GHz ISM, o padrão 802.11g hoje se tornou a escolha de dez entre dez usuários que desejam adquirir dispositivos WLAN. Se você possuísse uma rede 802.11b e quisesse usufruir das altas taxas proporcionadas pelo padrão 802.11a, era necessário fazer upgrade de toda a rede, devido à incompatibilidade do padrão 802.11a com qualquer outro. Com o surgimento do padrão 802.11g, o custo do investimento passou a ser preservado, já que o mesmo upgrade pode ser feito agora de forma gradativa e mais simples, devido à compatibilidade do 802.11g com os padrões anteriores a ele, com exceção do padrão 802.11a. Porém existe um sério agravante nisso tudo. Só é possível usufruir as altas taxas se todos os dispositivos da rede forem 802.11g. Se a rede for mista (802.11b e 802.11g) a maior taxa possível de ser alcançada é 11 Mbps, que é a maior taxa do 802.11b.

Para alcançar as altas taxas do padrão 802.11a, o 802.11g usa uma tecnologia de modulação chamada OFDM. Esses dispositivos têm a capacidade de chavear para a modulação QPSK para se comunicar com dispositivos 802.11b.

Outras Organizações

Enquanto o FCC e o IEEE são responsáveis pela criação de leis e padrões que regulamentam o uso das WLANs nos Estados Unidos, existem outras organizações americanas e de outros países que contribuem para o crescimento e a educação no mercado Wireless LAN.

Wireless Ethernet Compatibity Alliance (WECA)

Responsável por certificar a interoperabilidade de produtos Wi-Fi (802.11) e promover Wi-Fi como um padrão global de WLANs através de vários segmentos do mercado. Quando um produto satisfaz as requisições de interoperabilidade exigidas pela WECA, é garantida a esse produto uma certificação que permite ao vendedor usar o logo Wi-Fi. O logo Wi-Fi assegura ao usuário final que o produto que está adquirindo pode operar com outro produto que também tenha o logo, independente de fabricante.

European Telecommunications Standards Institute (ETSI)

O ETSI tem as mesmas responsabilidades já vistas com o IEEE, com uma ressalva: é voltado para a Europa. Os padrões estabelecidos pelo ETSI para a HiperLAN/2, por exemplo, competem diretamente com os criados pelo IEEE. Como não existe qualquer movimento no sentido de unificar os padrões, o IEEE procura a interoperabilidade com o HiperLAN/2 com o novo padrão que deve surgir, o 802.11h.

O HiperLAN original suportava taxas de até 24 Mbps usando tecnologia DSSS. O HiperLAN/1 usava as bandas inferior e central da UNII, e a HiperLAN/2 usa todas as bandas UNII, podendo chegar a taxas de 54 Mbps. A HiperLAN/2 possui suporte para QoS, criptografia DES e 3DES.

Wireless LAN Association (WLANA)

Responsável por prover conhecimento a aqueles que procuram aprender mais sobre WLANs. Também é útil na procura de um produto ou serviço específico. Mais informações em: http://www.wlana.org.

Tecnologias Concorrentes

Há diversas tecnologias que competem com a família de padrões 802.11. De acordo com a necessidade de mudança dos negócios e com o avanço das tecnologias, continuarão a surgir novas tecnologias para suportar as necessidades do mercado. Entre as tecnologias WLANs mais utilizadas hoje em dia, podemos citar:

- HomeRF;

- Bluetooth;
- Infravermelho;
- OpenAir.

HomeRF

HomeRF opera na banda de 2.4 GHz e usa a tecnologia de pulo da freqüência. A freqüência pula de cinco a vinte vezes mais rápido que os sistemas 802.11 usando FHSS.

O HomeRF 2.0 usa as novas regras para o pulo das freqüências aprovadas pelo FCC, que determina:

- Máximo de 5 MHz de largura para as freqüências de portadora;
- Mínimo de 15 pulos em uma seqüência;
- Máximo de 125 mW para a potência de saída.

O fato de possuir uma baixa potência de saída faz com que o alcance desses dispositivos não ultrapasse 50 m, o que restringe seu uso para ambientes domésticos.

Uma grande vantagem do HomeRF é a segurança em relação ao 802.11 usando WEP, devido a dois fatores:

- O vetor de inicialização é de 32 bits enquanto o do 802.11 é de 24 bits;
- Possibilidade de escolha de como esse vetor será escolhido durante a criptografia, o que não é possível com o 802.11.

A falta desse fator nas redes 802.11 as deixa muito mais vulneráveis a ataques devido a implementações fracas.

Bluetooth

Bluetooth é mais uma tecnologia de pulo de freqüência que opera na banda 2.4 GHz ISM. A taxa de pulo de um dispositivo Bluetooth é de 1.600 pulos por segundo e possui um overhead maior se comparado aos dispositivos FHSS do padrão 802.11.

A alta taxa de pulos dá a essa tecnologia uma grande resistência a ruídos espúrios de banda estreita. Sistemas Bluetooth não são projetados para altos throughput, mas para usos simples, baixa potência e curtas distâncias (WPANs). O padrão 802.15 para WPANs inclui especificações para o Bluetooth.

A grande desvantagem do Bluetooth é o fato de interferir com outras redes que operam em 2.4 GHz. A alta taxa de pulo sobre toda a banda utilizável de 2.4 GHz faz com que o sinal Bluetooth apareça para os outros sistemas como um ruído ou interferência em todas as bandas. Esse tipo de interferência afeta o sinal original por toda a faixa de freqüências utilizáveis. Dispositivos Bluetooth afetam severamente dispositivos 802.11, mas, curiosamente o mesmo não ocorre com dispositivos 802.11 interferindo com dispositivos bluetooth.

Dispositivos Bluetooth operam em três classes de potência: 1 mW, 2.5 mW e 100 mW. Atualmente há poucas implementações dos dispositivos da classe três. Já dispositivos da classe dois possuem um alcance máximo de 10 m. Se for necessário um alcance maior, antenas direcionais podem ser usadas.

Infravermelho (IR)

Infravermelho é uma tecnologia baseada na emissão de luz e não no espelhamento de espectro que usa radiação RF. Taxas de 4 Mbps podem ser alcançadas, embora o throughput nominal seja de 115 Kbps, o que é bom para a troca de dados entre dispositivos handhelds. A grande vantagem dessa tecnologia é que ela não interfere com tecnologias de espelhamento de espectro, o que as torna complementares e possibilita o uso das duas em conjunto, porém outras fontes de IR pode interferir em transmissões IR. Seu uso é muito comum em calculadoras, impressoras, conectividade prédio a prédio, redes localizadas em uma única sala e dispositivos handhelds.

Segurança

A segurança de dispositivos IR é excelente por duas razões:

- IR não pode atravessar paredes;
- Baixa potência (máximo de 2 mW).

Essas duas razões dificultam e muito o trabalho de um hacker que, para ter acesso à informação que está sendo transmitida, deve interceptar diretamente o feixe.

Redes simples localizadas em salas que necessitam de conectividade wireless deveriam se beneficiar da segurança proporcionada pelo IR.

Laptops e PDAs usam o IR para transferir dados a distâncias muito curtas em uma conexão ponto a ponto.

Estabilidade

O infravermelho não sofre qualquer tipo de interferência de sinais eletromagnéticos, o que prova a estabilidade de um sistema IR. Dispositivos broadcast IR estão disponíveis e podem ser montados em tetos. Um dispositivo broadcast IR (que é análogo a uma antena RF) transmite o sinal em todas as direções, de forma que esse sinal possa ser interceptado pelos clientes IR próximos. Por razões de potência, o IR é implementado indoor. Transmissores IR ponto a ponto podem ser usados outdoors e podem atingir a distância máxima de 1 km, porém essa distância pode sofrer uma redução drástica devido à luz solar.

A luz solar tem aproximadamente 60% de luz infravermelha, o que impacta drasticamente um sinal IR. Por causa disso, em dias ensolarados é bom assegurar que os dispositivos (handhelds ou PDAs) que se comunicam por infravermelho estejam a salvo da luz solar, para uma boa transferência de dados.

OpenAir

OpenAir foi um padrão criado pelo já extinto Wireless LAN Interoperability Fórum (WLIF) para ser uma alternativa ao 802.11, porém não existe qualquer compatibilidade entre os dois padrões. Duas velocidades foram especificadas: 800 Kbps e 1.6 Mbps.

Era voltado para dispositivos FHSS operando nessas duas velocidades.

Há linhas de produtos disponíveis no mercado, mas não há novos produtos sendo fabricados.

Capítulo 20

Arquitetura de uma rede 802.11

Muitos dos tópicos que serão descritos a seguir estão definidos diretamente nos padrões do 802.11 e seu entendimento é necessário para o projeto e para a implementação e a resolução de problemas em uma WLAN.

Localizando uma WLAN

Quando instalamos, configuramos e iniciamos um cliente WLAN (um cliente USB ou um cartão PCMCIA), o primeiro passo executado por ele é verificar a existência de alguma WLAN dentro do seu alcance. Se houver, ele descobre também se há alguma possibilidade de associação com a WLAN em questão. Esse processo é chamado de scanning e ocorre antes de qualquer outro, uma vez que é o modo como o cliente encontra a rede.

Service Set Identifier (SSID)

O SSID é um valor único, alfanumérico, sensível a maiúsculas e minúsculas, com comprimento que varia de 2 até 32 caracteres, usado em WLANs como um nome da rede. Essa medida tem basicamente duas finalidades: segmentar as redes como uma maneira de segurança rudimentar e facilitar a associação com a rede.

O SSID é enviado em vários tipos de frames, tais como: beacons, pedidos e respostas de probe. Um cliente deve estar configurado com o SSID correto para conseguir se associar a uma determinada rede. O mesmo deve ser feito no AP.

Caso os clientes participem de várias redes, todos os referidos SSIDs devem estar configurados no cliente.

É fundamental que o SSID configurado no cliente seja exatamente o mesmo configurado no AP, para que seja possível a associação.

Se o AP não estiver usando nenhum SSID, a associação de um cliente a ele será automática.

Beacons

São frames curtos enviados pelos APs a uma estação (modo infraestrutura) ou de uma estação a outra (modo ad-hoc) com o propósito de sincronizar a comunicação em uma WLAN. Entre as funções de um beacon, podemos destacar:

Sincronização do tempo

Quando um cliente recebe o beacon, ele muda seu clock de modo a refletir o clock do AP. Uma vez feita a mudança, os clocks estão sincronizados. A sincronização de clocks em unidades de comunicação garante que as funções dependentes do tempo sejam executadas sem erros. Um bom exemplo disso é o pulo da freqüência em sistemas FHSS.

Parâmetros FH ou DS

Contém informações direcionadas à tecnologia que estiver sendo utilizada. Em um sistema FHSS, os parâmetros de pulo e a seqüência do pulo são incluídos. Em sistemas DSSS, informações, como o canal utilizado, estarão presentes no beacon.

Informação de SSID

Estações procuram no beacon o SSID da rede a que elas querem se associar. Uma vez identificada essa informação, elas enviam um pedido de autenticação para o endereço MAC que originou o beacon, que, em nosso caso, é o do AP. Se as estações estiverem configuradas para se associar a qualquer rede (sem o SSID específico), elas se associarão à primeira rede encontrada. No caso de haver mais de um AP, aquele que tiver o sinal mais forte terá preferência.

Mapa de indicação de tráfego (TIM)

O TIM nada mais é que uma indicação de quais estações têm pacotes a serem processados, que estão na fila do AP. Essa informação é passada em cada beacon para todas as estações associadas. Quando estão em sleeping, as estações ouvem os beacons e checam o TIM para ver se elas estão presentes na lista, caso não estejam, voltam ao estado de sleeping.

Taxas suportadas

Há muitas velocidades suportadas, dependendo do padrão do hardware em uso. Essa informação é passada nos beacons para informar quais as velocidades suportadas pelo AP.

Scanning passivo

É o processo pela qual as estações procuram por beacons em cada canal, durante um determinado período de tempo, tão logo a

estação tenha sido iniciaada. Os beacons são enviados pelo AP e as estações procuram nesses beacons se o SSID da rede em que eles desejam entrar está listado. Se estiver, a estação tenta entrar na rede através do AP que enviou o beacon. Em configurações em que há diversos APs, vários beacons serão enviados, e a estação tentará entrar na rede através do AP que tiver o sinal mais forte.

O processo de scanning continua mesmo depois de a estação ter entrado na rede. Isso economiza tempo na reconexão à rede, caso a estação tenha perdido a conexão por algum motivo. Esse processo só é possível porque é através dos beacons que as estações mantêm uma lista de APs disponíveis e catalogam informações sobre os APs, tais como: canal, nível de sinal, SSID entre outras.

Uma estação migrará de uma célula para outra quando o nível de sinal do AP ao qual ela está conectada cair abaixo de um determinado nível. Essa migração ocorrerá sem o conhecimento do usuário, mas para que isso seja possível, as células devem se sobrepor em 20 a 30%.

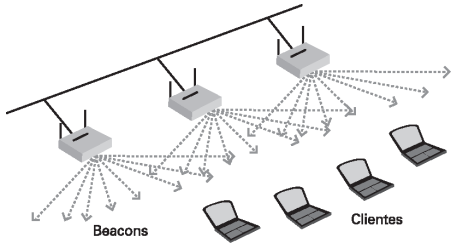

Figura 20.1: Scanning passivo.

Como ilustrado na figura anterior, no scanning passivo são os APs que iniciam o processo, através do envio de beacons.

Scanning ativo

Diferentemente do processo anterior, no scanning ativo são as estações que iniciam o processo, tornando-se portanto parte ativa deste.

Quando a estação procura por uma rede, ela envia um frame chamado probe request, contendo o SSID da rede que ela procura ou o de uma rede qualquer. O AP que tiver o SSID em questão envia um probe response. Se houver vários APs, somente o que tiver aquele SSID envia o probe response. Por outro lado, se o SSID de broad-

cast, que indica qualquer rede, for enviado no probe request, todos os APs enviarão um probe response.

Uma vez que o AP com o SSID específico tenha sido encontrado a estação inicia os passos de autenticação e associação para entrar na rede através daquele AP.

A informação passada nos probes responses pelos APs é idêntica aos beacons, com exceção do TIM.

O nível de sinal informado nos probes responses ajuda o cliente a determinar a qual AP ela tentará se associar. Geralmente a estação escolhe o AP com o melhor nível de sinal e a menor taxa de erro (BER). O BER é basicamente uma comparação de pacotes corrompidos comparados a pacotes bons, tipicamente determinada pela relação sinal-ruído.

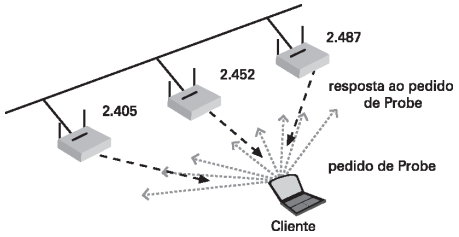

Figura 20.2: Scanning ativo.

Autenticação e Associação

O processo de conexão a uma WLAN consiste de dois subprocessos separados que ocorrem nessa ordem: autenticação e associação.

Quando dizemos que um PC Card está conectado a uma WLAN, na realidade estamos dizendo que o PC Card foi autenticado e está associado a um determinado AP.

É importante ter em mente que quando falamos de associação, estamos nos referindo à camada dois do modelo OSI e a autenticação se refere ao PC Card, não ao usuário.

Autenticação

É o processo pelo qual a identidade do nó wireless (PC Card ou USB) é verificada pela rede (AP). Essa verificação ocorre quando o

AP cujo cliente tenta conectar verifica se o cliente é quem diz ser. Nenhuma conexão é feita antes que essa verificação ocorra. Em alguns casos o resultado dessa verificação é nulo, indicando que o AP e o cliente que solicita conexão não têm uma identidade comum.

O processo tem início com o envio de um pedido de autenticação por parte do cliente para o AP (modo infraestrutura). Esse pedido será aceito ou negado pelo AP, com base em alguns critérios. A estação é notificada pelo AP da decisão tomada através de um frame de resposta de autenticação.

Em alguns casos, o AP poderá delegar essa responsabilidade a um servidor de autenticação, como o RADIUS. O servidor, portanto, tomará sua decisão baseado em uma lista de critérios e passará essa resposta ao AP, que por sua vez notificará ao cliente.

Associação

Uma vez que o cliente tenha sido autenticado pelo AP, tem início o processo de associação, que consiste na permissão dada ao cliente de poder passar dados através daquele AP. Em suma, se um cliente estiver associado a um AP, ele estará conectado àquele AP e, logicamente, à rede.

O processo ocorre da seguinte forma: após autenticar, o cliente envia um pedido de associação para o AP, que por sua vez autoriza ou não o pedido, enviando essa informação no frame de resposta de autorização.

Estados da autenticação e associação

O processo de autenticação e associação tem três fases distintas:

- Não autenticado e não associado;
- Autenticado e não associado;
- Autenticado e associado.

Não autenticado e não associado

Nessa fase inicial o nó wireless está desconectado da rede e é incapaz de passar frames através do AP. APs geralmente mantêm uma tabela de status de conexão de clientes conhecida como tabela de associação.

Autenticado e não associado

Nessa segunda fase, o cliente está autenticado mas não associado com o AP. O status da tabela de associação do AP mostrará *Autenticado*, mas o cliente ainda não pode passar dados através do AP. A passagem do processo de autenticação para o de associação é muito rápida (da ordem de milissegundos).

Autenticado e associado

Nessa última fase, o cliente, por estar associado, já pode passar dados através do AP, ou seja, está totalmente conectado à rede. A tabela de associação agora mostrará o status *Associado.*

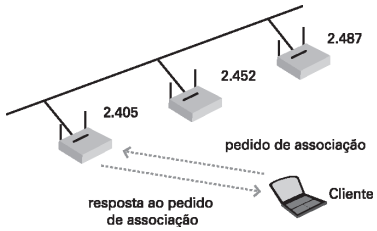

Figura 20.3: Processo de associação.

Capítulo 21

Métodos de autenticação

O padrão IEEE 802.11 especifica dois métodos de autenticação: autenticação de sistema aberto e autenticação de chave compartilhada. O mais simples e mais seguro dos dois é a autenticação de sistema aberto. Para se tornar autenticado, o cliente deve caminhar por uma série de passos durante esse processo; esses passos variam de um método para o outro.

Autenticação de Sistema Aberto

É o método padrão usado nos equipamentos wireless. Usando esse método, uma estação pode se associar a qualquer AP que também use o método. Esse método de autenticação é baseado no SSID, ou seja, basta que a estação e o AP tenham o mesmo SSID para que a autenticação ocorra. O processo de autenticação de sistema aberto é usado de forma eficaz tanto em ambientes seguros como não seguros.

Eis como o processo ocorre:

- O cliente faz um pedido para se associar ao AP;
- O AP toma conhecimento desse pedido, envia uma resposta positiva e autentica o cliente.

O processo é, portanto, muito simples, conforme ilustrado na **Figura 21.1**:

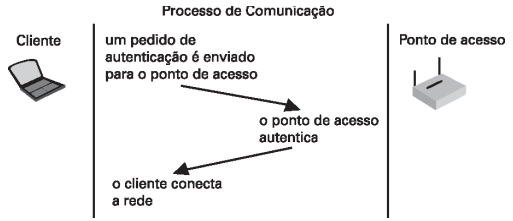

Figura 21.1: Processo de autenticação de sistema aberto.

Existe ainda a opção de se usar WEP (não é obrigatório) para criptografar o processo. Porém a criptografia não é feita durante o pro-

cesso de autenticação em si, ou seja, a chave WEP não é verificada por ambos os lados durante a autenticação, mas para criptografar os dados depois que o cliente já estiver autenticado e associado.

Esse método de autenticação é usado em diversos cenários, mas há duas razões principais para isso:

- É considerado o mais seguro dos dois métodos disponíveis;
- Já é usado por padrão nos dispositivos wireless, o que não requer configuração adicional.

Autenticação de Chave Compartilhada

Nesse método, o uso do WEP é obrigatório. A criptografia WEP usa chaves tanto no cliente como no AP, e elas devem ser as mesmas para que o WEP possa operar. Essas chaves são configuradas manualmente.

Eis como o processo ocorre:

1. O cliente faz um pedido de associação ao AP (esse passo é o mesmo da autenticação de sistema aberto).

2. O AP envia uma pergunta ao cliente. Essa pergunta é um texto gerado aleatoriamente e enviado ao cliente na forma de texto puro.

3. O cliente responde a essa pergunta. A chave WEP do cliente é usada para criptografar a pergunta e, por fim, ela é enviada já codificada de volta ao AP.

4. O AP replica a resposta do cliente. A resposta codificada enviada pelo cliente é então decodificada usando a chave WEP do AP, verificando, assim, se o cliente tem a mesma chave. Se a chave do cliente for a correta, o AP responderá positivamente e autenticará o cliente. Se a chave do cliente não for a correta, o AP responderá negativamente e não autenticará o cliente.

A **Figura 21.2** ilustra o processo:

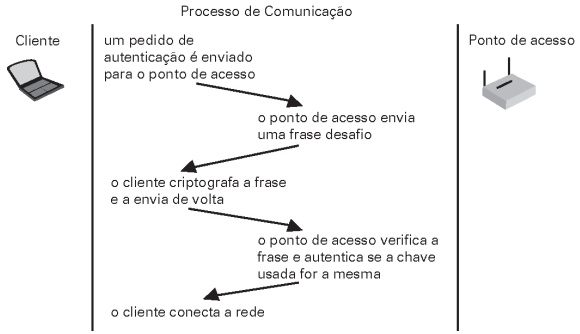

Figura 21.2: Processo de autenticação de chave compartilhada.

Diferentemente do que possa parecer, o processo de autenticação de chave compartilhada não é mais seguro que o processo de autenticação de sistema aberto. O processo de chave compartilhada abre uma porta para hackers.

Segurança da autenticação

O processo de chave compartilhada não é considerado seguro porque o AP transmite a pergunta em texto puro e recebe a mesma pergunta codificada com a chave WEP. Isso permite a um hacker usar um sniffer para ver tanto a pergunta em texto puro como a pergunta codificada. De posse desses dois valores, um programa cracker pode ser usado para gerar a chave WEP. Uma vez obtida a chave WEP, o hacker em questão pode descriptografar o tráfego codificado. Por essa razão, a autenticação de sistema aberto é mais segura que a de chave compartilhada.

É importante ressaltar que nenhum dos dois métodos é realmente seguro e, portanto, uma solução de segurança mais completa é importante e necessária.

Certificados e Shared Secrets

Shared Secrets são strings de números ou texto que são normalmente referidos como chave WEP. Certificados são outro método de identificação do usuário usados em redes wireless.

Da mesma forma que chaves WEP, certificados (que nada mais são do que documentos de autenticação) são colocados na máquina

cliente. Essa colocação é feita de tal forma que, quando o usuário deseja se autenticar com a rede wireless, o mecanismo de autenticação já se encontra na máquina cliente. Ambos os processos têm sido implementados ao longo dos anos, mas nos dias de hoje existem aplicações que permitem automatizar esses processos.

Protocolos de Autenticação Emergentes

Existem novas soluções de segurança de autenticação e protocolos no mercado hoje em dia, incluindo VPN e 802.1x usando EAP (protocolo de autenticação extensível).

Muitas dessas soluções de segurança envolvem a passagem da autenticação por servidores de autenticação, que por sua vez repassam a autorização ao AP, enquanto o cliente aguarda por essa autorização durante a fase de autenticação. O Windows XP tem suporte nativo a 802.11 ,802.1x e EAP, e o mesmo ocorre com Cisco e outros fabricantes WLAN. Por essas razões, não é difícil entender porque essas soluções são tão comuns no mercado hoje em dia.

802.1x e EAP

O padrão 802.1x é relativamente novo e os dispositivos que o suportam têm a habilidade de permitir a conexão para a rede na camada dois somente se a autenticação do usuário for bem-sucedida. EAP é um protocolo de camada dois que é uma substituição bem flexível ao PAP e ao CHAP, rodando sobre PPP, que trabalha nas LANs. No passado, PAP e /ou CHAP foram usados para autenticação do usuário e ambos usavam senhas. Ser esta uma alternativa para uma solução mais robusta e flexível em redes wireless fica cada vez mais evidente devido ao fato de que há muitas implementações variadas.

Tipicamente, a autenticação do usuário é realizada usando um servidor RADIUS e algum tipo de base de dados de usuários (RADIUS, NDS, Active Directory, LDAP) para sua validação. O novo padrão 802.1i, também conhecido como WPA, inclui suporte a 802.1x, EAP, AAA, autenticação mútua e geração de chave, e nenhum desses foi incluído no padrão original 802.11.

No modelo 802.1x padrão, a autenticação da rede consiste de três partes: o requerente (cliente), o autenticador (Ponto de Acesso) e o servidor de autenticação (RADIUS).

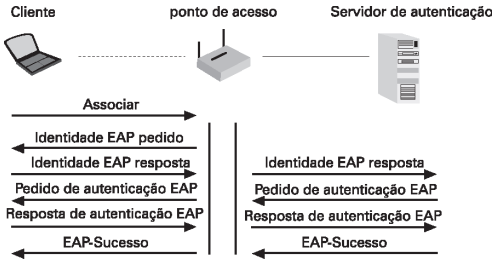

Figura 21.3: Processo de autenticação usando EAP.

Como a segurança de uma WLAN é essencial e a autenticação EAP fornece meios para assegurar uma conexão WLAN, fabricantes estão desenvolvendo e adicionando tipos de autenticação EAP aos seus Pontos de Acesso. Conhecer o tipo de autenticação EAP é importante no entendimento das características do método de autenticação que está sendo utilizado, tais como: senhas, geração de chave, autenticação mútua e protocolos. Porém é importante estar ciente de que somente o uso do EAP não é suficiente para estar bem protegido, já que é necessário escolher o tipo de EAP (protege a camada de transporte) que será usado. Alguns tipos de autenticação EAP mais comuns são:

EAP-MD-5 Challenge

O mais antigo dos tipos de autenticação. Basicamente duplica a proteção de senha CHAP em uma WLAN.

EAP-Cisco Wireless

Também chamado de LEAP, esse tipo de autenticação EAP é usado somente em APs Cisco. LEAP fornece segurança durante a troca de credenciais, criptografa os dados transmitidos usando chaves WEP dinâmicas e suporta autenticação mútua.

EAP-TLS (segurança na camada de transporte)

É baseada no uso de certificados e proporciona a autenticação mútua do cliente e da rede. EAP-TLS confia nos certificados do lado cliente e do servidor para realizar a autenticação usando chaves WEP

geradas dinamicamente, baseadas na sessão e no usuário, para proteger a conexão. Tanto o Windows XP como o Windows 2000 suportam o EAP-TLS.

EAP-TTLS (segurança na camada de transporte encapsulada)

É uma extensão do EAP-TLS. Diferentemente do EAP-TLS, necessita somente de certificados no lado servidor, eliminando a necessidade de configurar os certificados em cada cliente. Suporta vários tipos protocolos de senhas de modo que pode ser usado com sistemas de autenticação existentes, tais como: Active Directory e NDS. Encapsula em túneis a autenticação do cliente dentro do EAP-TLS, garantindo que o usuário permaneça anônimo no link wireless. Chaves WEP são distribuídas e geradas dinamicamente para proteger a conexão.

EAP-SRP (senha remota segura)

É um protocolo baseado em senha e troca de chaves com segurança. Soluciona o problema de autenticar o cliente ao servidor de uma forma segura, em casos em que o usuário do software cliente deve memorizar um pequeno segredo (como uma senha) e não carregar mais nenhum tipo de informação secreta. O servidor carrega um verificador para cada usuário, o que permite a ele autenticar o cliente. Se o verificador for comprometido, não é permitido a um hacker, por exemplo, se fazer passar pelo cliente. SRP usa um segredo baseado em criptografia forte, o que permite às duas partes se comunicarem de forma segura.

Capítulo 22

Soluções VPN

A tecnologia VPN proporciona os meios para dois dispositivos de rede transmitirem dados de forma segura em um meio não seguro. O uso mais comum da VPN é na comunicação entre redes de duas empresas distintas ou na comunicação de um cliente com um servidor corporativo via Internet. Porém, existem outras aplicações para a VPN, e uma delas é a proteção de dados em uma rede wireless. VPN trabalha criando um túnel no topo de um protocolo, como o IP. O tráfego dentro do túnel é codificado e totalmente isolado do restante da rede. A tecnologia VPN proporciona três níveis de segurança: autenticação do usuário, criptografia e autenticação dos dados.

Autenticação do Usuário

Garante que somente usuários autorizados (por um dispositivo específico) sejam capazes de conectar, enviar e receber dados em uma rede WLAN.

Criptografia

Oferece proteção adicional e garante que, mesmo que transmissões sejam interceptadas, elas não poderão ser decodificadas sem esforço e uma grande demanda de tempo.

Autenticação dos Dados

Garante a integridade dos dados em uma WLAN, dessa forma, há a certeza de que todo o tráfego provém somente de dispositivos autenticados.

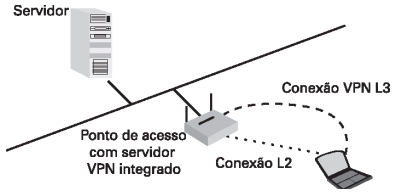

Figura 22.1: Ponto de Acesso com servidor VPN integrado.

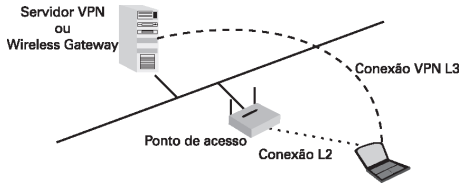

Figura 22.2: Ponto de Acesso com servidor VPN externo.

A aplicação da tecnologia VPN requer algumas adaptações em relação a LANs, quando usada em redes wireless, pelas seguintes razões:

- A função de repetidor, inerente aos Pontos de Acesso, automaticamente encaminha o tráfego entre estações WLAN que se comunicam juntas e aparentam estar na mesma WLAN;
- O alcance das redes WLAN geralmente ultrapassa os limites do escritório ou do prédio em que estão, dando aos invasores meios de comprometer a segurança da rede.

A implementação de uma solução VPN varia dependendo das necessidades de cada tipo de ambiente. Por exemplo, um hacker que conseguisse a chave WEP usando um sniffer em uma WLAN teria condições de decodificar os pacotes em tempo real. Porém, se a rede usasse também uma solução VPN, os pacotes estariam não somente codificados, mas também encapsulados. Essa camada extra de segurança fornece muitos benefícios em termos de acesso.

WPA

WEP não proporciona uma segurança robusta para WLANs corporativas. Devido ao fato de a chave ser estática, não é difícil para um hacker obter a chave sniffando a rede. Isso motivou o surgimento de uma implementação de WEP, em que as chaves são fortes e geradas dinamicamente, mas, por esse novo mecanismo ser um padrão proprietário, dificulta ou mesmo inviabiliza seu uso em redes

que têm dispositivos de vários fabricantes. O WPA especificado no padrão 802.1i veio para solucionar esses problemas.

WPA inclui TKIP (protocolo de integridade de chave temporal), além dos mecanismos 802.1x. Essa combinação fornece codificação de chave dinâmica e autenticação mútua, algo muito necessário em WLANs.

As seguintes características foram adicionadas ao WEP:

Vetores de inicialização de 48 bits

WEP produz o que é chamado de "agendamento de chave", concatenando a chave compartilhada com um vetor de inicialização de 24 bits gerado aleatoriamente (IV). Com um vetor de 24 bits (IV), WEP eventualmente usa o mesmo IV para diferentes pacotes de dados. Isso resulta na transmissão de frames, tendo frames codificados similares o suficiente para um hacker coletar esses frames baseados no mesmo IV, e determinar seus valores compartilhados decodificando esses frames. WPA com TKIP dificulta, e muito, o trabalho do hacker devido ao uso de um vetor de 48 bits, o que reduz de forma significativa a reutilização dos IVs e aumenta drasticamente a dificuldade para a quebra da codificação através da captura de frames.

Construção e distribuição de chave por pacote

WPA gera automaticamente e periodicamente uma chave de codificação para cada cliente. Uma única chave para cada frame 802.11 é utilizada. Isso evita que a mesma chave permaneça em uso por semanas ou meses. Portanto, é muito difícil que alguém, mesmo tendo uma cópia da chave, possa comprometer a maioria dos frames, uma vez que essa chave não serviria para todos os frames. Mal comparando, seria o mesmo que alguém trocar a fechadura de uma porta toda vez que a fechasse.

Código de integridade de mensagem (MIC)

WPA implementa um código de integridade de mensagem para se resguardar de ataques. WEP anexa um código verificador de integridade de 4 bytes (ICV) ao frame 802.11. O receptor vai calcular o ICV na recepção do frame para determinar se ele é igual àquele que está no frame. Se for igual, há uma grande chance de o frame não ter sido interceptado.

Embora WEP codifique o ICV, um hacker poderia mudar os bits e atualizar o ICV codificado sem ser detectado pelo receptor. WPA soluciona esse problema calculando um MIC de 8 bytes, que se localiza antes do ICV.

Para autenticação, o WPA usa uma combinação da autenticação de sistema aberto com o 802.1x. Eis como o processo ocorre:

1. O cliente wireless autentica com o AP, o qual, por sua vez, autoriza o cliente a enviar frames.

2. É feita uma autenticação de usuário com o 802.1x. WPA intermedia a comunicação com um servidor de autenticação corporativo (RADIUS ou LDAP) para validar o usuário.

WPA também é capaz de operar em um modo conhecido como chave pré-compartilhada, caso nenhum servidor de autenticação externo esteja disponível, como nos casos de ambientes domésticos.

Um problema que o WPA ainda não solucionou é o caso de ataques de negação de serviço (DoS). Se alguém mandar pacotes a cada dois segundos com uma chave de codificação errada, o AP encerrará todas as conexões por um minuto. Esse é um mecanismo de defesa, alertando que alguém não autorizado está tentando acessar a parte protegida da rede.

Se você tem um dispositivo WEP e quer usufruir os benefícios do WPA, basta fazer uma atualização de fireware do seu dispositivo wireless.

Service Sets

Service set é um termo usado para descrever os componentes básicos de uma WLAN operacional; pode ser também referenciado como topologia de uma WLAN.

As WLANs podem ser classificadas em três categorias: IBSS, BSS e ESS. WLANs fazem o broadcast de um sinal através de uma portadora de RF. A estação pode estar na faixa de vários transmissores, mas como o sinal carrega o SSID do transmissor, a estação receptora usa esse SSID (que deve ser o mesmo do usuário) para filtrar os sinais recebidos de um determinado transmissor e localizar a célula da qual ela faz parte. Veremos cada tipo em detalhes.

IBSS (Independent Basic Service Sets)

Um IBSS consiste de um grupo de estações 802.11 se comunicando diretamente umas com as outras. IBSS é também chamado de AD-HOC, porque ele é essencialmente uma rede peer to peer. Não há um ponto central que controle a rede.

Redes IBSS geralmente são pequenas e não têm interfaces com redes cabeadas. Não há um limite preestabelecido para o número máximo de estações. Porém, à medida que a rede cresce, problemas de comunicação podem ocorrer devido ao problema do nó escondido. Como não há um elemento central que faça o controle na rede, ou seja, para determinar qual estação tem autorização para transmitir naquele momento, essa autorização é controlada de uma maneira distribuída.

Se a transmissão de dados para fora do IBSS for necessária, um dos clientes deve atuar como gateway ou roteador usando uma solução de software para esse propósito.

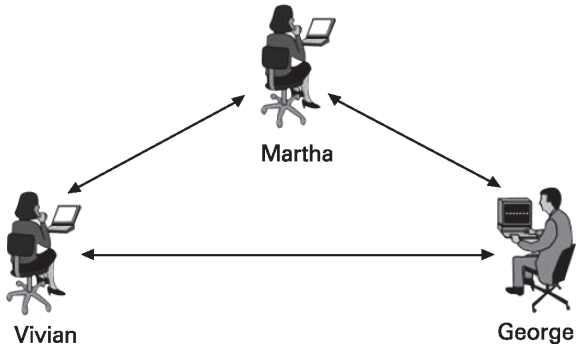

Figura 22.3: WLAN IBSS ou AD-HOC.

BSS (Basic Service Sets)

Um BSS consiste de um grupo de estações 802.11 se comunicando umas com as outras através de um dispositivo central, conhecido como Ponto de Acesso ou AP. Diferentemente do IBSS, em um BSS

as estações não se comunicam diretamente umas com as outras. Elas podem se comunicar somente com o AP e este encaminha os frames para a estação destino. Um Ponto de Acesso possui uma porta para conexão com uma estrutura cabeada (um backbone Ethernet, por exemplo) e por isso é também chamado de infra-estrutura BSS.

Uma rede BSS possui um throughput melhor que uma IBSS, devido a presença de um dispositivo que gerencia todo o tráfego.

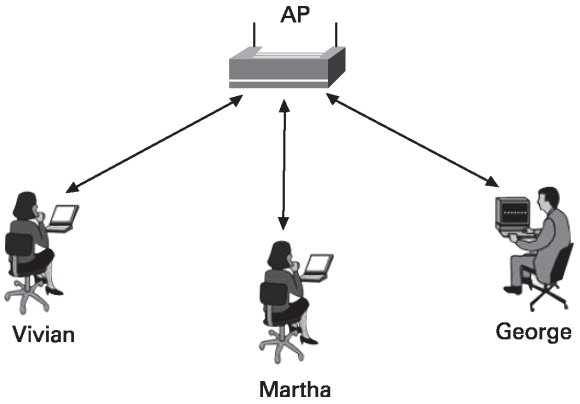

Figura 22.4: Uma WLAN BSS.

O BSS cobre uma simples célula ou área RF em torno do Ponto de Acesso, com várias zonas de taxas de dados (círculos concêntricos) de diferentes velocidades. A velocidade nesses círculos dependerá da tecnologia utilizada. Se o BSS for feito de equipamentos 802.11b, então os círculos podem ter velocidades de 11, 5.5, 2 e 1 Mbps. As velocidades se tornam menores à medida que os círculos se afastam do Ponto de Acesso. Um BSS tem um único SSID.

ESS (Extended Service Sets)

Dois ou mais BSS podem ser conectados via suas interfaces de uplink, formando uma estrutura ESS. A interface de uplink conecta o BSS a um sistema de distribuição (DS). O uplink para o sistema de distribuição pode ser uma conexão cabeada ou wireless, mas na maioria das vezes é uma conexão cabeada, geralmente Ethernet.

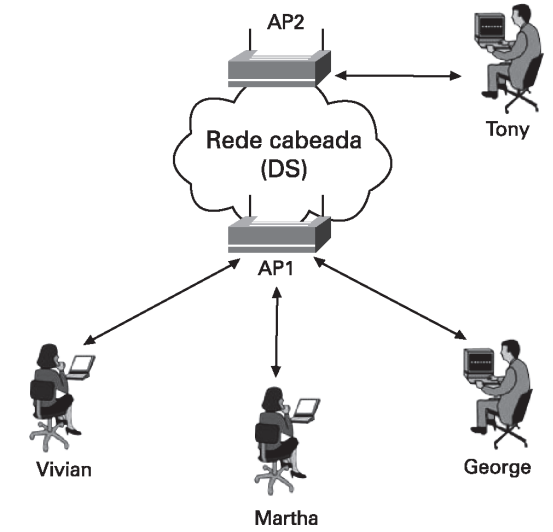

Figura 22.5: Uma estrutura ESS.

De acordo com o padrão 802.11, um ESS cobre múltiplas células e permite (mas não requer) capacidades de roaming e não necessita que as células tenham o mesmo SSID.

Capítulo 23

Roaming

É a habilidade de um cliente em se mover de uma célula para a outra sem perder a conectividade com a rede. Os Pontos de Acesso envolvidos nos BSS são os grandes responsáveis por esse processo, que é transparente para o cliente. Quando qualquer área em um prédio está dentro do alcance de um ou mais Pontos de Acesso, as células se sobrepõem. Áreas de cobertura sobrepostas são um aspecto importante no setup de WLANs, porque isso habilita o roaming entre elas. Um usuário com um notebook pode circular livremente entre essas células sem perder a conexão com a rede.

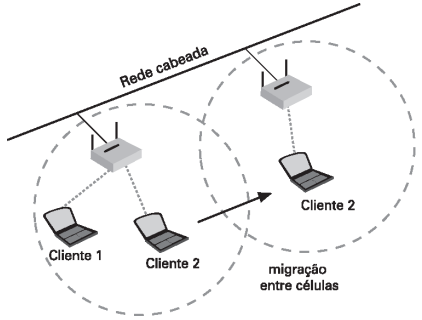

Figura 23.1: Roaming em um ESS.

Vários Pontos de Acesso podem proporcionar uma cobertura de roaming para um campus ou um prédio inteiro.

Quando as áreas de cobertura de dois ou mais Pontos de Acesso se sobrepõem, as estações nessa área sobreposta podem estabelecer a melhor conexão possível com um dos APs e, ao mesmo tempo, procurarem pelo melhor AP. Para minimizar a perda de pacotes durante o chaveamento, o AP novo e o antigo se comunicam para coordenar o processo de roaming.

Padrões

O padrão 802.11 não define a forma como o roaming deve ser feito, mas define os conceitos principais. Nesses conceitos estão incluídos um scanning passivo e ativo e um processo de reassociação. Toda vez que um cliente migrar de um AP para o outro, um processo de reassociação deverá ocorrer entre o cliente e o novo AP.

O padrão permite a migração de um cliente entre vários APs, operando ou não no mesmo canal.

Para satisfazer às necessidades de comunicação de rádios móveis, o padrão deve ser tolerante com conexões perdidas e restabelecidas. O padrão tenta garantir o mínimo de prejuízo à entrega dos dados e fornece algumas características para caching e encaminhamento de mensagens entre BSSs.

O padrão 802.11 deixa a cargo dos fabricantes muitos aspectos da operação detalhada dos sistemas de distribuição. Essa decisão foi deliberada por parte dos desenvolvedores de padrões, porque eles estavam preocupados com o fato de tornar o padrão independente de qualquer padrão de rede existente. Como resultado, a maioria de WLANs 802.11b que usam topologias ESS estão conectadas a LANs Ethernet e fazem uso pesado do TCP/IP.

Conectividade

A camada MAC 802.11 é responsável pela forma com que um cliente se associa a um AP.

Quando um cliente 802.11 entra no alcance de um ou mais pontos de acesso, ele escolhe um AP para se associar, baseado no nível do sinal e na taxa de erro de pacotes. Uma vez associado com o AP, o cliente periodicamente faz um survey em todos os canais na tentativa de encontrar um AP com melhor performance (melhor nível de sinal). Uma vez encontrado esse AP, o cliente se reassocia ao novo AP, mudando para o canal em qual o AP está configurado.

Reassociação

A reassociação geralmente ocorre porque o cliente se afastou demasiadamente do AP original, levando a um enfraquecimento no sinal. Mas existem outros casos em que a reassociação pode ocorrer. Um caso muito comum é quando há um alto tráfego na rede no AP original. Nesse caso, isso funciona também como balanceamento de carga, uma vez que a idéia principal é distribuir uniformemente a carga por toda a infra-estrutura WLAN disponível.

Associação e reassociação diferem quanto ao uso. Frames de pedido de associação são usados quando o cliente tenta entrar na rede pela primeira vez. Frames de pedido de reassociação são usados quando o cliente migra entre APs. No segundo caso, o novo AP tem conhecimento dos frames buferizados do AP antigo e deixa o sistema de distribuição saber que o cliente se moveu.

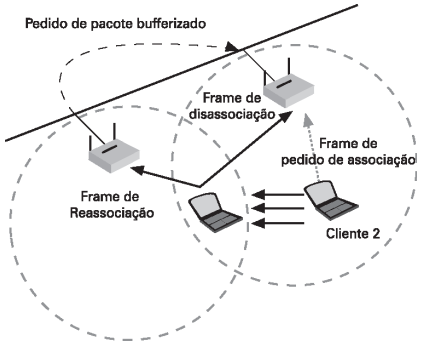

Figura 23.2: Roaming com reassociação.

Esse processo de associação e reassociação dinâmica permite configurar WLANs com áreas de cobertura muito largas, criando uma série de células sobrepostas através de um prédio ou campus. Para a implementação ser bem-sucedida, deve-se usar a reutilização de canal, tomando o cuidado de configurar cada AP com um canal que não venha a interferir com aquele utilizado pelo vizinho. Devemos lembrar que há somente três canais no DSSS que não se sobrepõem, e são esses que devem ser usados para implementações multicélulas. Se dois APs são configurados para usar o mesmo canal e estão próximos um do outro, isso causará interferência entre eles e a largura de banda na área da sobreposição das células sofrerá uma drástica redução.

Uso da VPN

Soluções de VPN wireless podem ser implementadas de duas formas. A primeira delas é através do uso de um servidor de VPN externo centralizado. Esse servidor de VPN pode ser uma solução de hardware proprietário ou um servidor com uma aplicação de VPN rodando nele. O servidor de VPN atua como gateway e firewall entre o usuário wireless e o núcleo da rede e fornece um nível de segurança similar às VPNs em LANs.

A segunda delas é através de um set distribuído de servidores VPN. Alguns fabricantes implementam funcionalidades de VPN em seus Pontos de Acesso. Esse tipo de solução é adequada para organizações de pequeno e médio porte, uma vez que não há um me-

canismo de autenticação externo como o RADIUS. Muitos desses Pontos de Acesso, além de serem servidores VPN, também suportam RADIUS.

Quando o cliente migra de uma célula para outra, na verdade está migrando entre Pontos de Acesso (supondo que eles não tenham funcionalidade VPN e não haja servidores VPN externos), esse processo ocorre dentro da camada dois. Porém, quando essa mesma migração ocorre e há servidores de VPN envolvidos, túneis são construídos para o Ponto de Acesso ou servidor de VPN centralizado, e o processo agora ultrapassa os limites da camada dois e passa a ser de camada três. Nesse caso, deve haver algum mecanismo que mantenha o túnel vivo quando ele ultrapassar os limites da camada dois.

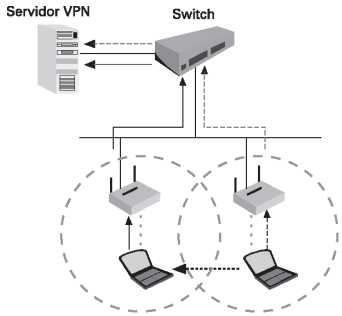

Figura 23.3: Roaming dentro de túneis VPN.

O problema aqui é que normalmente cada Ponto de Acesso está em uma subnet IP diferente, e quando o cliente migrar de uma célula para outra estará com novo IP, e com isso perderá a conexão com os servidores e aplicações. Para entender melhor essa questão vamos introduzir alguns conceitos.

Empresas que têm muitos prédios, muitas vezes implementam uma LAN em cada prédio e conectam essas LANs com roteadores ou switches-routers. Isso é uma segmentação de camada três e tem duas vantagens. A primeira é o bloqueio de broadcasts entre os segmentos; e a segunda é um controle de acesso entre os segmentos da rede. Esse tipo de segmentação pode ser feito também usando VLANs em switches. É como se partíssemos um switch em várias partes e cada parte virasse uma sub-rede separada (VLAN), lembrando que uma VLAN não se comunica com outra sem o uso de roteamento. Essa segmentação de camada dois segmenta a rede completamente.

Quando roteadores são usados, usuários devem ser capazes de ultrapassar os limites do roteador sem perder sua conectividade de camada três. A conexão de camada dois é mantida pelo AP, mas como houve uma mudança na subnet IP durante a migração, a conexão para os servidores (por exemplo) será quebrada. Uma boa medida para evitar esse problema é colocar todos os APs na mesma subnet IP, porém essa não é uma solução muito prática nem tão pouco simpática. Mesmo com o uso de VLANs, teríamos o mesmo tipo de problema porque o switch veria essa migração de usuários como uma mudança de uma VLAN para outra.

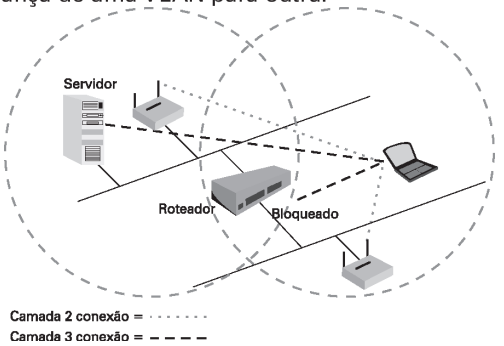

Figura 23.4: Roaming com roteador envolvido.

A solução de hardware definitiva para esse problema é colocar todos os APs em uma única VLAN, conforme pode ser visto na **Figura 23.5**. Dessa forma evitamos a mudança de IP durante o roaming dos usuários e, ainda nesse caso, um servidor DHCP não seria necessário. Usuários seriam então roteados como um grupo para dentro da rede corporativa, usando um firewall e um roteador. Essa solução pode ser difícil de implementar, mas é aceita como uma metodologia padrão.

Existem ainda muitas soluções no mercado, em que o AP possui um servidor de VPN embutido e executa roteamento, inclusive com protocolos de roteamento como o RIP.

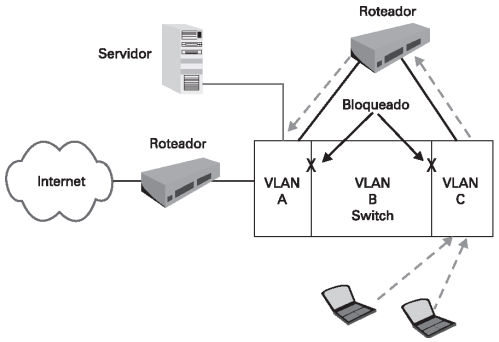

Figura 23.5: Roaming entre VLANs.

Balanceamento de Carga

Áreas congestionadas com muitos usuários e alta carga de tráfego por unidade necessitam de uma estrutura multicélula. Nessa estrutura, dois ou mais APs cobrem a mesma área, o que aumenta o throughput agregado. Clientes dentro dessa área de cobertura comum geralmente se associam ao AP menos carregado e com melhor qualidade de sinal. A eficiência é maximizada porque todos os APs trabalham no mesmo nível de carga. Em muitos casos o balanceamento de carga é configurado no AP e nas estações.