REDES WIRELESS

Enviada por:
Reginaldo Ferreira

Sumário

Introdução

Os links wireless entre computadores locais e o acesso à Internet são um avanço em direção ao amplo domínio da Internet sobre todo o universo conhecido. As conexões ativas em todos os lugares em um prédio, ou até mesmo um campus de faculdade inteiro ou um centro comercial, sem a necessidade de encontrar um local para instalar um fio, podem tornar a rede e as ferramentas conectadas à rede muito mais flexíveis. E um acesso rápido à Internet a partir de um cyber café, um saguão de um aeroporto ou um centro de convenção pode mudar a maneira como você trabalha e permanece online quando está distante da sua base habitual.

Neste módulo, se espera que você tenha duas coisas em mente: primeiramente, uma rede wireless local ideal deve ser absolutamente invisível – quando estiver funcionando, você nunca se deverá lembrar dela; o ideal é que você se preocupasse apenas em trocar mensagens ou visualizar o conteúdo de um site Web, em vez de ajustar a antena ou trocar a sua chave de criptografia.

Igualmente importante é que você esteja no comando. O computador e a rede devem fazer coisas da maneira que você deseja que façam, sem forçá-lo a ajustar sua vida ou forma de trabalho para atender as necessidades da máquina. Para isso é importante você se manter sempre informado e atualizado. Neste curso se mostram os princípios gerais que não são alterados porém sempre há a evolução. Os melhores lugares para aprender sobre novos recursos e funções de rede wireless, incluem o material de marketing e sites dos fabricantes de hardware de rede, e sites de terceiros, como o site 802.11b Networking News (http://802.11b.weblogger.com/).

Depois deste módulo, você terá uma idéia mais precisa para o funcionamento do Wi-Fi, e como usá-lo para que se beneficie mais do que a maioria das pessoas que utiliza redes wireless.

O funcionamento do Wi-Fi

Até certo ponto, é viável lidar com suas redes wireless como um conjunto de caixas pretas que se pode ativar e usar, sem precisar conhecer a fundo seu funcionamento. Em um mundo ideal, funcionaria dessa forma.

Porém, o Ethernet wireless está atualmente como as transmissões por rádio estavam em 1923. A tecnologia existia mas as pessoas gastavam muito tempo ajustando seus equipamentos e as que entediam internamente eram capazes de obter melhor desempenho de seus rádios.

Para utilizar com mais eficiência a tecnologia wireless, é importante entender o que acontece dentro das caixas que compõem a rede. Este tópico descreve padrões e especificações que controlam as redes wireless, explicando também como os dados são transportados através da rede de um computador para outro.

O transporte de dados através de uma rede wireless envolve três elementos distintos: os sinais de rádio, o formato dos dados e a estrutura da rede. Cada um desses elementos é independente dos outros dois; portanto, é necessário se definir todos os três quando se define uma nova rede. No que se refere ao modelo OSI, o sinal de rádio opera na camada Física, enquanto o formato dos dados controla várias das camadas mais elevadas. A estrutura de rede inclui os adaptadores de interface e as estações base, os quais enviam e recebem os sinais de rádio.

Em uma rede wireless, os adaptadores de rede em cada computador convertem os dados digitais para sinais de rádio, os quais são transmitidos para outros dispositivos na rede, e convertem os sinais de rádio que chegam em dados digitais. O IEEE (*Institute od Electrical and Electronics Engineers*), produziu um conjunto de padrões e especificações para redes wireless, sob o título "IEEE 802.11", o qual define o formato e a estrutura dos sinais.

O padrão 802.11 original foi lançado em 1997, e cobre tipos diferentes de mídia wireless: dois tipos de transmissões de rádio (explicados mais adiante) e redes que utilizam luz infra-vermelha. O padrão 802.11b, mais recente, oferece especificações adicionais para redes Ethernet wireless. Um documento relacionado, IEEE 802.11a, descreve redes wireless que operam em velocidades mais elevadas em diferentes frequências de rádio. Vale a pena ficar atento ao progresso dos outros padrões mas, por enquanto, o 802.11b é o que deverá ser usado (neste curso adota-se este padrão), especialmente se se espera conectar a redes nas quais não se controlará todos os componentes de hardware.

Você deve conhecer outros dois nomes no vasto jargão dos padrões de WLAN: WECa e Wi-Fi. O WECA (*Wireless Ethernet Capabilities Alliance*) é um grupo industrial que inclui todos os principais fabricantes do equipamento

802.11b. Suas duas missões, são testar os dispositivos de rede wireless de todas as suas empresas associadas e certificar que estes podem opera em conjunto na mesma rede, além de promover redes 802.11 como o padrão global para WLANs. O gabaritado pessoal de marketing da WECA adotou um nome mais "amigável": Wi-Fi (*Wireless Fidelity*) para as especificações 802.11, e mudou o próprio nome para Wi-Fi Alliance.

Sinais de rádio

As redes 802.11b operam em uma banda especial de frequência em torno dos 2,4 GHz, a qual foi reservada, na maior parte do mundo, para serviços de rádio ponto-a-ponto de espalhamento de espectro não licenciado (não necessidade de licença de estação de rádio). Teoricamente, a tecnologia de rádio espalhamento de espectro possibilita a coexistência com outros usuários (até certo ponto), sem uma interferência significativa.

Um serviço de rádio ponto-a-ponto opera um canal de comunicação que transporta informações de um transmissor até um único receptor. O oposto de um ponto-a-ponto é o serviço de rádiodifusão, que envia o mesmo sinal para muitos receptores ao mesmo tempo.

Espalhamento de espectro é uma família de métodos para a transmissão de um único sinal de rádio, usando um segmento relativamente amplo do espectro de rádio. As WLANs usam dois sistemas de transmissão de rádio diferentes: FHSS (*Frequency-Hopping Spread Spectrum*) e DSSS (*Direct-Sequence Spread Spectrum*).

Algumas redes 802.11 mais antigas usam o sistema FHSS mais lento, mas a geração atual das WLANs usam o DSSS.

O espalhamento de espectro oferece algumas vantagens importantes sobre outros tipos de sinais de rádio que usam um único canal menos amplo. O espalhamento de espectro é extremamente eficiente; portanto, os transmissores de rádio podem operar com muito pouca energia. Por operarem em uma banda relativamente ampla de frequências, são menos sensíveis a interferência de outros sinais de rádio e ruídos elétricos, o que significa que os sinais geralmente são capazes de ter acesso a ambientes onde um sinal de banda estreita convencional não poderia ser recebido ou entendido, e devido a uma determinada frequência deslocar-se entre múltiplos canais, pode ser extremamente difícil para um sintonizador não autorizado interceptar e decodificar o conteúdo de um sinal.

A história da tecnologia de espalhamento de espectro é bastante interessante. Foi inventada pela atriz Hedy Lamarr e pelo compositor de vanguarda americano George Antheil, como um "Sistema de Comunicação Secreto" para o direcionamento de torpedos controlados por rádio, que não estariam sujeitos à interferência inimiga. Lamarr, antes de começar a trabalhar em Hollywood, casou-se com um negociante de armas na Áustria, local em que aprendeu, com os clientes do marido, os problemas relacionados à orientação de torpedos. Anos mais tarde, durante a Segunda Guerra Mundial, ela apresentou o conceito de frequências de rádio variáveis, a fim de evitar a interferência. Antheil, aparentemente, era a pessoa ideal para colocar sua idéia em prática. Sua composição mais famosa era conhecida como Ballet Mechanique, e foi executada por 16 pianistas, duas hélices de avião, quatro xilofones, quatro zabumbas e uma sirene. Ele usou o mesmo tipo de mecanismo que havia usado anteriormente para sincronizar os pianistas, a fim de alterar as frequências de rádio em uma transmissão por espalhamento de espectro. O sistema original de fita de papel com ranhuras tinha 88 canais de rádio diferentes – um para cada uma das 88 teclas de um piano.

Teoricamente, o mesmo método poderia ser usado para a comunicação por voz ou de dados, bem como para a orientação de torpedos, mas na época das válvulas eletrônicas, da fita de papel e da sincronização mecânica, o processo inteiro era demasiado complicado para propiciar a efetiva construção e utilização. Em torno de 1962, um componente eletrônico de estado sólido substituiu as válvulas eletrônicas e os cilindros do piano, e a tecnologia foi usada a bordo dos navios da marinha dos EUA, a fim de proporcionar comunicações seguras durante a Crise dos Mísseis em Cuba, nos dias de hoje, os rádios de espalhamento de espectro são usados no sistema de comunicações por satélite Milstarda, do Comando Espacial da Força Aérea dos EUA; em telefones celulares digitais e em redes de dados wireless.

Frequency-Hopping Spread Spectrum (FHSS)

O projeto original de Lamarr e Antheil para o rádio de espalhamento de espectro usava um sistema de salto de frequência. Como sugere o nome, a tecnologia FHSS divide um sinal de rádio em pequenos segmentos e "salta" de uma frequência para outra várias vezes por segundo, à medida que transmite aqueles segmentos. O transmissor e o receptor estabelecem um padrão de saltos sincronizados que definem a ordem de sequência na qual serão usados diferentes canais.

Os sistemas FHSS evitam a transferência de outros usuários, por usar um sinal transportador estreito, que altera a frequência várias vezes por segundo. Pares de transmissor e receptor adicionais podem usar padrões diferentes de salto no mesmo conjunto de subcanais no mesmo instante. Em qualquer instante determinado no tempo, cada transmissão provavelmente estará usando um subcanal diferente, de maneira que não exista interferência entre os canais. No caso de ocorrência de conflitos, o sistema reenviaria o mesmo pacote até que o receptor obtenha uma cópia limpa e envie uma confirmação de volta para a estação transmissora.

Para serviços de dados wireless, a banda de 2,4 GHz não licenciada é dividida em 75 subcanais, cada um deles com 1 MHz de largura. Cada salto de frequência adiciona uma sobrecarga ao fluxo de dados; portanto, as transmissões FHSS são relativamente lentas.

Direct-Sequence Spread Spectrum (DSSS)

A tecnologia DSSS usa um método conhecido como sequência 11-chip Barker para espalhar o sinal de rádio através de um único canal com 22 MHz de largura, sem alterar as frequências. Cada link do DSSS utiliza um único canal, sem qualquer salto entre as frequências. Como mostra a Fig. 1.3 abaixo, a transmissão DSSS usa mais largura de banda mas energia menor em comparação a um sinal convencional. O sinal digital à esquerda representa uma transmissão convencional na qual a energia é concentrada dentro de uma largura de banda mais compacta. O sinal do DSSS à direita utiliza a mesma quantidade de energia mas a espalha através de uma banda mais ampla de frequências de rádio.

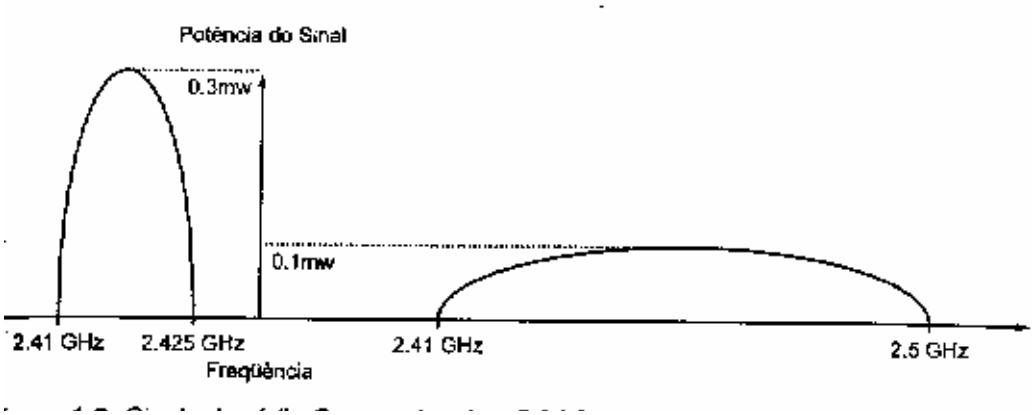

Fig. 1.3: sinais de rádio convencionais e DSSS

Evidentemente, o canal DSSS de 22 MHz é um pouco mais extenso do que os canais de 1 MHz usados no sistema FHSS.

Um transmissor DSSS quebra cada pedaço do fluxo de dados original em uma série de padrões de bits redundantes denominados *chips*, e os transmite para um receptor que reagrupa os chips de volta em um fluxo de dados idêntico ao original. A maior parte da interferência provavelmente ocupa uma largura de banda mais estreita do que um sinal DSSS e, além disso, cada bit é dividido em diversos chips; portanto, o receptor geralmente pode identificar ruídos e rejeitá-los, antes de decodificar o sinal.

Da mesma maneira que outros protocolos de rede, um link DSSS wireless troca mensagens de *estabelecimento de comunicação* dentro de cada pacote de dados para confirmar se o receptor consegue entender cada pacote. A taxa de transmissão de dados padrão em uma DSSS 802.11b é de 11 Mbps, mas quando a qualidade do sinal não suporta essa velocidade, o transmissor e o receptor usam um processo denominado *dynamic rate shifting*, para reduzir a velocidade até 5,5 Mbps. A velocidade deve ser reduzida quando existe uma fonte de ruído elétrico próximo ao receptor, ou quando o transmissor e o receptor estão afastados demais para suportar uma operação a total velocidade. Se a velocidade de 5,5 Mbps ainda for muito elevada, ela poderá ser reduzida novamente.

Alocação de frequência

De acordo com acordos internacionais, uma janela do espectro de rádio próxima a 2,4 GHz deve estar supostamente reservada para serviços industriais, científicos e médicos não licenciados, incluindo WLANs. A tabela abaixo mostra as atribuições de frequências em diversos países.

Região	Banda de Freqüência
América do Norte	2.4000 a 2.4835 GHz
Europa	2.4000 a 2.4835 GHz
França	2.4465 a 2.4835 GHz
Espanha	2.445 a 2.475 GHz
Japão	2.471 a 2.497 GHz

Tabela 1.1: Atribuições de frequência de espalhamento de espectro de 2.4 GHz não licenciadas

Normalmente, existe uma superposição suficiente entre os vários padrões nacionais a fim de permitir que o mesmo equipamento opere legalmente em qualquer lugar do mundo. Poderá ser necessário modificar seu adaptador de rede para um número de canal diferente quando se viaja para outro país, mas quase sempre haverá uma maneira de conectar, assumindo-se que exista uma rede dentro do intervalo do seu adaptador.

Nos EUA, os dispositivos Wi-Fi usam 11 canais. Muitos outros países usam 13 canais e o Japão usa 14. Mas na França somente 4 estão disponíveis. Felizmente, o mundo inteiro usa o mesmo conjunto de números de canal, como pode ser visto na tabela abaixo.

Tabela 1.2: Atribuições de Canal de Ethernet Wireless

Canal	Freqüência do Canal (MHz) e Local
1	2412 (Estados Unidos, Europa e Japão)
2	2417 (Estados Unidos, Europa e Japão)
3	2422 (Estados Unidos, Europa e Japão)
4	2427 (Estados Unidos, Europa e Japão)
5	2432 (Estados Unidos, Europa e Japão)
6	2437 (Estados Unidos, Europa e Japão)
7	2442 (Estados Unidos, Europa e Japão)
8	2447 (Estados Unidos, Europa e Japão)
9	2452 (Estados Unidos, Europa e Japão)
10	2457 (Estados Unidos, Europa, França e Japão)
11	2462 (Estados Unidos, Europa, França e Japão)
12	2467 (Europa, França e Japão)
13	2472 (Europa, França e Japão)
14	2484 (apenas Japão)

Na dúvida, pode-se usar os canais 10 e 11, que são legais em todos os lugares.

É bom lembrar que cada canal tem uma largura de 22 MHz e, portanto, se sobrepõe a diversos outros canais que estejam acima ou abaixo dele. A banda de 2.4 GHz inteira tem espaço para apenas três canais completamente separados. O uso de canais adjacentes gera interferência. Para minimizar este tipo de interferência, deve-se tentar coordenar o uso do canal com os gerentes da rede mais próxima. Se possível, cada rede deve usar canais com diferença de 25 MHz entre si (6 canais). Por exemplo, para três canais, as melhores opções seriam os canais 1, 6 e 11.

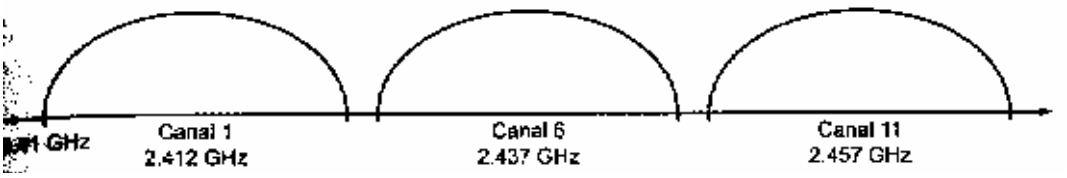

Fig. 1.4: Os canais 1, 6 e 11 não interferem uns com os outros

As especificações 802.11 e várias agências reguladoras nacionais (como a *Federal Communications Commission*, FCC, nos EUA) também definiram limites para a quantidade de potência do transmissor e do ganho de antena usada por um dispositivo wireless. Esta restrição pretende limitar a distância na qual um link de rádio pode alcançar, permitindo que mais redes operem nos mesmos canais, sem interferências.

Movimentação de dados

Até agora, temos vários transmissores e receptores de rádio, todos operando nas mesmas frequências, e todos usando o mesmo tipo de modulação (método usado para a adição de algum tipo de conteúdo, como voz ou dados digitais, a uma onda de rádio). O próximo passo consiste em enviar alguns dados da rede através desses rádios.

Verificação de erros

Em um circuito de transmissão ideal, o sinal observado em uma extremidade é absolutamente idêntico ao que surge na outra extremidade. Porém, no mundo real, quase sempre haverá algum tipo de ruído capaz de interferir com o sinal original. *Ruído* é definido como qualquer coisa que seja adicionado ao sinal original. Qualquer que seja a causa, o ruído no canal é capaz de interromper o fluxo de dados. Em um sistema de comunicações moderno, esses bits são transportados com extrema rapidez de forma que um ruído que ocorra por uma fração de segundo pode comprometer seriamente a comunicação.

Sendo assim, deve-se inserir um processo conhecido como *verificação de erros* no fluxo de dados. A verificação de erros é obtida pela inclusão de algum tipo de informação padronizada, conhecida como *checksum*, em cada byte. Se o checksum apurado pelo receptor não for o esperado é solicitada uma retransmissão.

Estabelecimento de comunicações (handshaking)

Evidentemente, não basta que o computador que origina uma mensagem ou um fluxo de dados esteja online e inicie o envio de bytes. Primeiramente, é preciso avisar o dispositivo na outra extremidade, de que está pronto para o envio e certificar se o destinatário pretendido está pronto para aceitar os dados. Para isso, uma série de solicitações e respostas de um estabelecimento de comunicações deve envolver os dados reais.

Descobrindo o destino

Para se estabelecer uma comunicação normalmente se necessita, primeiramente, configurar a conexão (por meio de uma ligação telefônica, por exemplo), mas depois que já estiver conectado, o link permanece ativo até que se instrua o sistema para desconectar. Este tipo de conexão é adequado para links de voz e de dados simples mas não é particularmente eficiente para dados digitais em uma rede complexa que sirva a muitas origens e destinos, pois amarra o circuito o tempo todo, mesmo quando nenhum dado está sendo transferido através do canal.

A alternativa consiste em enviar a mensagem para um centro de comutação que irá mantê-la até que um link com o destino seja disponibilizado. Isto é conhecido como um sistema *store and forward*. Se a rede de comunicações cobrir um amplo território, a mensagem poderá ser encaminhada para um ou mais centros de comutação intermediários, antes de alcançar os destino. A principal vantagem desta abordagem é que muitas mensagens podem compartilhar os mesmos circuitos, de acordo com a disponibilidade.

Para tornar a rede ainda mais eficiente, é possível dividir mensagens mais longas do que algum limite arbitrário, em pedaços separados, denominados *pacotes*. Os pacotes provenientes de mais de uma mensagem podem viajar juntos no mesmo circuito, sendo reagrupados ao chegar ao destino. Cada pacote de dados deve conter ainda outro conjunto de informações: o endereço do destino do pacote, a ordem de sequência desse pacote e outras.

Um pacote de dados que inclua informações de endereço e de controle na frente dos bits que compõem o conteúdo da mensagem, seguidas por uma sequência para verificação de erros, é chamado de *frame*. Tanto as redes com fio quanto as wireless dividem o fluxo de dados em frames, contendo várias informações sobre o estabelecimento de comunicações, junto com os dados originais.

É importante ressaltar que cada item adicionado aos dados originais, aumenta o tamanho do pacote e, automaticamente, aumenta o tempo necessário para a transmissão. A velocidade nominal inclui esses dados adicionais. Em outras palavras, mesmo que se tenha uma conexão a 11 Mbps, sua velocidade de transferência de arquivo real deverá ser de apenas 6 ou 7 Mbps.

Controles de rede wireless 802.11b

A especificação 802.11b controla a maneira como os dados são transportados através da camada física (o link do rádio), definindo uma camada *Media Access Control* (MAC) que manipula a interface entre a camada física e o restante da estrutura da rede.

A camada física

Em uma rede 802.11, o transmissor adiciona um preâmbulo de 144 bits a cada pacote, incluindo 128 bits, utilizados pelo receptor para se sincronizar com o transmissor, e um campo *start-of-frame* de 16 bits. Isso tudo é seguido por um campo de 48 bits, contendo informações sobre a velocidade de transferência dos dados, o comprimento dos dados contidos no pacote e uma sequência de verificação de erros. Esse cabeçalho é conhecido como *preâmbulo PHY*, pois controla a camada física do link de comunicações.

O cabeçalho especifica a velocidade dos dados que o seguem; portanto, o preâmbulo e o cabeçalho sempre são transmitidos em 1 Mbps. Assim, mesmo que um link esteja operando em 11 Mbps plenos, a velocidade efetiva será consideravelmente mais lenta. Na prática, pode-se esperar, no máximo, 85 por cento da velocidade nominal.

Esse preâmbulo de 144 bits é remanescente dos sistemas DSSS mais antigos e lentos, tendo permanecido na especificação para garantir a compatibilidade dos dispositivos 802.11b com os padrões mais antigos mas, na prática, ele não faz nada de útil. Existe uma alternativa opcional que usa um preâmbulo de 72 bits, mais curto.

Em um preâmbulo mais curto, o campo de sincronização possui 56 bits combinados com o mesmo campo start-of-frame de 16 bits, usado em preâmbulos longos. O preâmbulo curto é incompatível com os hardware 802.11 antigo.

Uma rede leva o máximo de 192 milisegundos para manipular um preâmbulo longo, se comparado aos 96 milisegundos para um preâmbulo curto. Em outras palavras, o preâmbulo curto reduz a sobrecarga em cada pacote pela metade, o que constitui uma significativa diferença no que se refere ao *throughput* (quantidade de dados transmitidos em uma unidade de tempo) de dados real, especialmente para fatos como fluxo de serviços de áudio, vídeo e de voz na Internet.

Alguns fabricantes usam o preâmbulo como padrão, enquanto outros usam o preâmbulo curto. Geralmente, é possível alterar o comprimento do preâmbulo no software de configuração de adaptadores de rede e pontos de acesso (AP – Access Point).

Para a maioria dos usuários, o comprimento do preâmbulo é um dos detalhes técnicos com os quais não é preciso se preocupar, pois ele é o mesmo para todos os dispositivos da rede. Há dez anos, todos nós precisávamos nos preocupar com a configuração dos "bits de dados" e "bits de parada", toda vez que efetuávamos uma chamada através do modem.

A camada MAC

A camada MAC controla o tráfego que ocorre na rede de rádio, evitando as colisões e os conflitos de dados, ao usar um conjunto de regras denominado *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA), e suportando as

funções de segurança especificadas no padrão 802.11b. Quando a rede inclui mais de um AP, a camada MAC, associa cada cliente de rede com o AP que proporciona a melhor qualidade de sinal.

Quando mais de um nó na rede tenta transmitir dados no mesmo instante, o CSMA/CA instrui todos os nós conflitantes, exceto um, para recuar e tentar novamente mais tarde, e permite que o nó sobrevivente envie seu pacote.

O CSMA/CA também possui um recurso opcional que define um AP (a ponte entre a LAN wireless e o backbone da rede) como um ponto coordenador, capaz de conceder a prioridade para um nó de rede que esteja tentando enviar tipos de dados críticos com relação ao tempo, como de voz ou *streaming media*.

A camada MAC pode suportar dois tipos de autenticação para confirmar se um dispositivo de rede está autorizado a se associar à rede: *autenticação aberta* e *autenticação de chave compartilhada*. Quando se configura a rede, todos os nós na rede devem usar o mesmo tipo de autenticação.

A camada MAC também define diversas opções no adaptador de rede:

- **Power mode** – o adaptador de rede suporta dois modos de energia: *Continuous Aware Mode* e *Power Save Polling Mode*. No primeiro, o receptor de rádio sempre estará ligado e consumindo energia. No Power Save Polling Mode, o rádio está ocioso na maior parte do tempo, mas efetua sondagens periódicas ao AP em busca de novas mensagens.
- **Access Control** – o adaptador de rede contém o controle de acesso que mantém os usuários não autorizados longe da rede. Uma rede 802.11b pode usar duas formas de controle de acesso: o SSID (*Service Set Identification*) (o nome da rede) e o endereço MAC (uma string de caracteres única, identificando cada nó da rede). Cada nó na rede deve ter o SSID programado nele, ou o AP não se associará com aquele nó. Uma tabela opcional de endereços MAC pode restringir o acesso aos rádios cujos endereços estejam na lista.
- **WEP encryption** – o adaptador de rede controla a função de criptografia *Wired Equivalent Privacy* (WEP). A rede pode usar uma chave de criptografia de 64 ou 128 bits, para codificar ou decodificar dados.

Dispositivos de rede

Quando já se tiver definido os links de rádio e o formato dos dados, o próximo passo será configurar uma estrutura de rede. Como os computadores usam os rádios e o formato dos dados para realmente trocar os dados?

As redes 802.11b incluem duas categorias de rádios: *estações* e *pontos de acesso*. Uma estação é um computador – ou algum outro tipo de dispositivo, como uma impressora – conectado a uma rede wireless através de um adaptador de interface de rede wireless interno ou externo.

Um ponto de acesso é a estação base para uma rede wireless e uma ponte entre esta rede e uma com fio tradicional.

Adaptadores de rede

Os adaptadores de rede para estações podem apresentar diversas formas físicas:

- *PC Cards embutidas (PCMCIA) para laptops*. Para suplantar a blindagem interna dos computadores, as antenas e luzes de status na maioria dos adaptadores de PC Cards wireless se estendem cerca de 2,75 cm além da abertura do soquete na placa. Outros adaptadores possuem soquetes para antenas externas.
- *Adaptadores de rede internos (PCI)*. A maioria dos adaptadores PCI são, na realidade, soquetes PCMCIA que podem ser conectados a uma placa de PC.
- *Adaptadores USB externos*. Estes geralmente constituem uma opção melhor que placas, pois quase sempre é mais fácil movimentar um adaptador localizado na extremidade de um cabo para uma posição de melhor recepção.
- *Adaptadores wireless on board para laptop*. Estes já vêm conectados à placa-mãe do computador. As antenas embutidas para rádio geralmente ficam ocultas dentro da tela *fold-over* do computador.
- *Adaptadores embutidos em PDAs e outros dispositivos handheld*.
- *Interfaces de rede internas embutidas em outros dispositivos, como sets telefônicos compatíveis com Internet e dispositivos de escritório ou residência.*

Um adaptador de rede deve trabalhar com qualquer sistema operacional, desde que esteja disponível um driver para esse adaptador.

Pontos de acesso

Os pontos de acesso geralmente são combinados com outras funções de rede. Dentre as configurações de AP comuns, estão incluídas:

- Estações base simples com uma ponte para uma porta Ethernet para conexão com uma LAN.
- Estações base que incluem um switch, hub ou roteador com uma ou mais portas de Ethernet com fio, junto com o ponto de acesso wireless.
- Roteadores de banda larga que proporcionam uma ponte entre um modem a cabo, ou postal DSL, e o ponto de acesso wireless.
- Pontos de acesso de software que utilizam um dos adaptadores de interface de rede wireless como estação base.
- Gateways residenciais que suportam uma quantidade limitada de canais operacionais.

O projeto físico dos pontos de acesso varia de acordo com os fabricantes. Independentemente de seu tamanho ou forma, cada AP inclui um rádio que envia e recebe mensagens e dados entre estações de redes, e uma porta Ethernet que se conecta a uma rede com fio.

Modos de operação

As redes 802.11b operam em dois modos: redes *ad-hoc* e redes de *infra-estrutura*. Uma rede ad-hoc geralmente é temporária. Trata-se de um grupo de estações autocontidas sem conexão com uma LAN mais ampla ou com a Internet. Inclui duas ou mais estações wireless sem nenhum AP ou conexão com o restante do mundo. Estas redes também são conhecidas como redes ponto-a-ponto e *Independent Basic Service Sets* (IBSS). A figura 1.6 mostra uma rede ad-hoc simples.

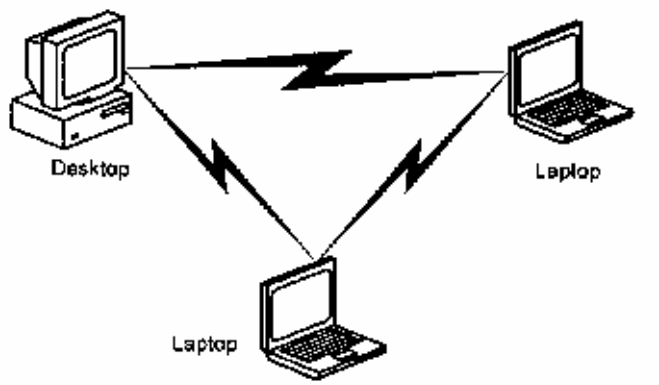

Fig. 1.6: Uma rede wireless ad hoc com três estações

As redes de infra-estrutura possuem um ou mais pontos de acesso, quase sempre conectados a uma rede com fio. Cada estação wireless troca mensagens e dados com o AP, que troca com outros nós na rede wireless ou com a LAN com fio. Qualquer rede que requeira uma conexão com fio através de um AP com uma impressora, ou servidor de arquivos ou gateway de Internet, é uma rede de infra-estrutura. A figura 1.7 mostra uma rede de infra-estrutura.

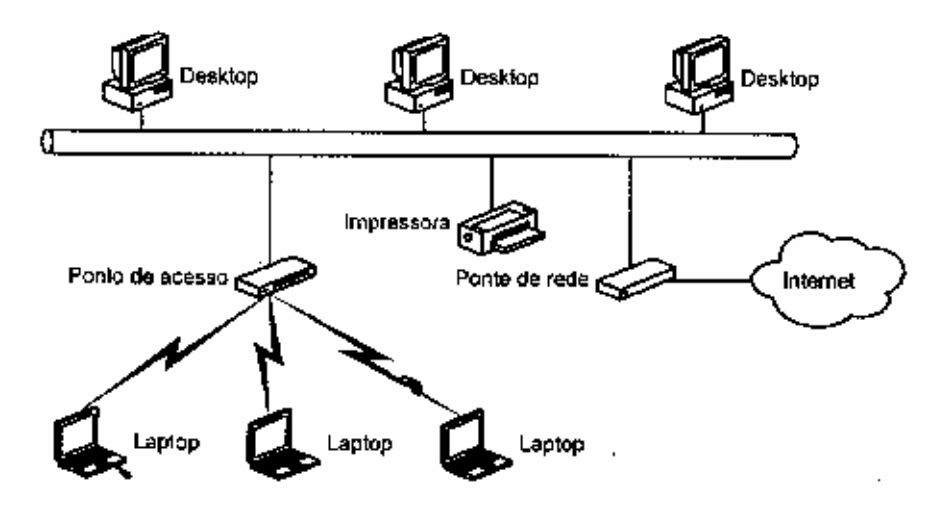

Fig. 1.7: Uma rede de infra-estrutura simples

Uma rede de infra-estrutura com uma única estação base também é conhecida como *Basic Service Set* (BSS). Quando a rede wireless usa dois ou mais pontos de acesso, a estrutura de rede é um *Extendend Service Set* (ESS). Já foi citado que o nome técnico de um ID de rede é SSID, mas também pode aparecer como BSSID ou como ESSID dependendo do modo de operação.

Uma rede com mais de um ponto de acesso (ESS) causa novas complicações. Primeiramente, a rede deve possibilitar que uma única estação base manipule os dados de uma estação em particular, mesmo que a estação esteja dentro do intervalo de mais de uma estação base. Além disso, se a estação estiver se movimentando durante uma sessão de rede, a rede poderá precisar ignorar a conexão entre um AP e outro. Uma rede 802.11b trata esse problema associando uma estação com um único AP de cada vez, ignorando os sinais das estações que não estão associadas. Quando o sinal enfraquece em um AP e aumenta em outro, ou o volume de tráfego força a rede a promover um rebalanceamento de carga, a rede reassocia a estação com um novo AP que seja capaz de proporcionar um serviço aceitável. Isto é chamado de *roaming*.

O que é necessário para o wireless

Este capítulo identifica os elementos que compõem uma rede wireless, oferecendo também conselhos para ajudar a decidir quais componentes melhor atenderão a necessidades específicas.

Todos falam a mesma língua (mais ou menos)

Dezenas de empresas produziram equipamentos que se qualificaram para a certificação do Wi-Fi. Para receber essa qualificação, cada dispositivo deve ser submetido a testes de interoperabilidade pelo laboratório de testes independente da Wi-Fi Alliance.

Os pontos de acesso e os adaptadores de rede de diferentes fabricantes podem ter aparências diferentes e seu próprio software de configuração, porém todos os circuitos internos de rádio são bastante parecidos e quase todos usam um dos poucos chips set padrão.

Em outras palavras, é possível usar qualquer combinação de adaptadores e pontos de acesso Wi-Fi, tudo junto na mesma rede. A palavra crítica nesta última sentença é *possível*. Um técnico, familiarizado com o funcionamento interno das redes 802.11b, é capaz de fazer uma rede com fornecedores mistos operar adequadamente.

Mas será que um leigo conseguiria? Provavelmente sim, mas não na primeira tentativa. A definição de todas as opções de configuração, de acordo com os valores corretos, pode levar bastante tempo e causar muitos aborrecimentos. Quase sempre os dispositivos de diferentes fabricantes terão diferentes configurações padrão. Por exemplo, alguns sistemas usam preâmbulos curtos como padrão enquanto outros usam preâmbulos longos; algumas configurações exigem chaves WEP na forma de caracteres ASCII, enquanto outras usam hexadecimais.

Quase sempre é mais fácil equipar a rede inteira com componentes de hardware de um único fabricante mas isso nem sempre é possível ou nem mesmo recomendável.

De qualquer forma, em algum momento será necessário integrar componentes de hardware e software de mais de um fabricante na mesma rede. As informações aqui contidas ajudarão a entender o que se precisa fazer para que tudo trabalhe em conjunto nessa situação.

Adaptadores de rede

Um adaptador de rede é a interface entre um computador e uma rede. Em uma rede wireless, o adaptador contém um transmissor de rádio que envia os dados do computador para a rede, e um receptor que detecta os sinais que chegam e os passa para o computador.

Deve-se considerar vários aspectos ao selecionar um adaptador de interface: o pacote físico, o tipo de antena, a compatibilidade com os pontos de acesso e outros nós da rede, e a compatibilidade com o sistema operacional do computador.

Fator forma

Na maioria dos casos, o adaptador se conecta a uma das portas de I/O de alta velocidade do computador. As exceções são os modernos notebooks que incluem interfaces 802.11b internas opcionais, os quais usam slots de expansão internos, como mini-PCI ou Apple AirPort, ou são montados nas placas-mãe dos computadores.

PC Cards

Adaptadores de rede em PC Cards são o tipo mais popular, pois a utilização mais frequente é a adição de computadores portáteis a LANs existentes. Praticamente todos os fabricantes de padrão 802.11b possuem, pelo menos, um adaptador de PC Cards em sua linha de produtos.

Os adaptadores são compactos e leves. Entretanto, é importante remover o adaptador do computador quando não estiver em uso, caso contrário, o adaptador continuará a irradiar sinais indesejáveis e possivelmente permitirá que um invasor se conecte ao seu computador sem que você saiba.

Todos os adaptadores PC Cards têm uma aparência bastante parecida, pois todos precisam se encaixar no soquete PCMCIA do computador. Como mostra a figura 2.1, eles têm o tamanho aproximado de um cartão de crédito, com um conector em uma ponta e, na outra, uma cobertura de plástico para a antena interna ou um conector para uma antena externa.

Fig. 2.1: Um adaptador Xircom Wireless Ethernet com uma antena interna

A maioria dos adaptadores PC Cards inclui uma ou duas luzes indicadoras na seção externa ao computador. Uma luz que indica se o adaptador está recendo energia do computador e o outro se acende quando o adaptador detecta um link de rádio ativo de um outro dispositivo.

Muitos adaptadores contêm duas antenas internas com uma diversidade de sistemas que comparam constantemente a qualidade dos sinais que chegam nas antenas e seleciona automaticamente o mais forte. Embora as duas antenas estejam apenas três a cinco centímetros separadas uma da outra, a melhoria proporcionada pode ser marcante.

Os adaptadores PC Cards geralmente possuem antenas onidirecionais embutidas mas alguns fabricantes também oferecem versões com conectores para antenas externas. A opção entre a interna e a externa é sempre difícil. Porém, é bom salientar que as antenas externas podem ser unidirecionais o que melhora consideravelmente sua performance.

Adaptadores USB

Caso o computador possua uma porta USB (*Universal Seria Bus*), uma adaptador USB wireless poderia ser a melhor maneira de conectar esse computador à rede 802.11b. O adaptador se conecta através de um cabo; portanto, nunca é um problema mover o adaptador inteiro para uma melhor posição.

A maioria dos adaptadores USB possui antenas cativas, geralmente montadas em articulações ou suportes que permitem promover ajustes finos em suas posições. As antenas também costumam ser maiores e mais fáceis de manipular neste padrão. Assim, pode-se esperar uma melhor qualidade de sinal em um dispositivo USB.

Placas de expansão internas

Os adaptadores wireless internos mais comuns são, na realidade, PC Cards montadas em soquetes PCMCIA que se encaixam em um slot de expansão PCI ou ISA. Porém, esta solução tem uma série de desvantagens, principalmente, na questão de interferências e posicionamento para obtenção de um melhor sinal.

Se houver problemas, existem duas maneiras de lidar com isso. Uma, seria usar um adaptador que possuísse conector para a instalação de antena externa. E a outra, seria a utilização de um adaptador USB pois, caso o computador não tivesse esse tipo de porta, há a possibilidade de se adicioná-la em placas de expansão PCI ou ISA.

Adaptadores internos

Diversas marcas importantes de notebooks começaram a apresentar adaptadores de rede wireless on-board. A vantagem óbvia é que o adaptador interno não exige transporte e já vem configurado.

Se for esse o caso, é bom certificar-se de ter uma maneira fácil de desativar o adaptador quando não estiver em uso.

Antenas internas x externas

Muitos pontos de acesso e a maioria dos adaptadores de rede wireless acompanham as antenas onidirecionais cativas. Isso é satisfatório na maioria dos casos. Entretanto, se os adaptadores com antenas embutidas não proporcionarem um sinal suficientemente adequado, por qualquer motivo, uma antena externa poderá ser a melhor maneira de resolver o problema. Via de regra, espera-se que uma antena externa proporcione um sinal pelo menos 15 por cento mais forte do que com antena embutida.

Uma antena unidirecional focalizará a maior parte do sinal em uma direção sendo mais eficiente em certos casos; porém, uma antena direcional em um AP é capaz de prejudicar a qualidade dos links para os outros nós das rede, como mostrado na figura 2.3.

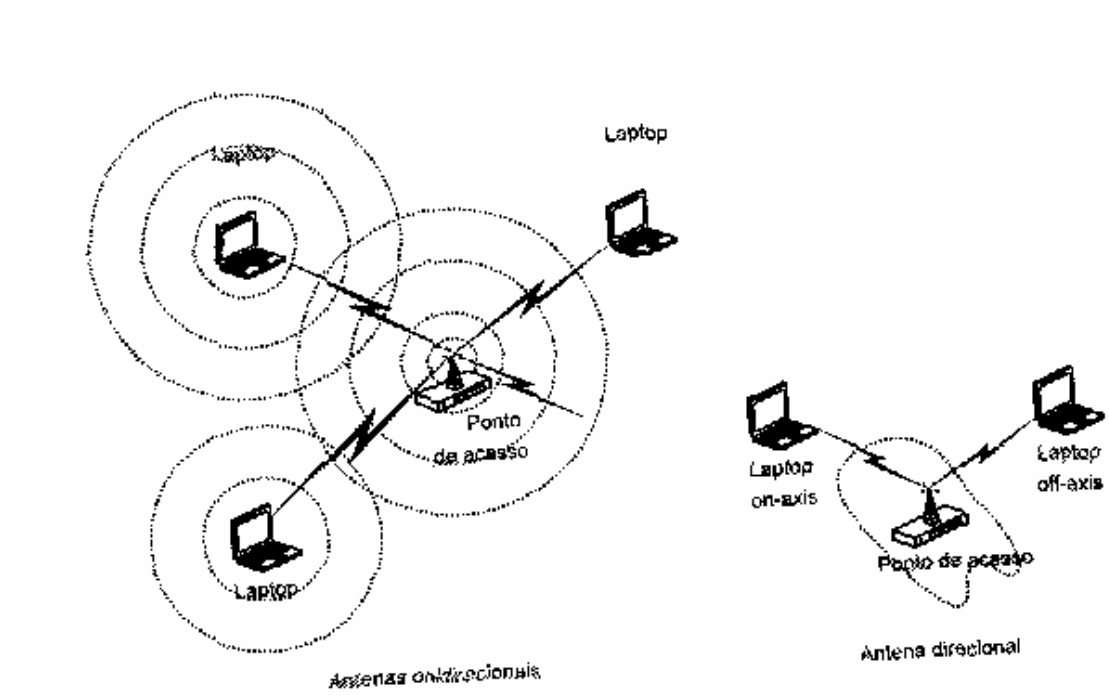

Fig. 2.3: Diferentes combinações de antenas direcionais e não-direcionais podem alterar a área de cobertura de uma rede.

Compatibilidade de sistema operacional

Da mesma maneira que qualquer outro dispositivo que seja usado com o computador, um adaptador de rede wireless exige um driver específico que contenha controles e interfaces que permitam ao adaptador trocar dados com o computador. Normalmente, esses drivers deverão acompanhar o equipamento. Caso contrário, será necessário encontrá-lo em algum outro lugar (site do fabricante, por exemplo) ou escolher um adaptador diferente que suporte seu sistema operacional.

Facilidade de utilização

Cada adaptador wireless usa um programa utilitário de configuração que controla o modo de operação, o número do canal e todas as outras opções de configuração que devem combinar com as configurações para os outros nós da rede. O fabricante geralmente fornece o programa em um CD ou disquete que vem junto com o adaptador.

Em condições ideais, um usuário comum nunca precisaria examinar o utilitário de configuração. Mas, eventualmente, se faz necessário modificar tais parâmetros. Portanto, tanto o utilitário de configuração quanto o display de status devem ser de fácil entendimento e utilização. Para isso, a pergunta chave deve ser satisfeita: Você consegue examinar a janela de configuração e entender como alterar as definições?

Segurança

A especificação 802.11b inclui um esquema de segurança denominado WEP (Wired Equivalence Privacy) que usa uma chave de criptografia de 64 ou 128 bits. O formato de 64 bits é um padrão comum mas existem algumas diferenças entre as técnicas de criptografia de 128 bits oferecidas por diversos fabricantes. Portanto, nem sempre é possível que diferentes marcas de adaptadores e pontos de acesso troquem dados, quando seus recursos de segurança aprimorada estão ativos.

Se a segurança aprimorada for indispensável, poderá ser necessário adotar uma padronização, por uma única marca de hardware ou por um grupo de marcas que compartilhem o mesmo tipo de criptografia de 128 bits (como Cisco e Xircom, ou Orinoco e AirPort da Apple).

Documentação e suporte técnico

Todos os fabricantes de hardware Ethernet wireless oferecem algum tipo de suporte técnico para seus usuários. Entretanto, a qualidade e a utilidade do suporte variam amplamente de um fornecedor para outro. No mínimo, um nível adequado de suporte técnico deve incluir um manual de usuário preciso e escrito com clareza, um centro de suporte que responda a perguntas específicas por telefone e e-mail, um site com respostas a perguntas frequentes e um centro de download que ofereça as versões mais recentes dos drivers de dispositivo, os utilitários de configuração, e software de display de status, disponíveis para download gratuito.

Não esquecer a regra do **LPM**.

Reputação

Quase sempre é útil aprender com a experiência das outras pessoas, com relação aos adaptadores wireless (ou qualquer outra coisa) antes de gastar seu dinheiro. Os fabricantes nem sempre (ou nunca) são imparciais. Grupos de usuários locais, publicações de revisões de produtos e discussões na Internet podem ser fontes úteis para a obtenção de informações sobre equipamentos wireless. Por exemplo, o site da *Practically Networked* (http://www.practicallynetworked.com) é um bom local para procurar revisões e avaliações dos usuários quanto ao dispositivo wireless.

Adaptadores para redes Ad-Hoc

Em uma rede ad-hoc, cada adaptador de rede troca dados com todos os demais nós por meio de links diretos, sem um AP atuando como um nó central. As redes ad-hoc são úteis para redes isoladas e de pequeno porte, e compartilhamento de arquivos ponto-a-ponto direto. Por exemplo, alguém que use um notebook e um computador desktop, pode configurar uma rede ad-hoc para transferir arquivos entre os dois.

As redes ad-hoc wireless são bem menos comuns do que redes de infra-estrutura, mas fazem parte da especificação 802.11b; portanto, quase todas as interfaces de adaptador de rede wireless e programas de configuração oferecem uma opção para rede ad-hoc.

Adaptadores de dupla finalidade

As redes Wi-Fi tornaram-se amplamente populares mas não se trata da única tecnologia disponível. Também estão disponíveis diversos outros sistemas, incluindo Bluetooth (que proporciona conexões com intervalo muito curto para

dispositivos periféricos e acessórios para computadores, como headfones e teclados) e 802.11a (que usa um conjunto diferente de frequências de rádio para proporcionar um link de velocidade mais elevada com uma rede, do que a 802.11b). Cada uma dessas opções oferece soluções, até certo ponto, para um conjunto diferente de problemas, e cada uma atende um nicho de mercado específico. Vários fabricantes anunciaram novos produtos que combinam uma interface de adaptador de rede 802.11b com uma interface com algum outro serviço wireless. Alguns podem detectar e utilizar tanto redes 802.11b (2.4 GHz) quanto 802.11a (5.4 GHz), enquanto outros integram redes 802.11b com o Bluetooth. Outros podem, ainda, combinar o acesso a LANs Wi-Fi com dados de celular ou outros serviços de rede de área ampla (WANs). Os benefícios de um ponto de acesso combinado são óbvios – um dispositivo é mais indicado para ser transportado e de mais fácil instalação do que dois dispositivos e proporciona acesso a mais redes e serviços. Além disso, devido ao mesmo transmissor e receptor de rádio manipular ambos os serviços, o potencial para a interferência também é reduzido.

Um adaptador de rede dupla finalidade ideal detectaria automaticamente os sinais de rádio de todas as redes compatíveis, dentro de um intervalo, e permitiria que um usuário configurasse uma conexão instantânea com qualquer uma dessas redes, sem a necessidade de se preocupar com o tipo de link que está sendo usado pela rede. É possível que esse adaptador de rede wireless surja nos próximos anos.

Por exemplo, no início de 2002 foi introduzida a Blue802 pela Intersil e a Silicon Wave. A Blue802 permite que conexões Bluetooth e 802.11b operem simultaneamente por meio de um único adaptador; dessa forma, um computador pode usar links Bluetooth para um mouse, um teclado, uma impressora ou outro computador no mesmo instante em que está conectado à Internet ou a uma LAN através da rede Wi-Fi. Isso é um grande negócio, pois tanto o 802.11b quanto o Bluetooth usam as mesmas frequências de rádio (2.4 GHz) e cada serviço geralmente pode causar interferências nos outros. O Blue802 coordena os dois tipos de transmissão de rádio a fim de otimizar a performance de ambos.

Pontos de acesso

A maioria dos adaptadores de rede têm uma única função: trocar dados entre um computador e uma rede. Os pontos de acesso, por outro lado, oferecem uma ampla variedade de recursos e funções. Eles estão disponíveis como pontos de acesso simples em combinação com hubs, switches e roteadores para conexões com fio, computadores e outros dispositivos próximos. Existe uma categoria completa de pontos de acesso wireless para redes domésticas, denominada *gateways residenciais*.

Existem algumas características que se pode desejar atender ao selecionar um AP. Se, por exemplo, a inspeção do local da instalação sugerir que se necessita de antenas de alto ganho, deve-se usar um AP com um conector de antena externa em vez de uma antena cativa montada em caráter permanente. Em uma rede com um grande volume de tráfego, em que se planeja usar mais de um canal de rádio no mesmo instante, um único AP contendo dois módulos de rádio pode substituir dois pontos de acesso separados.

A melhor maneira de escolher o tipo de AP para sua rede consiste em decidir de quais tipos de conexão você provavelmente precisará. Você está acrescentando um acesso wireless a uma rede com fio existente? Ou você deseja proporcionar alguns novos links com fio junto com o serviço wireless? Você deseja usar a rede wireless para compartilhar o acesso à Internet? As respostas para todas essas perguntas ajudarão a escolher o AP adequado para a rede.

LANs wireless puras

Quando todos os nós em uma LAN trocam dados por rádio, o ponto de acesso atua como um hub que proporciona o ponto de controle central para a rede, como mostra a figura 2.6. Na verdade, o "ponto de acesso" nesse tipo de rede não proporciona acesso a coisa nenhuma, exceto a outros nós wireless. Esse tipo de arranjo wireless constitui uma das funções básicas de qualquer AP; portanto, se for esse o projeto, deve-se usar um modelo mais simples e mais barato que seja capaz de proporcionar um sinal útil para sua área de cobertura.

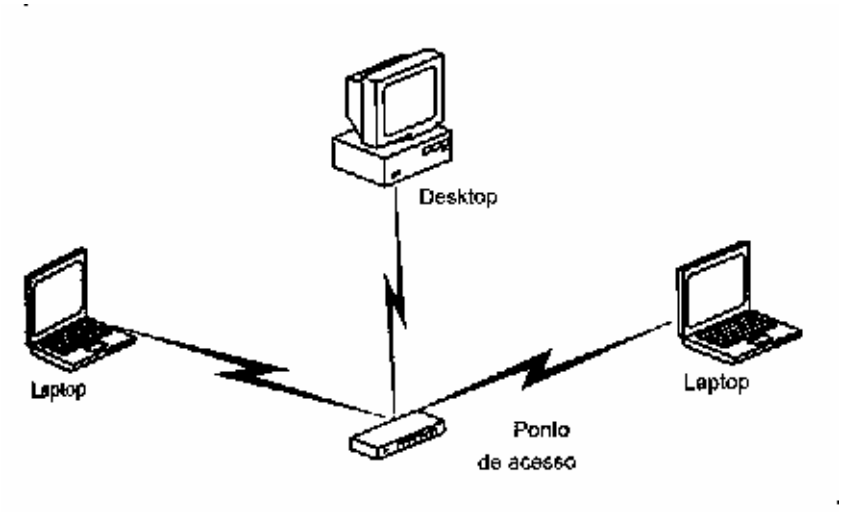

Fig. 2.6: Uma rede wireless simples sem nenhuma conexão externa

Acesso wireless a uma LAN com fio

Qualquer AP pode atuar como uma estação base, adicionando links wireless a uma LAN com fio existente, como mostra a figura 2.7. O AP apresenta a mesma aparência que o restante da rede, como faz um hub subsidiário ou switch que conecta nós com fio à rede.

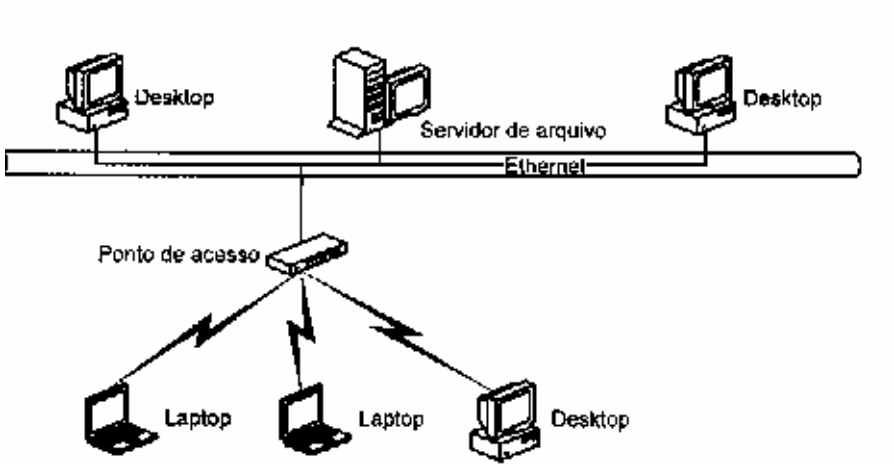

Fig. 2.7: Um ponto de acesso wireless conectado a uma rede Ethernet com fio

Nesse tipo de LAN híbrida *wired-and-wireless*, cada dispositivo na rede pode trocar dados com todos os outros nós da rede, independente de como está conectado.

Um AP que atue como uma ponte entre as seções com fio e sem da rede, geralmente possui uma única porta Ethernet RJ-45 de 10Mbps, 100Mbps ou 1Gbps para conectar um cabo à LAN com fio. Geralmente, existe uma porta serial adicional para um terminal remoto que pode ser usada pelo gerente da rede para inserir comandos de configuração e receber informações sobre o status.

Combinando o ponto de acesso com um Hub com fio

Em uma nova LAN que inclui tanto conexões com fio quanto links wireless, a mlhor abordagem pode ser um único dispositivo que combine as funções de um ponto de acesso wireless com um hub ou switch com fio, como mostra a figura 2.8. Esse tipo de AP algumas vezes é descrito como roteador de banda larga.

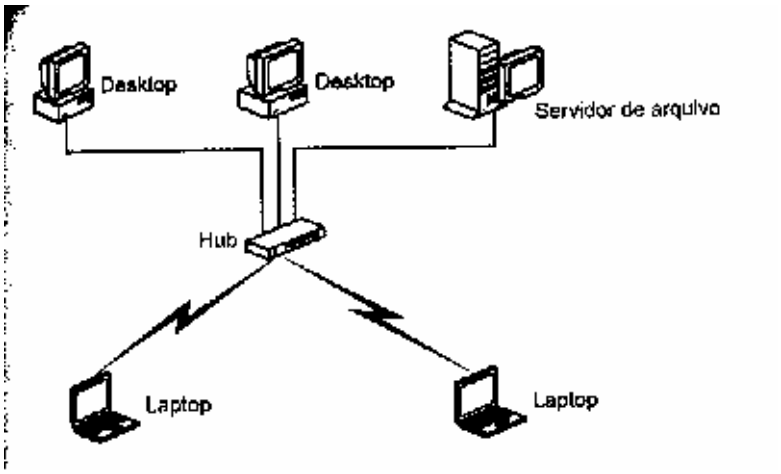

Fig. 2.8: Um ponto de acesso wireless combinado com um switch de banda larga controla tanto os segmentos wireless quanto com fio de uma rede híbrida

O roteador de banda larga possui tipicamente três tipos de conexões de rede:

- Links de rádio para computadores equipados com adaptadores Ethernet wireless.
- Uma ou mais portas Ethernet para links com fio para computadores com interface de placas de rede.
- Uma porta WAN de banda larga para a conexão do roteador com o backbone da rede ou para empilhar o roteador com hubs ou switches adicionais.

Alguns roteadores também incluem um servidor de impressão.

Os principais benefícios de pontos de acesso e hubs combinados são a conveniência e a economia em um escritório residencial ou de pequeno porte, onde é fácil passar cabos entre alguns dos computadores da rede. Uma unidade combinada também pode constituir a maneira mais rápida de ampliar uma rede existente, tanto para os nós com fio quanto wireless em um local remoto.

Gateways de banda larga

Um *gateway de banda larga* é um AP que inclui uma porta para uma conexão direta com um DSL, ou modem a cabo, que fornece acesso de alta velocidade à Internet, como mostra a figura 2.9. Alguns dispositivos de gateway também incluem diversas portas RJ-45 Ethernet para conexões com fio com computadores locais.

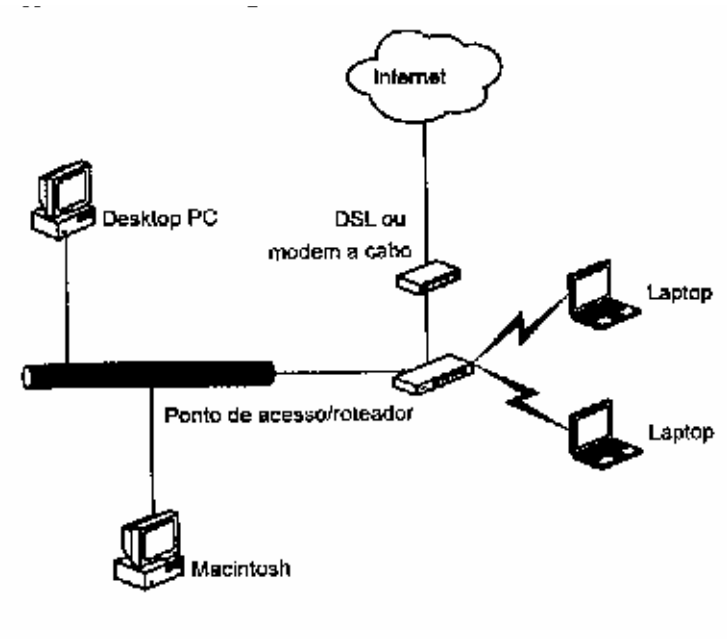

Fig. 2.9: Um ponto de acesso combinado com um gateway de banda larga suporta uma rede wireless que compartilha uma conexão de alta velocidade com a Internet

Essa abordagem é mais prática em uma rede doméstica ou em um pequeno negócio, em que o serviço de Internet banda larga necessite ser compartilhado pois o AP deve ser posicionado no melhor local possível para proporcionar uma cobertura wireless.

Múltiplos pontos de acesso

Um único AP pode ser completamente adequado para suportar uma WLAN em um espaço aberto e relativamente pequeno, com um volume moderado de tráfego. Porém, quando a rede precisar cobrir uma área muito ampla, ou um espaço com obstruções causadas por paredes, mobílias ou outros objetos, ou por interferência de outros rádios, provavelmente se precisará adicionais mais pontos de acesso.

A maioria das redes domésticas, e muitas redes em pontos comerciais muito pequenos, precisa de um único AP; portanto, a escolha de um AP que suporte *roaming* caracteriza um problema para os gerentes de redes extensas e complexas.

A especificação 802.11b inclui uma função roaming que muda de AP quando a qualidade de sinal do novo AP é melhor que o original. Depois de se associar a um novo AP, ele inspeciona todos os outros canais de rádio a fim de determinar se algum outro AP, operando em um canal diferente, oferece um serviço melhor. Caso encontre, a troca se efetua novamente.

Portanto, os pontos de acesso com áreas de cobertura sobrepostas devem ser definidos com diferentes números de canal. Para a menor quantidade de interferência de um AP até o próximo, os números de canal de qualquer par de pontos de acesso adjacentes deve ter, pelo menos, cinco canais de diferença.

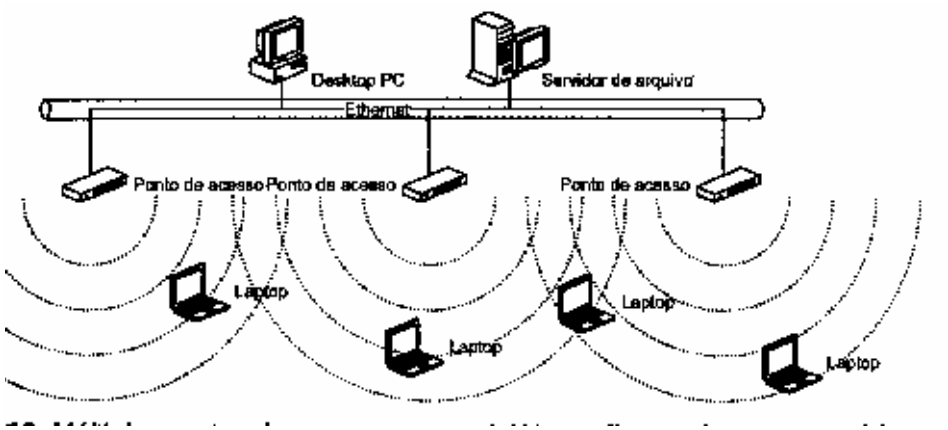

Fig. 2.10: Múltiplos pontos de acesso em uma LAN com fio permitem que usuários wireless possam se utilizar desse serviço.

Na maioria dos casos, um cliente de rede não se associará a um AP diferente, a menos que o cliente se mova para um local diferente enquanto o link com a rede está ativo ou quando ocorre o aumento do volume de tráfego no canal atual.

Na maioria das situações, múltiplos pontos de acesso devem ser posicionados de forma a proporcionar uma cobertura que sobreponha em cerca de 30 por cento um AP para o próximo. Entretanto, se a WLAN precisar suportar uma grande quantidade de usuários simultâneos, a melhor maneira de promover o balanceamento de carga consistirá em instalar dois ou mais pontos de acesso no mesmo local, com cada AP definido com um canal de rádio diferente e não-interferente.

Antenas externas

Se se consegue estabelecer um link de dados confiável de alta velocidade com qualquer local da sua rede, usando as antenas embutidas nos adaptadores e pontos de acesso, certamente não haverá motivo para desperdiçar tempo, dinheiro ou energia, com antenas externas.

Mas quando as condições de recepção não forem perfeitas, ou quando se quer enviar um sinal de rádio o mais distante possível, uma antena separada poderá evitar a interferência, aumentar a velocidade de transferência dos dados, expandir a área de cobertura e estabelecer links de comunicação confiáveis em locais onde seriam pouco mais que um "ruído" com antenas internas comuns.

Em uma análise preliminar, poderá parecer que a maneira mais fácil de melhorar a qualidade de um sinal de rádio consiste em aumentar a potência que sai do transmissor. Em vez dos ínfimos 30 miliwatts produzidos pela maioria dos adaptadores, por que não elevar esse valor para 10 ou 20 watts, ou ainda mais? Isso não produziria um sinal muito mais forte?

É claro que sim, mas o FCC e as demais agência reguladoras espalhadas pelo mundo, não permitem. Rádios mais poderosos produziriam sinais mais fortes, que causariam muito mais interferências em áreas mais amplas, o que significa que menos usuários poderiam compartilhar o mesmo trecho do espectro de rádio.

Por comparação, a estação de TV que usa o canal 4 na cidade de Nova Iorque transmite com 100 mil watts de potência de saída mas a estação mais próxima que usa o mesmo canal está situada em Boston, cerca de 320 Km de distância. Os rádios em uma WLAN utilizam menos que um watt; portanto, o sinal quase sempre é inaudível a algumas dezenas de metros de distância.

Por não ser possível aumentar a quantidade de energia produzida pelos transmissores de rádio, o próximo método mais indicado para melhorar a qualidade do sinal consiste em otimizar a performance das antenas.

As antenas são de dois tipos: onidirecionais, que transmitem e recebem em todas as direções, com a mesma força; e antenas direcionais, que concentram suas energias e sensitividades em uma direção específica. Em uma WLAN, um AP com uma antena onidirecional é mais útil para se cobrir uma área ampla. Um adaptador de rede com antena onidirecional pode se comunicar igualmente bem com qualquer AP próximo.

Só para referência, uma antena externa onidirecional amplia a área de sinal útil para cerca de 35 metros de distância, ao invés dos 10 metros para antenas embutidas. Usando-se antenas externas nas duas extremidades, pode-se esperar um alcance de 40 metros.

A forma da área de cobertura da antena direcional e sua quantidade de ganho (força do sinal do transmissor e sensitividade do receptor) dependem do desenho exato de cada antena. Algumas antenas direcionais podem proporcionar uma quantidade moderada de ganho com relação a um padrão mais amplo, enquanto outras podem focalizar três ou quatro vezes (ou ainda mais), e o ganho se dará em uma área muito mais restrita.

Antenas direcionais podem proporcionar uma enorme melhoria na qualidade do sinal sobre uma área de cobertura firmemente focalizada, podendo também reduzir a interferência de áreas "nulas" fora daquele padrão de cobertura, o que significa que podem apresentar diversas utilizações em uma WLAN:

- Podem permitir que um usuário fora da área "normal" de cobertura se associe à rede.
- Podem aumentar a área de cobertura efetiva, servida por um AP, limitando a cobertura a uma direção.
- Podem reduzir ou eliminar o efeito da interferência *off-axis* de outros sinais de rádio.
- Podem reduzir a quantidade de interferência que uma WLAN cria para outros rádios.
- Podem estabelecer links ponto-a-ponto de longa distância e estacionários entre prédios.

Características da antena

As antenas externas apresentam formas e tamanhos variados. Ao selecionar uma antena, deve-se considerar vários itens, incluindo o padrão de cobertura, o ganho, o fator de formação e a resistência às intempéries.

Padrão de cobertura

A folha de especificação de uma antena inclui um diagrama mostrando a forma do padrão de cobertura da antena. De modo geral, o padrão é *onidirecional* (irradia e recebe igualmente bem em todas as direções), *direcional* (com a radiação ou recepção mais forte em uma direção) ou *figureeight* (boa cobertura para a parte frontal e posterior e cobertura fraca nas laterais).

Os catálogos e as folhas de especificação para antenas direcionais geralmente incluem um ângulo de abertura, largura do feixe, ou área de captura, expressos em graus. O ângulo de abertura é a seção de um círculo que contém a cobertura ou sensitividade de energia máxima da antena. Por exemplo, se uma antena tiver um ângulo de abertura de 45 graus, a cobertura ou sensitividade máxima se estenderá para fora da parte frontal da antena, em um ângulo de 45 graus.

Ganho

O *ganho* de uma antena é a proporção entre a energia da transmissão ou da sensitividade da recepção, quando comparada a uma antena bipolar padrão (um bipolo é uma antena direta, alimentada pelo centro, com metade do comprimento de onda, como a antena *twin-lead* em forma de T, fornecida com muitos rádios e sintonizadores de FM). O ganho geralmente é expresso em dB*i* (decibéis over isotrópico).

Fator de formação

Uma antena bipolar para um rádio com 2.4 GHz tem somente cerca de 2,75 cm de comprimento, mas os refletores e outros elementos que adicionam ganho e características direcionais podem ser muito mais longos. Muitas antenas são fornecidas dentro de uma tampa protetora que não afeta sua performance, mas que é capaz de manter a antena propriamente dita, limpa e seca, e facilitar a montagem da antena em um poste ou uma parede.

As antenas onidirecionais são sempre cabos ou hastes verticais, sem mais de cinco ou oito centímetros de diâmetro. Algumas antenas onidirecionais de alto ganho podem ter até 60 ou 90 centímetros de comprimento. Para a utilização em ambientes fechados, especialmente em ambientes com tetos rebaixados, antenas onidirecionais especiais montadas no teto, podem constituir uma excelente opção para uma rede wireless.

As antenas direcionais podem apresentar várias formas, incluindo pratos e painéis parabólicos que incluem um refletor atrás da parte ativa da antena; as antenas que se assemelham a uma versão mais curta de uma antena de TV de telhado; e antenas *patch* ou de painel com diversos elementos, geralmente dentro de uma caixa protetora que se assemelha a um detector de fumaça ou montado em um suporte giratório que possibilita ajeitar a antena com mais precisão.

Proteção contra intempéries

As antenas que ficam expostas no ambiente geralmente precisam de algum tipo de proteção contra a chuva e, em certos lugares, contra a neve ou contra a radiação ultra-violeta, que podem deteriorar os materiais dos quais a antena é construída. Portanto, muitos fabricantes oferecem antenas com elementos fechados hermeticamente dentro de caixas protetoras contra intempéries.

Em ambientes fechados, tais caixas não têm utilidade, já que o objetivo é que a antena esteja o mais desobstruída possível.

Como escolher uma antena

É importante lembrar que não existe motivo razoável para instalar uma antena com um ganho maior do que aquele que efetivamente se utilizará. Se se estabelecer um link limpo com uma antena de baixo ganho, a rede não funcionará melhor nem transferirá os dados com mais velocidade se usar uma antena “maior”. De fato, a qualidade do sinal pode até ser pior pois está mais sujeito a mais ruído e interferência de outras redes ou dispositivos.

A antena onidirecional padrão deve ser a primeira opção a menos que se tenha um bom motivo para usar alguma outra. Se você precisar de uma antena direcional, escolha uma que cubra a área que você deseja alcançar o mais eficientemente possível. Se você não precisa cobrir uma área enorme, não gaste dinheiro com uma antena de alto ganho.

Onde usar uma antena direcional

Existem três maneiras de usar antenas direcionais em um AP, em um adaptador ou em ambos.

Em um ponto de acesso

Uma antena direcional em um AP proporciona um sinal mais forte para todos os nós da rede dentro da área de cobertura do AP. Portanto, é possível alcançar os usuários que estejam mais distantes, e melhorar a qualidade do sinal para aqueles que estão mais próximos, à custa dos usuários que não estejam localizados dentro do padrão de cobertura da antena.

Numa rede que exige diversos pontos de acesso para proporcionar uma cobertura completa, um AP com uma antena direcional em uma extremidade da área de cobertura pretendida pode ser mais eficiente que uma antena onidirecional.

Em um adaptador de rede

A Segunda opção consiste em posicionar uma antena direcional de alto ganho em um adaptador de rede wireless e apontar a antena para um AP com uma antena onidirecional. Essa poderia ser a melhor maneira de adicionar um nó a uma rede por meio de um AP que também esteja servindo outros clientes de rede mais próximos. Para eliminar o custo e a inconveniência da instalação de outro AP, tente usar uma antena direcional no adaptador de rede daquele usuário.

Tanto em um ponto de acesso quanto em um adaptador de rede

Um link que usa antenas direcionais de alto desempenho em ambas as extremidades pode cobrir uma grande quantidade de terreno. Porém, isso pode ser bastante crítico para links de grande distância já que a rotação de uma antena (ou ambas) em apenas alguns poucos graus pode significar a diferença entre um sinal forte e nenhum sinal. Os ângulos de cobertura de antenas côncavas e de parabólicas podem ser extremamente fechados.

Quando você afasta as duas extremidades de um link de rádio, surgem duas novas complicações. A curvatura da terra e um fenômeno conhecido como *Fresnel Zone*, podem atrapalhar, a menos que as antenas sejam suficientemente altas para evitá-los. A 2.4 GHz, a altura média das duas antenas deve ser de pelo menos quatro metros acima do solo, ou de outras obstruções, para um link de 1.500 metros. Em 8 Km, a altura mínima sobre para dez metros e, em 16 Km, a altura mínima é de 18 metros.

As antenas são um mundo completamente diferente

Links de longo intervalo quase sempre são necessários como soluções para problemas específicos, como proporcionar acesso a um local onde nenhum outro serviço de rede está disponível ou a adição de usuários em um prédio à rede remota de um campus ou empresa. A adição de uma antena direcional para atender uma necessidade específica não torna a sua rede muito mais complicada que o uso de pontos de acesso com antenas onidirecionais. Mas se você começar a pensar em antenas com padrões complexos e um ganho muito alto, provavelmente, um estudo mais profundo se fará necessário.

Antes de instalar uma poderosa antena de grande porte, deve-se prestar atenção a aspectos como o vento (você não gostaria que a antena fosse arrancada em uma tempestade), os costumes (muitas pessoas pensam que as antenas são feias ou perigosas), ou ambos. Portanto, são impostas regras sobre onde e como instalá-las. Além disso, você provavelmente desejará usar um equipamento (caro!), chamado de *analisador de espectro*, para apontar as duas antenas.

Instalação e configuração dos pontos de acesso

Quando você decide começar a usar uma WLAN, tem pelo menos duas opções: pode desempacotar todas as caixas, conectar os rádios aos computadores e tentar fazer tudo isso funcionar; ou fazer algum planejamento avançado e pensar sobre o melhor local para cada componente.

Este capítulo serve para ajudar no planejamento para depois promover as instalações necessárias.

A primeira coisa a fazer quando você estiver começando a planejar sua WLAN - ou qualquer LAN - é investir algum tempo sobre como exatamente você espera usar a rede. Todos os computadores da sua rede estão em locais fixos, com um acesso fácil para a passagem de cabos? Você está considerando o uso do wireless por ser a melhor maneira de adicionar computadores e usuários ou por estar na moda?

Quantos pontos de acesso?

Uma rede wireless simples opera com um único AP e vários nós de rede. Entretanto, quando você estiver tentando cobrir um espaço amplo, você provavelmente precisará de pelo menos um ponto adicional.

O local exato de cada AP em uma rede complexa não é nem mais nem menos óbvio do que o melhor local onde colocar um único AP. Para um amplo espaço aberto, você poderá incluí-los a espaços regulares, porém será mais difícil descobrir como cobrir um espaço irregular.

A colocação de pontos de acesso não é uma ciência exata. Talvez o melhor método consista em começar com um único AP em uma das extremidades e verificar se proporciona uma cobertura aceitável dentro de 15 a 30 metros, usando um computador que esteja executando um programa de sondagem de local. Quando o sinal começar a enfraquecer, deve-se retornar ao local onde o sinal seja adequado e instalar o segundo AP. E assim sucessivamente. O objetivo deve ser de uma superposição de, no máximo, cerca de 30 por cento na cobertura entre qualquer par de pontos de acesso.

Quando você precisa de mais de dois pontos de acesso em um espaço complexo, você deve começar a cogitar a utilização de uma combinação de antenas onidirecionais e direcionais, em vez das onidirecionais embutidas em alguns pontos de acesso.

Uma dica seria cortar alguns círculos que cubram o equivalente a 45 ou 60 metros, e outros que combinem com o padrão de antenas direcionais, e movê-los até encontrar uma combinação de locais que proporcione a máxima cobertura.

A quantidade de pessoas que utiliza a rede também pode apresentar um efeito sobre a quantidade de pontos de acesso necessários. Como um limite prático, se mais de meia dúzia de computadores estiverem se tentando se conectar ao mesmo AP no mesmo instante, haverá uma queda na performance da rede. "Meia dúzia" em determinado pode significar 20 a 30 usuários ao longo do dia.

Se a quantidade de usuários aumentar ao longo do tempo, você poderá descobrir que a performance se deteriora devido aos pontos de acesso estarem operando em plena capacidade, ou próximo a ela. Quando isso ocorre, é hora de pensar na adição de mais pontos de acesso. Sempre que possível, defina os novos pontos de acesso com uma quantidade de canais diferentes e não interferentes e reconfigure metade dos nós da rede para que utilizem esse canal.

Ao operar no modo de infra-estrutura, cada nó está se comunicando com a rede através de um AP. Portanto, não é necessário que todos os nós estejam usando o mesmo número de canal. Se você puder distribuir seus nós entre dois ou três canais não interferentes, reduzirá a quantidade de links em cada canal, o que melhorará a performance para toda a rede.

Sondando um local

As ondas de rádio passam através de alguns materiais e são barrados por outros; portanto, as estimativas gerais do intervalo e da força do sinal de um rádio em um ambiente ideal são menos importantes que a performance real. Você precisa realizar uma sondagem no local para saber como seus próprios rádios operarão em seu próprio espaço.

O primeiro passo para fazer uma sondagem no local consiste em identificar a área que você deseja que seja coberta pela rede. Para isso, é bom ter em mente que os sinais de rádio a 2.4 GHz podem passar através de paredes, tetos e pisos; portanto, provavelmente alcançarão espaços adjacentes, mesmo que você não os aponte para esses espaços.

Para a sondagem deve-se posicionar o AP no melhor local possível e, usando um notebook com um cliente de rede, se movimentar pelo local enquanto uma conexão com a rede está ativa.

Os espaços cobertos por uma única rede não precisam ser contínuos (ou contíguos), embora seja essa a maneira como a maioria das redes são construídas. Por exemplo, seu escritório pode ocupar o terceiro, o quarto e o nono andares de um prédio, mas nenhum dos intermediários. Nesse caso, pode-se colocar pontos de acesso em seus escritórios, conectá-los juntos com cabos Ethernet, e ignorar os outros andares. Se sua LAN se estender por mais de um prédio, você poderá colocar pontos de acesso em cada prédio e vinculá-los (se ainda não houver nenhum link) com uma linha alugada, uma conexão de rede privada virtual (VPN) através de Internet ou um link de rádio ponto-a-ponto.

Planejamento

Se você tem uma idéia aproximada do espaço coberto pela sua rede, é hora de criar uma planta baixa mais detalhada. Se sua rede precisar cobrir mais de um andar de um prédio, e em outros prédios, será necessário uma planta para cada andar, um diagrama vertical de cada prédio e outro diagrama mostrando a área de cobertura inteira da rede.

Sua planta baixa deve incluir o local de cada parede e divisória, junto com cada conexão existente com a rede e com uma tomada de energia de corrente alternada. Se existirem outras fontes potenciais de interferência, como telefones sem fio de 2.4GHz, uma rede Bluetooth ou um forno de micro-ondas, marque também esses locais no plano.

Se a área de cobertura antecipada da rede de um ambiente interno se estender por mais de 45 metros do AP, considere usar mais de um AP. No ambiente externo, deve-se ter condições de obter um sinal confiável a pelo menos 60 metros de distância, desde que tenha uma linha de visão desobstruída.

É bom frisar que, como as antenas onidirecionais irradiam em todas as direções, o AP que as use deve ser colocado aproximadamente no meio do espaço que se deseja cobrir.

Outra provável causa de perda de sinal é a interferência de múltiplos caminhos. Em um sinal de televisão, os múltiplos caminhos são “traduzidos” na tela como imagem “fantasma” ou “sombra”. Em uma rede de dados, o receptor trata essa interferência como ruído, que pode afetar a velocidade de transmissão.

Muitos pontos de acesso e adaptadores usam duas antenas separadas em um arranjo de *diversity receiving* para reduzir ou eliminar o impacto causado pela interferência de múltiplos caminhos. O receptor compara a força do sinal de cada antena e seleciona automaticamente o melhor. Embora as duas antenas possam estar localizadas a apenas três ou cinco centímetros de distância, um sistema de diversidade geralmente pode proporcionar um output mais limpo do que uma única antena. A melhor maneira de descobrir se seu hardware usa essa diversidade é ler as especificações (LPM).

Para o ambiente externo, a regra geral é “quanto mais, melhor”. Se for possível, use um AP com conector para antena externa. Um antena vertical à prova de intempéries num telhado, ou uma antena de painel plano montada em uma elevação ao lado de um prédio, pode proporcionar uma cobertura razoável na linha de visão, a até 90 metros de distância. Ao colocar uma antena no telhado, deve-se montá-la de forma elevada o suficiente para que fique visível a partir do chão, a fim de evitar a atenuação do próprio prédio, como mostra a figura 3.2. Se não se puder ver a antena do AP, a qualidade do sinal poderá ser afetada.

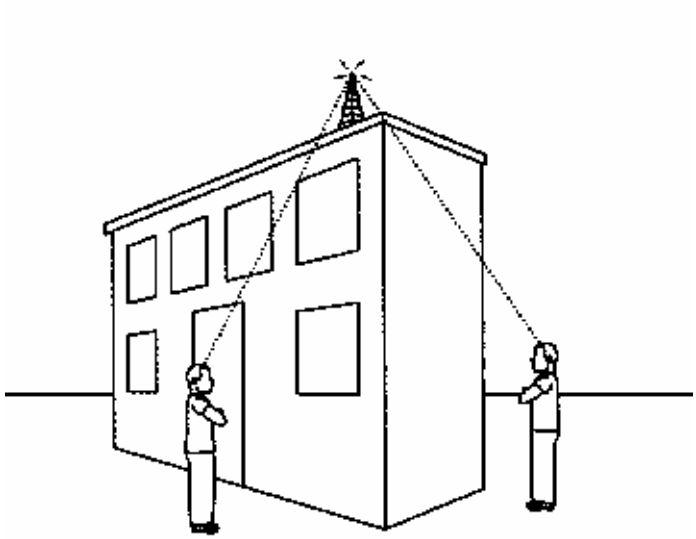

Fig. 3.2: Uma antena no telhado pode não alcançar usuários perto da parede.

A movimentação de veículos ou outros objetos metálicos de grande porte entre o AP e um cliente de rede, pode ser interpor no caminho de um sinal que seria, de outra forma, limpo, produzindo quedas temporárias. Se você estiver tentando proporcionar cobertura a um pátio de carregamento de carga ou algo semelhante, você deverá montar sua antena o mais alto possível ou colocar um segundo AP no outro lado da área que você deseja alcançar com a sua rede.

Testando, testando...

Uma planta baixa pode proporcionar uma boa idéia de como a rede *deve* funcionar, mas a única maneira de descobrir realmente é configurar uma instalação temporária e realizar alguns testes no mundo real.

Existem três opções para se fazer um levantamento em um local:

- Permita que outra pessoa faça isso para você – seja um consultor contratado ou o fornecedor que espera vender o hardware para você.
- Use o software de sondagem de local fornecido com alguns componentes de hardware wireless.
- Use o programa de configuração ou o de status fornecido com uma interface de rede.

Muito provavelmente o primeiro AP que você vier a testar proporcionará a você uma cobertura adequada, especialmente em uma rede de pequeno porte. Porém, quando você estiver configurando uma rede mais complexa, poderá ser muito útil convencer o fornecedor a permitir que você teste as interfaces de rede e os pontos de acesso para mais de um fabricante. Devido aos fabricantes usarem diferentes desenhos de antenas e diferentes softwares de configuração, você pode descobrir que um modelo de adaptador de rede ou de AP funciona melhor do que outro em sua rede.

Veja o que você deve fazer para concluir um levantamento em um local:

1. Escolha um local para seu ponto de acesso. Pode até ser mudado depois mas tem que se ter um ponto de partida.
2. Se já existe uma LAN com fio, conecte seu ponto de acesso de amostra a ela e conecte o fornecimento de energia. Se não existir a LAN, basta conectar ao fornecimento de energia. Ative o ponto de acesso.
3. Instale um adaptador de rede wireless em um notebook. Se seu ponto de acesso não estiver conectado a uma LAN, instale outra inferface de rede em um segundo computador. Este deve estar localizado próximo ao ponto de acesso, de maneira que você pode esperar um caminho limpo para o sinal.
4. Use as ferramentas de configuração no seu ponto de acesso e seus adaptadores de interface para garantir que estão operando nos mesmos números de canal com o mesmo SSID e o mesmo comprimento de preâmbulo. Defina o software do adaptador e o utilitário de configuração do ponto de acesso como modo de infra-estrutura e defina a taxa de transmissão como 11 Mbps ou Automatic. Para esses testes, desative a segurança WEP.
5. Usando a planta baixa como guia, prepare um formulário de sondagem do local, como o da figura 3.4. Crie uma entrada na coluna Local para cada sala/local dentro de sua área de cobertura.

6. Leve o notebook ao primeiro local de seu formulário de sondagem.
7. Realize a sondagem em um programa de configuração ou um programa de status no notebook. O programa deverá relatar uma associação de sinal entre o nó da rede e o ponto de acesso, bem como a força e qualidade do sinal.
8. Alguns programas de configuração medem a qualidade do sinal somente quando uma transferência de arquivo está em progresso. Nesse caso, tente abrir algum arquivo da rede.
9. Anote a força e a qualidade do sinal, e a velocidade do link para o local atual no seu formulário de sondagem. Se você não estiver usando uma ferramenta de sondagem de local, seu display poderá não informar a velocidade do link.
10. Com o programa de status ou de configuração sendo executado, movimente-se para o próximo local da sua lista. Se necessário, atualize (*refresh*) sua tela para obter novas leituras. Anote a força, a qualidade e a velocidade do link no formulário.
11. Repita o processo para cada local da sua lista.

Local	Força do Sinal	Qualidade do Sinal	Velocidade do Link
Sala de Conferência			
Extremidade Norte			
Sala de Conferência			
Extremidade Sul			
Área de Recepção			
Escritório do Mike			
Escritório da Sarah			

Figura 3.4: Um formulário de sondagem de local para uma rede wireless

Não se surpreenda se você descobrir um ou mais pontos mortes inesperados onde a força ou qualidade do sinal cai abaixo de um nível aproveitável. Isso pode ocorrer devido a algum tipo de obstrução (como um arquivo metálico) entre o ponto de acesso e a unidade portátil, ou devido a alguma fonte de interferência local. Esse é um dos motivos pelos quais se está fazendo a sondagem no local. Se você encontrar muitos pontos mortos, ou se algum deles estiver em local crítico. tente mover o ponto de acesso.

Se a qualidade do sinal não for aceitável para a maior parte da área que se deseja cobrir, tente mover o ponto de acesso para um local diferente, ou se o ponto de acesso tiver uma antena externa, tente mover a antena. Repita a sondagem com o ponto de acesso no novo local.

Problemas de interferência

Se ninguém estiver usando uma WLAN ou outro dispositivo de 2.4 GHz a, aproximadamente, 800 metros de distância, você não precisará se preocupar com interferência na rede. Isso está se tornando pouco provável a cada dia. Outros serviços de rede, junto com os telefones sem fio, fornos de microondas, sistemas de iluminação externa e brinquedos controlados por rádio, usam o mesmo conjunto de frequências.

O tipo de modulação de rádio usado pelas WLANs supostamente supera a interferência de todos aqueles serviços. Isso na teoria. Na prática, entretanto, os receptores, nos seus pontos de acesso e adaptadores de redes, podem sintonizar com o canal que supostamente contém um sinal Wi-Fi adequado.

Se existir muita interferência de rádio ao seu redor, você provavelmente descobrirá isso durante a sondagem do local.

Você pode fazer duas tentativas para reduzir ou eliminar a interferência: remover a fonte de interferência ou mover a rede para um canal diferente. A alteração dos canais geralmente é a mais fácil, mas nem sempre é eficiente, pois a fonte de interferência pode ser uma frequência de rádio que salta através da banda de 2.4 GHz.

Para tentar eliminar a interferência siga os seguintes passos, na ordem:

1. Mova para um canal diferente pelo menos cinco números distante daquele no qual se encontrou o problema.
2. Tente descobrir se existe um telefone sem fio, um forno de microondas ou algum outro dispositivo que opere a 2.4 GHz. Se possível, substitua o dispositivo por outro que opere em uma frequência diferente, como um telefone sem fio de 900 MHz.
3. Se você puder alterar a potência de saída dos rádios nos seus pontos de acesso e adaptadores de interface, certifique-se se estão definidos com a configuração alta (geralmente 100 mW).
4. Pergunte aos seus vizinhos se eles estão usando uma rede wireless.
5. Tente substituir as antenas onidirecionais por direcionais, a fim de aumentar a força do sinal e a sensitividade dos receptores. Talvez você precise mudar o ponto de acesso para outro local, ou adicionar mais pontos de acesso, para cobrir a mesma área.

Após isso, você não tem muito o que fazer, exceto se conformar com uma fraca performance ou substituir a sua rede Wi-Fi de 2.4 GHz por uma rede wireless 802.11a que opere a 5.2 GHz.

Você pode encontrar outra fonte de interferência, mas ela provavelmente não ficará evidente até que sua rede tenha sido colocada em operação por algum tempo. À medida que a WLAN se popularizar entre seus usuários, cada vez mais estes poderão usar a rede no mesmo instante, e a performance geral será deteriorada. Para resolver esse tipo de problema, adicione mais pontos de acesso que operem em canais diferentes.

Instalando pontos de acesso

Como já citado, muitos pontos de acesso são combinados com outros dispositivos, como roteadores de rede, roteadores de Internet de banda larga e hubs de Ethernet tradicionais. No mínimo, cada ponto de acesso deve incluir um transmissor e um receptor de rádio, uma ou duas antenas cativas ou conectores para antenas externas, e uma porta Ethernet para conectar a uma rede com fio. O ponto de acesso também deve possuir algum tipo de software de configuração interno que exiba as configurações atuais e aceite comandos para a efetivação de alterações.

Devido ao fato de cada ponto de acesso acompanhar um pacote diferente com diferentes inputs, outputs e controles, você deverá seguir as instruções de instalação e configuração específicas, fornecidas com o próprio dispositivo. Infelizmente, os manuais dos fabricantes nem sempre proporcionam todas as informações necessárias.

Instalação física

Vejamos os passos necessários para a instalação de um ponto de acesso:

1. Se necessário, monte o ponto de acesso usando, para isso, o manual do usuário.

2. Com base na sondagem no local, posicione o ponto de acesso definido.

3. Se o ponto de acesso tiver uma antena cativa em um suporte giratório ou outro que permita movimento, ajuste a antena para uma posição o mais vertical possível. Se você pretende colocar a antena no teto, ou próxima a ele, se possível posicione-a de forma que ela aponte diretamente para baixo.

   Se o ponto de acesso tiver um conector para uma antena externa, instale a antena e passe um cabo desde a antena até o ponto de acesso. Mantenha o cabo entre o ponto de acesso e a antena, o mais curto possível, sem esticá-lo nem deixar que se formem ondulações.

4. Conecte a energia ao ponto de acesso. A maioria dos pontos de acesso é fornecida com adaptadores de energia DC, mas alguns possuem fios de energia de corrente alternada.
   Um ponto de acesso não exige muita energia; portanto, não é necessário usar uma fonte de energia dedicada.

5. Conecte um cabo Ethernet entre o conector de LAN no seu ponto de acesso e o hub de rede, switch ou outro ponto de presença de rede mais próximo.

6. Consulte o manual para descobrir como conectar um cabo de controle ao ponto de acesso. Alguns pontos usam um cabo serial proveniente de um computador próximo, enquanto outros se conectam através da rede. Use essa conexão para definir a configuração do ponto de acesso.

   Se o ponto de acesso usar uma conexão serial, poderá ser mais fácil conduzir um notebook para um local temporário, próximo ao ponto de acesso, onde você possa ver as luzes indicadoras do LED quando você executar a rotina de configuração, em vez de passar um cabo mais longo para um computador existente.

7. Ligue a chave de energia do ponto de acesso. Você provavelmente verá uma luz indicadora do LED. Poderão transcorrer alguns minutos antes que o processador interno do ponto de acesso esteja pronto para operar. O manual do ponto de acesso deve explicar a função dos indicadores do LED.

Após a conclusão da instalação física, o passo seguinte consiste em configurar o ponto de acesso. Se se estiver o mesmo fabricante do ponto de acesso e dos adaptadores, as configurações padrão provavelmente serão as mesmas; portanto, você terá condições de instalar um adaptador em um computador pr]oximo e testar a rede imediatamente.

Configurando o ponto de acesso por meio de um browser

A maioria dos pontos de acesso possui portas de LAN com fio; dessa forma, eles geralmente aceitam comandos de configuração através de um endereço IP numérico local dedicado. Pode ser usado qualquer browser gráfico para visualizar e alterar as configurações. Devido ao fato do ponto de acesso possuir seu próprio software, o programa de configuração será usado em qualquer sistema operacional. O ponto de acesso vem com uma configuração padrão de fábrica, a menos que você altere algumas dessas configurações, usuários não autorizados e usuários de rede (autorizados ou não) poderão obter acesso à sua rede para fazer alterações que somente possam ser feitas pelo gerente da rede.

Novamente, o procedimento de configuração específico é diferente para cada tipo de ponto de acesso, mas os princípios gerais são similares. Use o procedimento seguinte como complemento ao manual do usuário (LPM):

1. Confirme se o ponto de acesso está conectado à LAN.

2. Em um computador conectado à LAN, abra o browser Web de sua preferência.

3. No campo Browser Address, digite o endereço IP numérico padrão para o ponto de acesso, conforme especificado no manual do ponto de acesso e, a seguir, pressione ENTER.

4. Nesse ponto, deve ser aberta uma janela de login semelhante à da figura 3.6. Informe os dados solicitados.

5. Deve ser mostrada uma página de configuração semelhante à da figura 3.7, que mostra a tela de configuração do ponto de acesso Zoom/Air AP11.

Fig. 3.6:A janela de senha do ponto de acesso controla o acesso ao utilitário de configuração.

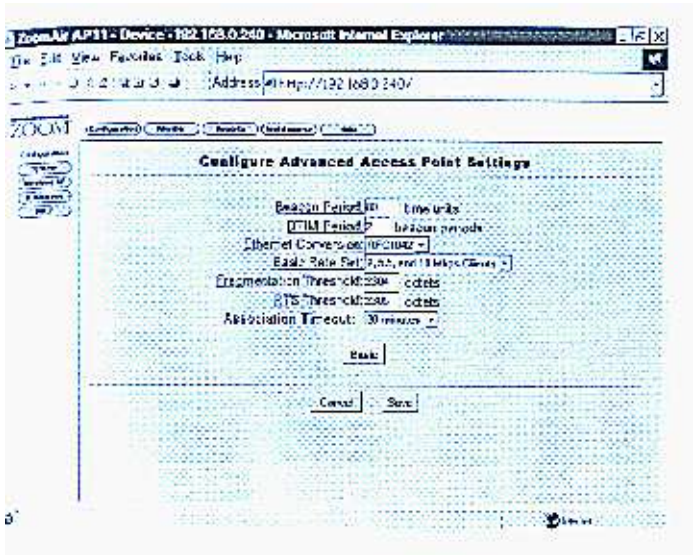

Fig. 3.7: A tela de configuração para um ponto de acesso ZoomAir.

Se você obtiver uma mensagem "Unable to connect", em vez da janela de login, envie uma requisição de ping para o ponto de acesso, através do comando (no Prompt do DOS): PING [endereço IP (endereço IP do ponto numérico)].

Se o comando retornar "host unreachable" provavelmente existe um conflito entre o servidor de *Dynamic Host configuration Protocol* (DHCP) na sua LAN e o endereço padrão do ponto de acesso.

DHCP e outros desastres

O DHCP atribui automaticamente um endereço IP a cada computador da rede. Ele economiza muito tempo e evita problemas.

Servidores de DHCP conflitantes podem causar problemas quando você adiciona um ponto de acesso a uma LAN. Alguns pontos de acesso esperam receber configurações através de um endereço IP fixo. Entretanto, quando esse ponto de acesso está conectado a um hub que está atuando como servidor DHCP, o servidor atribui um endereço IP diferente ao ponto de acesso. Portanto, quando o usuário tenta conectar ao endereço IP listado no manual do ponto de acesso, nada acontece (ou o browser relata "unable to find this address").

Existem várias maneiras de lidar com isto. Você pode usar o programa de configuração por meio de uma porta serial, mas isso significa que você deve usar uma linguagem de comando. Alguns pontos de acesso não aceitam comandos através de suas portas seriais.

A segunda alternativa seria usar a função de configuração, pelo browser, através do endereço IP atribuído pelo DHCP para o ponto de acesso. A maioria dos servidores DHCP inclui um display de endereços atribuídos.

A terceira alternativa seria desativar o servidor DHCP e usar o endereço IP padrão do ponto de acesso.

Se todos estes métodos parecem muito complicados, existe outra maneira de fazer isso: passando um cabo *crossover* da porta LAN do ponto de acesso até um computador com uma porta Ethernet.

De qualquer forma, normalmente o manual de configuração do hardware deve conter instruções para atender todas as situações, mesmo as citadas aqui. (LPM). Além disso, é sempre importante manter documentadas as alterações de configuração que foram efetuadas para futura referência.

Configurando o ponto de acesso através de uma porta serial

Como citado, a maioria dos pontos de acesso aceitam configurações por meio da porta serial. A porta serial em um ponto de acesso pode ser tanto um conector de dados DB-9 de 9 pinos quando um conector RJ-45 que se parece com uma versão do conector RJ-11. Se seu ponto de acesso usa um RJ-45, o fabricante provavelmente proporcionou um

cabo e um adaptador. Se o conector é um DB-9, ele provavelmente requer um cabo direto a partir da porta COM de um computador. Se o ponto de acesso exigir um cabo modem null, esse fato deverá ser mencionado especificamente no manual.

Para enviar comandos ao ponto de acesso através da porta serial, siga estes passos:

1. Passe um cabo entre o ponto de acesso e uma das portas COM do computador.
2. Inicie um programa emulador de terminal, como o HyperTerminal e configure uma conexão através da porta COM conectada ao ponto de acesso.
3. Abra uma conexão com o ponto de acesso.
4. Se ainda não estiver ligado, ligue o ponto de acesso.
5. Quando o ponto de acesso está pronto para aceitar comandos ele exibe um prompt. Para confirmar se o emulador de terminal está funcionando, pressione ENTER. O ponto de acesso deve exibir outro prompt em uma nova linha.

Comandos de configuração e definições

Cada utilitário de configuração manipula comandos de configuração e definições de diferentes maneiras, mas cada ponto de acesso, que obedece às especificações da 802.11b, deve incluir o mesmo conjunto básico de opções. Ao configurar sua rede, você provavelmente desejará alterar algumas dessa opções, a partir dos valores padrão.

Caso algum comando particular não esteja óbvia na tela de nível mais alto, tente abrir as telas de nível mais baixo para descobrir o que deseja, ou então tente no manual do ponto de acesso.

A linguagem de comando para alterar a configuração através da porta serial também deve estar descrita no manual. Em muitas situações, um comando de ajuda produz uma lista on-screen de outros comandos e suas sintaxes.

Em geral, o utilitário de configuração deve incluir as opções: endereço IP, máscara de sub-rede, ID de rede wireless, canal, segurança e DHCP.

Endereço IP

Este campo exibe o endereço IP numérico usado atualmente pelo ponto de acesso. Este pode ser um endereço padrão atribuído na fábrica, um endereço atribuído pelo gerente da rede ou um endereço atribuído pelo servidor de DHCP.

Máscara de sub-rede

Este campo identifica a sub-rede que inclui o ponto de acesso e os clientes wireless que se conectam à LAN por meio do ponto de acesso. O endereço da sub-rede é atribuído pelo gerente da rede. Se a sua LAN não incluir uma sub-rede, use o valor padrão 255.255.255.0.

Wireless Network ID (SSID)

O **SSID** é o “nome” da WLAN que inclui esse ponto de acesso. Quando um cliente da rede tenta se conectar, ele procura um ponto de acesso com o mesmo SSID que o seu.

Portanto, o SSID serve a dois propósitos: atua como a primeira linha de defesa contra um acesso não autorizado e, em uma rede com mais de uma WLAN operando, associa cada cliente com a rede correta. Entretanto, o SSID por si mesmo não é uma ferramenta de segurança particularmente eficiente, pois alguns adaptadores de rede aceitam um SSID de ANY, o que permite ao cliente se associar com o primeiro ponto de acesso que encontra, independentemente do SSID do ponto de acesso.

Canal

A configuração do canal equivale ao número do canal de rádio que será usado pelo AP para trocar dados com o dispositivo cliente na WLAN. Cada AP opera em um canal único, mas a maioria dos adaptadores varre os canais para encontrar o melhor sinal disponível com o mesmo SSID. Caso se tente usar um adaptador com um canal predefinido, esse número de canal terá que combinar com o do AP.

Se sua rede incluir mais de um AP, você deverá definir pontos de acesso adjacentes a canais diferentes conforme já visto anteriormente.

Segurança

O WEP é o sistema de segurança que supostamente mantém as pessoas que não tenham o código-chave eletrônico apropriado, afastadas da sua rede. Todos os componentes de hardware 802.11b vêm acompanhados com a criptografia WEP opcional; portanto você deve saber como usá-la.

Cada ponto de acesso pode usar uma chave WEP de criptografia de 64 ou 128 bits para restringir o acesso não autorizado. Devido à chave de 64 bits tratar-se, na realidade, de uma chave de 40 bits combinada com uma string de vetor de 24 bits, alguns programas de configuração a chamam de criptografia de 40 bits. Os adaptadores e APs que usam criptografia de 40 bits são totalmente compatíveis com aqueles que usam criptografia de 64 bits.

Infelizmente, alguns fabricantes requerem uma string composta por letras e número como chave uma WEP, enquanto outros esperam que você forneça uma série de números hexadecimais, seja como cinco grupos de dois ou como uma única string de dez dígitos.

Geralmente, é mais fácil configurar uma WLAN com a criptografia desativada mas é uma idéia muito boa ativá-la quando começar a trafegar dados reais através da rede.

DHCP

Um ponto de acesso pode atuar como servidor de DHCP, porém é bom lembrar que somente um servidor DHCP pode estar ativo em qualquer momento; portanto, se a rede já tem um servidor DHCP ativo, desative essa função do AP.

Quando o servidor de DHCP do ponto de acesso estiver ativo, o utilitário de configuração deverá exibir uma lista de clientes DHCP atualmente ativos na mesma tela que contém as opções ativar/desativar (enable/disable), ou o utilitário pode se oferecer para abrir outra janela com os dados.

Outras configurações

O manual do AP deve proporcionar a você as informações necessárias para configurar outras funções não relacionadas aqui. Quando a finalidade de uma configuração não estiver clara, ou se ela aparentemente não vier a apresentar nenhum defeito na rede, a abordagem mais segura consiste em aceitar o valor padrão. Ou seja, na dúvida, deixe como está!!!

Múltiplos pontos de acesso

Muitas redes usam mais de um AP para ampliar a cobertura da rede além do intervalo do sinal de uma única estação-base. No caso do cliente da rede se movimentar ocorre o roaming.

A especificação 802.11b possibilita que o cliente se mova de um AP para outro, mas não define o processo de troca (hand-off). Nesse caso, cada fabricante de AP lançou seu próprio método, que pode não ser compatível com nenhum outro. Isso provavelmente será alterado num futuro próximo mas, no momento, é de fundamental importância usar apenas um tipo de AP na sua rede. Pode-se esperar que um adaptador Wi-Fi trabalhe com qualquer tipo de AP, mas não é seguro que dois tipos diferentes de pontos de acesso funcionem em conjunto.

Para configurar uma WLAN com mais de um ponto de acesso, simplesmente conecte todos os pontos à mesma rede Ethernet com fio e configure-os para que manipulem as mesmas chaves SSID e WEP. Se você não estiver usando um servidor de DHCP, atribua um endereço IP diferente para cada um dos APs, mas utilize as mesmas (mesmos endereços de) sub-rede e gateway para a rede inteira. Se um AP estiver atuando como servidor de DHCP, lembre-se de desativar a função de DHCP em todos os outros APs da rede.

Pontos de acesso combinados com Hubs e Roteadores de Gateway

Diversos fabricantes oferecem produtos que combinam as funções de um AP wireless com um hub, switch ou roteador de rede. Outras combinações de produtos incluem servidores de impressão em rede ou acesso à Internet em banda larga (cabo ou DSL) junto com pontos de acesso. Uma unidade de combinação pode ser um excelente ponto de partida para uma nova rede de pequeno porte ou para a adição tanto de clientes com fio quanto wireless a uma rede existente. Normalmente o dispositivo combinado terá um custo bem menor que o custo dos componentes separados.

Para decidir se uma dessas unidades de combinação é a melhor maneira de atender seus requisitos particulares, primeiro identifique esses requisitos, e a seguir examine os catálogos dos diversos fabricantes e os sites a fim de encontrar um dispositivo que atenda ao máximo as suas necessidades. Entre outros, a D-Link, a Linksys, a Intel e a Buffalo oferecem uma ampla variedade de APs combinados com outras funções.

Na maioria das redes Wi-Fi, os pontos de acesso são praticamente invisíveis na operação diária. Quando já estiver com o ponto de acesso funcionando, você poderá praticamente esquecê-lo até precisar alterar a configuração.

Wi-Fi para Windows

Em um mundo de redes ideal, seria possível conectar um adaptador de rede ao computador, ligá-lo e se conectar à rede imediatamente.

Infelizmente, nada é assim tão simples. Normalmente, antes de você poder transportar dados através de uma WLAN, você terá que informar exatamente como e onde encontrar a rede e como conectar à Internet.

Este capítulo contém uma explicação sobre os conceitos gerais envolvidos com o funcionamento do Windows em uma WLAN e os procedimentos específicos para configurar as ferramentas e recursos de rede em diferentes versões do Windows.

No XP, tudo deve ocorrer automaticamente, desde que (e este é um fator preponderante), o seu adaptador de rede contenha um firmware compatível com a ferramenta de configuração automática do Windows.

Se você for experiente em configuração de redes Windows, não deverá encontrar problemas com o wireless. Infelizmente, o Windows espalha as opções de configuração sobre todo o mapa virtual, portanto um conjunto de indicações para cada uma dessas opções pode ser extremamente útil.

Configuração geral de rede no Windows

Diferentes versões do Windows usam ferramentas de configuração diferentes mas todas com o mesmo objetivo: as configurações de endereço IP, máscara de sub-rede e endereço de gateway do computador devem combinar com os valores requeridos pelo resto da rede.

Endereços IP

O endereço IP de um cliente é a identidade formal usada pelos outros computadores para chegar àquele dispositivo. Todos os computadores em uma rede devem ter endereços diferentes.

As agências que administram a Internet estabeleceram um sistema de numeração complexo com um endereço único para cada dispositivo conectado à Internet. Endereços IP sempre aparecem com quatro grupos de números no intervalo de 0 a 255. Esses grupos de número também são conhecidos como "octetos", pois usam oito dígitos binários (o binário 11111111 é igual a 255).

Um endereço IP pode identificar um único computador ou identificar um gateway para uma LAN (ou uma rede de maior porte) com dois ou mais computadores conectados a ele através de um roteador.

Para evitar conflitos entre endereços IP locais e endereços de Internet, diversos intervalos de números foram reservados para utilização por redes locais:

- 10.0.0.0 a 10.255.255.255.255
- 172.16.0.0 a 172.31.255.255
- 192.168.0.0 a 192.168.255.255

Atribuição de Endereços

Em algumas redes, um servidor de DHCP (Dynamic Host Configuration Protocol) atribui um endereço diferente para cada dispositivo cliente sempre que ele se associa à rede.

O servidor DHCP normalmente está localizado no roteador que controla todos os dispositivos na rede. Em uma WLAN provavelmente esteja localizado num AP.; numa rede mista, o servidor DHCP provavelmente estará no gateway de Internet. A fig. 5.1 mostra o servidor em uma rede típica.

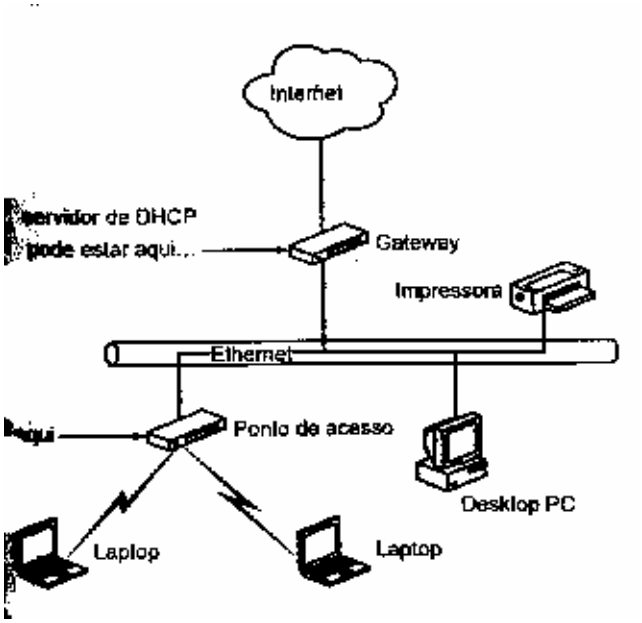

Fig. 5.1: Um servidor de DHCP proporciona endereços IP locais para todos os dispositivos em uma LAN.

Se a rede não possui DHCP, o gerente de rede deve atribuir um endereço permanente para cada cliente. O gerente também deverá controlar essa numeração para que não haja conflitos.

Máscara de sub-rede

A máscara de sub-rede é uma string de quatro números que especifica qual parte de uma rede de maior porte contém um computador ou outro nó de rede. Cada um dos quatro números geralmente é 255 ou 0. Os números especificam quais partes do endereço IP identificam a rede ou sub-rede local (a *subnet*), e quais partes identificam computadores individuais ou nós da rede. Por exemplo, se a máscara de sub-rede for 255.255.255.0, então todos os endereços IP na rede deverão ser XXX.XXX.XXX.ZZZ, onde XXX.XXX.XXX é o mesmo para todos os endereços e ZZZ é diferente para cada endereço. A máscara de sub-rede deve ser idêntica todos os pontos de acesso e todos os clientes wireless servidos por aqueles pontos de acesso. Em redes de pequeno e médio porte, a máscara de sub-rede quase sempre é 255.255.255.0.

Gateways

O *gateway* é o ponto de acesso, roteador ou outro dispositivo wireless que atua como a interface entre os computadores em uma LAN e outros dispositivos ou redes que não façam parte da rede local. A qualquer instante em que um computador não faça parte da rede local tentar se comunicar com um dispositivo na rede, ele deverá transportar os dados através do gateway.

Servidores de DNS

Um servidor de DNS (*Domain Name System*) é um computador que converte nomes de domínio para os endereços IP respectivos. Alguns servidores de DHCP oferecem um endereço de servidor de DNS automaticamente enquanto outros exigem que cada usuário adicione manualmente o servidor de DNS à configuração de TCP/IP de cada cliente. Se você não estiver usando o DHCP, deverá especificar pelo menos um endereço de servidor de DNS. O gerente da sua rede ou o seu provedor de Internet devem proporcionar a você os endereços dos servidores de DNS da sua rede.

Alguns pontos de acesso e gateways de rede também exigem um endereço de servidor de DNS. A lista de servidores no ponto de acesso ou gateway deve ser idêntica à lista de servidores em cada cliente.

Compartilhamento de arquivos e impressoras

Funciona de forma idêntica ao compartilhamento de arquivos e impressoras das redes com fio.

Opções do adaptador de interface de rede

Se você não conseguir encontrar uma configuração ou opção no utilitário de configuração, procure na janela Propriedades (no Windows XP, ir em Configurações + Painel de Controle + Sistema + Gerenciador de Dispositivos) o seu adaptador wireless. A lista de opções está abaixo da guia Avançado.

Dando um nome ao seu computador

Para os usuários humanos, normalmente, é mais fácil guardar um nome do que um endereço IP para efeito de identificação. Portanto, você (ou o gerente da rede) deve atribuir um nome a cada computador na rede. Este nome aparecerá em todos os diretórios e listas de computadores que podem ser alcançados através da sua rede. Cada computador deve ter um nome único, com um comprimento máximo de 15 caracteres e espaços.

O Windows também proporciona um espaço para a atribuição de cada computador da rede a um *workgroup*. Em uma LAN de pequeno porte, você provavelmente desejará atribuir todos os computadores a um único workgroup. Portanto, a definição Workgroup Name deve ser idêntica em todos os computadores da rede.

Em algumas redes wireless, o nome do workgroup deve ser o mesmo que o SSID usado pelo ponto de acesso, especialmente quando o utilitário de configuração não exibe uma lista das redes próximas. Se você estiver tendo problema com a conexão, tente alterar o nome do workgroup para o SSID da rede à qual você deseja se associar.

Configurando o Windows 98 e o ME

O Windows 98, o 98SE e o ME, possuem ferramentas de configuração de rede similares.

Endereço IP e máscara de sub-rede

Siga estes passos para definir o endereço IP e a máscara de sub-rede:

1. No Painel de Controle, clique sobre o ícone *Rede*
2. Na guia *Configuração*, selecione o adaptador de rede e clique sobre o botão *Propriedades*.
3. Se ainda não estiver visível, clique na guia *Endereço IP*.
4. Se o servidor de DHCP estiver ativo, selecione a opção *Obter um Endereço IP Automaticamente*. Se não estiver usando um servidor de DHCP, escolha a opção *Especificar um Endereço IP* e digite o endereço IP atribuído a este computador no campo *Endereço IP*.
5. O campo *Máscara de sub-Rede* está localizado logo abaixo do endereço IP. Se você não estiver usando um servidor de DHCP, digite a mesma máscara de sub-rede que é usada pelo AP.

Gateway

Siga estes passos para definir o endereço do gateway:

1. Na mesma janela usada para definir o endereço IP, clique sobre a guia *Gateway*.
2. Digite o endereço IP da LAN do ponto de acesso wireless no campo *Novo gateway* e clique no botão *Adicionar*.

Servidores de DNS

Siga estes passos para definir as opções de DNS:

1. Na mesma janela usada para definir o endereço IP, clique sobre a guia *Configuração DNS*.
2. Se um servidor de DHCP atribui endereços de DNS a clientes, selecione a opção *Desativar DNS*. Se a rede usa um servidor DNS estático, selecione a opção *Ativar DNS*.
3. Se ainda não estiver visível, digite o nome atribuído a este computador no campo *Host*.
4. Se a LAN, o AP ou o servidor de DHCP, usa um nome de domínio, digito o nome de domínio no campo *Domínio*.

5. Digite o endereço de cada servidor de DNS usado pela sua rede no campo *Ordem de Pesquisa Servidor DNS* e clique sobre o botão *Adicionar*. O gerente de sua rede ou o provedor de Internet, podem fornecer os endereços de DNS corretos para a sua rede.
6. Clique sobre o botão OK na janela *Propriedades de TCP/IP* e novamente na janela de *Rede* para salvar as novas configurações.

Opções do adaptador de interface de rede

Para alteraras configurações de interface de rede, siga estes passos:

1. No Painel de Controle, clique sobre o ícone *Rede*
2. Na guia *Configuração*, selecione o adaptador de rede e clique sobre o botão *Propriedades*.
3. Clique sobre a guia *Avançado*.
4. Selecione cada um dos itens na lista de propriedades para ver a definição atual no campo *Valor*.
5. Após feitas as alterações necessárias clique sobre o botão *OK* para salvar suas alterações e feche a janela. Clique no botão *OK* da janela *Rede* para voltar ao desktop.

Alguns adaptadores de rede wireless, incluindo os produtos da Orinoco, não aceitam nenhuma opção de configuração. Se você não vir uma guia *Avançado* na janela *Propriedades do Adaptador*, use o programa utilitário de configuração do fornecedor.

Identidade de rede

Antes de poder conectar a uma rede, você deve atribuir um nome ao seu computador. No Windows 98 e ME, as opções de configuração estão localizadas na guia *Identificação* da janela *Rede*. Siga estes passos para alterar essas configurações:

1. No Painel de Controle, clique sobre o ícone *Rede*
2. Clique sobre a guia *Identificação*.
3. Digite o nome que identifica este computador na rede, no campo *Nome do Computador*.
4. Digite o SSID da rede no campo *Workgroup*.
5. Se quiser oferecer uma descrição mais detalhada, preencha o campo *Descrição do computador*.
6. Após feitas as alterações necessárias clique sobre o botão *OK* para salvar suas alterações e feche a janela. Clique no botão *OK* da janela *Rede* para voltar ao desktop.

Configurando o Windows 2000

O Windows 2000 possui todas as mesmas opções de configuração que as versões anteriores, mas algumas delas estão localizadas em diferentes locais.

Endereço IP e máscara de sub-rede

Siga estes passos para definir o endereço IP e a máscara de sub-rede:

1. No Painel de Controle, clique sobre o ícone *Rede*.
2. O perfil de conexão com a rede para a sua conexão Ethernet wireless á a *Local Area Connection*. Clique com o botão direito sobre o ícone e selecione *Propriedades* no menu pop-up. Na janela que se abrirá, você deve confirmar se o nome do seu adaptador de interface de rede está visível no campo *Usando Conexão*.
3. Na lista de itens instalados, selecione o item *Internet Protocol* (TCP/IP) e clique sobre o botão *Propriedades*.
4. Se o servidor de DHCP estiver ativo, selecione a opção *Obter um Endereço IP Automaticamente*. Se não estiver usando um servidor de DHCP, escolha a opção *Use o Endereço IP Seguinte* e digite o endereço IP atribuído a este computador no campo *Endereço IP*.
5. O campo *Máscara de sub-Rede* está localizado logo abaixo do endereço IP. Se você não estiver usando um servidor de DHCP, digite a mesma máscara de sub-rede que é usada pelo AP.
6. Digite o endereço IP da LAN do ponto de acesso wireless no campo *GatewayDefault*.

7. Se um servidor de DHCP atribui endereços de DNS a clientes, selecione a opção *Obter Endereço do Servidor DNS automaticamente*. Se a rede usa um servidor DNS estático, selecione a opção *Use os seguintes Endereços de Servidores DNS*, e insira os endereços de DNS fornecidos pelo gerente da rede ou pelo provedor de Internet.

Compartilhamento de arquivos e impressoras

Funciona de forma idêntica ao compartilhamento de arquivos e impressoras das redes com fio.

Opções do adaptador de interface de rede

Siga estes passos para alterar as opções do adaptador de rede:

1. No Painel de Controle, clique sobre o ícone *Rede e Conexões Dial-Up*.
2. Clique com o botão direito sobre o ícone do perfil da conexão wireless. Escolha *Propriedades* no menu pop-up.
3. Na guia *Geral*, clique sobre o botão *Configurar*.
4. Clique sobre a guia *Avançado*.
5. Selecione cada um dos itens na lista de propriedades para ver a definição atual no campo *Valor*.
6. Após feitas as alterações necessárias clique sobre o botão *OK* para salvar suas alterações e feche a janela. Clique no botão *OK* da janela *Rede* para voltar ao desktop.

Alguns adaptadores de rede wireless, incluindo os produtos da Orinoco, não aceitam nenhuma opção de configuração. Se você não vir uma guia *Avançado* na janela *Propriedades do Adaptador*, use o programa utilitário de configuração do fornecedor.

Identidade de rede

As configurações da opção de identificação no Windows 2000 estão localizadas na guia *Identificação da Rede* da janela *Propriedades do Sistema*. Siga estes passos para alterar essas configurações:

1. No Painel de Controle, clique sobre o ícone *Sistema*.
2. Clique sobre a guia *Identificação da Rede.*
3. Clique sobre o botão *Propriedades* para abrir a janela *Alteração de Identificação*.
4. Digite o nome que identifica este computador na rede, no campo *Nome do computador*.
5. Digite o SSID da rede no campo *Workgroup*.
6. Clique no botão OK para salvar suas alterações e fechar a janela.

Configurando o Windows XP

A Microsoft introduziu o suporte específico para redes 802.11b no Windows XP, que supostamente integra a configuração wireless com outras configurações do Windows. Teoricamente, isto pode facilitar a configuração e utilização de redes wireless, mas este ainda não é um processo Plug-and-Play simples.

O objetivo é a configuração wireless automática; o Windows deve detectar automaticamente o adaptador de rede e procurar por sinais de rede wireless acessíveis. Quando detecta uma rede próxima, o Windows deve permitir que um usuário se associe à rede apenas com alguns cliques de mouse.

Status de conexão de rede wireless

Para abrir a janela de status, dê um clique duplo sobre o rede ícone na barra de status.

A janela *Status de conexão da rede wireless* mostra o estado atual do seu link, incluindo o status da conexão, a quantidade de tempo em que o link atual está ativo, a velocidade de transferência de dados, a qualidade do sinal e o número de bytes que foram enviados e recebidos pelo adaptador, desde que o adaptador se conectou à rede.

Para desabilitar o link de rádio, clique sobre o botão *Desabilitar* na parte inferior da janela de status. Para alterar as configurações de rede mais comuns, clique sobre o botão *Propriedades*.

Definições da configuração da rede

Para definir as opções de configuração da WLAN, selecionar *Start * Settings * Network Connections* e dê um clique duplo sobre o ícone da sua conexão wireless. Para configurar a sua conexão wireless siga estes passos:

1. Na lista de itens instalados, selecione o item Internet Protocol (TCP/IP) e clique sobre o botão *Propriedades*. Clique sobre a guia *Geral* se ela ainda não estiver selecionada.
2. Se o servidor de DHCP estiver ativo, selecione a opção *Obter um Endereço IP Automaticamente*. Se não estiver usando um servidor de DHCP, escolha a opção *Use o Endereço IP Seguinte* e digite o endereço IP atribuído a este computador no campo *Endereço IP*.
3. O campo *Máscara de sub-Rede* está localizado logo abaixo do endereço IP. Se você não estiver usando um servidor de DHCP, digite a mesma máscara de sub-rede que é usada pelo AP.
4. Digite o endereço IP da LAN do ponto de acesso wireless no campo *GatewayDefault*.
5. Se um servidor de DHCP atribui endereços de DNS a clientes, selecione a opção *Obter Endereço do Servidor DNS automaticamente*. Se a rede usa um servidor DNS estático, selecione a opção *Use os seguintes Endereços de Servidores DNS*, e insira os endereços de DNS fornecidos pelo gerente da rede ou pelo provedor de Internet.
6. Clique em OK para salvar as suas configurações e feche esta janela.

Compartilhamento de arquivos e impressoras

Funciona de forma idêntica ao compartilhamento de arquivos e impressoras das redes com fio.

Opções do adaptador de interface de rede

Siga estes passos para alterar as opções do adaptador de rede:

1. Na janela *Propriedades da conexão de rede sem fio*, clique sobre o botão *Configurar*.
2. Clique sobre a guia *Avançcado*.
3. Selecione cada um dos itens na lista de propriedades para ver a definição atual no campo *Valor*.
4. Após feitas as alterações necessárias clique sobre o botão *OK* para salvar suas alterações e feche a janela. Clique no botão *OK* da janela *Rede* para voltar ao desktop.

Alguns adaptadores de rede wireless, incluindo os produtos da Orinoco, não aceitam nenhuma opção de configuração. Se você não vir uma guia *Avançado* na janela *Propriedades do Adaptador*, use o programa utilitário de configuração do fornecedor.

Identidade de rede

Para definir ou alterar o nome atribuído ao computador no Windows XP, abra a guia *Nome do computador* da janela *Propriedades do Sistema*. Siga estes passos para alterar as definições:

1. No *Painel de Controle*, dê um clique duplo sobre o ícone *Sistema*.
2. Clique sobre a guia *Nome do computador*.
3. Digite o nome que identifica o computador, no campo *Descrição do computador*.
4. Clique no botão *Alterar*.
5. Digite o SSID da rede no campo *Workgroup*.
6. Clique sobre o botão OK para salvar as alterações e fechar a janela.

Configurando a Rede Wireless no Windows XP

As ferramentas de configuração do XP destinam-se a ser uma interface comum capaz de controlar muitas marcas de adaptadores de rede. Para abrir a janela de *Propriedades da conexão da rede sem fio*, siga estes passos:

1. Dê um clique duplo sobre o ícone Rede na barra de status do Windows, próximo ao relógio no canto inferior direito da tela.

2. Clique sobre o botão *Propriedades* na parte inferior da janela.

Selecionando uma rede

Se o seu computador estiver dentro do intervalo de mais de uma rede, você deve escolher a que deseja usar. O utilitário *Propriedades Sem Fio* inclui uma lista de redes preferidas, mas não o limita às redes que constam na lista.

A lista de redes disponíveis na janela *Propriedades* mostra os SSIDs de todas as redes que aeitarão um link a partir do seu adaptador wireless. Se o adaptador detectar apenas uma rede, o Windows automaticamente se conectará àquela rede. Quando um adaptador detecta mais de uma rede, ele comparará o SSID de cada rede aos nomes na lista de *Redes Preferidas* e o conectará automaticamente à rede com a prioridade mais alta. Você pode alterar a ordem na qual o Windows procura as redes com os botões *Mover para cima* ou *Mover para baixo* na janela *Propriedades*.

A Microsoft ocultou cuidadosamente a caixa de diálogo que especifica se o Windows se limitará, ou não, às redes na lista de redes preferidas. Se o seu adaptador detectar uma rede que não esteja na sua lista de preferidas, ele configurará uma conexão, ***se*** a opção não-preferida na janela *Avançada* estiver ativa. Clique sobre o botão *Avançado* na janela *Propriedades* para abrir essa janela.

Evidentemente, é possível que o computador venha a fazer a escolha errada. Quando isso acontecer, selecione o SSID da rede correta na lista de *Redes Disponíveis* e clique sobre o botão *Configurar*. Isso abrirá outra janela com mais informações sobre a rede, e configurará uma conexão para essa rede.

Ativando ou desativando a criptografia

A janela *Propriedades Locais*, que pode ser aberta na janela de *Propriedades* principal com o botão *Configurar* ou o botão *propriedades*, inclui um conjunto de opções de criptografia WEP. Se você estiver usando uma rede com a criptografia WEP ativa, ative a opção *Data Encryption*.

Resumo: criando a conexão

Qualquer que seja o Windows, deve ser possível configurar um link com uma rede wireless. Se a função de conexão automática não funcionar, não se assuste. Veja algumas coisas que devem ser verificadas:

- SSID usado pelo seu computador é exatamente o mesmo que o SSID da rede à qual você está tentando se associar?
- A criptografia WEP está ativada ou desativada? Se estiver ativada, você está usando a chave de criptografia correta? A criptografia está definida como 64 ou 128 bits?
- O ponto de acesso usa filtragem de endereço MAC? O seu adaptador wireless está na lista de usuários qualificados?
- O nome do Workgroup combina com o SSID?
- O seu ponto de acesso usa o servidor de DHCP? Se não usar, o endereço IP, a máscara de sub-rede e o gateway estão configurados corretamente?
- O comprimento do preâmbulo está definido corretamente?

Wi-Fi para Linux

Todos os adaptadores wireless (exceto a placa AirPort da Apple) vem acompanhados com drivers e ferramentas de configuração para o Windows. Porém, normalmente, existem drivers para todos os sistemas operacionais (Unix, Linux, MAC).

Encontrar o driver correto nem sempre é fácil quanto parece. Este capítulo explicará como encontrar os drivers Linux corretos para diversos adaptadores e como instalá-los e usá-los para conectar a uma WLAN.

Drivers

Um driver de dispositivo é o software de interface entre o sistema operacional do computador e os inputs e outputs de um dispositivo periférico conectado ao computador. A figura 7.1 mostra o relacionamento entre um computador e um driver de dispositivo.

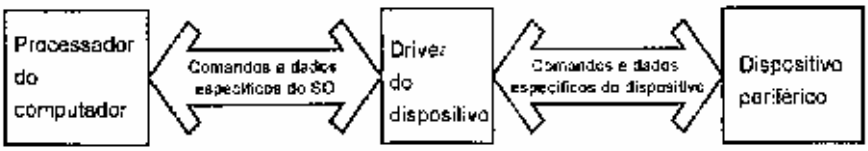

Fig. 7.1: Um driver de dispositivo é a interface de dados e controle entre um computador e um periférico

Os drivers possibilitam que o mesmo componente de hardware funcione em diferentes sistemas operacionais. Portanto, se o seu computador executa o Linux, ele exige drivers de dispositivos escritos especificamente para esse sistema operacional. Pode ser útil pensar em um driver como o manual de instruções para um dispositivo. Os manuais escritos em inglês, espanhol e japonês contêm o mesmo conjunto de instruções mas estas são fornecidas em linguagens que os diferentes usuários compreenderão.

Onde encontrar drivers

O primeiro lugar onde procurar um driver Linux para o seu adaptador é o CD que acompanha o adaptador. Alguns fabricantes incluem os drivers junto com os drivers do Windows, mas não conte com isso.

Se você tiver opção, será melhor comprar um adaptador que acompanhe o driver de que você precisa para o seu sistema operacional.

Se um driver não acompanhar o adaptador, verifique o site do fabricante em busca dos drivers que estejam disponíveis para download gratuito. Muitos fabricantes imprimem endereços de sites nas etiquetas de seus adaptadores e em seus manuais, mas se você não conseguir um endereço tente *www.[nome da marca].com*, ou procure em um dos diretórios de driver de dispositivos online como *'www.windrivers.com*, *www.driverzone.com* ou *www.driversplanet.com*.

Se você tiver um adaptador produzido por uma empresa que não ofereça suporte para Linux, talvez precise se utilizar do amplo universo de grupos de usuários, listas de e-mails e sites.

Drivers do Linux

Mais de 80 diferentes marcas de adaptadores de WLANs ostentam as etiquetas da certificação Wi-Fi, mas quase todas usam somente um dentre quatro ou cinco chip sets internos. Portanto, somente alguns drivers Linux são necessários para controlar praticamente todos os adaptadores possíveis.

A Tabela 7.1 contém uma lista parcial de drivers para Linux.

Adaptador	Origem do Driver
Adaptadores que utilizam o Intersil Prims chip set (incluindo Actiontec, Addtron, Bromax, Compaq, D-Link, Gem Tek,	Faça o download da versão mais recente dos drivers wlan-ng, em www.linux-wlan.com/pub/linux-wlan-ng, ou tente os drivers HostAP em www.epitest.fi/Prism2

Linksys, Nokia, Samsung, SMC, Z-com, ZoomAir e outros)	
Orinoco	Drivers para Linux estão incluídos nos CDs e em www.orinocowireless.com. Para obter informações sobre drivers alternativos, consulte www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Orinoco.html
Apple	Consulte Orinoco
BreezeCom DS11	http://www.xs4all.nl/~bvermeul/swallow
Cisco 340 e 350	www.cisco.com/public/sw~center/sw~wireless.shtml. Uma versão ligeiramente diferente está incluída no pacote Linux PCMCIA e no kernel do Linux. Como airo.o (PCI e ISA) e airo_cs.o (PCMCIA)
Dell TrueMobile 1100	Consulte Cisco 340
D-Link DWL-500	ftp://ftp.dlink.com/Wireless/DWL-500/Driver/DWL500_linux_driver_034.tar.gz
Ericsson 11Mb DSSS WLAN	www.ericsson.com/wlan/su_downloads11.asp
Intel PRO/Wireless 2011	http://appsr.cps.intel.com/scripts-df/Product_Filter.asp?ProductID=450
Lucent	Consulte Orinoco
Nokia C110/C111	www.nokia.com/phones/productsupport/wlan/c110_c111/
Samsung MagicLan	www.magiclan.com/product/magiclan/download.mlist.jsp
Symbol Spectrum24 High Rate	http://sourceforge.net/projects/spectrum24
3Com AirConnect	http://sourceforge.net/projects/spectrum24
3Com WLAN Xjack	http://www.xs4all.nl/~bvermeul/swallow

Se você não conseguir achar o seu adaptador nesta lista, tente o site "Wireless LAN Resources for Linux" em http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux. Este site serve como uma referência sobre WLANs no Linux. Nem todas as informações no site se aplicam a redes 802.11b mas existe bastante material útil nele.

A comunidade Linux é famosa por oferecer ajuda aos novos usuários. O grupo de discussão comp.os.linux.networking é o local onde se pode fazer perguntas sobre como encontrar drivers para adaptadores de rede wireless. Faça sua pergunta caso não encontre sua resposta em um arquivo de perguntas e respostas antigo. Procure na seção http://groups.google.com.

O Prism chip set da Intersil são usados em uma grande quantidade de adaptadores que ostentam muitos nomes de marca. O site da Intersil possui uma lista atual dos usuários da Prism, em http://www.intersil.com/design/prism/prismuser/index.asp. Se o seu adaptador contém um Prism cip set, você poderá usar o driver linux-wlan, que está disponível em http://www.linux-wlan.com/download.html.

Se, assim mesmo, você não encontrar seu adaptador, o próximo passo consistirá em identificar o chip set do adaptador e encontrar um driver para ele. Você quase sempre poderá encontrar essas informações inserindo o código de FCC ID do adaptador na FCC ID Search Page da Federal Communications Commision, em http://www.fcc.gov/oet/fccid.

Outros programas wireless do Linux

Alguns dos drivers Linux para adaptadores wireless específicos acompanham utilitários de configuração que controlam a atribuição de canais, a seleção de SSID, etc. Pacotes de aplicação wireless separados também estão disponíveis e podem simplificar os processos de configuração e utilização de uma conexão wireless a uma WLAN.

Vários desses pacotes se baseiam nas Wireless Extensions para Linux API que estão incluídas na maioria dos lançamentos recentes e nos programas Wireless Tools que usam as extensões wireless. A documentação combinada para Wireless Extensions e Tools está disponível online em http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Linux.Wireless.Extensions.html.

À medida que outros softwares para Linux wireless surgirem, a página Wireless Tools for Linux (http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html) provavelmente será um dos melhores locais para aprender sobre eles.

Se um driver suportar extensões wireless, o usuário poderá alterar a configuração da rede, sem a necessidade de reiniciar o driver. As extensões wireless estão desativadas, por padrão, portanto um usuário deve ativar a opção *CONFIG_NET_RADIO* na configuração do kernel.

Wireless Tools

As Wireless Tools são um conjunto de programas que manipulam as extensões wireless. Eles são programas de linha de comando mas também oferecem um alicerce para outros programas que adicionam uma interface gráfica (GUI).

As Wireless Tools contém uma entrada /proc e três programas: iwconfig, iwspy e iwpriv. Os programas são mais um framework para desenvolvedores de software do que recursos amigáveis para usuários finais. Eles fazem o trabalho efetivo para outros programas, portanto é útil saber que eles existem e o que fazem. Na operação real, programas como Korinoco e gWireless são bem mais fáceis de usar por todos.

/proc/net/wireless

A entrada /proc é uma listagem no sistema de pseudo-arquivos /proc que mostra algumas informações estatística sobre a interface wireless. As entradas /proc atuam como arquivos, portanto o comando cat /proc/net/wireless exibirá informações estatísticas sobre o wireless:

```
>cat /proc/net/wireless
Inter-|sta|  Quality        |Discarded packets
face |tus|link level noise|  nwid  crypt   misc
eth2: 0000   15.  24.  4      181     0      0
```

Pode parecer misterioso mas pode ser entendido:

- A listagem de status mostra o estado atual do dispositivo de rede.
- Os valores Quality mostram a qualidade do sinal do link, o nível do sinal no receptor e a quantidade de ruído no receptor quando não existe um sinal presente.
- Os valores Discarded packets mostram a quantidade de pacotes descartados devido a um ID de rede inválido (nwid) ou devido ao adaptador não ter conseguido decriptografar o conteúdo dos pacotes.

iwconfig

O programa iwconfig controla as opções de configuração do adaptador wireless. Em uma rede 802.11b, são incluídos os seguintes parâmetros:

- Channel - o número do canal que será usado pelo adaptador
- Nwid - A identificação da rede. Em uma rede 802.11b, o nwid será o mesmo que o SSID.
- Name - O nome do tipo de rede wireless ou protocolo usado nesta rede. Pode ser o tipo do adaptador ou um nome genérico como "802.11b".
- Enc - A chave de criptografia usada atualmente.

O comando iwconfig, sem argumentos, produz uma lista dos valores iwconfig e /proc/net/wireless atuais.

iwspy

O programa iwspy define e exibe o endereço IP do computador local e o endereço MAC.

iwpriv

O programa iwpriv proporciona um suporte adicional para extensões específicas para o dispositivo.

KOrinoco

Este é um programa que usa as configurações e informações do Wireless Tools com ambiente gráfico KDE e imita o Orinoco para Windows. Além dos adaptadores Orinoco, ele também deve funcionar para outras marcas, desde que os drivers suportem as extensões wireless do Linux. (http://korinoco.sourceforge.net).

gWireless

Este é um programa que usa as configurações e informações do Wireless Tools. Inclui um applet Gnome que altera a cor, de vermelho até verde, à medida em que a qualidade de conexão atual melhora, e uma interface gráfica para as opções e informações controlados por iwconfig (http://gwifiapplet. sourceforge.net).

NetCfg

É uma ferramenta de configuração de rede para o ambiente Gnome. Permite que um usuário crie e gerencie perfis de conexão e que altere as configurações da rede em tempo real (http://netcfg.sourceforge.net).

Wavemon

O Wavemon usa o *ncurses* para monitorar e configurar o adaptador wireless Inclui uma tela Overview com todas as informações importantes do Wireless Tools na forma gráfica, um "nível de alarme" que é disparado quando a forá do sinal cai abaixo de um nível predefinido e um display de histórico, de tela inteira que mostra alterações no nível do sinal, no nível do ruído e na qualidade do sinal, ao longo do tempo. Também apresenta uma ferramenta de configuração que usa menus para possibilitar uma fácil configuração (http://www.jm-music.de/projects.html).

Configurando um ponto de acesso

Com exceção do Apple AirPort Base Station, a maioria dos utilitários de configuração usa uma interface baseada em Web, uma interface de linha de comando interna a partir de um terminal remoto ou ambas, portanto não deve fazer diferença qual o sistema operacional que é usado no computador host que se conecta ao AP.

Estendendo a rede para além das suas próprias paredes

A idéia original por trás das especificações 802.11b era proporcionar conexões wireless a LANs em áreas limitadas. Era este o plano, mas o mecanismo do Wi-Fi é barato, não requer uma licença e é relativamente fácil de configurar e usar. Hobbystas e organizadores de comunidade estão instalando antenas em telhados e em ladeiras onde podem proporcionar acesso wireless público ou privado à Internet, para toda a vizinhança, e criar links de dados ponto-a-ponto ao longo de vários quilômetros.

Aqui passaremos informações sobre os aspectos legais e práticos relacionados à operação e utilização de uma WLAN fora da sua própria propriedade, proporcionando também informações técnicas sobre pontos de acesso e antenas externas.

Aspectos legais

As redes Wi-Fi não exigem licenças mas o FCC e outras agências reguladoras estabeleceram algumas regras sobre as transmissões de rádio que possibilitam essas redes. A maioria dessas regras existe para minimizar a probabilidade de interferência entre WLANs, telefones sem fio e outros serviços. Por exemplo, existe uma relação direta entre a força do sinal e a distância que ele pode percorrer, portanto é essencial entender o que, exatamente, é permitido pelas regulamentações.

As regras específicas aplicadas aos dispositivos wireless 802.11b nos EUA aparecem na Parte 15, Seção 15.247 das regulamentações do FCC. Veja o que elas dizem:

(b) A potência de output de pico máxima do irradiador intencional não deve exceder o seguinte valor:
- *(1) Para todos [...] todos os sistemas de sequência diretos: 1 watt.*
- *(3) Excedto para o que é indicado nos parágrafos (b)(3)(i) e (iii) desta seção, se as antenas transmissoras de ganho direcional maior do que 6 dBi forem usadas, a potência de output de pico para o irradiador intencional deve ser reduzida para abaixo dos valores indicados nos parágrafos (b)(1) ou (b)(2) desta seção, de acordo com o apropriado, pela quantidade em dB que o ganho direcional exceda 6 dBi.*
  - *(i) Os sistemas operando na banda 2400 – 2483,5 MHz que são usados exclusivamente para operações ponto-a-ponto fixos podem empregar antenas transmissoras com ganho direcional maior do que 6 dBi que oferecem a potência de output de pico máxima do irradiador intencional é reduzido em 1 dB para cada 3 dB em que o ganho direcional da antena exceda os 6dBi.*

O que tudo isso significa? Em primeiro lugar, os transmissores de rádio dos APs e dos adaptadores podem ter uma potência máxima de 1 watt. Em segundo lugar, o ganho máximo da antena é de 6 dBi, a menos que se reduza a potência do transmissor à medida em que aumenta o ganho. Sistemas ponto-a-ponto altamente direcionais podem usar mais ganho da antena do que sistemas ponto-a-multiponto. A potência máxima de uma antena não pode ser maior do que 1 watt, mas você pode usar uma antena direcional para aumentar a potência irradiada efetiva para 4 watts.

Para permanecer estritamente de acordo com as regulamentações do FCC, cada antena deve ser certificada com o AP específico com o qual se deseje usá-la. Essas certificações devem ser disponibilizadas pela empresa que vende as antenas.

Quando se calcula a energia do output de um rádio, também se deve considerar a perda de sinal no cabo, entre o rádio e a antena. Por exemplo, o output de um AP pode ser de 20 dBm (menos da metade de um watt), mas um cabo em particular para a antena pode apresentar uma perda de 6 dB a 2.4 GHz. Portanto, a antena recebira somente 14 dBm do rádio.

Os rádios embutidos transmitem a cerca de somente 0,030 watt, portanto estão perfeitamente dentro dos limites legais.

Dois diferentes tipos de sinal Wi-Fi podem se beneficiar de mais potência do transmissor: sinais ponto-a-ponto, para viabilizar o aumento da distância entre os dois locais; e ponto-a-multiponto, para expandir a área de cobertura.

As restrições de energia do FCC para transmissores de rádio são bastante conservadoras. As empresas telefônicas e outros provedores de serviços de dados têm muita influência sobre os reguladores, para preservar as regras de baixa energia.

É bom lembrar que as regras do FCC se aplicam somente aos EUA. É importante consultar técnicos e especialistas em leis do seu próprio país (Anatel – www.anatel.gov.br, no caso do Brasil), antes de tentar instalar uma antena de alto ganho ou um amplificador de RF na sua rede.

Embora o output de energia da maioria das WLANs – mesmo as com antenas de alto ganho – deva estar dentro de níveis seguros, geralmente não é boa idéia ficar próximo a elas, principalmente quando se usa equipamentos de amplificação ou antenas de alto ganho.

Antenas externas e pontos de acesso

Diversos fatores contribuem para a força do sinal (e portanto a distância máxima) de um link de rádio entre um AP e um cliente:

- Ganho da antena
- Energia transmitida
- Altura da antena
- Atenuação do cabo

Tenha em mente que um link Wi-Fi transporta os dados nas duas direções (AP para o cliente e vice-versa). Assim, as antenas e rádios no link devem ter condições de receber e enviar sinais de rádio. Felizmente, o ganho e as características direcionais de uma antena são idênticos tanto para a transmissão quanto para a recepção.

Características da antena

As características mais importantes que definem a performance de uma antena são o *ângulo de abertura* e o *ganho.*

O ângulo de abertura de uma antena é o ângulo ou arco no qual a antena irradia ou detecta a energia em uma potência ou sensitividade máxima. Se, por exemplo, o ângulo de abertura da antena for de 20 graus, a "janela" da força de sinal máxima se estende 10 graus para cada lado da parte frontal da antena, como mostrado na fig. 10.1.

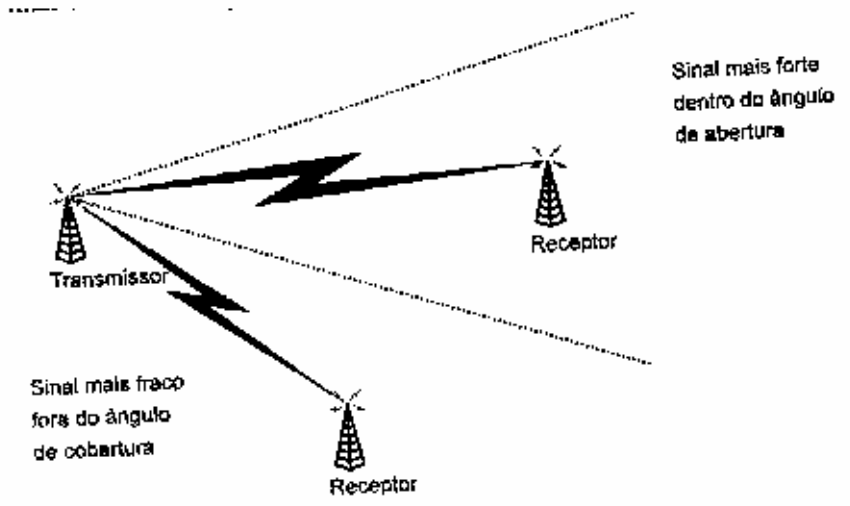

Fig. 10.1: Antenas direcionais podem aumentar a força do sinal, restringindo a mesma energia a uma área menor.

O ganho de uma antena aumenta com o tamanho da antena e à medida em que o sinal é focalizado dentro de uma abertura pequena. Pense nos ângulos das antenas e no ganho como luzes focalizadas.

Uma antena com uma maior área superficial é mais eficiente do que uma antena menor, mas o tamanho exato da antena também é extremamente importante. É importante usar uma antena projetada especificamente para operação em 2.4 GHz com a sua rede 802.11b.

Potência

A quantidade máxima de potência produzida por um transmissor é determinada pelo desenho do rádio; as pessoas que operam a rede geralmente não podem ajustá-la ou, se puderem, quase sempre não haverá nenhuma opção a mais que potência “alta” ou “baixa”.

A única maneira de aumentar a potência do sinal em um rádio consiste em colocar um amplificador de RF entre o rádio e a antena.

O Hyperlink Tecnologies e outros fabricantes oferecem amplificadores RF para uso a 2.4 GHz. Muitos desses dispositivos amplificam tanto a transmissão quanto a recepção. Este é um recurso útil, pois possibilita a instalação de um amplificador em apenas uma extremidade de um link e ainda aumenta a força do sinal em ambas as direções.

Altura da antena

Sinais de rádio a 2,4 GHz viajam ao longo de uma caminho de uma linha de visão, de maneira que se pode aumentar a distância que pode ser transposta por um sinal, elevando uma ou ambas as antenas. É este o motivo de uma prática comum, a de colocar as antenas de rádio em telhados, ladeiras e torres elevadas. Para compensar a curvatura da terra, a altura médias das duas antenas deve aumentar à medida em que a distância entre elas aumenta.

A “linha de visão” do rádio é, na realidade, mais extensa que o caminho visual entre as duas antenas. As ondas de rádio viajam dentro de uma região em forma de charuto, conhecida como *Fresnel Zone* que circunda o caminho direto entre as antenas transmissora e receptora. Para obter a melhor transmissão possível, o Fresnel Zone deve ser livre de colinas, árvores, construções e outras obstruções.

A Tabela 10.1 lista um conjunto de alturas mínimas estimadas necessárias, para várias distâncias, a 2,4 GHz.

Tabela 10.1: A Relação Entre Altura da Antena e Caminho Máximo do Sinal

Distância Média	Altura da Antena
1 milha	13 pés
3 milhas	27 pés
5 milhas	35 pés
8 milhas	48 pés
10 milhas	57 pés
15 milhas	83 pés
20 milhas	115 pés

Fonte: HyperLink Technologies, Inc.

Observe que a altera das duas antenas é a altura média acima da média do terreno; se uma antena é maior que a altura média, a outra pode estar mais próximo do chão.

Quando você estiver tentando proporcionar uma cobertura ampla, será mais eficiente posicionar a antena do AP o mais alta possível, ao invés de tentar manter elevadas as antenas dos clientes.

Atenuação do cabo

O cabo que transporta um sinal de rádio de um transmissor até uma antena não é um meio de transmissão perfeitamente eficiente; cada metro de cabo absorve um pequena, mas mensurável, quantidade de energia, o que significa que a quantidade de energia que alcança a antena decai à medida em que cresce o comprimento do cabo.

A quantidade de perda em um tipo particular de cabo depende do diâmetro do mesmo e dos materiais usados para produzi-lo. As especificações para cada tipo de cabo incluem a quantidade da atenuação, geralmente expressa em dB por 100 pés, à diferentes frequências de operação.

Ligando a vizinhança em rede

Você pode compartilhar uma conexão de alta velocidade com a Internet com vizinhos próximos. Porém, antes de você decidir pendurar uma antena no telhado da casa, considere exatamente o que você pretende conseguir com a sua rede de vizinhança e como você planeja manter a segurança no restante da sua rede. Se você estiver tentando adicionar um local particular à sua rede, use a antena direcional que focalizará o sinal para o local específico que deseja alcançar. Por outro lado, se você quiser proporcionar um hot spot de Internet para todas as pessoas das redondezas, você poderá colocar uma antena onidirecional de alto ganho no ponto mais alto do seu próprio prédio. Além disso, se você estiver usando a mesma LAN tanto para o uso dentro de casa quanto na vizinhança, certifique-se que um firewall mantém seus próprios computadores separados da porção pública da rede.

Mantendo seu provedor contente

Parece uma idéia perfeitamente lógica: compartilhar o seu modem a cabo de alta velocidade ou serviço DSL com os seus vizinhos, dividindo custos. Mas, e o seu provedor? Muitos provedores possuem políticas específicas que não permitem que os clientes compartilhem conexões através de redes de vizinhança.

O problema aí é o fato de redes de vizinhança poderem gerar uma demanda maior para a largura de banda de rede que se espera, sobrecarregando o sistema inteiro. No caso de uma conta de Internet, o provedor inclui largura de banda suficiente para atender a demanda do pico. Se a demanda aumentar será necessário instalar mais equipamentos e encontrar fonte de receita para pagar por eles.

Portanto, você tem duas opções: pergunta ao seu ISP se ele possui uma política sobre conexões compartilhadas e seguir suas diretrizes (ou procurar outro ISP); ou seguir adiante e instalar seus APs na vizinhança e ficar esperando que ninguém descubra.

Segurança de rede: Todos são seus vizinhos

A mais simples configuração de rede de vizinhança é representada por um AP com uma ampla área de cobertura e uma conexão não protegia à Internet. Qualquer pessoa com um adaptador de rede dentro da área coberta pode usar a sua rede para trocar dados através da Internet, isso inclui seu vizinho mas também o sujeito, no carro, parado na frente da sua cada com um notebook.

A menos que você esteja criando intencionalmente um hot spot de Internet público para todos os que queiram, você deve usar pelo menos uma das ferramentas de segurança embutida na 802.11b:

- Ative a criptografia de chave WEP. É verdade que um invasor dedicado pode violar uma chave WEP em menos de uma hora mas isso desencoraja o usuário casual.
- Uma filtragem de endereço MAC para restringir o acesso à sua rede. Novamente, não seria difícil criar um endereço MAC com o software apropriado mas seria uma dificuldade a mais.
- Desative a função DHCP e atribua um endereço específico a cada usuário autorizado.
- Ative a função de firewall no seu AP ou roteador.
- Use um servidor externo ou outro firewall que force cada usuário a fornecer um nome de usuário e respectiva senha, antes de conectar à Internet.
- Use uma rede privada virtual (VPN).

Além disso, encoraje todos os usuários legítimos da sua rede a prestarem bastante atenção ao compartilhamento de arquivos, de maneira que não permitam que forasteiros leiam ou gravem dados indesejáveis em seus computadores. Finalmente, troque a senha administrativa do AP. Não use *admin* nem nenhuma outra senha que seja amplamente usada como padrão. Um invasor que consiga violar o seu ponto de acesso, pode causar sérios estragos na sua rede.

Construir sua própria antena?

Muitos entusiastas de redes de vizinhança projetaram e construíram suas próprias antenas feitas de materiais curiosos, espaçadores de plástico, fios de cobre, latas vazias e latas de batatas chips. Dependendo do conteúdo da sua cesta de lixo e da sua despensa, os materiais para uma antena direcional de alto ganho, de fabricação caseira, podem custar bem pouco.

O tipo mais comum de antena direcional para comunicação ponto-a-ponto é conhecido como "yagi", ou mais apropriadamente, um sistema de antena Yagi-Uda, que recebeu seu nome de engenheiros japoneses, Professor Hidetsugu Yagi e Professor Shintaro Uda da Universidade de Tohuku, que projetaram e construíram as primeira, por volta de 1926. Uma antena yagi típica, como mostra a fig. 11.7, possui um único elemento ativo, cujo comprimento é exatamente metade do comprimento de onda da frequência de rádio na qual a antena operará (a 2.4 GHz que é cerca de 2,35 polegadas). Elementos com um quarto do comprimento de onda também funcionarão. Elementos adicionais, chamados de refletores e diretores, estão localizados paralelos ao elemento ativo e a intervalos específicos determinados pelo tamanho do elemento ativo. Os refletores estão localizados atrás do elemento ativo e os diretores estão à sua frente. A maioria das antenas de TV de telhado convencionais eram yagis.

Uma yagi tem sempre um único refletor que é cerca de 5 por cento mais longo que o elemento ativo, e diversos diretores, que são cerca de 5 por cento mais curtos que o elemento ativo (cada diretor adicional deve ser ligeiramente mais curto que o anterior).

À medida que você adiciona mais elementos a uma yagi, a quantidade de ganho aumenta. Se você quiser construir, você mesmo, uma yagi, examine a antena de Rob Flickenger, embutida dentro de uma lata de batatas chips Pringles, em http://www.oreillynet.com/cs/weblog/view/wlg/448. O projeto de 13 elementos, mais tradicional, de Darren Fulton, mostrado na Figura 11.8, usa elementos de antena cortada no comprimento do metal ou fio de cobre heavy-gauge, e um refletor feito de folha de alumínio (o projeto está disponível em http://www.users.bigpond.com/darren.fulton/yagi/13_element_yagi_antenna_for_2.htm).

Fig. 11.8: A antena Yagi caseira de Darren Fulton tem um total de 13 elementos.

Uma yagi não é o único tipo de antena direcional que serve para projetos “contrua-você-mesmo”. Antenas *waveguide*, com um elemento emissor dentro de um cilindro ou cone de metal reflexivo, usam outro desenho extremamente eficiente. A performance da antena depende do tamanho da caixa, do comprimento do elemento emissor e de sua posição exata. As instruções de Greg Rehm para a montagem de uma antena waveguide usando latas de metal estão disponíveis em http://www.turnpoint.net/wireless/cantennahowto.html.

Se você quiser impulsionar o seu ganho de sinal em todas as direções, deverá usar uma antena onidirecional. O desenho de Tim Kyle em http://njivy.org/user/kyleti?page=project&old_project=80211b_Discone deve ser um bom lugar de onde começar.

È importante ressaltar que, provavelmente, as antenas caseiras valem mais pela realização pessoal do que propriamente pela economia.

Segurança de rede wireless

As redes wireless não são seguras. São suficientemente seguras para muitos usuários a maior parte do tempo, mas é impossível tornar uma rede Wi-Fi absolutamente privada.

A mais pura verdade é que alguém que queira dedicar tempo e esforço suficientes para monitorar os sinais de rádio provavelmente poderá descobrir uma maneira de interceptar e ler os dados neles contidos.

A criptografia e outros métodos de segurança podem dificultar o roubo dos dados, mas não proporcionam uma proteção completa contra um bisbilhoteiro realmente dedicado.

Para tornar as coisas ainda mais perigosas, muitos gerentes de rede e usuários wireless domésticos deixam as portas e janelas de suas redes escancaradas para invasores, ao negligenciar o uso da criptografia e de outros recursos de segurança incorporados em cada AP e nó de rede do 802.11b.

Na primavera de 2001, o *San Francisco Chronicle* publicou que um especialista em segurança de rede, com uma antena direcional montada no teto de uma van, consegui fazer o logon em uma média de meia dúzia de redes wireless *por quarteirão*.

É importante entender que estamos falando de dois tipos diferentes de ameaças à segurança em uma WLAN. O primeiro é o perigo de um forasteiro conectar-se à sua rede sem o seu conhecimento ou permissão; o segundo, é a possibilidade de que um invasor dedicado roube dados à medida em que você os envia ou recebe. Cada um representa um diferente problema em potencial e exige uma abordagem diferente para a prevenção e proteção.

Protegendo a sua rede e os seus dados

Como operador de uma WLAN, o que você pode fazer para manter os forasteiros distantes? As suas opções são basicamente duas: você pode aceitar o fato de que as redes 802.11b não são completamente seguras mas ainda assim usar os recursos de segurança de rede incorporados para desmotivar os possíveis invasores; ou pode ignorar as ferramentas incorporadas e usar um firewall para isolar a WLAN.

A ameaça mais grave talvez não seja que as pessoas venham a bisbilhotar as suas mensagens mas que venham a criar suas próprias conexões com a sua rede e que leiam arquivos armazenados na sua rede e em outras ou usar a sua conexão de banda larga com a Internet sem o seu conhecimento ou permissão.

Faz sentido você seguir alguns passos para manter o controle sobre a sua WLAN. Se você optar por implementar a segurança do 802.11b, veja alguns passos específicos:

- Se possível, coloque seu AP no meio do prédio ao invés de próximo a uma janela. Isto reduz a distância que os seus sinais de rede percorrerão além das paredes.
- Use a função de criptografia WEP.
- Altere as suas chaves WEP com frequëncia. Isso dificulta sobremaneira a intrusão.
- Não armazene as suas chaves WEP em uma rede onde elas são usadas.
- Não use e-mails para distribuir chaves WEP.
- Adicione outra camada de criptografia, como Kerberos, SSH ou uma VPN no tpo da criptografia WEP incorporada na WLAN.
- Não use o SSID padrão do seu ponto de acesso. Esses padrões são bem conhecidos dos crackers de rede.
- Altere o SSID para algo que não identifique o seu negócio ou o seu local.
- Não use um SSID que dê a impressão que a sua rede contenha algum tipo de conteúdo fascinante - use um nome desinteressante, como oh, "rede", ou ainda uma string de informações desarticuladas como W23mQ.
- Altere o endereço IP e a senha do seu ponto de acesso. As senhas padrão de fábrica são fáceis de descobrir (dica: não use admin).
- Caso exista esta opção, desative, no AP, o recurso "broadcast SSID", que aceita conexões de clientes sem o SSID correto.

- Se possível, ative o recurso de controle de acesso no seu ponto de acesso. Ele limita as conexões com a rede aos clientes com endereços MAC especificados. Isso poderá não ser prático para o uso por visitantes já que o AP se recusará a se associar com adaptadores que não estejam na lista.
- Teste a segurança da sua rede, tentando detectar a sua rede do lado de fora do seu prédio. Use um computador portátil executando um programa rastreador, como o Network Stumbler ou o utilitário de status do seu adaptador de rede. Se você conseguir detectar sua rede a uma quadra de distância, um invasor também poderá fazê-lo. Lembre-se que os invasores podem estar usando antenas direcionais de alto ganho que podem ampliar esta distância.
- Trate a rede como se ela fosse amplamente aberta para acesso público. Certifique-se se todos que usam a rede entendem que estão utilizando um sistema desprotegido.
- Limite os compartilhamentos de arquivo aos arquivos que você deseja compartilhar; não compartilhe unidades inteiras. Use proteção por senha em todos os compartilhamentos.
- Use as mesmas ferramentas de segurança que usaria em uma rede com fio.
- Considere a utilização de uma rede privada virtual (VPN) para uma segurança aprimorada.

Ferramentas de segurança do 802.11b

As ferramentas de segurança nas especificações 802.11b não são perfeitas, mas são melhor que nada. Mesmo que você opte por não usá-las, é importante entender do que se tratam e como funcionam, mesmo que seja apenas para desativá-las.

Nome da rede (SSID)

Ao definir o nome da rede (SSID) você restringirá o acesso àqueles clientes que devem usar esse nome.

Quando o cliente detecta dois ou mais APs com o mesmo SSID, ele assume que todos fazem parte da mesma rede (mesmo que eles esteja operando em canais diferentes), e se associa com o AP que tenha o sinal mais forte e limpo.

As exceções para o nome de SSID único são as redes públicas e de comunidade, que proporcionam acesso apenas à Internet, mas não a outros computadores. Essas redes geralmente têm um SSID comum e conhecido.

Alguns APs, incluem um recurso que oferece uma opção entre acesso "aberto" ou "fechado". Quando o AP é definido como "aberto", ele aceitará uma conexão a partir de um cliente cujo SSID seja definido como "ANY" bem como a partir de dispositivos configurados para conectar com o próprio SSID do AP. Quando o AP é definido como "fechado", ele comente aceita conexões cujo SSID combine com o do AP.

Cada ponto de acesso vem com uma definição de SSID padrão, esses padrões são bem conhecidos e documentados na comunidades de bisbilhoteiros de rede (consulte, por exemplo, http://www.wi2600.org/mediawhore/nf0/wireless/ssid_defaults). Lógico que os padrões não devem ser usados em uma rede.

Criptografia WEP

A criptografia WEP destina-se a servir a três funções: evita o acesso não autorizado a uma rede, realiza uma verificação de integridade em cada pacote e protege os dados de bisbilhoteiros. Ela usa uma chave de criptografia secreta para codificar pacotes de dados no processo de transmissão ou decodificar os pacotes na recepção.

Quantidade de bits na chave WEP

A chave WEP pode ter tanto 64 (40 + 24) quanto 128 (104 + 24) bits; as chaves de 128 bits são mais difíceis de violar mas também aumentam a quantidade de tempo para transmitir cada pacote.

A sua chave é ASCII ou hexadecimal

Alguns programas exigem que a chave esteja na forma de uma string de caracteres ASCII mas muitos outros exigem em forma hexadecimal.

Cada caracter ASCII possui 8 bits e 5 caracteres para um WEP de 64 bits e 13 caracteres para um WEP de 128 bits. Em hexadecimal, cada caracter usa 4 bits e 10 caracteres em uma chave WEP de 64 bits e 26 caracteres para uma chave WEP de 128 bits.

Muitos utilitários de cliente oferecem uma opção tanto para hexadecimal quanto para ASCII, portanto pode-se usar o formato que combina com o especificado no AP.

Misturando chaves hexadecimal e ASCII

Se a rede for mista (nós que usam apenas hexadecimais e nós que usam chaves ASCII), você deverá seguir as regras seguintes para a configuração das chaves WEP:

- Converta todas as suas chaves para hexadecimal. Se um programa de configuração solicitar uma chave ASCII, insira os caracteres 0x (zero e x minúsculo), seguidos pela string hexadecimal. Se estiver usando o software AirPort da Apple, deverá inserir um sinal de dólar ($) no início de uma chave decimal em vez do 0x.
- Certifique-se de que todas as suas chaves de criptografia têm exatamente a quantidade correta de caracteres.
- Se tudo o mais falhar, leia os manuais. É possível que um ou mais dos dispositivos tenham algum recurso proprietário que possa resolver.

Alterando chaves WEP

Muitos APs e adaptadores de cliente podem ter quatro diferentes chaves WEP de 64 bits, mas apenas uma está disponível em um determinado momento. As outras chaves são reservas. Os adaptadores e APs que suportam WEP de 128 bits têm apenas uma chave em um determinado momento.

As chaves WEP devem ser alteradas de acordo com um cronograma regular. Não esquecer de manter um log offline das chaves WEP atuais em um local seguro.

O WEP é suficientemente seguro para ser usado

Diversos cientistas acadêmicos de computadores publicaram relatórios sobre criptografia WEP que questionam sua eficiência em proteger dados confidenciais. Esses especialistas são unânimes em recomendar que não se deve confiar no WEP, no que se refere à segurança deve-se empregar outros métodos para proteger as redes.

Um grupo da Universidade da Califórnia identificou numerosas falhas no algoritmo WEP que o tornam vulnerável a pelo menos quatro diferentes tipos de ataque:

- Ataques passivos que usam análises estatística para descriptografar dados.
- Ataques ativos que constroem pacotes criptografados que enganam o AP, fazendo-o aceitar comandos falsos.
- Ataques que analisam pacotes criptografados para construir um dicionário que poderá ser usado para descriptografar os dados em tempo real.
- Ataques que alteram os cabeçalhos do pacote para desviar os dados para um destino controlado pelo atacante.

Os pesquisadores, de uma forma geral, têm opinião semelhante: "O WEP do 802.11 é totalmente desprotegido". Suas conclusões são claras mas seus métodos assumem que o invasor tem um vasto conhecimento técnico. Entretanto, ferramentas para violadores de código menos sofisticados também são fáceis de encontrar. Tanto o AriSnort (http://airsnorte.shmoo.com) quanto o WEPCrack (http://sourceforge.net/projects/wepcrack) são programas Linux que monitoram sinais de WLAN e exploram as deficiências do algoritmo WEP, para extrair a chave de criptografia.

Se você aceita uma sugestão, siga em frente e criptografe os dados da sua rede. É sempre uma segurança adicional.

Controle de acesso

Com o controle de acesso, somente os clientes cujo endereço MAC esteja relacionado poderão se associar à rede.

Se você planeja usar uma lista de endereços MAC, verifique se o seu AP aceita uma lista suficientemente grande para um futuro crescimento.

Da mesma forma, tudo que o atacante precisa fazer é observar o tráfego na rede o tempo suficiente para encontrar um usuário válido e clonar seu endereço MAC.

Autenticação: o padrão 802.11x

O padrão 802.11x define uma estrutura que pode suportar diversas formas adicionais de autenticação, incluindo certificados, cartões inteligentes e senhas one-time, todas elas oferecendo mais proteção que a do 802.11.

Firewalls

Se você não acredita na proteção dos padrões 802.11 e WEP seja suficiente, você precisa de um firewall.

Um firewall é um servidor de proxy que filtra todos os dados que passam através dele, através da rede, em ambos os sentidos, com base em um conjunto de regras estabelecidas por um gerente de rede.

Em uma WLAN, um firewall também pode estar localizado no gateway entre os APs e a rede com fio. Este firewall isola a porção sem fio da LAN com fio, de forma que os invasores que tenham conectados seus computadores à rede com fio, não tenham acesso à WLAN, ou vice-versa.

Um firewall para uma WLAN deve usar algum tipo de autenticação para permitir usuários legítimos através do gateway e rejeitar todos os demais.

O firewall mais fácil de usar com uma rede wireless é um que esteja embutido em um AP. Alguns combinam as funções de um AP com um roteador de banda larga e um switch de Ethernet, de maneira que suportam tanto clientes com fio como sem fio.

O firewall usa os números de porta para identificar o serviço que está sendo solicitado. Dessa forma, pode ser feito um filtro do tráfego através do firewall.

A tabela 14.1 lista os números de porta de serviço mais comuns.

Número da Porta	Serviço de Internet
20	dados-FTP (dados padrão do FTP)
21	FTP (transferência de arquivos)
23	Telnet
25	SMTP (e-mail enviado)
37	Time
53	DNS (Domain Name System)
70	Gopher
79	Finger
80	HTTP (servidor Web)
88	Kerberos
110	POP3 (e-mail recebido)
119	NNTP (notícias)
1863	Microsoft MSN Messenger
5190	AOL Instant Messenger
7070	RealAudio

Centenas de outros números de porta foram atribuídos mas você nunca verá a maioria deles sendo usado. A lista oficial de atribuições pode ser obtida em http://www.iana.org/atribuicoes/port-numbers.

Diversos produtos de firewall de boa qualidade estão disponíveis como shareware enquanto outros são gratuitos para usuários não-comerciais, portanto é fácil tentar usá-los no seu próprio sistema. Vejamos alguns programas para Windows:

- ZoneAlarm (http://www.zonelabs.com/store/content/home.jsp).
- Tiny Personal (http://www.tinysoftware.com/pwall.php)
- Sygate Personal Firewall (http://www.sygate.com/produtos/shield_ov.htm)
- Norton Desktop Firewall (http://enterprisesecurity.symantec.com)
- Norton Personal Firewall (http://www.symantec.com)
- GFI Languard (http://www.languard.com)

Os usuários Linux também têm muitas opções de firewall. Ele é parte do kernel – seja como ipchains ou iptabels. Ambos são bem documentados em http://linuxdoc.org/HOWTO/IPCHAINS-HOWTO.html e http://www.netfilter.org/unreliable-guides/pacote-filtering-HOWTO/, respectivamente.

O PortSentry é uma ferramenta de detecção de varredura de porta integrada em várias distribuições do Linux, incluindo Red Har, Caldera, Debian e Turbo Linux. Está disponível para download em http://www.psionic.com/produtos/portsentry.html.

Redes privadas virtuais (VPNs)

A rede privativa virtual (VPN) pode adiciona outra forma eficiente de segurança para os dados que são transportados de um cliente wireless para um host.

A VPN usa um "túnel de dados" para conectar dois pontos em uma rede através de um canal criptografado. Os dados que passam através da rede pública, como a Internet, são completamente isolados dos outros tráfegos da rede. Utilizam autenticação de login e senha para restringir o acesso aos usuário autorizados, criptografam os dados para torná-los ininteligíveis para os invasores que interceptem os dados; e utilizam autenticação de dados para preservar a integridade de cada pacote de dados e para garantir que todos os dados foram originados em clientes de rede legítimos. As funções VPN ocorrem na camada de IP, ou rede, , do modelo OSI. Portanto, podem operar no topo dos protocolos 802.11 que operam na camada física. As VPNs também podem passar dados através de uma conexão que inclua mais de um meio físico. Em outas palavras, a VPN é um serviço extremo-a-extremo, não importa se usando um link wireless, um cabo Ethernet, uma linha telefônica convencional ou alguma combinação destes e outros meios de transmissão.

As VPNs são usadas frequentemente para estender as redes corporativas para filiais e para conectar usuários à LAN a partir de suas residências ou de locais externos.

Um dispositivo de cliente conectado através de um servidor de VPN apresenta a mesma aparência para o restante da rede (VPN protegida) que um dispositivo na mesma sala ou prédio. A única diferença é que os dados da VPN passam através de um driver de VPN e de rede pública em vez de diretamente a partir do adaptador de rede para a LAN. A figura 15.1 mostra uma conexão VPN típica com uma rede remota.

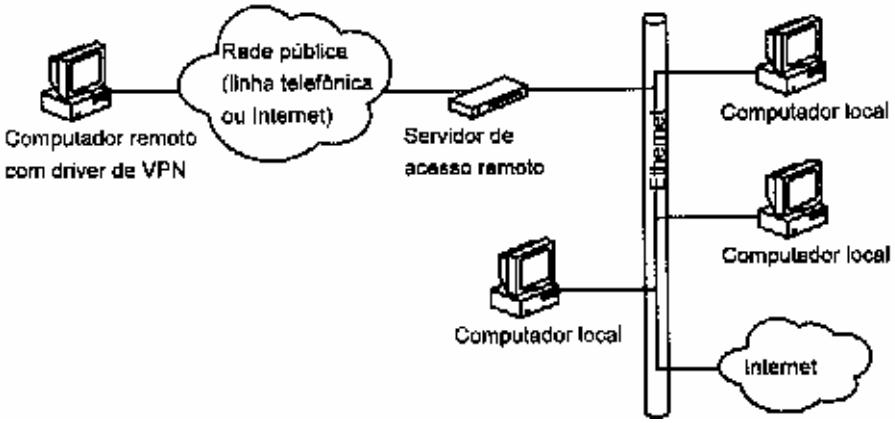

Fig. 15.1: A rede remota pode conectar a uma LAN através da VPN

O objetivo de uma VPN wireless é proteger o link wireless entre os clientes e o AP, e bloquear os usuários não autorizados.

A figura 15.2 mostra uma conexão wireless com uma VPN. O servidor VPN está localizado entre o AP e o host LAN, portanto todos os pacotes transferidos através da porção wireless da rede são criptografados.

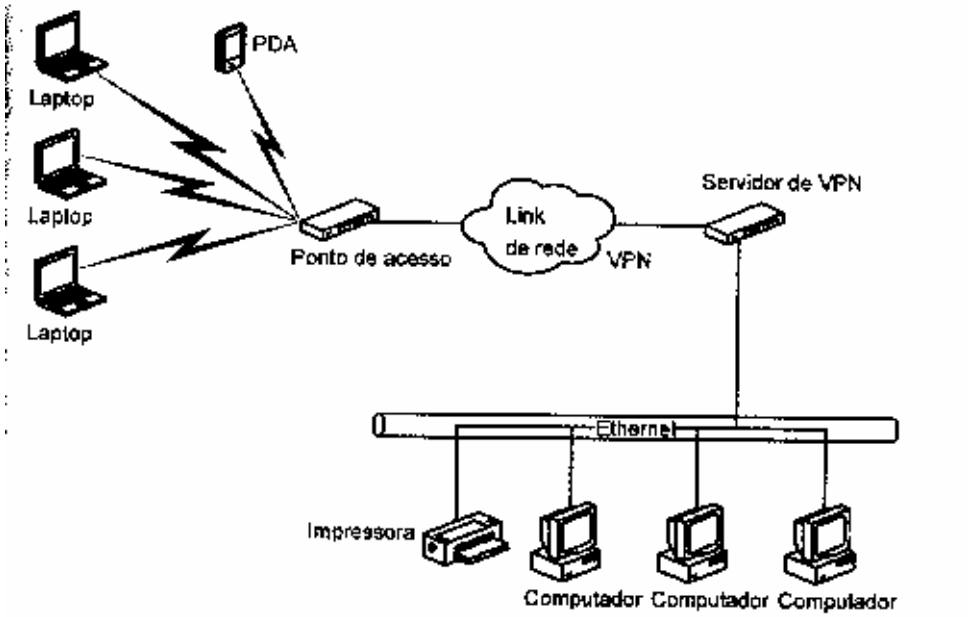

Fig. 15.2.: Uma VPN proporciona uma conexão segura entre a WLAN e um gateway de Internet ou uma LAN

Métodos de VPN

A VPN transfere os dados através de uma ou mais redes intermediárias para um destino ou outra rede. O cliente de tunneling da VPN encapsula os pacotes de dados ou frames existentes, adicionando um novo cabeçalho com as informações de roteamento que instruem como alcançar a extremidade da VPN. O caminho de transmissão através das redes intermediárias é chamado de *túnel*. Na outra extremidade, o servidor VPN retira o cabeçalho de tunneling e encaminha os dados para o destino especificado pela próxima camada de cabeçalhos. A forma exata do túnel não faz diferença no que se refere aos dados, pois estes tratam o túnel como uma conexão ponto-a-ponto.

Os métodos mais amplamente usados nas VPNs são Point-to-Point Tunneling Protocol (PPTP), Layer Two Tunneling Protocol (L2TP) e modo IP Security (IPSec). O PPTP e o L2TP podem transferir dados através de redes IP, IPX e NetBEUI; o IPSec limita-se a redes IP. Tanto o cliente como o servidor devem usar o mesmo protocolo.

No PPTP e L2TP, o cliente e o servidor devem configurar o túnel para cada transmissão antes de começarem a trocar dados. Os parâmetros de configuração incluem a rota através da rede intermediária e as especificações de criptografia e compactação. Ao terminar a conexão, o túnel é fechado.

Em um link IPSec, o cliente e o servidor devem estabelecer o túnel através das redes intermediárias em uma transação à parte, antes de começarem a trocar dados.

Servidores de VPN

Um servidor de VPN pode ser parte de um servidor Unix ou Windows ou ser embutido em um roteador de rede ou gateway standalone. Se já existir um servidor na rede, você poderá usá-lo como o servidor de VPN.

O servidor também exige duas placas de interface de rede: uma conectada à LAN com fio ou ao gateway de Internet e a outra conectada à WLAN. A placa de interface conectada à porta wireless normalmente conecta diretamente à porta Ethernet do AP.

Configurando um servidor do Windows para VPN wireless

Se você pretende usar um servidor Windows, o PPTP provavelmente será o protocolo mais fácil de ser usado, pois foi originado com uma especificação da Microsoft.

Configurando a conexão VPN

A conexão VPN geralmente é um link Ethernet com um ou mais pontos de acesso. O perfil de conexão no servidor para a conexão VPN deve incluir o endereço IP e a máscara de sub-rede atribuída a esta porta e os endereços dos servidores DNS e nome WINS usados por esta rede.

Configurando o servidor de acesso remoto como um roteador

O servidor deve usar rotas estáticas ou protocolos de roteamento que tornam cada cliente wireless alcançável através de uma rede com fio.

Ativando e configurando o servidor para clientes PPTP ou L2TP

O Windows utiliza o Remote Access Service (RAS) e o Point-to-Point Protocol (PPP), para estabelecer conexões VPN. O serviço Routing and Remote Access ativa o RAS e a conexão VPN exige essas opções de Configuração do RAS:

Authentication Method	As conexões PPTP criptografadas usam os métodos de autenticação MS-CHAP ou EAPTLS.
Authentication Provider	A segurança do Windows 2000 ou um servidor RADIUS externo podem verificar os clientes de rede.
IP Routing	IP Routing e acesso remoto baseado em IP devem estar ativosSe a rede com fio atuar como um servidor DHCP para os clientes wireless, o DHCP deverá estar ativo.

Configurando portas PPTP ou L2TP

Define cada porta PPTP ou L2TPpara aeitar o acesso remoto.

Definindo filtros de rede

Filtros de entrada e saída evitam que o servidor de acesso remoto envie e receba dados que não tenham sido originados em um cliente VPN.

Configurando políticas de acesso remoto

A permissão de acesso remoto para cada cliente wireless deve ser definida de maneira a permitir o acesso ao servidor RAS. O tipo de porta deve ser definido com o Protocolo VPN correto (por exemplo, PPTP ou L2TP) e o perfil de cada conexão deve incluir o tipo de criptografia que está sendo usado. No Windows, existem três opções de comprimento de criptografia:

- Básico: chave de 40 bits.
- Robusto: chave de 56 bits.
- Mais robusto: chave de 128 bits.

Hardware de rede com suporte a VPN incorporado

Um computador dedicado executando o Linux pode ser um servidor de VPN barato; ou se você estiver usando um servidor Windows para outras finalidades, também pode proporcionar suporte a VPN, sem custo adicional, ou com custo muito reduzido.

Como mostra a figura 15.3, um roteador localizado entre o AP e a porção com fio de uma rede corporativa, pode também atuar facilmente como um servidor de VPN. Em uma rede doméstica, o servidor de VPN pode operar entre o AP e um DSL ou modem a cabo.

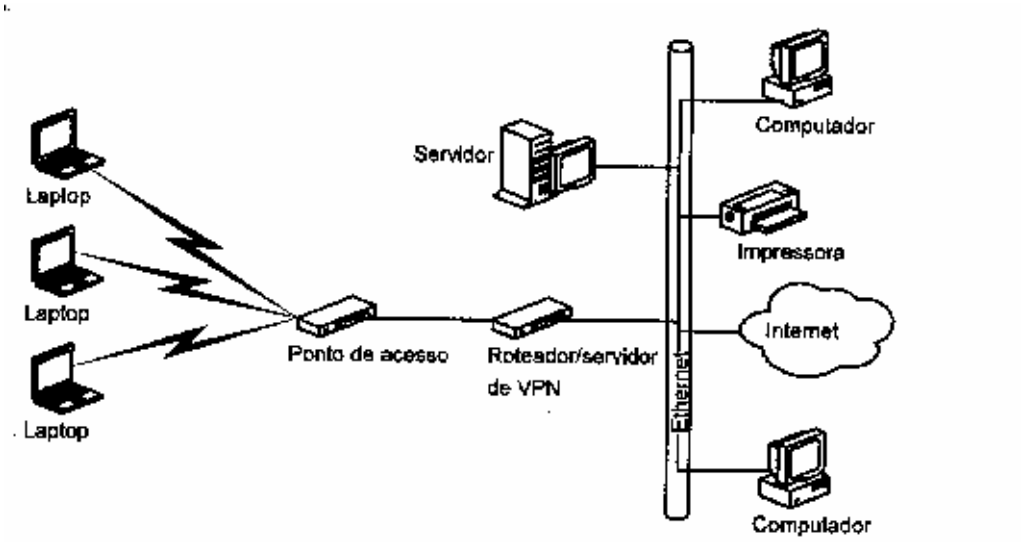

Fig. 15.3: Um roteador de rede também pode atuar como um servidor de VPN de uma WLAN

O hardware de cliente VPN stand-alone situado entre o computador e a rede também está disponível, mas isto não é tão prático em uma WLAN pois um adaptador de rede wireless está quase sempre conectado diretamente ao próprio computador.

Software de cliente VPN

Um cliente wireless se conecta a um servidor VPN, através de seu link Ethernet wireless, a um AP, que o sistema operacional reconhece como uma conexão LAN. Para configurar um túnel VPN através dessa conexão, é necessário instalar o protocolo de tunneling como um serviço de rede.

Configurando o Windows para VPN

O Windows inclui suporte para VPNs na maioria das versões mas isso não faz parte da instalação padrão. Portanto, o primeiro passo na configuração de um cliente VPN consiste em instalar o protocolo. Nas versões para o consumidor do Windows, siga os seguintes passos:

1. No *Painel de Controle*, selecione *Adicionar/Remover Programas*.
2. Abra a guia *Instalação do Windows*
3. Selecione *Comunicações* na lista de componentes e clique sobre o botão *Detalhes.*
4. Role a lista até encontrar a opção *Rede Privada Virtual*. Marque a caixa próxima a ela.
5. Clique sobre os botões *OK* na janela *Comunicações* e na janela *Adicionar/Remover Programas*
6. Reinicie o sistema quando for solicitado.

No Windows NT e no 2000, siga os seguintes passos:

1. No *Painel de Controle*, selecione a opção *Rede*.
2. Na guia *Protocolos*, clique sobre o botão *Adicionar.*
3. Selecione *Protocolo de Tunelamento Ponto-a-Ponto* na lista de *Protocolos de Rede* e clique no OK.
4. Quando aparecer a janela de *Configuração PPTP*, selecione o número de dispositivos de VPN que você deseja suportar neste cliente. Na maioria das vezes, um dispositivo é suficiente para um cliente wireless.
5. Clique sobre o botão OK em todas as janelas abertas.
6. Reinicie o computador para ativar o cliente VPN.
7. Para adicionar o cliente VPN como uma porta do RAS, abra o *Painel de Controle* e selecione *Rede* novamente. Escolha a guia *Serviços* e selecione a opção *Serviço de Acesso Remoto (RAS).*
8. Clique sobre o botão *Propriedades*.
9. Clique no botão *Adicionar* para adicionar um dispositivo RAS.
10. Caso *VPN1-RASPPTPM* não esteja visível, abra a lista drop-down de dispositivos, selecione *VPN1-RASPPTP* e clique em OK.

11. Selecione a porta VPN e clique sobre o botão *Configurar*. Escolha a opção que especifica a porta da WLAN e clique em OK.

Finalmente, você deve criar um perfil de conexão que faça a conexão com o servidor de VPN:

1. No *Painel de Controle*, ou na janela *Meu Computador*, abra *Acesso à Rede Dial-UP*.
2. Dê um clique duplo sobre *Fazer nova conexão*.
3. Na primeira tela do assistente, insira um nome para o servidor de VPN no campo *Digite um nome*.
4. Abara o menu *Selecione um dispositivo* e escolha a opção *Adaptador VPN*. Clique em *Próximo* para passar à próxima tela do assistente.
5. Insira o endereço IP do servidor VPN no campo *Nome do Host ou Endereço IP*. Clique em *Próximo*. O assistente confirmará que foi criado um novo perfil de conexão.
6. Clique em *Fim* para fechar o assistente. Você deverá ver um ícone para o novo perfil de conexão na janela *Rede Dial-Up*.

No Windows XP, um assistente simplifica bastante o processo inteiro:

1. No *Painel de Controle*, abra *Conexões de Rede*.
2. Dê um clique duplo sobre o ícone *Assistente para nova conexão*.
3. Quando a janela *Tipo de conexão de rede*, for aberta, escolha a opção *Conectar à rede em minha área de trabalho*.
4. Na janela *Conexões de Rede*, escolha a opção *Conexão com Rede Virtual Privada* e clique em *Próximo*.
5. Na janela *Nome da conexão*, digite um nome para a conexão VPN wireless. Este nome aparecerá nos atalhos do desktop para esta conexão. Clique em *Próximo*.
6. Na janela *Rede Pública*, escolha a opção *Não Discar*, pois você não deseja conectar através de linha telefônica. Clique em *Próximo*.
7. Na janela *Seleção de servidor VPN*, digite o endereço IP do servidor de VPN.
8. Clique em *Próximo* e a seguir, em *Fim* para concluir o assistente.

O cliente VPN Microsoft L2TP/IPSec

A Microsoft inclui um cliente para conexões L2TP com o IPSec no Windows 2000 e no XP. Um programa similar para as versões anteriores foi disponibilizado, para download gratuito, pela Microsoft. Em http://www.microsoft.com/windows2000/downloads/tools/default.asp, escolha o link apropriado.

Criando a conexão no Windows

Quando o perfil de conexão estiver pronto, será fácil conectar um cliente do Windows à LAN host ou à Internet através do link VPN wireless: basta dar um clique duplo sobre o ícone do perfil de conexão. O Windows solicitará um login e senha e a seguir criará a conexão.

Se a sua conexão wireless for o método que você usar com a maior regularidade para se conectar à Internet, você poderá torná-la a conexão padrão, que será aberta sempre que você executar uma aplicação de rede como um browser ou programa de e-mail de cliente. Para fazer do VPN o perfil padrão, siga os seguintes passos:

1. Abra a janela *Propriedades da Internet* no *Painel de Controle*.
2. Selecione a guia *Conexões*.
3. Na seção *Dial-Up* Settings, selecione o perfil de conexão VPN da lista e clique sobre o botão *Set Default*.
4. Clique sobre o botão *Settings*. Na seção *Dial-Up* Settings, digite o seu login e sua senha no servidor de VPN.
5. Escolha a opção *Dial Whenever a Network Connection is Not Present*.

Opções do Windows XP

O Windows XP oferece muitas opções de VPN que não estavam disponíveis nas versões anteriores. Para definir essas opções, siga os seguintes passos:

1. Abra a janela *Conexões de Rede* no *Painel de Controle*.
2. Dê um clique duplo sobre o ícone VPN. Será aberta a janela *Conectar*.

3. Clique sobre o botão *Propriedades*.
4. O endereço IP do servidor de VPN já deverá estar disponível no campo *Nome do Host*. A opção *Disque outra conexão primeiro* deverá estar desativada. Clique sobre a guia *Rede*.
5. Escolha o tipo de servidor VPN que será usado em sua rede, no menu *Tipo de VPN*. Se você não souber qual o tipo de VPN, escolha a opção *Automática*.
6. Selecione *TCP/IP* na lista de itens de conexão, e clique sobre o botão *Propriedades* para alterar as configurações de rede, incluindo se você usará um servidor de DHCP ou configurações manuais para o endereço IP e o DNS.
7. Clique sobre a guia *Avançado*. Se a sua rede ainda não estiver protegida por um firewall, ative a opção *Firewall para conexão Internet*, isto protegerá o cliente wireless de ataques provenientes da Internet.

As guias Opções e Segurança da janela Propriedades controlam as opções de conexão que normalmente não são alteradas a partir das configurações padrão. Os gerentes de rede que desejem alterar as configurações de segurança devem instruir seus usuários como configurar essas opções para satisfazer os requisitos específicos da rede.

Usando uma VPN Wireless

Quando você projeta uma VPN para proteger os dados da sua rede, é importante entender onde as extremidades do túnel VPN estão localizadas.

Se a sua rede wireless precisar suportar dispositivos portáteis no seu escritório, fábrica ou campus, fará sentido colocar o servidor entre a rede de APs e a conexão com a sua LAN corporativa, o que protegerá os dados dos seus usuários wireless e manterá os usuários não autorizados distantes da rede, mas não afetará os outros usuários cujos computadores conectem à LAN através de cabos.

Em redes domésticas ou de uma pequena empresa, os APs provavelmente conectam a um roteador de gateway de Internet. Se o AP e o gateway forem dispositivos separados, você poderá posicionar o servidor de VPN entre os dois. Porém, se o AP e o gateway forem combinados na mesma caixa, você precisará tanto usar clientes VPN quanto posicionar o cliente entre o gateway e o modem de Internet, como mostra a Fig. 15.16, ou ignorar as portas Ethernet com fio no gateway e adicionar um novo hub ou switch entre o servidor de VPN e o modem de Internet como mostra a Fig. 15.17.

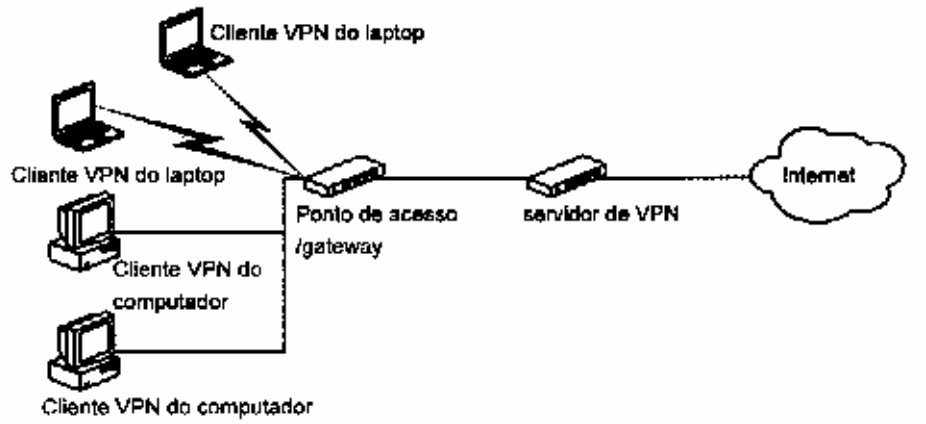

Fig. 15.16: Em uma pequena rede, você pode usar clientes VPN em todos os computadores

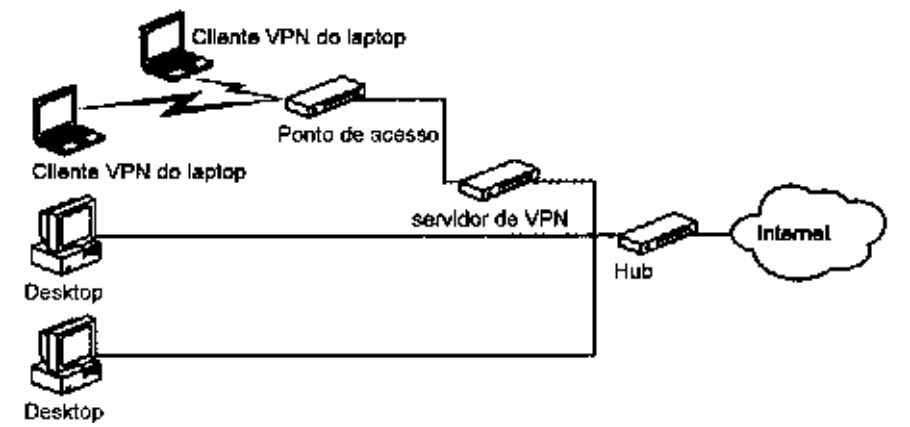

Fig. 15.17: Nesta rede, a VPN protege somente os links wireless

Criando a conexão

Se você usa a WLAN com a proteção VPN a maior parte do tempo, você deve fazer do perfil VPN a sua conexão padrão

Para definir um perfil de conexão padrão no Windows, abra a janela *Rede Dial-Up* (no XP, use a janela *Conexões de Rede*). Dê um clique com o botão direito do mouse sobre o perfil que você deseja escolher, e selecione a opção *Set as Default* no menu.

Para conectar a uma VPN que não seja o seu padrão, dê um clique duplo sobre o ícone do perfil da conexão da VPN.

Usando uma VPN através da rede pública

Quando você conecta o seu notebook à sua LAN corporativa através da rede pública em um aeroporto ou centro de convenções, pode conectar através de suas redes à Internet e ao seu próprio servidor de VPN corporativo. Por precisar fazer o logon na rede pública antes de iniciar a conexão VPN, você deve criar um perfil de conexão "VPN através de rede pública" separado, além daquele que você usa no seu próprio escritório. O perfil deve apontar para o seu servidor de VPN corporativo, mas não deve ser a sua conexão padrão.

Para conectar através da rede pública a um computador que esteja executando o Windows, siga os seguintes passos:

1. Use o seu utilitário de configuração wireless para selecionar a rede pública que você quer usar.
2. Inicie o seu browser. Você deverá ver a tela de login da rede pública.
3. Insira o nome e senha da sua conta na rede pública.
4. Minimize a janela do browser e abra a janela Dial-Up Networking.
5. Dê um clique duplo sobre o ícone do seu perfil *VPN através da rede pública.* O computador conectará através da Internet à sua LAN corporativa.
6. Insira o login e senha para sua rede corporativa.