Traduzido, implementado e adaptado por Alexandre Guimarães (ALEDEGUI)

O que são Redes Wireless?

A palavra wireless provém do inglês: wire (fio, cabo); less (sem); ou seja: sem fios. Wireless então caracteriza qualquer tipo de conexão para transmissão de informação sem a utilização de fios ou cabos. Uma rede sem fio é um conjunto de sistemas conectados por tecnologia de rádio através do ar. Pela extrema facilidade de instalação e uso, as redes sem fio estão crescendo cada vez mais. Dentro deste modelo de comunicação, enquadram-se várias tecnologias, como Wi-Fi, InfraRed (infravermelho), bluetooth e Wi-Max.

Seu controle remoto de televisão ou aparelho de som, seu telefone celular e uma infinidade de aparelhos trabalham com conexões wireless. Podemos dizer, como exemplo lúdico, que durante uma conversa entre duas pessoas, temos uma conexão wireless, partindo do principio de que sua voz não utiliza cabos para chegar até o receptor da mensagem.

Nesta categoria de redes, há vários tipos de redes que são: Redes Locais sem Fio ou WLAN (Wireless Local Area Network), Redes Metropolitanas sem Fio ou WMAN (Wireless Metropolitan Area Network), Redes de Longa Distância sem Fio ou WWAN (Wireless Wide Area Network), redes WLL (Wireless Local Loop) e o novo conceito de Redes Pessoais Sem Fio ou WPAN (Wireless Personal Area Network).

As aplicações de rede estão dividas em dois tipos: aplicações indoor e aplicações outdoor. Basicamente, se a rede necessita de comunicação entre dois ambientes, a comunicação é realizada por uma aplicação outdoor (dois prédios de uma mesma empresa, por exemplo). A comunicação dentro de cada um dos prédios é caracterizada como indoor. A comunicação entre os dois prédios é realizada por uma aplicação outdoor.

Como funcionam?

Através da utilização portadoras de rádio ou infravermelho, as WLANs estabelecem a comunicação de dados entre os pontos da rede. Os dados são modulados na portadora de rádio e transmitidos através de ondas eletromagnéticas.

Múltiplas portadoras de rádio podem coexistir num mesmo meio, sem que uma interfira na outra. Para extrair os dados, o receptor sintoniza numa freqüência específica e rejeita as outras portadoras de freqüências diferentes.

Num ambiente típico, o dispositivo transceptor (transmissor/receptor) ou ponto de acesso (access point) é conectado a uma rede local Ethernet convencional (com fio). Os pontos de acesso não apenas fornecem a comunicação com a rede convencional, como também intermediam o tráfego com os pontos de acesso vizinhos, num esquema de micro células com roaming semelhante a um sistema de telefonia celular.

A topologia da rede é composta de que?

- BSS (Basic Service Set) - Corresponde a uma célula de comunicação da rede sem fio.
- STA (Wireless LAN Stations) - São os diversos clientes da rede.
- AP (Access Point) - É o nó que coordena a comunicação entre as STAs dentro da BSS. Funciona como uma ponte de comunicação entre a rede sem fio e a rede convencional.

- DS (Distribution System) - Corresponde ao backbone da WLAN, realizando a comunicação entre os APs.
- ESS (Extended Service Set) - Conjunto de células BSS cujos APs estão conectados a uma mesma rede convencional. Nestas condições uma STA pode se movimentar de uma célula BSS para outra permanecendo conectada à rede. Este processo é denominado de Roaming.

< modos dois de configuradas ser podem WLANs redes>

As Redes WLAN Podem ser configuradas como:

- Ad-hoc mode – Independent Basic Service Set (IBSS)

A comunicação entre as estações de trabalho é estabelecida diretamente, sem a necessidade de um AP e de uma rede física para conectar as estações.

- Infrastructure mode – Infrastructure Basic Service Set

A rede possui pontos de acessos (AP) fixos que conectam a rede sem fio à rede convencional e estabelecem a comunicação entre os diversos clientes.

Tecnologias empregadas

Há várias tecnologias envolvidas nas redes locais sem fio e cada uma tem suas particularidades, suas limitações e suas vantagens. A seguir, são apresentadas algumas das mais empregadas.

- Sistemas Narrowband: Os sistemas narrowband (banda estreita) operam numa freqüência de rádio específica, mantendo o sinal de de rádio o mais estreito possível o suficiente para passar as informações. O crosstalk indesejável entre os vários canais de comunicação pode ser evitado coordenando cuidadosamente os diferentes usuários nos diferentes canais de freqüência.

- Spread Spectrum: É uma técnica de rádio freqüência desenvolvida pelo exército e utilizado em sistemas de comunicação de missão crítica, garantindo segurança e rentabilidade. O Spread Spectrum é o mais utilizado atualmente. Utiliza a técnica de espalhamento espectral com sinais de rádio freqüência de banda larga, foi desenvolvida para dar segurança, integridade e confiabilidade deixando de lado a eficiência no uso da largura de banda. Em outras palavras, maior largura de banda é consumida que no caso de transmissão narrowaband, mas deixar de lado este aspecto produz um sinal que é, com efeito, muito mais ruidoso e assim mais fácil de detectar, proporcionando aos receptores conhecer os parâmetros do sinal spread-spectrum via broadcast. Se um receptor não é sintonizado na freqüência correta, um sinal spread-spectrum inspeciona o ruído de fundo. Existem duas alternativas principais: Direct Sequence Spread Spectrum (DSSS) e Frequency Hopping Spread Spectrum (FHSS).

Direct Sequence Spread Spectrum (DSSS): Gera um bit-code (também chamado de chip ou chipping code) redundante para cada bit transmitido. Quanto maior o chip maior será a probabilidade de recuperação da informação original. Contudo, uma maior banda é requerida. Mesmo que um ou mais bits no chip sejam danificados durante a transmissão, técnicas estatísticas embutidas no rádio são capazes de recuperar os dados originais sem a necessidade de retransmissão. A maioria dos fabricantes de produtos para Wireless LAN tem adotado a tecnologia DSSS depois de considerar os benefícios versus os custos e benefício que se obtém com ela. Tal é o caso dos produtos Wireless da D-Link.

Frequency-hopping spread-spectrum (FHSS): Utiliza um sinal portador que troca de freqüência no padrão que é conhecido pelo transmissor e receptor. Devidamente sincronizada, a rede efetua esta troca para manter um único canal analógico de operação.

Outras Tecnologias

A comunicação wireless está presente há um bom tempo no nosso cotidiano. Falemos da conexão sem fio mais comum – os controles remotos para televisores, som, DVD, entre outros, utilizam conexão por raios infravermelhos (InfraRed). Essa conexão atua em um alcance máximo de 5m aproximadamente, e com ângulo de 45 graus a partir da fonte.

Apesar de oferecer conexão, o InfraRed trazia a inconveniência de sempre necessitar do alinhamento dos dispositivos, o que criava uma certa dificuldade para locomoção, além de ter a mesma velocidade de uma porta serial. Foi então desenvolvida a tecnologia conhecida como bluetooth. Essa tecnologia atua em um raio de 10m, com uma velocidade maior que o InfraRed, utilizando a Rádio Freqüência.
Com bluetooth, o sinal se propaga em todas as direções, não necessita alinhamento e torna a locomoção mais fácil. Os padrões de velocidade são:

- Assíncrono, a uma taxa máxima de 723,2 kbit/s (unidirecional).
- Bidirecional síncrono, com taxa de 64 kbit/s, que suporta tráfego de voz entre os dois dispositivos.

Com o sucesso do Wi-Fi, a Intel começou a apoiar uma outra nova tecnologia denominada Wi-Max. Esta conexão wireless de alta velocidade permite um alcance de até cerca de 48 quilômetros.
Uma outra solução é a Mobile-Fi, uma tecnologia que permite banda larga sem fio em veículos em movimento. A NTT DoCoMo e alguns startups trabalham atualmente na definição de um protocolo, o que deve acontecer em 2005 ou 2006. A Nextel também está conduzindo testes com o Mobile-Fi.
Uma outra tecnologia nova que desponta é a UltraWideband, que permite a transmissão de arquivos enormes sobre distâncias curtas – mesmo através de

paredes. Existe no momento uma disputa pela definição deste protocolo entre Texas Instruments e Intel de um lado, e Motorola do outro.

Segurança

As principais dicas para se ter uma rede Wireless Segura

Uma rede sem fio é um conjunto de sistemas conectados por tecnologia de rádio através do ar, Com um transmissor irradiando os dados transmitidos através da rede em todas as direções, como impedir que qualquer um possa se conectar a ela e roubar seus dados? Um ponto de acesso instalado próximo à janela da sala provavelmente permitirá que um vizinho a dois quarteirões da sua casa consiga captar o sinal da sua rede, uma preocupação agravada pela popularidade que as redes sem fio vêm ganhando. Para garantir a segurança, existem vários sistemas que podem ser implementados, apesar de nem sempre eles virem ativados por default nos pontos de acesso.

O que realmente precisamos saber para que a rede sem fio implementada esteja com o nível correto de segurança? Em primeiro lugar é preciso conhecer os padrões disponíveis, o que eles podem oferecer e então, de acordo com sua aplicação, política de segurança e objetivo, implementar o nível correto e desejado. Ser o último disponível não garante, dependendo de sua configuração, que a segurança será eficiente. É preciso entender, avaliar bem as alternativas e então decidir-se de acordo com sua experiência e as características disponíveis nos produtos que vai utilizar, objetivando também o melhor custo.

A segurança wireless é um trabalho em andamento, com padrões em evolução. Com tempo e acesso suficientes, um hacker persistente provavelmente conseguirá invadir seu sistema wireless. Ainda assim, você pode tomar algumas atitudes para dificultar ao máximo possível o trabalho do intruso. , nas variantes de conotação maléfica da palavra. Temos, assim, práticas típicas concernentes a redes sem fio, sejam estas comerciais ou não, conhecidas como wardriving e warchalking.

Wardriving

O termo wardriving foi escolhido por Peter Shipley (http://www.dis.org/shipley/) para batizar a atividade de dirigir um automóvel à procura de redes sem fio abertas, passíveis de invasão. Para efetuar a prática do wardriving, são necessários um automóvel, um computador, uma placa Ethernet configurada no modo "promíscuo" (o dispositivo efetua a interceptação e leitura dos pacotes de comunicação de maneira completa), e um tipo de antena, que pode ser posicionada dentro ou fora do veículo (uma lata de famosa marca de batatas fritas norte-americana costuma ser utilizada para a construção de antenas) . Tal atividade não é danosa em si, pois alguns se contentam em encontrar a rede wireless desprotegida, enquanto outros efetuam login e uso destas redes, o que já ultrapassa o escopo da atividade. Tivemos notícia, no ano passado, da verificação de desproteção de uma rede wireless pertencente a um banco internacional na zona Sul de São Paulo mediante wardriving, entre outros casos semelhantes. Os aficionados em wardriving consideram a atividade totalmente legítima.

Warchalking

Inspirado em prática surgida na Grande Depressão norte-americana, quando andarilhos desempregados (conhecidos como "hobos") criaram uma linguagem de marcas de giz ou carvão em cercas, calçadas e paredes, indicando assim uns aos outros o que esperar de determinados lugares, casas ou instituições onde poderiam conseguir comida e abrigo temporário, o warchalking é a prática de escrever símbolos indicando a existência de redes wireless e informando sobre suas configurações. As marcas usualmente feitas em giz em calçadas indicam a posição de redes sem fio, facilitando a localização para uso de conexões alheias pelos simpatizantes da idéia.

O padrão IEEE 802.11 fornece o serviço de segurança dos dados através de dois métodos: autenticação e criptografia. Este padrão 802.11 define duas formas de autenticação: open system e shared key. Independente da forma escolhida, qualquer autenticação deve ser realizada entre pares de estações, jamais havendo comunicação multicast. Em sistemas BSS as estações devem se autenticar e realizar a troca de informações através do Access Point (AP). As formas de autenticação previstas definem:

- Autenticação Open System - é o sistema de autenticação padrão. Neste sistema, qualquer estação será aceita na rede, bastando requisitar uma autorização. É o sistema de autenticação nulo.
- Autenticação Shared key – neste sistema de autenticação, ambas as estações (requisitante e autenticadora) devem compartilhar uma chave secreta. A forma de obtenção desta chave não é especificada no padrão, ficando a cargo dos fabricantes a criação deste mecanismo. A troca de informações durante o funcionamento normal da rede é realizada através da utilização do protocolo WEP.

Autenticação do cliente feita com "shared keys"

A autenticação do tipo Open System foi desenvolvida focando redes que não precisam de segurança para autenticidade de dispositivos. Nenhuma informação sigilosa deve trafegar nestas redes já que não existe qualquer proteção. Também se aconselha que estas redes permaneçam separadas da rede interna por um firewall (a semelhança de uma zona desmilitarizada – DMZ).

A autenticação Shared Key utiliza mecanismos de criptografia para realizar a autenticação dos dispositivos. Um segredo é utilizado como semente para o algoritmo de criptografia do WEP na cifragem dos quadros. A forma de obter esta autenticação é a seguinte:

1. Estação que deseja autenticar-se na rede envia uma requisição de autenticação para o AP.
2. O AP responde a esta requisição com um texto desafio contendo 128 bytes de informações pseudorandômicas.
3.A estação requisitante deve então provar que conhece o segredo compartilhado, utilizando-o para cifrar os 128 bytes enviados pelo AP e devolvendo estes dados ao AP.
4.O AP conhece o segredo, então compara o texto originalmente enviado com a resposta da estação. Se a cifragem da estação foi realizada com o segredo correto, então esta estação pode acessar a rede.

Dentro do utilitário de configuração você poderá habilitar os recursos de segurança. Na maioria dos casos todos os recursos abaixo vêm desativados por default a fim de que a rede funcione imediatamente, mesmo antes de qualquer coisa ser configurada. Para os fabricantes, quanto mais simples for a instalação da rede, melhor, pois haverá um número menor de usuários insatisfeitos por não conseguir fazer a coisa funcionar. Mas, você não é qualquer um. Vamos então às configurações:

SSID

A primeira linha de defesa é o SSID (Service Set ID), um código alfanumérico que identifica os computadores e pontos de acesso que fazem parte da rede. Cada fabricante utiliza um valor default para esta opção, mas você deve alterá-la para um valor alfanumérico qualquer que seja difícil de adivinhar.

Geralmente estará disponível no utilitário de configuração do ponto de acesso a opção "broadcast SSID". Ao ativar esta opção o ponto de acesso envia periodicamente o código SSID da rede, permitindo que todos os clientes próximos possam conectar-se na rede sem saber previamente o código. Ativar esta opção significa abrir mão desta camada de segurança, em troca de tornar a rede mais "plug-and-play". Você não precisará mais configurar manualmente o código SSID em todos os micros.

Esta é uma opção desejável em redes de acesso público, como muitas redes implantadas em escolas, aeroportos, etc., mas caso a sua preocupação maior seja a segurança, o melhor é desativar a opção. Desta forma, apenas quem souber o valor ESSID poderá acessar a rede.

WEP

O Wired Equivalency Privacy (WEP) é o método criptográfico usado nas redes wireless 802.11. O WEP opera na camada de enlace de dados (data-link layer) e fornece criptografia entre o cliente e o Access Point. O WEP é baseado no método criptográfico RC4 da RSA, que usa um vetor de inicialização (IV) de 24 bits e uma chave secreta compartilhada (secret shared key) de 40 ou 104 bits. O IV é concatenado com a secret shared key para formar uma chave de 64 ou 128 bits que é usada para criptografar os dados. Além disso, o WEP utiliza CRC-32 para calcular o checksum da mensagem, que é incluso no pacote, para garantir a integridade dos dados. O receptor então recalcula o checksum para garantir que a mensagem não foi alterada.

Apenas o SSID, oferece uma proteção muito fraca. Mesmo que a opção broadcast SSID esteja desativada, já existem sniffers que podem descobrir rapidamente o SSID da rede monitorando o tráfego de dados. Eis que surge o WEP, abreviação de Wired-Equivalent Privacy, que como o nome sugere traz como promessa um nível de segurança equivalente à das redes cabeadas. Na prática o WEP também tem suas falhas, mas não deixa de ser uma camada de proteção essencial, muito mais difícil de penetrar que o SSID sozinho.

O WEP se encarrega de encriptar os dados transmitidos através da rede. Existem dois padrões WEP, de 64 e de 128 bits. O padrão de 64 bits é suportado por qualquer ponto de acesso ou interface que siga o padrão WI-FI, o que engloba todos os produtos comercializados atualmente. O padrão de 128 bits por sua vez não é suportado por todos os produtos. Para habilitá-lo será preciso que todos os componentes usados na sua rede suportem o padrão, caso contrário os nós que suportarem apenas o padrão de 64 bits ficarão fora da rede.

Na verdade, o WEP é composto de duas chaves distintas, de 40 e 24 bits no padrão de 64 bits e de 104 e 24 bits no padrão de 128. Por isso, a complexidade encriptação usada nos dois padrões não é a mesma que seria em padrões de 64 e 128 de verdade. Além do detalhe do número de bits nas chaves de encriptação, o WEP possui outras vulnerabilidades. Alguns programas já largamente disponíveis são capazes de quebrar as chaves de encriptação caso seja possível monitorar o tráfego da rede durante algumas horas e a tendência é que estas ferramentas se tornem ainda mais sofisticadas com o tempo. Como disse, o WEP não é perfeito, mas já garante um nível básico de proteção. Esta é uma chave que foi amplamente utilizada, e ainda é, mas que possui falhas conhecidas e facilmente exploradas por softwares como AirSnort ou WEPCrack. Em resumo o problema consiste na forma com que se trata a chave e como ela é "empacotada" ao ser agregada ao pacote de dados.

O WEP vem desativado na grande maioria dos pontos de acesso, mas pode ser facilmente ativado através do utilitário de configuração. O mais complicado é que você precisará definir manualmente uma chave de encriptação (um valor alfanumérico ou hexadecimal, dependendo do utilitário) que deverá ser a mesma em todos os pontos de acesso e estações da rede. Nas estações a chave, assim como o endereço ESSID e outras configurações de rede podem ser definidos através de outro utilitário, fornecido pelo fabricante da placa.

WPA, um WEP melhorado

Também chamado de WEP2, ou TKIP (Temporal Key Integrity Protocol), essa primeira versão do WPA (Wi-Fi Protected Access) surgiu de um esforço conjunto de membros da Wi-Fi Aliança e de membros do IEEE, empenhados em aumentar o nível de segurança das redes sem fio ainda no ano de 2003, combatendo algumas das vulnerabilidades do WEP.

A partir desse esforço, pretende-se colocar no mercado brevemente produtos que utilizam WPA, que apesar de não ser um padrão IEEE 802.11 ainda, é baseado neste padrão e tem algumas características que fazem dele uma ótima opção para quem precisa de segurança rapidamente: Pode-se utilizar WPA numa rede híbrida que tenha WEP instalado. Migrar para WPA requer somente atualização de software. WPA é desenhado para ser compatível com o próximo padrão IEEE 802.11i.

Vantagens do WPA sobre o WEP

Com a substituição do WEP pelo WPA, temos como vantagem melhorar a criptografia dos dados ao utilizar um protocolo de chave temporária (TKIP) que possibilita a criação de chaves por pacotes, além de possuir função detectora de erros chamada Michael, um vetor de inicialização de 48 bits, ao invés de 24 como no WEP e um mecanismo de distribuição de chaves.

Além disso, uma outra vantagem é a melhoria no processo de autenticação de usuários. Essa autenticação se utiliza do 802.11x e do EAP (Extensible Authentication Protocol), que através de um servidor de autenticação central faz a autenticação de cada usuário antes deste ter acesso a rede.

RADIUS

Este é um padrão de encriptação proprietário que utiliza chaves de encriptação de 128 bits reais, o que o torna muito mais seguro que o WEP. Infelizmente este padrão é suportado apenas por alguns produtos. Se estiver interessado nesta camada extra de proteção, você precisará pesquisar quais modelos suportam o padrão e selecionar suas placas e pontos de acesso dentro desse círculo restrito. Os componentes geralmente serão um pouco mais caro, já que você estará pagando também pela camada extra de encriptação.

Permissões de acesso

Além da encriptação você pode considerar implantar também um sistema de segurança baseado em permissões de acesso. O Windows 95/98/ME permite colocar senhas nos compartilhamentos, enquanto o Windows NT, 2000 Server, já permitem uma segurança mais refinada, baseada em permissões de acesso por endereço IP, por usuário, por grupo, etc. Usando estes recursos, mesmo que

alguém consiga penetrar na sua rede, ainda terá que quebrar a segurança do sistema operacional para conseguir chegar aos seus arquivos. Isso vale não apenas para redes sem fio, mas também para redes cabeadas, onde qualquer um que tenha acesso a um dos cabos ou a um PC conectado à rede é um invasor em potencial.
Alguns pontos de acesso oferecem a possibilidade de estabelecer uma lista com as placas que têm permissão para utilizar a rede e rejeitar qualquer tentativa de conexão de placas não autorizadas. O controle é feito através dos endereços MAC das placas, que precisam ser incluídos um a um na lista de permissões, através do utilitário do ponto de acesso. Muitos oferecem ainda a possibilidade de estabelecer senhas de acesso.

Somando o uso de todos os recursos acima, a rede sem fio pode tornar-se até mais segura do que uma rede cabeada, embora implantar tantas camadas de proteção torne a implantação da rede muito mais trabalhosa.

ACL (Access Control List)

Esta é uma prática herdada das redes cabeadas e dos administradores de redes que gostam de manter controle sobre que equipamentos acessam sua rede. O controle consiste em uma lista de endereços MAC (físico) dos adaptadores de rede que se deseja permitir a entrada na rede wireless. Seu uso é bem simples e apesar de técnicas de MAC Spoofing serem hoje bastante conhecidas é algo que agrega boa segurança e pode ser usado em conjunto com qualquer outro padrão, como WEP, WPA etc. A lista pode ficar no ponto de acesso ou em um PC ou equipamento de rede cabeada, e a cada novo cliente que tenta se conectar seu endereço MAC é validado e comparado aos valores da lista. Caso ele exista nesta lista, o acesso é liberado.

Para que o invasor possa se conectar e se fazer passar por um cliente válido ele precisa descobrir o MAC utilizado. Como disse, descobrir isso pode ser relativamente fácil para um hacker experiente que utilize um analisador de protocolo (Ethereal, por exemplo) e um software de mudança de MAC (MACShift por exemplo). De novo, para aplicações onde é possível agregar mais esta camada, vale a pena pensar e investir em sua implementação, já que o custo é praticamente zero. O endereço MAC, em geral, está impresso em uma etiqueta fixada a uma placa de rede ou na parte de baixo de um notebook. Para descobrir o endereço MAC do seu computador no Windows XP, abra uma caixa de comando (Iniciar/Todos os Programas/Acessórios/Prompt de Comando), digite `getmac` e pressione a tecla Enter. Faça isso para cada computador na rede e entre com a informação na lista do seu roteador.

Mantendo a sua rede sem fio segura

Na verdade essa lista de sugestões se aplica para todos os casos, sejam redes sem ou com fios.

1. Habilite o WEP. Como já vimos o WEP é frágil, mas ao mesmo tempo é uma barreira a mais no sistema de segurança.

2. Altere o SSID default dos produtos de rede. SSID é um identificador de grupos de redes. Para se juntar a uma rede, o novo dispositivo terá que conhecer previamente o número do SSID, que é configurado no ponto de acesso, para se juntar ao resto dos dispositivos. Mantendo esse valor default fica mais fácil para o invasor entrar na rede.

3. Não coloque o SSID como nome da empresa, de divisões ou departamentos.

4. Não coloque o SSI como nome de ruas ou logradouros.

5. Se o ponto de acesso suporta broadcast SSID, desabilite essa opção.

6. Troque a senha default dos pontos de acessos e dos roteadores. Essas senhas são de conhecimento de todos os hackers.

7. Tente colocar o ponto de acesso no centro da empresa. Diminui a área de abrangência do sinal para fora da empresa.

8. Como administrador você deve repetir esse teste periodicamente na sua empresa a procura de pontos de acessos novos que você não tenha sido informado.

9. Aponte o equipamento notebook com o Netstumbler para fora da empresa para procurar se tem alguém lendo os sinais que transitam na sua rede.

10. Muitos pontos de acessos permitem que você controle o acesso a ele baseado no endereço MAC dos dispositivos clientes. Crie uma tabela de endereços MAC que possam acessar aquele ponto de acesso. E mantenha essa tabela atualizada.

11. Utilize um nível extra de autenticação, como o RADIUS, por exemplo, antes de permitir uma associação de um dispositivo novo ao seu ponto de acesso. Muitas implementações já trazer esse nível de autenticação dentro do protocolo IEEE 802.11b.

12. Pense em criar uma subrede específica para os dispositivos móveis, e disponibilizar um servidor DHCP só para essa sub-rede.

13. Não compre pontos de acesso ou dispositivos móveis que só utilizem WEP com chave de tamanho 40 bits.

14. Somente compre pontos de acessos com memória flash. Há um grande número de pesquisas na área de segurança nesse momento e você vai querer fazer um upgrade de software no futuro.

Protocolos

Porquê a Necessidade de Padrões para uma LAN Sem Fios

Antes da adesão do protocolo 802.11, vendedores de redes de dados sem fios faziam equipamentos que eram baseados em tecnologia proprietária. Sabendo que iam ficar presos ao comprar do mesmo fabricante, os clientes potenciais de redes sem fios viraram para tecnologias mais viradas a protocolos.Em resultado disto, desenvolvimento de redes sem fios não existia em larga escala, e era considerado um luxo só estando ao alcance de grandes companhias com grandes orçamentos.O único caminho para redes LAN sem fios (WLAN - Wireless Local Area Network) ser geralmente aceite era se o hardware envolvido era de baixo custo e compatível com os restantes equipamentos.

Reconhecendo que o único caminho para isto acontecer era se existisse um protocolo de redes de dados sem fios. O grupo 802 do Instituto de Engenheiros da Eletrônica e Eletricidade (IEEE -Institute of Electrical and Electronics Engineers, uma associação sem fins lucrativos que reúne aproximadamente 380.000 membros, em 150 países. Composto de engenheiros das áreas de telecomunicações, computação, eletrônica e ciências aeroespaciais, entre outras, o IEEE definiu algo em torno de 900 padrões tecnológicos ativos e utilizados pela indústria, e conta com mais 700 em desenvolvimento), tomou o seu décimo primeiro desafio. Porque uma grande parte dos membros do grupo 802.11 era constituído de empregados dos fabricantes de tecnologias sem fios, existiam muitos empurrões para incluir certas funções na especificação final. Isto, no entanto atrasou o progresso da finalização do protocolo 802.11, mas também forneceu um protocolo rico em atributos ficando aberto para futuras expansões.No dia 26 de Junho em 1997, o IEEE anunciou a retificação do protocolo 802.11 para WLAN. Desde dessa altura, custo associado a desenvolvimento de uma rede baseada no protocolo 802.11 tem descido.

Desde o primeiro protocolo 802.11 ser aprovado em 1997, ainda houve várias tentativas em melhorar o protocolo.Na introdução dos protocolos, primeiro veio o 802.11, sendo seguido pelo 802.11b. A seguir veio 802.11a, que fornece até cinco vezes a capacidade de largura de banda do 802.11b. Agora com a grande procura de serviços de multimídia, vem o desenvolvimento do 802.11e. A seguir será explicado cada protocolo falando entre outros. Cada grupo, que segue tem como objetivo acelerar o protocolo 802.11, tornando-o globalmente acessível, não sendo necessário reinventar a camada física (MAC - Media Access Control) do 802.11.

 Mais Informações: www.ieee.org

802.11b

A camada física do 802.11b utiliza espalhamento espectral por seqüência direta (DSSS – Direct Sequence Spread Spectrum) que usa transmissão aberta (broadcast) de rádio e opera na freqüência de 2.4000 a 2.4835GHz no total de 14 canais com uma capacidade de transferência de 11 Mbps, em ambientes abertos (~ 450 metros) ou fechados (~ 50 metros). Esta taxa pode ser reduzida a 5.5 Mbps ou até menos, dependendo das condições do ambiente no qual as ondas estão se propagando (paredes, interferências, etc).

Dentro do conceito de WLAN (Wireless Local Area Network) temos o conhecido Wi-Fi. O Wi-Fi nada mais é do que um nome comercial para um padrão de rede wireless chamado de 802.11b, utilizado em aplicações indoor. Hoje em dia existem vários dispositivos a competir para o espaço aéreo no espectro de 2.4GHz. Infelizmente a maior parte que causam interferências são comuns em cada lar, como por exemplo, o microondas e os telefones sem fios. Uma das mais recentes aquisições do 802.11b é do novo protocolo Bluetooth, desenhado para transmissões de curtas distâncias. Os dispositivos Bluetooth utilizam espalhamento espectral por salto na freqüência (FHSS – Frequency Hopping Spread Spectrum) para comunicar entre eles.

A topologia das redes 802.11b é semelhante a das redes de par trançado, com um Hub central. A diferença no caso é que simplesmente não existem os fios e que o equipamento central é chamado Access Point cuja função não defere muito da hub: retransmitir os pacotes de dados, de forma que todos os micros da rede os recebam, existem tanto placas PC-Card, que podem ser utilizadas em notebooks e em alguns handhelds, e para placas de micros de mesa.

Exemplo de uma rede 802.11b

802.11g

Este é o irmão mais novo do 802.11b e que traz, de uma forma simples e direta, uma única diferença: Sua velocidade alcança 54 Mbits/s contra os 11 Mbits/s do 802.11b. Não vamos entrar na matemática da largura efetiva de banda dessas tecnologias, mas em resumo temos uma velocidade três ou quatro vezes maior num mesmo raio de alcance. A freqüência e número de canais são exatamente iguais aos do 802.11b, ou seja, 2.4GHz com 11 canais (3 non overlaping).

Não há muito que falar em termos de 802.11g senão que sua tecnologia mantém total compatibilidade com dispositivos 802.11b e que tudo o que é suportado hoje em segurança também pode ser aplicado a este padrão. Exemplificando, se temos um ponto de acesso 802.11g e temos dois laptops conectados a ele, sendo um 802.11b e outro 802.11g, a velocidade da rede será 11 Mbits/s obrigatoriamente. O ponto de acesso irá utilizar a menor velocidade como regra para manter a compatibilidade entre todos os dispositivos conectados.

No mais, o 802.11g traz com suporte nativo o padrão WPA de segurança, que também hoje já se encontra implementado em alguns produtos 802.11b, porém não sendo regra. O alcance e aplicações também são basicamente os mesmos do 802.11b e ele é claramente uma tecnologia que, aos poucos, irá substituir as implementações do 802.11b, já que mantém a compatibilidade e oferece maior velocidade. Esta migração já começou e não deve parar tão cedo. Hoje, o custo ainda é mais alto que o do 802.11b, porém esta curva deve se aproximar assim que o mercado começar a usá-lo em aplicações também industriais e robustas.

802.11a

Por causa da grande procura de mais largura de banda, e o número crescente de tecnologias a trabalhar na banda 2,4GHz, foi criado o 802.11a para WLAN a ser utilizado nos Estados Unidos. Este padrão utiliza a freqüência de 5GHz, onde a interferência não é problema. Graças à freqüência mais alta, o padrão também é quase cinco vezes mais rápido, atingindo respeitáveis 54 megabits.
Note que esta é a velocidade de transmissão nominal que inclui todos os sinais de modulação, cabeçalhos de pacotes, correção de erros, etc. a velocidade real das redes 802.11a é de 24 a 27 megabits por segundo, pouco mais de 4 vezes mais rápido que no 802.11b. Outra vantagem é que o 802.11a permite um total de 8 canais simultâneos, contra apenas 3 canais no 802.11b. Isso permite que mais pontos de acesso sejam utilizados no mesmo ambiente, sem que haja perda de desempenho.
O grande problema é que o padrão também é mais caro, por isso a primeira leva de produtos vai ser destinada ao mercado corporativo, onde existe mais dinheiro e mais necessidade de redes mais rápidas. Além disso, por utilizarem uma frequência mais alta, os transmissores 8021.11a também possuem um alcance mais curto, teoricamente metade do alcance dos transmissores 802.11b, o que torna necessário usar mais pontos de acesso para cobrir a mesma área, o que contribui para aumentar ainda mais os custos.

802.11e

O 802.11e do IEEE fornece melhoramentos ao protocolo 802.11, sendo também compatível com o 802.11b e o 802.11a. Os melhoramentos inclui capacidade multimídia feito possível com a adesão da funcionalidade de qualidade de serviços (QoS – Quality of Service), como também melhoramentos em aspectos de segurança. O que significa isto aos ISP's? Isto significa a habilidade de oferecer vídeo e áudio à ordem (on demand), serviços de acesso de alta velocidade a Internet e Voz sobre IP (VoIP – Voice over Internet Protocol). O que significa isto ao cliente final? Isto permite multimídia de alta-fidelidade na forma de vídeo no formato MPEG2, e som com a qualidade de CD, e a redefinição do tradicional uso do telefone utilizando VoIP. QoS é a chave da funcionalidade do 802.11e. Ele fornece a funcionalidade necessária para acomodar aplicações sensíveis a tempo com vídeo e áudio.

802.11f

Está a desenvolver Inter-Access Point Protocol (Protocolo de acesso entre pontos), por causa da corrente limitação de proibir roaming entre pontos de acesso de diferentes fabricantes. Este protocolo permitiria dispositivos sem fios passar por vários pontos de acesso feitos por diferentes fabricantes.
Grupo 802.11g – Estão a trabalhar em conseguir maiores taxas de transmissão na banda de rádio 2,4GHz.

Grupos do IEEE que estão desenvolvendo outros protocolos:

Grupo 802.11d – Está concentrado no desenvolvimento de equipamentos para definir 802.11 WLAN para funcionar em mercados não suportados pelo protocolo corrente (O corrente protocolo 802.11 só define operações WLAN em alguns países).

Grupo 802.11h – Está em desenvolvimento do espectro e gestão de extensões de potência para o 802.11a do IEEE para ser utilizado na Europa.

Como montar um provedor wireless desde a entrada Internet até o cliente

VISADA

Com esta solução duas redes distantes (ou computadores) podem ser conectadas sem ter que contratar uma empresa de telecomunicações ou ter que realizar obras externas. O transmissor pode ser conectado, dependendo do tipo, num HUB ou num Servidor GATEWAY Network Server. Uma vez estabelecida à conexão, o trafego IP, Netbeui ou IPX pode fluir em velocidade até 11Mbit/s ou maior.

A ENTRADA

O que já sabemos é que precisamos de um roteador para conectar o link principal. Muitos cometem aqui o primeiro erro. Este erro logo aparece de forma sutil. Um roteador de baixa qualidade causará inúmeros problemas que serão difíceis para descobrir e corrigir. Temos algumas marcas que parecem econômicas, mas a partir de certa quantidade de tráfego elas perdem pacotes. Outro problema destes roteadores é que eles parem de aceitar, especialmente na configuração de Frame-Relay, quando houve um reset na ponta remota. Ou seja, de repente para seu link e ninguém sabe porque. Isto sempre acontece no período noturno, quando as teles fazem manutenção e você descobre somente quando chegar à firma. Somando depois todos estes detalhes sugerimos, compre um CISCO, se pretende usar conexões de 512Kbit/s ou maior.

FIREWALL

- O guarda costas O Firewall na Internet é a sua garantia. Não é nem tanto ataques e invasões. Existe uma grande quantidade de tráfego desnecessário para o acesso Internet. Começamos com o tráfego ICMP. Podemos cortá-lo tranquilamente porque este não necessita de nada. Tráfego Broadcast, desnecessário. Tráfego de redes IP "inválidos. Também este tráfego vem muitas vezes de redes caseiras incorretamente configuradas e não de ataques. Tráfego "Microsoft" NETBIOS. E assim podemos juntar uma lista gigantesca. Só estes "pacotinhos" somam pelo menos 10% do seu LINK. Pegue 10% do dinheiro que você paga cada mês, com certeza adquire algumas legalidades. O Firewall pode rejeitar também, e isso é a tarefa principal, qualquer tipo de ataque e tentativa de invasão. Pois sem ele a sua rede talvez não para, mas pode ser congestionada ou até certos recursos como SMTP, DNS ou IMAP podem sofrer alguns problemas. Para não ter nenhuma preocupação com isto, precisa colocar um Firewall.

PROXY

- O Nitrogénio Muitos negam este fato ou desconhecem. Um Proxy preparado com

detalhe pode aumentar a velocidade de acesso de forma drástica. O Hitrate, a taxa de acertos, dos nossos proxies está em torno de 30-45%. Este valor em efetivo poupa em torno de 15-30% do seu link. E não é só isso. O Proxy protege ainda mais os seus clientes, ficam mais difíceis para hacker descobrir a origem e ter acesso direto ao PC do internauta. Conversas tais como "com Proxy não acessa bancos ou semelhantes" é pura conversa. Com Proxy acessa tudo, só mais rápido. Proxy e Firewall em conjunto Você faz a conta com base no seu custo de link. O valor que você gasta em Proxy e Firewall será pago sozinho em Três ou 4 meses. O certo também seria deixar o proxy junto com o Firewall em uma máquina adequada na ponta da sua rede. Esta máquina ficaria com duas ou mais placas de rede, uma para conectar com o roteador, outra para por exemplo a rede interna (LAN) ou com uma subrede com os servidores RAS e outra, que inclusive poderia ser uma placa wireless, para a rede de rádio.

N-SERVER

Wireless Apesar que falei que o servidor Proxy-firewall poderia ter uma placa Wireless, a melhor solução seria um servidor a parte para ser o gateway para a sua rede sem fio. Os motivos são simples. Controlando os dois segmentos separados é Melhor, qualquer manutenção e fica só uma parte afetada. O mesmo vale para problemas de hardware que obviamente podem ocorrer. Depende, porém de seu bolso e mais ainda do tamanho da sua rede. Talvez pode começar com 3 em UMA, mas assim que crecse você separa. Outro motivo seria a admintração da rede wireless. Como você sabe, as placas de rádio podem trafegar em até 11Mbit/s. Significa que um cliente só poderia complicar a sua vida ao menos que tenha um link de igual capacidade. Por isto precisa de uma ferramenta para limitar a banda vendida para o cliente. Noss N-Server ADM WL, por exemplo, permite que você limite a velocidade do cliente a 128Kbit/s e ele não puxa nenhum bit a mais. A Estação Central de Rádio Esta estação seria um Acesspoint com capacidade adequada para suportar o seu projeto de rede. Esta central fica ligada diretamente no N-Server ADM-WL ou através de cabo de rede (até 100m) ou através de um link de rádio também. A central atende depois seus clientes remotos e ela retransmite para o ADM-WL.

Etapas da Implantação Wireless – 4 passos

Primeiro Passo

O LINK Internet. Você pode adquirir o link internet de várias maneiras...

1.Adquirindo com a Telefônica, Embratel ou operadora de telecomunicação ativa na sua região, o custo é de aproximadamente R$ 3200,00 para cada 1Mbps de velocidade, são links robustos que garantem qualidade e velocidade de banda, por esta razão, possui um valor mais elevado.

2. Através de um ADSL ou CableModem (Speedy ou EasyBand por exemplo). Neste caso você fica com um link "menos robusto" que não tem garantia de banda, repassando um serviço menos profissional para seu cliente, porém, o valor é bem mais acessível, uns R$ 800,00 para cada 2Mbps. Lembre-se, se você optar por este tipo de serviço não poderá oferecer venda de IPs válidos, ou seja, para empresas ou corporações que necessitam de servidores com IP´s válidos na Internet para hospedagem de sites, VPN ou banco de dados por exemplo.

3. Adquirindo de um provedor de internet que já possui um link grande, mas neste caso, você deve ter uma pessoa de extrema confiança, na maioria dos casos o provedor cobra um valor menor que o das teles, não "agüenta o tranco" e diminui sua velocidade sem que você perceba, atingindo seu cliente diretamente e desqualificando seu negócio.
Minha opinião: Adquirir um link com uma operadora de telecomunicações de grande porte, apesar do custo maior o serviço será de qualidade e com seriedade.

Segundo Passo - Montando o Projeto

1. Visada

Verifique se os pontos onde você irá atender os clientes possui visada direta, ou seja, pontos visíveis e diretos para todos os pontos remotos. Um bom LOCAL sugerido é um prédio grande ou uma torre vistosa. Um prédio seria até melhor, os condonimos poderiam acessar internet através de cabos LAN que são baratos e você ganha na assinatura dos apartamentos.

2. Calculo do número máximo de clientes

Assegure-se da média de clientes atendidos na região, um bom número de clientes para cada Access Point (SWL3300 ou AP200 por exemplo) é de NO máximo 35 clientes Wlan, ou seja, kits PCI ou Ethernet Converters, anexos à ela. Depois deste número o equipamento começa a ficar lento, começa a perder pacotes, ficando quase impossível trabalhar com níveis de segurança e qualidade. Quando isso acontece você tem que optar pela implementação de novos equipamentos ou novos pontos de distribuição.

3. Número de repetidoras

Para cada repetidora você precisa de vários novos equipamentos, tenha sempre em mente prédios ou torres próximas uma à outra para poder montar novos pontos de distribuição.Para cada novo ponto você precisa de 2 rádios somente para o link (enviar o sinal de um ponto ao outro) mais um equipamento para distribuir o sinal em modo Access Point.

4. Antenas

Procure utilizar antenas direcionais de ganhos menores e de boa qualidade, são antenas mais caras porém asseguram uma grande redução NO problema de interferências e ruídos. O mesmo se aplica aos amplificadores de potência, somente utilize quando não FOR possível realmente o enlace, caso contrário, quanto menos amplificação melhor !

Terceiro passo

– Homologação 5. Produtos Homologados Devido AS novas normas da Anatel, você precisa utilizar produtos registrados e homologados. Somente são aceitos novos provedores com projetos de infra-estrutura e licença de funcionamento SCM. para que isso seja possível a Anatel exige a certificação do fabricante e um projeto assinado por um engenheiro de redes ou elétrico. 6. Provedor de Acesso para Prédios Se você tem a finalidade de atender somente prédios, convém centralizar o provedor em locais onde existem vários condomínios, certifique-se de que o LOCAL onde está sendo instalado não exista concorrência, nunca utilize duas antenas omni NO mesmo LOCAL, com certeza você encontrará problemas de interferência. O modo de interligação entre prédios deve ser realizado com protocolos de comunicação especiais desenvolvidos para redes externas, como o MultiLink da Samsung, TurboCell da Karlnet ou Worp da Proxim, são protocolos específicos para conexão outdoor e garantem melhor desempenho e robustez NO link entre os pontos de conexão diminuindo problemas com interferências e

aumentando o nível de Throughput. 7. Provedor de Acesso para Residências Quando o seu cliente é um "Access Point Client" isso significa que você estará trabalhando com o equipamento em modo 802.11b OPEN Share (Kits PCI por exemplo). Neste modo de operação AS distâncias são limitadas entre 4 a 5Km NO máximo, com isso, você deve escolher um LOCAL onde a abrangência de clientes é bastante grande para garantir o uso total do equipamento. 8. Provedor Misto Se você vai trabalhar com clientes residenciais e condomínios ao mesmo tempo, deve utilizar um equipamento para cada finalidade. Uma central fará o trabalho de Access Point enquanto outra fará MultiLink para os prédios. Desta forma você evita o comprometimento do link com os clientes evitando saturação da banda para determinados locais.

Quarto Passo

- Custos Se você oferece aos clientes 256Kbps compartilhado, significa que cada estação chave (cliente central) irá receber 256Kbps 24h por dia 7 dias por semana. Com isso você deverá se atentar ao consumo de banda em excesso pois o seu lucro vem da utilização do link ou não. Um cliente empresarial consome maior quantidade de banda que um residencial, por isso o valor da mensalidade deste deve ser maior que um usuário residencial. Em contra-partida este cliente exige maior seriedade NO link sendo que o mesmo deve possuir menor nível de problemas que um usuário residencial. Em geral a média é de 10 para 1, ou seja, para cada 256Kbps reais você poderá pendurar até dez clientes com a mesma velocidade. Com o tempo a optimização do consumo é medida e adequada para cada caso. Então se 1Mbps tem 4 X 256Kbps você pode colocar até 40 clientes em cada Mb Não. Em cada caso devemos analisar o consumo da banda, sendo que, a optimização do sistema é fundamental, se você tem clientes residenciais e empresariais, por exemplo, deve saber que o consumo da residência é na maioria dos casos noturno ao passo que o de uma empresa é diurno. Cada caso deve ser estudado cautelosamente. Cuidado! Esta é a jogada para se ganhar ou não dinheiro com o negócio. Neste período você sabe se irá crescer ou afundar, o segredo é não ter pressa para vender e fazer vendas bem feitas, todos querem ganhar dinheiro, certo

Resumindo, você precisa de um roteador, dois servidores, as máquinas suas para atendimento etc, e uma central de rádio. Este conjunto corretamente configurado atende perfeitamente as necessidades de seus clientes e especialmente as suas, falando em termo de baixa ou zero manutenção, segurança e capacidade.

Ponto de Acesso (Access Point)

Um número limite de estações que podem ser conectadas a cada ponto de acesso depende do equipamento utilizado, mas, assim como nas redes Ethernet, a velocidade da rede cai conforme aumenta o número de estações, já que apenas uma pode transmitir de cada vez. A maior arma do 802.11b contra as redes cabeadas é a versatilidade. O simples fato de poder interligar os PCs sem precisar passar cabos pelas paredes já é o suficiente para convencer algumas pessoas, mas existem mais alguns recursos interessantes que podem ser explorados.
Sem dúvidas, a possibilidade mais interessante é a mobilidade para os portáteis. Tanto os notebooks quanto handhelds e as futuras webpads podem ser movidos livremente dentro da área coberta pelos pontos de acesso sem que seja perdido o acesso à rede. Esta possibilidade lhe dará alguma mobilidade dentro de casa para levar o notebook para onde quiser, sem perder o acesso à Web, mas é ainda mais

interessante para empresas e escolas. No caso das empresas a rede permitiria que os funcionários pudessem se deslocar pela empresa sem perder a conectividade com a rede e bastaria entrar pela porta para que o notebook automaticamente se conectasse à rede e sincronizasse os dados necessários. No caso das escolas a principal utilidade seria fornecer acesso à Web aos alunos. Esta já é uma realidade em algumas universidades e pode tornar-se algo muito comum dentro dos próximos anos.
A velocidade das redes 802.11b é de 11 megabits, comparável à das redes Ethernet de 10 megabits, mas muito atrás da velocidade das redes de 100 megabits. Estes 11 megabits não são adequados para redes com um tráfego muito pesado, mas são mais do que suficientes para compartilhar o acesso à web, trocar pequenos arquivos, jogar games multiplayer, etc. Note que os 11 megabits são a taxa bruta de transmissão de dados, que incluem modulação, códigos de correção de erro, retransmissões de pacotes, etc., como em outras arquiteturas de rede. A velocidade real de conexão fica em torno de 6 megabits, o suficiente para transmitir arquivos a 750 KB/s, uma velocidade real semelhante à das redes Ethernet de 10 megabits.

Mas, existe a possibilidade de combinar o melhor das duas tecnologias, conectando um ponto de acesso 802.11b a uma rede Ethernet já existente. No ponto de acesso da figura abaixo você pode notar que existem portas RJ-45 da tecnologia Ethernet que trabalham a 100Mbps, veja figura:

Isto adiciona uma grande versatilidade à rede e permite diminuir os custos. Você pode interligar os PCs através de cabos de par trançado e placas Ethernet que são baratos e usar as placas 802.11b apenas nos notebooks e aparelhos onde for necessário ter mobilidade. Não existe mistério aqui, basta conectar o ponto de acesso ao Hub usando um cabo de par trançado comum para interligar as duas redes. O próprio Hub 802.11b passará a trabalhar como um switch, gerenciando o tráfego entre as duas redes.
O alcance do sinal varia entre 15 e 100 metros, dependendo da quantidade de obstáculos entre o ponto de acesso e cada uma das placas. Paredes, portas e até mesmo pessoas atrapalham a propagação do sinal. Numa construção com muitas paredes, ou paredes muito grossas, o alcance pode se aproximar dos 15 metros mínimos, enquanto num ambiente aberto, como o pátio de uma escola o alcance vai se aproximar dos 100 metros máximos.

Você pode utilizar o utilitário que acompanha a placa de rede para verificar a qualidade do sinal em cada parte do ambiente onde a rede deverá estar disponível ou então utilizar o Windows XP que mostra nas propriedades da conexão o nível do sinal e a velocidade da conexão veja figura:

A potência do sinal decai conforme aumenta a distância, enquanto a qualidade decai pela combinação do aumento da distância e dos obstáculos pelo caminho. É por isso que num campo aberto o alcance será muito maior do que dentro de um prédio, por exemplo. Conforme a potência e qualidade do sinal se degrada, o ponto de acesso pode diminuir a velocidade de transmissão a fim de melhorar a confiabilidade da transmissão. A velocidade pode cair para 5.5 megabits, 2 megabits ou chegar a apenas 1 megabit por segundo antes do sinal se perder completamente. Algumas placas e pontos de acesso são capazes de negociar velocidades ainda mais baixas, possibilitando a conexão a distâncias ainda maiores. Nestes casos extremos o acesso à rede pode se parecer mais com uma conexão via modem do que via rede local.

O alcance de 15 a 100 metros do 802.11b é mais do que suficiente para uma loja, escritório ou restaurante. No caso de locais maiores, bastaria combinar vários pontos de acesso para cobrir toda a área. Estes pontos podem ser configurados para automaticamente dar acesso a todos os aparelhos dentro da área de cobertura. Neste caso não haveria maiores preocupações quanto à segurança, já que estará sendo compartilhado apenas acesso a web.

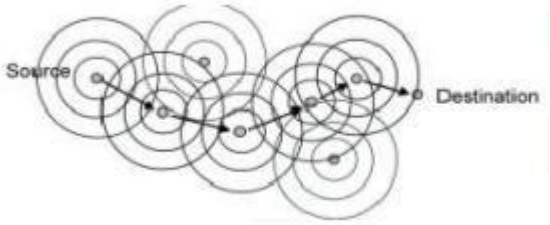
Redes Ad-Hoc

O termo "ad hoc" é geralmente entendido como algo que é criado ou usado para um problema específico ou imediato. Do Latin, ad hoc, significa literalmente "para isto", um outro significado seria: "apenas para este propósito", e dessa forma, temporário. Contudo, "ad hoc" em termos de "redes ad hoc sem fio" significa mais que isso. Geralmente, numa rede ad hoc não há topologia predeterminada, e nem controle centralizado. Redes ad hoc não requerem uma infra-estrutura tal como backbone, ou pontos de acesso configurados antecipadamente. Os nós ou nodos numa rede ad hoc se comunicam sem conexão física entre eles criando uma rede "on the fly", na qual alguns dos dispositivos da rede fazem parte da rede de fato apenas durante a duração da sessão de comunicação, ou, no caso de dispositivos móveis ou portáteis, por enquanto que estão a uma certa proximidade do restante da rede.

Assim como é possível ligar dois micros diretamente usando duas placas Ethernet e um cabo cross-over, sem usar hub, também é possível criar uma rede Wireless entre dois PCs sem usar um ponto de acesso. Basta configurar ambas as placas

para operar em modo Ad-hoc (através do utilitário de configuração). A velocidade de transmissão é a mesma, mas o alcance do sinal é bem menor, já que os transmissores e antenas das interfaces não possuem a mesma potência do ponto de acesso.
Este modo pode servir para pequenas redes domésticas, com dois PCs próximos, embora mesmo neste caso seja mais recomendável utilizar um ponto de acesso, interligado ao primeiro PC através de uma placa Ethernet e usar uma placa wireless no segundo PC ou notebook, já que a diferenças entre o custo das placas e pontos de acesso não é muito grande.

Outras características incluem um modo de operação ponto a ponto distribuído, roteamento multi-hop, e mudanças relativamente freqüentes na concentração dos nós da rede. A responsabilidade por organizar e controlar a rede é distribuída entre os próprios terminais. Em redes ad hoc, alguns pares de terminais não são capazes de se comunicar diretamente entre si, então alguma forma de re-transmissão de mensagens é necessária, para que assim estes pacotes sejam entregues ao seu destino. Com base nessas características.



Rede Wireless Doméstica

Aprenda como montar uma WLAN e dividir a sua banda larga entre vários micros

Nada de quebradeira, nem de fios passando de um lado para outro da casa. Uma maneira pratica de compartilhar o acesso em banda larga entre vários micros é montar uma rede sem fio. Os procedimentos não são complicados, mas há muitas variáveis que podem interferir no funcionamento de uma solução como essa. Alem disso nas redes Wireless é preciso redobrar a atenção com os procedimentos de segurança. Neste nosso exemplo vamos montar uma rede com 3 micros, que vão compartilhar uma mesma conexão com a Internet e uma impressora, além de trocar arquivos entre si.

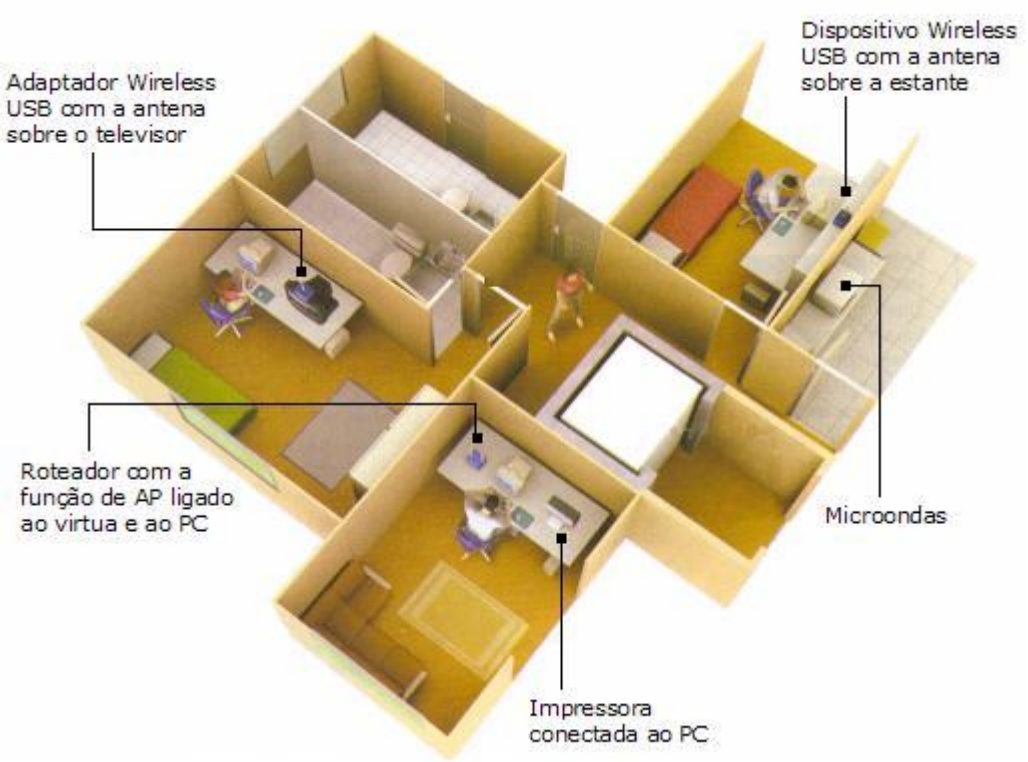
Vamos utilizar o roteador BEFW11S4, da Linksys, que vai funcionar como ponto de acesso. O equipamento tem 4 portas Ethernet e uma up-link para Internet a cabo ou DSL e suporte para conexão de até 32 dispositivos sem fio. Como ele usa a tecnologia 802.11b, o alcance nominal é de 100 metros, mas o valor real é bem menor uma vez que paredes e interferências acabam por diminuir esse alcance. A velocidade nominal é de 11Mbps.

Para o nosso exemplo de rede domestica sem fio que será demonstrado utilizaremos 3 micros com Windows XP, nas maquinas clientes utilizamos dois dispositivos Wireless USB WUSB11, também da Linksys. Uma impressora ligada a um dos micros foi compartilhada com os demais. A conexão de banda larga empregada é o virtua, de 256Kbps, com endereço IP dinâmico.

Vamos começar a montar a rede pelo computador que tem, hoje, a conexão de banda larga. Primeiro, conecte o cabo de par trançado que sai do modem do virtua à porta WAN do roteador, que esta na parte de trás do equipamento. Ligue a ponta de um segundo cabo de rede a placa Ethernet do computador e outra ponta em qualquer uma das 4 portas LAN do roteador. Conecte o cabo de força ao roteador, e ligue-o na tomada. Uma dica importante que varia de acordo com o provedor de link utilizado: no nosso exemplo o virtua mantém o numero do MAC Address da placa de rede na memória do modem. Por isso, deixe o modem desligado por 15 minutos antes de continuar os passos do tutorial. Passando esse período, ligue novamente o modem e veja se o acesso esta funcionando normalmente.

Agora que você já acessa a Internet, é hora de conectar e configurar as outras estações da rede Wireless. O adaptador da Linksys usado no nosso exemplo vem com um cabo de extensão USB que permite colocá-lo numa posição mais alta para melhorar a performance da rede. Conecte o cabo ao adaptador, e o adaptador a uma porta USB livre do micro. Mantenha a antena na posição vertical e no local mais alto possível. Agora vamos instalar o driver do adaptador. Ligue o computador e rode o CD que acompanha a placa. O Windows XP vai reconhecer que um novo dispositivo foi conectado. A janela "Encontrado Novo hardware'' será aberta. Selecione a opção "instale o software Automaticamente''. Clique no botão Avançar. Uma janela informando que o driver encontrado não passou no teste de logotipo do Windows é mostrada. Clique em OK e vá adiante com a instalação. No final, vai aparecer a janela Concluindo o Assistente. Clique no botão concluir.

Depois, um ícone de rede aparece na bandeja do sistema, no canto inferior direito da tela. Clique duas vezes nesse ícone. A janela permitir que eu conecte a Rede sem fio Selecionada Mesmo que Insegura é mostrada. Clique no botão Conectar. Abra o Internet Explorer para ver se você esta navegando na web.



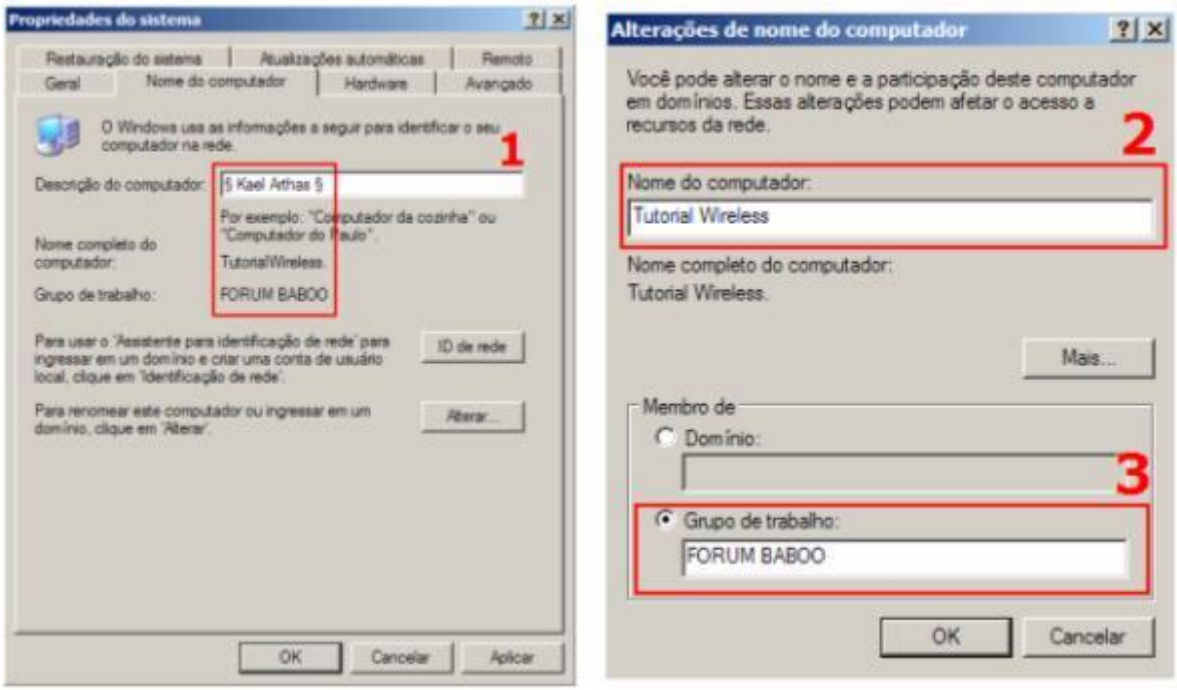
Deixar a rede nas configurações padrão do fabricante é fazer um convite aos crackers para invadi-la. Pos isso é fundamental que se ajuste as configurações do roteador e de todos os adaptadores. Agora vamos ajustar as configurações do roteador e das placas para ter mais segurança. Abra o Internet Explorer e digite, no campo Endereço, http://192.168.1.1/. Uma janela para digitação da senha é mostrada. Deixe o nome do usuário em branco, escreva a palavra admin no campo Senha e clique em OK. As configurações do roteador aparecem no navegador. Clique na aba Adminstration. Digite uma nova senha para o roteador no campo Router Password e redigite-a em Re-enter to Confirm. Clique no botão Save Settings. Outro movimento importante é trocar o nome-padrão da rede. Vá à aba Wireless, no submenu Basic Wireless Name (SSID), digitando um novo nome. Clique em Save Settings.

Agora, vamos ativar a criptografia usando o protocolo WEP. O objetivo é impedir que alguém intercepte a comunicação. Primeiro, na aba Wireless, clique na opção Wireless Security e selecione Enable. Depois, no campo Security Mode, selecione WEP e, em Wireless Encription Level, 128 bits, coloque uma frase com até 16 caracteres no campo Passphrase e clique no botão Generate. No campo Key, aparecerá a chave criptográfica, com 26 dígitos hexadecimais. Copie a chave num papel e clique no botão Save Settings. A janela Close This Window é mostrada. Clique em Apply. Agora, precisamos colocar a chave criptográfica nos micros. No nosso caso, trabalhamos com o Firmware 3.0 nas interfaces Wireless. Na estação cliente, dê dois cliques no ícone da rede sem fio na bandeja do sistema. Clique no botão propriedades e na aba redes sem fio, clique no nome da rede e no botão configurar. Na janela de configuração, digite a chave criptográfica. Repita-a no campo Redigitar. Vá até a aba Autenticação e deixe a opção usar 802.1x desmarcada. Clique agora no botão Conectar e você já deverá ter acesso a Internet.

Para conseguir uma segurança adicional, vamos permitir que apenas dispositivos cadastrados no roteador tenham acesso a ele. Isso é feito por meio do MAC Address, código com 12 dígitos hexadecimais que identifica cada dispositivo na rede. Para configurar a filtragem, abra, no navegador a tela de gerenciamento do roteador. No menu no alto da janela, clique em Wireless/Wireless Network Access. Selecione a opção Restrict Access. Clique, então no botão Wireless Client MAC List. Será apresentada uma tabela com os dispositivos conectados. Na coluna Enable MAC Filter, assinale os equipamentos que deverão ter permissão de acesso. No caso do nosso exemplo deveríamos marcar os dois PCs ligados via Wireless. Clique em Save e, em seguida, em Save Settings.

Se caso você possuir o Norton Internet Security 2004 instalado veja como configurá-lo, pois na configuração padrão, o firewall do NIS impede que um micro tenha acesso aos recursos dos demais. Vamos alterar isso para possibilitar o compartilhamento de arquivos e impressoras. Abra o NIS, clique em Firewall Pessoal e, em seguida, no botão Configurar. Clique na aba Rede Domestica e, no quadro abaixo, na aba confiável. O NIS mostra uma lista de maquinas com permissão para acesso. A lista deverá estar vazia. Vamos incluir os endereços da rede local nela. Assinale a opção Usando um Intervalo. O roteador atribui aos computadores, em sua configuração padrão, endereços IP começando em 192.168.0.100. Esse IP é associado ao primeiro PC. O Segundo vai ser 192.168.0.101 e assim por diante. Como no nosso exemplo temos três micros na rede, preenchemos os campo exibidos pelo NIS com o endereço inicial 192.168.0.100 e o final 192.168.0.102. Note que, usando o utilitário de gerenciamento do roteador é possível alterar os endereços IP dos micros. Se você fizer isso, deverá reconfigurar o firewall.

Vamos criar uma pasta de acesso compartilhado em cada micro. Arquivos colocados neles ficaram disponíveis para os demais. Isso é feito por meio do protocolo NetBIOS. Para começar vamos criar uma identificação para o micro. Clique com o botão direito no ícone meu computador e escolha propriedades. Na aba nome do computador digite uma descrição do PC (1). Clique no botão alterar. Na janela que se abre, digite um nome para identificar o micro na rede (2). No campo grupo de trabalho, coloque um nome para a rede local (3).



Esse nome do NetBIOS não tem relação com o SSID do Wireless. Por razoes de segurança, evite o nome Microsoft HOME, que é o padrão do Windows XP. Vá clicando em OK para fechar as janelas. Repita esse procedimento nos demais micros, tendo o cuidado de digitar o mesmo nome do grupo de trabalho neles. Embora seja possível compartilhar qualquer pasta, uma boa escolha é a documentos compartilhados. Para achá-la, abra a pasta Meus Documentos e, na coluna da esquerda, clique em Documentos Compartilhados e, depois, em compartilhar esta pasta. Assinale a opção Compartilhar esta Pasta na Rede e dê um nome para identificar a pasta. Se o Windows emitir um aviso dizendo que o compartilhamento esta desabilitado por razões de segurança, escolha a opção de compartilhar a pasta sem executar o assistente de configuração e confirme-a na caixa de dialogo seguinte. Para ter acesso a pasta num outro micro, abra a janela Meus locais de Rede.

Hotspot

Veja como fazer um diferencial no seu negocio

Uma rede sem fio pode ter dupla função em pequenos negócios como bares, Cafés, livrarias, ou qualquer outro local aberto ao público. Pode servir para os funcionários do negocio terem acesso a sistemas de automação comercial e para clientes navegarem na Internet, num esquema de hotspot (as redes sem fio públicas), montar um hotspot pode ser uma boa idéia para atrair mais clientes, E o acesso em Wireless acaba criando um diferencial em relação aos concorrentes. No Brasil, elas já habitam locais como aeroportos, hotéis e restaurantes em varias cidades. O movimento mais forte começou nos aeroportos.

Além da placa de rede Wireless, o navegante sem fio vai precisar de um provedor de acesso especifico, o uso de um provedor acaba resolvendo um grande problema: a tremenda mão-de-obra para achar a freqüência certa e acertar a configuração da rede. Cada hotspot funciona exatamente como uma WLAN (Wireless Local Area

Network, ou rede local sem fio) e técnicamente usa uma freqüência que deve estar configurada para não gerar interferência em outros sistemas. Para quem tem um provedor de acesso, esse caminho é tranqüilo: é preciso apenas selecionar o local e acertar as especificações sem dores de cabeça.

Um ponto de preocupação para usuários de rede sem fio é a questão da segurança. Na área da proteção digital, alguns especialistas afirmam que o meio de acesso hoje é seguro. Mas, como se sabe, não existe solução 100% segura em computação, e as limitações de segurança Wireless são largamente manjadas. A assinatura de um provedor de acesso teoricamente poderia aumentar a segurança, uma vez que os clientes recebem uma senha e passam por um processo de autenticação antes de entrar na rede. O maior problema está mesmo na segurança física, uma vez que o numero de roubos de PDAs e de notebooks tem crescido. A principal empresa de infra-estrutura de hotspot no Brasil é a Vex, temos como outros provedores o WiFiG do iG e o Velox Wi-Fi da Oi/Telemar.

Como Montar um Hotspot?

Se você já possui um computador com banda larga, o único investimento que vai ter de fazer para montar uma solução como essa é a compra de um Ponto de acesso com função de roteador, no nosso exemplo será utilizado um AP (Access Point, ou Ponto de Acesso) no padrão 802.11b, no computador estará rodando o Windows 2000, onde ficaram os aplicativos comerciais. O mecanismo de autenticação do Windows 2000 impedi que os clientes do hotspot tenham acesso a esses aplicativos. Cada visitante da rede, por sua vez, precisará de uma placa Wireless para notebook ou handheld. Dois notebooks com Windows XP e um palmtop com Pocket PC serão conectados à rede para serem usados pelos funcionários da empresa, para que tenham toda a mobilidade na hora de entrar com os dados ou de consultá-los.

Na teoria como já foi demonstrado, o alcance nominal da tecnologia 802.11b é de até 100 metros de distância do AP para os clientes. Mas na pratica a historia é

diferente, em um ambiente como o do nosso exemplo com divisórias, a distancia máxima deve chegar a 50 metros, alertando que Wireless não é uma ciência exata e como cada caso é um caso, possa ser que este valor se tornar maior ou menor, então uma dica importante antes de começar é colocar o roteador no ponto mais alto que você conseguir, pois quanto mais alto, melhor o alcance do sinal.

A instalação não é complicada, mas é preciso considerar as diversas variáveis que interferem na montagem de uma rede Wireless. Fora algumas trocas de cabos, o processo consiste basicamente em configuração de software. Pode-se montar uma rede Wireless de duas formas: deixando o acesso aberto para qualquer pessoa ou mantendo-o exclusivo para quem é autorizado. No caso do hotspot, a primeira alternativa é a que faz mais sentido.

Vamos a instalação, Com o micro ligado à Internet, rode o CD de instalação do roteador. Escolha Run the setup Wizard e, em seguida, Configure Your Router. Clique em Next. A partir daí, o roteador vai ler o endereço de hardware da placa de rede instalada no servidor e usada para o acesso a Internet, o chamado MAC address. Aguarde até que 100% da captura esteja completa.

O próximo passo é selecionar o tipo de modem (cable modem ou ADSL). No nosso caso marcamos cable modem. Feito isso, retire do micro o cabo de rede usado para acesso à Internet e ligue-o à entrada WAN do roteador (1). Depois, use o cabo de rede que vem com o equipamento para conectar qualquer uma das quatro portas do roteador à placa de rede do servidor (2). Clique em Next.

Ligue o roteador na tomada. Escolha uma senha de administrador e dê um nome de identificação para a rede (o SSID, ou Service Set Identifier). Fuja dos nomes óbvios por segurança. Selecione um canal de 1 a 11. Se houver uma rede Wireless operando num dos canais, evite-o.

A próxima tela é o DHCP setup. Nela, aparecera o endereço de hardware da placa de rede. É preciso colocar o Host Name e um domínio. Utilize qualquer nome como Host e não registre o domínio. Clique em Next e pronto. Você já pode testar se seu hotspot está funcionando. Como nossa rede, que abriga um hotspot, deverá ter acesso publico, mantenha a criptografia desabilitada no item WEP (Wired Equivalent Privacy).

Vamos conectar o primeiro notebook da empresa ao hotspot. A primeira coisa a fazer é instalar o cartão. Para começar insira o CD-ROM que acompanha o dispositivo no driver do notebook. Na tela que aparece, escolha a opção de instalar o software de controle. Terminada a instalação, mantenha o CD-ROM no driver e encaixe o cartão Wireless num conector PCMCIA do notebook. O Windows XP detecta o novo dispositivo e inicia o Assistente para instalação de novo hardware. Vá clicando em avançar até concluir a instalação do driver. Instalado o cartão podemos prosseguir com a configuração do notebook, abra a janela Meu Computador. Na coluna da esquerda, clique em meus locais de Rede. Em seguida, na mesma coluna, acione o link Exibir conexões de rede.

Clique com o botão direito no ícone correspondente a conexão de rede sem fio e escolha propriedades. Na aba redes sem fio, desmarque a opção Usar o Windows para definir configurações da rede sem fio. Fazendo isso, estamos passando o controle do acesso a rede sem fio para o software do roteador. Clique em OK para fechar a janela.

O Segundo notebook que conectamos à nossa rede é baseado no chip set Centrino, da Intel, que já possui uma interface para redes Wireless. Por isso, não é necessário instalar nenhum dispositivo adicional. Quando ligamos o notebook, o utilitário de gerenciamento da Intel é ativado. Se isso não acontecer automaticamente, procure, no canto inferior direito da tela, o ícone do programa Intel Pro/Wireless Lan e dê um duplo clique no botão Conectar. O programa inicia um assistente que tem somente dois passos. No primeiro, digite um nome qualquer para o perfil da conexão e clique em Avançar. No passo 2, apenas clique em Concluir. Depois disso, o notebook já deve ser capaz de navegar na web.

As Sete Armadilhas das redes Wireless

Veja as principais barreiras que podem afetar a propagação do sinal Wireless

- Antenas Baixas

Um dos mantras repetidos à exaustão pelos manuais de pontos de acesso se refere a localização do equipamento. Quanto mais altas as antenas estiverem posicionadas, menos barreiras o sinal encontrará no caminho até os computadores. Trinta centímetros podem fazer enorme diferença.

- Telefones sem fio

Nas casas e nos escritórios, a maioria dos telefones sem fio operam na freqüência de 900Mhz. Mas há modelos que já trabalham na de 2.4GHz, justamente a mesma usada pelos equipamentos 802.11b e 802.11g. Em ambientes com esse tipo de telefone, ou próximos a áreas com eles, a qualidade do sinal Wireless pode ser afetada. Mas isso não acontece necessariamente em todos os casos.

- Concreto e Trepadeira

Eis uma combinação explosiva para a rede Wireless. Se o concreto e as plantas mais vistosas já costumam prejudicar a propagação das ondas quando estão sozinhos, imagine o efeito somado. Pode ser um verdadeiro firewall...

- Microondas

A lógica é a mesma dos aparelhos de telefone sem fio. Os microondas também usam a disputada freqüência livre de 2,4GHz. Por isso, o ideal é que fiquem isolados do ambiente onde está a rede. Dependendo do caso, as interferências podem afetar apenas os usuários mais próximos ou toda a rede.

- Micro no Chão

O principio das antenas dos pontos de acesso que quanto mais alta melhor, também vale para as placas e os adaptadores colocados nos micros. Se o seu desktop é do tipo torre e fica no chão e o seu dispositivo não vier acompanhado de um fio longo, é recomendável usar um cabo de extensão USB para colocar a antena numa posição mais favorável.

- Água

Grandes recipientes com água, como aquários e bebedouros, são inimigos da boa propagação do sinal de Wireless. Evite que esse tipo de material possa virar uma barreira no caminho entre o ponto de acesso é as maquinas da rede.

- Vidros e Árvores

O vidro é outro material que pode influenciar negativamente na qualidade do sinal. Na ligação entre dois prédios por wireless, eles se somam a árvores altas, o que compromete a transmissão do sinal de uma antena para outra.

Equipamentos

Veja alguns equipamentos com suas principais especificações

DI-614+ AirPlus 2.4GHz Wireless Router (D-Link)

Standards

- IEEE 802.11b (Wireless)

  IEEE 802.3 (10BaseT)
- IEEE 802.3u (100BaseTX)

Wireless Data RatesWith Automatic Fallbacks

- 22Mbps
- 11Mbps
- 5.5Mbps
- 2Mbps
- 1Mbps

Encryption

64/128/256-bit

Wireless Frequency Range

2.4GHz to 2.462GHz

Wireless Modulation Technology

- PBCC - Packet Binary Convolutional Coding
- Direct Sequence Spread Spectrum (DSSS)
- 11-chip Barker sequence

Wireless Operating Range

- Indoors:
  Up to 100 meters (328 feet)
- Outdoors:
  Up to 400 meters (1,312 feet)

Wireless Transmit Power15dBm ± 2dBDimensions

- L = 190.5mm (7.5 inches)
- W = 116.84mm (4.6 inches)
- H = 35mm (1.375 inches)

DWL-900AP+ AirPlus 2.4GHz Wireless Access Point (D-Link)

Standards

- IEEE 802.11
- IEEE 802.11b
- IEEE 802.3
- IEEE 802.3u

Wireless Data Rates

With Automatic Fallbacks

- 22Mbps
- 11Mbps
- 5.5Mbps
- 2Mbps
- 1Mbps

Port

10/100 Mbps Fast Ethernet

Encryption

64-, 128-, 256-bit RC4

Wireless Frequency Range

2.4GHz to 2.462GHz

Wireless Modulation Technology

- PBCC - Packet Binary Convolutional Coding
- Direct Sequence Spread Spectrum (DSSS)
- 11-chip Barker sequence

Wireless Operating Range

- Indoors:
  Up to 100 meters (328 feet)
- Outdoors:
  Up to 400 meters (1,312 feet)

Wireless Transmit Power

15dBm ± 2dB

Dimensions

- L = 142mm (5.6 inches)
- W = 109mm (4.3 inches)
- H = 31mm (1.2 inches)

BEFW11S4 v2, 3, 3.2 Wireless Router (Linksys)

Standards

- IEEE 802.11b (Wireless)
- IEEE 802.3 (10BaseT)
- IEEE 802.3u (100BaseTX)

Wireless Data Rates

With Automatic Fallbacks

- 11Mbps
- 5.5Mbps
- 2Mbps
- 1Mbps

Encryption

64/128-bit

Protocol

CSMA/CD

Ports

Wan

- One 10Base-T RJ-45 Port for Cable/DSL Modem

LAN

- Four 10/100 RJ-45 Switched Ports
- One Shared Uplink Port

Speed

Router

- 10Mbps

Switch

- 10/100Mbps (Half Duplex)
- 20/200 (Full Duplex)

Wireless Operating Range

- Indoors:
  30 m (100 ft.) 11 Mbps
  50 m (165 ft.) 5.5 Mbps
  70 m (230 ft.) 2 Mbps
  91 m (300 ft.) 1 Mbps
- Outdoors:
  152 m (500 ft.) 11 Mbps
  270 m (885 ft.) 5.5 Mbps
  396 m (1300 ft.) 2 Mbps
  457 m (1500 ft.) 1 Mbps

Wireless Transmit Power

19dBm

Dimensions

- L = 186 mm (7.31 inches)
- W = 154 mm (6.16 inches)
- H = 62mm (2.44 inches)

WRT54G Wireless-G Broadband Router (Linksys)

Standards

- IEEE draft 802.11g (Wireless-G)
- IEEE 802.11b (Wireless)
- IEEE 802.3 (10BaseT)
- IEEE 802.3u (100BaseTX)

Channels

- 11 Channels (USA, Canada)
- 13 Channels (Europe)
- 14 Channels (Japan)

Ethernet Data Rates

- 10/100Mbps

Encryption

64/128-bit

Frequency Band

2.4GHz

Modulation

IEEE 802.11b

- Direct Sequence Spread Spectrum (DSSS)

IEEE draft 802.11g

- Orthogonal Frequency Division Multiplexing (OFDM)

Network Protocols

- TCP/IP
- IPX/SPX
- NetBEUI

Ports

Wan

- One 10Base-T RJ-45 Port for Cable/DSL Modem

LAN

- Four 10/100 RJ-45 Switched Ports
- One Power Port

Cabling Type

Category 5 Ethernet Network Cabling or better

Wireless Operating Range

- Short operating range compared to that of 802.11b
- Mixing 802.11b and Wireless-G clients results in poor 802.11b performance

Wireless Transmit Power

15dBm

Dimensions

- L = 186 mm (7.32 inches)
- W = 175 mm (6.89 inches)
- H = 48mm (1.89 inches)

WAP11 v1 Wireless Access Point (Linksys)

Standards

- IEEE 802.11b (Wireless)
- IEEE 802.3 (10BaseT)
- IEEE 802.3u (100BaseTX)

Data Rate

Up to 11Mbps

Ports

One 10BaseT RJ-45 Port

Cabling Type

10BaseT: UTP Category 3 or better

Wireless Operating Range

- Indoors:
  up to 50M (164 ft.) 11 Mbps
  up to 80M (262 ft.) 5.5 Mbps
  up to 120M (393 ft.) 2 Mbps
  up to 150M (492 ft.) 1 Mpbs
- Outdoors:
  up to 250M (820 ft.) 11 Mbps
  up to 350M (1148 ft.) 5.5 Mbps
  up to 400M (1312 ft.) 2 Mbps
  up to 500M (1640 ft.) 1 Mbps

Power Input

5V, 550mA TX, 230mA RX

Dimensions

- L = 226 mm (8.9 inches)
- W = 127 mm (5 inches)
- H = 41mm (1.7 inches)

Weight

0.35 kg (12 oz.)

WAP11 v2.2 Wireless Access Point (Linksys)

Standards

- IEEE 802.11b (Wireless)
- IEEE 802.3 (10BaseT)
- IEEE 802.3u (100BaseTX)

Data Rate

Up to 11Mbps

Ports

One 10BaseT RJ-45 Port

Cabling Type

10BaseT: UTP Category 3 or better

Wireless Operating Range

- Indoors:
  up to 100M (300 ft)
- Outdoors:
  up to 450M (1500 ft)

Operating Temperature

0ºC to 55ºC (32ºF to 131ºF)

Power Input

5V DC, 2A, RF Output 20 dBm

Safety & Emissions

- CE
- FCC class B
- UL Listed
- ICS-03
- WiFi
- MIC

Dimensions

- L = 186 mm (7.31 inches)
- W = 154 mm (6.16 inches)
- H = 48mm (1.88 inches)

Weight

0.35 kg (12 oz.)

WAP11 v2.6 Wireless Access Point (Linksys)

Standards

- IEEE 802.11b (Wireless)
- IEEE 802.3 (10BaseT)

Data Rate

Wireless

- Up to 11Mbps

Ethernet

- 10Mbps

Transmit

18 dBm

Receive Sensitivity

-84 dBm

Modulation

- DSSS
- DBPSK
- DQPSK
- CCK

Network Protocols

- TCP/IP
- IPX
- NetBEUI

Wireless Operating Range

- Indoors:
  up to 100M (300 ft)
- Outdoors:
  up to 450M (1500 ft)

Operating Temperature

0ºC to 40ºC (32ºF to 104ºF)

Power Input

5V, 2.5 A

Dimensions

- L = 186 mm (7.31 inches)
- W = 154 mm (6.16 inches)
- H = 48mm (1.88 inches)

Weight

.0.55 kg (16 oz.)

Warranty

1-Year Limited

Perguntas mais Freqüentes (FAQ)

Veja 51 Perguntas sobre Wireless

- O que é preciso para montar uma rede Wireless?

Nos projetos mais simples, como é o caso das redes domesticas e dos pequenos escritórios, o principal componente é um equipamento chamado ponto de acesso ou Access point. Dá para encontrar nas lojas brasileiras diversas opções de modelos, de marcas tão diversas quanto Linksys, D-Link, 3Com, Trendware, USRobotics e NetGear, por preços que começam na faixa de 300 reais. Vários equipamentos incluem também as funções de roteador, o que permite compartilhar o acesso à Internet entre os computadores da rede. Além do ponto de acesso, cada máquina vai precisar de uma placa wireless, que pode ser interna ou externa. No caso dos notebooks e dos handhelds, há modelos que já tem a tecnologia wireless embutida no próprio processador (caso dos notebooks com Centrino) ou no equipamento (como alguns handhelds Axim da Dell, Tungsten da Palm, e Clié da Sony), dispensando o uso de um adaptador adicional.

- Qual é a velocidade da tecnologia Wireless?

Depende de qual tecnologia utilizada. O IEEE (Institute of Electrical and Electronics Engineers), a entidade responsável pelas questões de padronização, prevê hoje três tipos de tecnologia. A mais usada e mais antiga é o 802.11b, que tem velocidade nominal de 11Mbps e opera na freqüência de 2.4Ghz. O 802.11a, por sua vez, trabalha na freqüência de 5Ghz (mais especificamente de 5.725 a 5.850Ghz), com uma taxa de transferência nominal de 54Mbps. Já o 802.11g é considerado o sucessor do 802.11b. Também opera na freqüência de 2.4GHz, mas usa uma tecnologia de radio diferente para atingir até 54Mbps nominais. A vantagem é que os equipamentos g podem falar com o b nativamente, no caso do a, é preciso comprar um equipamento que funcione também com o b. No Brasil, por enquanto apenas a tecnologia 802.11b esta homologada pela Anatel (Agencia Nacional de Telecomunicações). Mas não é difícil encontrar nas lojas equipamentos a e g. Alem disso, conforme os preços dos dispositivos g caiam, a tendência é que a vá havendo uma migração natural para essa tecnologia, e o b acabe desaparecendo com o tempo.

- Em uma rede que combina equipamentos B e G, qual a velocidade predomina?

Se houver um único equipamento 802.11b rodando numa rede g, ele acabará diminuindo a performance da rede para algo mais próximo da velocidade da rede b, Entretanto, alguns fabricantes já incluíram em seus pontos de acesso g ferramentas que bloqueiam a conexão b na rede, para evitar esse tipo de queda de velocidade.

- Que cuidados devo ter com um cliente wireless?

Vários cuidados devem ser observados quando pretende-se conectar à uma rede wireless como cliente, quer seja com notebooks, PDAs, estações de trabalho, etc. Dentre eles, podem-se citar:

Considerar que, ao conectar a uma WLAN, você estará conectando-se a uma rede pública e, portanto, seu computador estará exposto a ameaças. É muito importante que você tome os seguintes cuidados com o seu computador:
- Possuir um firewall pessoal;
- Possuir um antivírus instalado e atualizado;
- Aplicar as últimas correções em seus softwares (sistema operacional, programas que utiliza, etc);
- Desligar compartilhamento de disco, impressora, etc.
- Desabilitar o modo ad-hoc. Utilize esse modo apenas se for absolutamente necessário e desligue-o assim que não precisar mais;
- Usar WEP (Wired Equivalent Privacy) sempre que possível, que permite criptografar o tráfego entre o cliente e o AP. Fale com o seu administrador de rede para verificar se o WEP está habilitado e se a chave é diferente daquelas que acompanham a configuração padrão do equipamento. O protocolo WEP possui diversas fragilidades e deve ser encarado como uma camada adicional para evitar a escuta não autorizada;
- Considerar o uso de criptografia nas aplicações, como por exemplo o uso de PGP para o envio de e-mails, SSH para conexões remotas ou ainda o uso de VPNs;
- Habilitar a rede wireless somente quando for usá-la e desabilitá-la após o uso. Algumas estações de trabalho e notebooks permitem habilitar e desabilitar o uso de redes wireless através de comandos ou botões específicos. No caso de notebooks com cartões wireless PCMCIA, insira o cartão apenas quando for usar a rede e retire-o ao terminar de usar.

- Que cuidados devo ter ao montar uma rede wireless doméstica?

Pela conveniência e facilidade de configuração das redes wireless, muitas pessoas tem instalado estas redes em suas casas. Nestes casos, além das preocupações com os clientes da rede, também são necessários alguns cuidados na configuração do AP. Algumas recomendações são:

- Ter em mente que, dependendo da potência da antena de seu AP, sua rede doméstica pode abranger uma área muito maior que apenas a da sua casa. Com isto sua rede pode ser utilizada sem o seu conhecimento ou ter seu tráfego capturado por vizinhos ou pessoas que estejam nas proximidades da sua casa. mudar configurações padrão que acompanham o seu AP. Alguns exemplos são:
- Alterar as senhas. Use senhas dificeis, que misturem caracteres e com tamanho mínimo de 8 caracteres;
- Alterar o SSID (Server Set ID);
- Desabilitar o broadcast de SSID;
- Usar sempre que possível WEP (Wired Equivalent Privacy), para criptografar o tráfego entre os clientes e o AP. Vale lembrar que o protocolo WEP possui diversas fragilidades e deve ser encarado como uma camada adicional para evitar a escuta não autorizada;
- Trocar as chaves WEP que acompanham a configuração padrão do equipamento. Procure usar o maior tamanho de chave possível (128 bits);
- Desligue seu AP quando não estiver usando sua rede.

Existem configurações de segurança mais avançadas para redes wireless, que requerem conhecimentos de administração de redes como 802.1X, RADIUS, WPA.

- Que equipamentos podem interferir no sinal de uma rede Wireless?

As redes 802.11b operam na freqüência de 2.4Ghz, que é liberada e usada por uma série de aparelhos. Os mais comuns são os fornos de microondas. Há também telefones sem fio que trabalham nessa freqüência, embora no Brasil sejam mais comuns os modelos de 900MHz. Portanto, dependendo da localização de aparelhos como esses em caso ou no escritório, eles podem acabar baixando a potencia da rede e eventualmente até derrubar o sinal. Uma vantagem de quem usa as redes 802.11ª é que a freqüência de 5GHz não é tão disputada quanto a de 2.4GHz e tem mais canais de radio, Isso evita a interferência causada por microondas ou telefones sem fio.

- Há algum material que possa causar interferência no sinal da rede?

Sim, vários. Quanto mais barreiras houver no caminho em que o sinal da rede passa, mais interferências você pode ter. Reservatórios de água (como aquários, bebedouros e aquecedores de água), metal, vidro e paredes de concreto são alguns exemplos clássicos na lista dos especialistas de Wireless. Um inofensivo garrafão de água no caminho entre o ponto de acesso e o computador pode acabar estragando os planos de uma rede Wireless estável. A lista não termina ai. Materiais como cobre, madeiras pesadas e grandes pilhas de papel também devem ser evitados. Entretanto, como Wireless não é uma ciência exata: o que afeta um projeto pode não interferir em outro. Só a instalação na prática vai dizer.

- A altura em que se coloca o ponto de acesso e as placas Wireless faz diferença?

Demais. É preciso levar isso muito a sério. Colocar desktops com adaptadores wireless perto do chão é algo proibido na etiqueta da rede Wireless. Quanto mais perto do piso os dispositivos wireless estiverem, mais fraco o sinal fica. Os fabricantes recomendam colocar equipamentos Wireless o quanto mais alto possível, com as antenas posicionadas verticalmente. Isso vale tanto para os pontos de acesso como para as placas ou adaptadores que serão instalados nos computadores. No caso de placas USB, algumas já vêm com cabos longos. Há também extensões para USB que podem ser usadas para essa finalidade.

- Em que lugar devo instalar o ponto de acesso?

O Ideal é colocá-lo em uma área central da casa ou do escritório. Quanto mais perto os equipamentos estiverem dele, melhor a potencia do sinal. Se você mora ou trabalha numa casa e também quer que a conexão chegue a áreas como quintal ou piscina, coloque o ponto de acesso próximo a uma janela do interior do imóvel (mas cuidado com as janelas externas, que dão para a rua, que podem fazer o sinal vazar para áreas estranhas e comprometer a segurança da sua rede). Depois de instalar o Access point, teste a potencia em diferentes áreas. Algumas placas incluem um software que permite fazer o chamado site survey, o estudo do sinal, uma pratica que se tornou obrigatória antes da instalação de redes wireless nas empresas. Se você não tiver essa ferramenta, uma saída é recorrer ao Windows XP. No painel de controle, vá a Conexões de Rede e de Internet e depois em Conexões de Rede. Clique com o botão direito na rede Wireless que você esta usando e depois em Status. Cheque a intensidade do sinal em cada um dos cômodos da casa ou áreas do escritório. As cores verde e amarelo são aceitáveis, mas se aparecer o vermelho esse computador acessará a rede inconsistentemente.

- O Que fazer quando o sinal estiver ruim numa determinada área?

A primeira providencia é checar se não há nenhuma barreira obstruindo o sinal no caminho do ponto de acesso. Os suspeitos de sempre são os reservatórios de água,

paredes de concreto, metais e vidros, principalmente se tiverem bastante reflexo. Caso o caminho esteja livre, o próximo passo é posicionar o ponto de acesso. Desloque-o por alguns centímetros e cheque a intensidade do sinal novamente. Nada feito? Isso pode significar que você precise fazer mais um investimento em hardware. Talvez uma antena de maior alcance resolva o problema. Dependendo da área e das barreiras, principalmente em escritórios, será preciso acrescentar pontos de acesso adicionais para cobrir todos os usuários. Tipicamente em áreas internas, o alcance nominal do 802.11b fica entre 30 e 90 metros. Em externas, pode chegar a distancias bem maiores.

- Dá para aumentar a velocidade de uma rede 802.11b ou 802.11g?

Sim. Há tecnologias que permitem aumentar a performance de redes 802.11b e 802.11g. Fabricantes como a Texas Instruments e a Atheros desenvolveram chipset para levar o wireless a novos patamares de velocidade. No caso Texas Instruments, as tecnologias são o 802.11b+ e 802.11g+, que dobram a velocidade nominal da rede para 22Mbps e 108Mbps. Já o alcance da rede pode ser aumentado com o uso de antenas mais potentes e de equipamentos como as bridges, que permitem alcançar quilômetros no caso de uma solução LAN a LAN.

- Quantos usuários podem ser suportados por um ponto de acesso?

Cada usuário que se conecta à sua rede wireless vai diminuindo a velocidade nominal. Tipicamente, um ponto de acesso 802.11b pode suportar até 15 ou 20 usuários. Mas tudo depende do tipo de aplicação que as pessoas estão trafegando. Para e-mail e acesso à web, OK. Para quem usa aplicações multimídia ou arquivos pesados na rede, essa situação pode ser critica. Basta lembrar que nas redes cabeadas o padrão é 100Mbps. Assim, para usuários que mexem com arquivos gigantescos, trabalhar numa rede sem fios ainda pode ser a melhor saída.

- Há alguma versão do Windows que funciona melhor em redes Wireless?

Sim, as versões mais recentes, como o Windows 2000 e XP, foram desenvolvidas para detectar automaticamente redes Wireless. Elas trazem ferramentas que facilitam o trabalho de configuração e já incorporam drivers importantes. Mas a Wireless também pode funcionar nas versões 98, ME e NT. Tem alguma máquina que ainda esta na era do Windows 95? Nada feito, é melhor esquecer as conexões sem fio nessa maquina.

- As redes Wireless aumentam o consumo da bateria em notebooks e handhelds?

Sim, essa é uma reclamação constante dos usuários de Wireless que tem de usar equipamentos portáteis por longos períodos. Entretanto, tecnologias alternativas têm sido estudadas nos laboratórios de fabricantes de chips, de baterias e de equipamentos wireless. O processador Centrino, da Intel, por exemplo, que foi concebido justamente para incorporar a tecnologia wireless, já traz um bom índice de economia de bateria saltando de duas horas de autonomia para quatro em alguns equipamentos. A HP, por sua vez, vende no Brasil, desde março passado um modelo de notebook, o nx5000, que pode receber uma bateria extra no lugar de driver de CD. Com isso, o portátil pode funcionar por oito horas seguidas.

- Hackers podem invadir minha rede Wireless?

Não existe uma rede 100% segura principalmente se ela for sem fio. Há vários softwares disponíveis na Internet que permitem rastrear redes wireless, e eles são

fáceis de serem usados, não apenas por hackers. Entretanto, se você não bobear na segurança, esse tipo de software vai apenas identificar a sua rede, mas não será possível acessar os seus dados. A menos que um cracker se disponha a ficar quebrando chaves para acessar algum dado especifico.

- Que procedimentos de segurança são recomendados em uma rede Wireless?

Muitos usuários colocam a rede para funcionar e deixam para depois o arsenal de segurança. Não faça isso, nas redes wireless, os dados trafegam pelo ar e podem ser facilmente acessados se não houver proteção. Uma vulnerabilidade muito comum entre os usuários sem fio é que eles não mudam o SSID (o nome da rede, o chamado Service Set IDentifier) e a senha padrão do fabricante do ponto de acesso. Isso é um erro primário, porque o SSID e as senhas colocadas pelos fabricantes são obvias. O SSID de um roteador da Linksys, por exemplo, você sabe qual é? Linksys! Por isso, é preciso caprichar no SSID e na senha, nada de escolhas óbvias. Outro procedimento recomendado é configurar a rede para que apenas os computadores conhecidos, com seus MAC Addresses determinados, tenham acesso a ela. Depois parta para o WEP ou WPA (Wireless Protected Access). Apesar de o WEP ter falhas manjadas principalmente por causa das senhas estáticas, é mais uma camada de proteção. Por isso, mude a senha do WEP regularmente pelo menos uma ou duas vezes por mês. Se você tiver WPA, melhor ainda, pois esse protocolo troca a chave de criptografia em intervalos definidos pelo usuário. O Ideal, tanto no caso do WEP como no do WPA, é criar uma senha com números e letras aleatórios, para dificultar o trabalho de um eventual cracker que tente quebrá-la. Alem disso, nada de descuidar das figurinhas carimbadas da segurança como antivírus, firewall e anti-spyware. A Wi-Fi Alliance, entidade que reúne mais de 200 fabricantes de produtos Wireless, e as próprias empresas vêm trabalhando com novos protocolos de segurança. Alguns exemplos são o 802.11i e o 802.1x. Do lado da turma especializada em segurança, também começam a aparecer novos tipos de solução. A Symantec, por exemplo, desenvolveu um firewall com sistema de detecção de intrusos que funciona como ponto de acesso wireless.

- Meu vizinho pode navegar pela minha rede Wireless?

Tecnicamente, sim, depende de como você configurou a rede. Se tiver trabalhado direito nos procedimentos de segurança, seu vizinho pode até identificá-la, mas não vai ter acesso. Se ela tiver aberta, a tarefa é fácil e não requer nenhuma habilidade hacker. Em países como os Estados Unidos e a Inglaterra, esse tipo de pratica tem até nome: é o warchalking. Quando descobrem uma rede aberta, as pessoas escrevem o nome do SSID na calçada com giz, para que qualquer um navegue por ela. Uma forma de verificar se alguém anda usando a sua rede sem ser convidado é ficar de olho nos leds do ponto de acesso. Se eles estiverem piscando enquanto os usuários "oficiais" não estiverem ativos, sinal vermelho. Na melhor das hipóteses, pode ser alguém apenas querendo pegar carona na sua banda. Ou, na pior, bisbilhotando is dados dos arquivos compartilhados entre as maquinas da rede.

- O que faço para não me conectar a rede Wireless do vizinho?

Se você mora numa região em que há muitas redes sem fio, também precisa checar se não anda captando o sinal do seu vizinho sem querer. No Windows XP, vá ao Painel de Controle e, em Conexões de Rede, selecione a sua rede Wireless. Clique com o botão direito para acessar Propriedades. Vá a aba Rede sem Fio e clique o botão Avançado. Certifique-se de que a opção Conectar-se Automaticamente a Redes Não-Preferenciais esteja desmarcada.

- Hotspots são seguros para acessar dados confidenciais?

Como os dados trafegam pelas ondas do ar, se você estiver num hotspot, a comunicação entre a sua máquina e o Access point acaba ficando vulnerável. Nesse caso, diferentemente do acesso wireless em caso ou no escritório, não da para contar com recursos como o WEP e a configuração do MAC Address. Por isso, avalie bem o que você vai acessar. Se sua empresa tiver uma VPN, essa pode ser uma boa saída para enviar dados de forma segura, pois eles já saem criptografados do seu próprio notebook.

- Preciso Pagar um provedor para navegar em Hotspot?

Na maioria das vezes, sim. A menos que você esteja num local que franqueie o acesso a seus clientes, será preciso pagar por um provedor especifico para redes Wireless de empresas como Terra, iG, Oi, Ajato e Brasil Telecom. Em algumas delas é preciso pagar uma assinatura mensal, mas a tendência é que o acesso seja vendido pelo sistema pré-pago.

- É Possível transformar a impressora que tenho em um equipamento Wireless?

Sim, mas você vai precisar investir em hardware, é necessário comprar um servidor de impressão Wireless. Assim, você fará impressões de qualquer PC, notebook ou handheld da rede. Uma alternativa para colocar a impressora na rede Wireless sem gastar nada é ligá-la a um dos computadores. A desvantagem é que essa máquina sempre terá de estar ligada para que os outros usuários da rede possam imprimir seus arquivos. Mas já estão saindo impressoras Wireless, como a Deskjet 5850, da HP.

- Dá para montar uma rede com dispositivos Wireless de diferentes fabricantes?

Na teoria, sim, mas na pratica a historia é diferente. Principalmente por causa das questões relacionadas à segurança, vários fabricantes começaram a desenvolver suas próprias ferramentas de reforço. O resultado é que nem sempre um vai falar com o equipamento do outro, pois não usam os protocolos padronizados. Um caso clássico é o do WEP. O padrão inicial previa criptografia de 40 bits, quem usa 128 bits não tem nenhuma garantia que dispositivos de marcas diferentes possam conversar. Se você quer evitar dor de cabeça com questões de compatibilidade, vale a pena usar na sua rede pontos de acesso e placas do mesmo fabricante.

- O que é uma célula?

É a área na qual o rádio de sinal de um Access Point é o suficientemente boa para que um modo Wireless possa conectar-se com ela.

- A informação transmitida pelo ar pode ser interceptada?

A wireless LAN possui dois níveis de proteção em segurança. No Hardware, a tecnologia DSSS incorpora a característica de segurança mediante o scrambling. No Software as WLANs oferecem a função de encriptação (WEP) para ampliar a segurança e o Controle de Acesso pode ser configurado dependendo de suas necessidades.

- O que é WEP?

O WEP (Wired Equivalent Protection) é um mecanismo para a privacidade de Dados e descrito no padrão IEEE 802.11, também previsto nos produtos WLAN da D-Link. Os produtos da D-Link suportam 40-bit e 128-bit de encriptação.

- O que é Access Point? (Ponto de Acesso)

Um Access Point é um Bridge em Nível MAC (transparent media Access control - MAC) que proporciona o acesso a estações Wireless até redes de área local cabeadas. Por intermédio destes dispositivos, as estações Wireless podem integrar-se rápida e facilmente a qualquer rede cabeada existente.

- O que é uma LAN sem fio (WLAN - Wireless LAN)?

Uma WLAN é um tipo de rede local (LAN - Local Area Network) que utiliza ondas de rádio de alta freqüência em vez de cabos para comunicação e transmissão de dados entre os nós. É um sistema de comunicação de dados flexível, implementado como extensão ou como alternativa a uma rede local com fios em um prédio ou um campus.

- O que é IEEE 802.11b?

IEEE 802.11b é uma especificação técnica emitida pelo IEEE (Institute of Electrical and Electronic Engineers - Instituto dos Engenheiros Elétricos e Eletrônicos) que define a operação de WLANs (Wireless Local Area Networks- Redes locais sem fio) com sistema DSSS (Direct Sequence Spread Spectrum) de 2,4 GHz e a 11 Mbps.

- O que é IEEE 802.11g?

IEEE 802.11b é uma especificação técnica emitida pelo IEEE (Institute of Electrical and Electronic Engineers - Instituto dos Engenheiros Elétricos e Eletrônicos) que define a operação de WLANs (Wireless Local Area Networks- Redes locais sem fio) com sistema DSSS (Direct Sequence Spread Spectrum) de 2,4 GHz e a até 54 Mbps e mantém compatibilidade com o IEEE 802.11b.

- Qual é o alcance da transmissão dos produtos WLAN?

O alcance de rádio-freqüência (RF), principalmente em ambientes fechados, é função do projeto do produto, incluindo potência de transmissão e projeto do receptor, interferência e caminho de propagação. Interações com objetos comuns em edificações, como paredes, metais e até pessoas, podem afetar a forma de propagação da energia e, portanto, a distância e a cobertura alcançadas por determinado sistema. Os sistemas de redes locais Wireless usam RF porque as ondas de rádio penetram em muitas superfícies e paredes internas. O alcance ou raio de cobertura de sistemas WLAN característicos chega a 200 metros dependendo do número e do tipo de obstáculos encontrados. A cobertura pode ser ampliada e a liberdade de verdadeira mobilidade e o roaming podem ser proporcionados a uma área maior com a utilização de vários pontos de acesso.

- O que é WECA?

A WECA (Wireless Ethernet Compatibility Alliance) é uma organização sem fins lucrativos formada em 1999 e seu lançamento oficial e público ocorreu em 23 de agosto de 1999, em Santa Clara, na CA (EUA). A missão da WECA é certificar a interoperabilidade de produtos WLAN Wi-Fi (IEEE 802.11b de alta velocidade) e promover o Wi-Fi como padrão para implementação de redes locais sem fio em todos os segmentos do mercado.

- O que é Wi-Fi?

Wi-Fi é o nome da marca comercial utilizada pela WECA para indicar a interoperabilidade de produtos WLAN. O nome provém de "wireless fidelity" (fidelidade sem fio). A WECA submete os produtos WLAN a testes avançados; os produtos que atendem ao padrão de interoperabilidade recebem o logotipo Wi-Fi.

- Qual a velocidade de transferência de dados das conexões de rede WLAN padrão 802.11b? E no padrão 802.11g?

As WLANs 802.11b operam em velocidades de até 11 Mbps. Os usuários WLAN encontram velocidades comparáveis às oferecidas pelas redes com fios e a velocidade de transferência nas redes WLAN, assim como nas redes com fios, depende da topologia de rede, carga, distância do ponto de acesso etc. Geralmente não se percebe diferença de desempenho em comparação com as redes com fios. Já no 802.11g as velocidades podem chegar a 54 Mbps mantendo o mesmo alcance e funcionalidades do 802.11b.

- Quantos usuários um sistema WLAN pode suportar?

O número de usuários é potencialmente ilimitado. Para aumentar o número de usuários, basta incluir pontos de acesso na rede. Com a inclusão de pontos de acesso sobrepostos, definidos em freqüências (canais) diferentes, a rede sem fio pode ser ampliada para acomodar usuários adicionais simultâneos na mesma área. Até três canais sobrepostos podem ser utilizados concorrentemente sem interferências, o que efetivamente triplica o número de usuários permitidos na rede. De forma semelhante, a WLAN permite um número maior de usuários com a instalação de pontos de acesso adicionais em vários locais do prédio. Isso aumenta o total de usuários e permite o roaming em todo o prédio ou pelo campus.

- Quantos usuários simultâneos um único ponto de acesso pode suportar?

O número de usuários simultâneos suportados pelo ponto de acesso depende principalmente do volume de tráfego de dados (downloads e uploads pesados ou leves). A largura de banda é compartilhada pelos usuários em uma WLAN, da mesma forma como nas conexões de redes com fios. O desempenho da rede, medido pelo número de usuários simultâneos, depende do tipo de atividade exercida pelos usuários.

- Por que as WLANs operam na faixa de freqüência de 2,4 GHz?

Esta faixa de freqüência foi reservada pela FCC e costuma ser chamada como a banda ISM (Industrial, Scientific and Medical). Há alguns anos, a Apple e várias outras grandes empresas solicitaram à FCC permissão para o desenvolvimento de redes sem fio nessa faixa de freqüência. Hoje existe um protocolo e um sistema que permite o uso não-licenciado de rádios em um nível de potência prescrito. A banda ISM é ocupada por dispositivos industriais, científicos e médicos de baixa potência.

- O que é WEP?

WEP (Wired Equivalent Privacy - Privacidade equivalente à das redes com fios) é uma característica IEEE 802.11 opcional, utilizada para proporcionar segurança de dados equivalente à de uma rede com fios sem técnicas de criptografia avançada de privacidade. A WEP permite que os links de rede local sem fio sejam tão seguros quanto os links com fios. De acordo com o padrão 802.11, a criptografia de dados WEP é utilizada para impedir acesso à rede por "intrusos" com equipamentos similares de rede local sem fio e (ii) captura do tráfego de redes sem fio por curiosos. A WEP permite ao administrador definir o conjunto das "chaves" respectivas de cada usuário da rede sem fio, de acordo com uma "seqüência de chaves" passada pelo algoritmo de criptografia WEP. É negado o acesso a quem não possui a chave necessária. Conforme especifica o padrão, a WEP usa o algoritmo RC4 com chave de 40 ou 128 bits. Quando a WEP é ativada, cada estação (clientes e pontos de acesso) possui uma chave. A chave é utilizada para criptografar os dados antes de serem transmitidos pelas emissões de rádio. Quando uma estação recebe um pacote não criptografado com a chave adequada, o pacote é descartado e não é entregue ao host; isso impede o acesso à rede por curiosos e pessoas não autorizadas.

- O que é FHSS (Frequency Hopping Spread Spectrum)?

FHSS (Frequency-Hopping Spread-Spectrum) é um esquema de modulação spread-spectrum que utiliza uma portadora de banda estreita alterando a freqüência segundo um padrão conhecido pelo transmissor e pelo receptor. Sincronizados adequadamente, eles mantêm um único canal lógico. Para um receptor não desejado, o FHSS aparece como ruído de pulso de curta-duração. A tecnologia FHSS usa a largura de banda de forma ineficaz para garantir alta segurança; portanto, os sistemas FHSS costumam apresentar velocidades de transferência menores do que as de sistemas DSSS (Direct Sequence Spread Spectrum). Dispositivos WLAN com desempenho mais lento (1 Mbps) utilizam FHSS.

- Quais são as vantagens do uso de uma WLAN em vez da conexão de rede com fios?

Maior produtividade - a WLAN proporciona acesso "liberado" à rede em todo o campus e à Internet. A WLAN oferece a liberdade de deslocamento mantendo-se a conexão.
Configuração rápida e simples da rede - sem cabos a serem instalados.
Flexibilidade de instalação - as WLANs podem ser instaladas em locais impossíveis para cabos e facilitam configurações temporárias e remanejamentos.
Redução do custo de propriedade - as LANS sem fio reduzem os custos de instalação porque dispensam cabeamento; por isso, a economia é ainda maior em ambientes sujeitos a mudanças freqüentes.
Crescimento progressivo - a expansão e a reconfiguração não apresentam complicações e, para incluir usuários, basta instalar o adaptador de LAN sem fio no dispositivo cliente.

Interoperabilidade - os clientes podem ficar tranqüilos com a garantia de que outras marcas de produtos compatíveis de rede e cliente funcionarão com as soluções proposta.

- Os produtos de WLAN de uma determinada marca oferecem interoperabilidade com outras marcas de produtos?

Sim. Os produtos de WLAN são compatíveis com produtos de diferentes fornecedores que empregam a mesma tecnologia (DSSS - Direct Sequence Spread Spectrum); dessa forma, é possível usar adaptadores clientes de vários fornecedores. O propósito dos padrões do mercado, inclusive as especificações IEEE 802.11, é permitir a interoperabilidade de produtos compatíveis sem a colaboração explícita entre fornecedores. A WECA (Wireless Ethernet Compatibility Alliance - Aliança para a compatibilidade de Ethernet sem fio) é a organização do mercado que certifica a interoperabilidade de produtos WLAN. A especificação 802.11b fornece diretrizes para a interoperabilidade de WLAN e a WECA (Wireless Ethernet Compatibility Alliance) assegura a interoperação dos produtos nas aplicações do mundo real. Os sistemas interoperam desde que as placas PC cliente e os pontos de acesso obedeçam à especificação 802.11b e sejam certificados pela WECA.

- É difícil instalar e administrar uma WLAN?

Não. A instalação de uma rede local sem fio é mais simples do que a de uma rede com fios e a administração dos dois tipos de rede é muito semelhante. A solução de WLAN para o lado cliente oferece a simplicidade Plug-and-Play para conexão à rede ou a outros computadores (conexões ponto-a-ponto, não hierarquizadas).

- As WLANs são seguras?

Sim, as WLANs são altamente seguras. Como a tecnologia sem fio tem sua origem em aplicações militares, os mecanismos de segurança para dispositivos sem fio são projetados há muito tempo e as redes locais sem fio costumam ser mais seguras do que a maioria das redes locais com fios. As WLANs usam tecnologia DSSS (Direct Sequence Spread Spectrum), que é extremamente resistente a falhas, interferências, congestionamentos e detecções. Além disso, todos os usuários sem fio da rede são reconhecidos por um sistema de identificação que impede o acesso de usuários não autorizados. Os usuários com dados altamente confidenciais podem ativar a WEP (Wired Equivalent Privacy - Privacidade equivalente à das redes com fios), que aplica criptografia avançada ao sinal e verifica os dados com uma "chave de segurança" eletrônica. Além disso, hoje existem padrões como 802.1X Radius e WPA que garantem ainda mais segurança. Em geral, os nós individuais precisam ter a segurança ativada antes de participar do tráfego da rede. As WLANs 802.11b podem usar criptografia de 40 e de 128 bits juntamente com a autenticação do usuário para proporcionar alto grau de segurança à rede. É praticamente impossível a intrusos e receptores não desejados escutar o tráfego de uma rede sem fio.

- Quando o ponto de acesso é necessário?

Os pontos de acesso são necessários para o acesso à rede, mas não para conexões não hierarquizadas. A rede sem fio precisa de um ponto de acesso somente para conectar notebooks ou computadores de mesa a uma rede com fios. Algumas vantagens importantes tornam os pontos de acesso um complemento valioso para as redes sem fio, havendo ou não uma rede com fios. Primeiro, um único ponto de acesso é capaz de quase dobrar o alcance da rede local sem fio comparada a redes não hierarquizadas (ad-hoc) simples. Segundo, o ponto de acesso sem fio funciona como controlador de tráfego, direcionando todos os dados da rede e permitindo aos clientes operar na velocidade máxima. Por fim, o ponto de acesso pode ser a conexão central ao mundo externo, proporcionando compartilhamento de Internet.

- Qual a diferença entre o ponto de acesso e um produto de ponte?

As pontes permitem às redes locais com fios estabelecer conexões sem fio a outras redes com fios. Usa-se uma ponte para conectar um segmento da rede local a outro segmento no mesmo prédio ou em outro prédio da cidade. Os pontos de acesso são utilizados para conectar clientes sem fio a redes locais com fios.

- O que é DSSS (Direct Sequence Spread Spectrum)?

DSSS (Direct Sequence Spread-Spectrum) é um esquema de modulação spread-spectrum que gera um padrão redundante de bits para cada bit transmitido. O padrão de bits, chamado chip ou código de chip, permite aos receptores filtrar sinais que não utilizam o mesmo padrão, incluindo ruídos ou interferências. O código de chip cumpre duas funções principais: 1) Identifica os dados para que o receptor possa reconhecê-los como pertencentes a determinado transmissor. O transmissor gera o código de chip e apenas os receptores que conhecem o código são capazes de decifrar os dados. 2) O código de chip distribui os dados pela largura de banda disponível. Os chips maiores exigem maior largura de banda, mas permitem maior probabilidade de recuperação dos dados originais. Ainda que um ou mais bits do chip sejam danificados durante a transmissão, a tecnologia incorporada no rádio recupera os dados originais, usando técnicas estatísticas sem necessidade de retransmissão. Os receptores não desejados em banda estreita ignoram os sinais de DSSS, considerando-os como ruídos de potência baixa em banda larga. As WLANs 802.11b usam DSSS e apresentam maior transferência de dados do que a contraparte FHSS, devido à menor sobrecarga do protocolo DSSS.

- A tecnologia WLAN se destina apenas a notebooks?

Não. Embora sejam ideais para computadores móveis em rede, os sistemas WLAN são igualmente úteis para conectar computadores de mesa e várias novas plataformas de unidades móveis. As soluções WLAN são projetadas para eliminar cabos em dispositivos de rede, eliminando custos de cabeamento e aumentando a flexibilidade e a mobilidade das conexões.

- Preciso trocar de computador para utilizar as soluções WLAN?

Não. Os produtos WLAN podem ser utilizados com o seu notebook ou PC de mesa atual.

- Existem efeitos prejudiciais à saúde causados pelos produtos WLAN?

A potência de saída dos sistemas de redes locais sem fio é muito menor do que a dos telefones celulares. Como as ondas de rádio desaparecem rapidamente em uma certa distância, quem estiver dentro da área de um sistema de rede local sem fio estará exposto a pouquíssima energia de RF. As redes locais sem fio precisam atender rigorosamente às regulamentações sobre segurança do governo e do mercado.

- As WLANs recebem interferência de outros dispositivos sem fio? Ou de outras WLANs?

A natureza não licenciada das redes locais sem fio baseadas em rádio significa que outros produtos (telefones sem fio, fornos de microondas, portas de garagem automáticas) que transmitem energia no mesmo espectro de freqüência potencialmente podem interferir em um sistema WLAN. Os fornos de microondas são uma preocupação, mas a maioria dos fabricantes de WLAN projetam seus produtos de forma a evitar a interferência das microondas. Outra preocupação é a proximidade de mais de um sistema WLAN. Porém, existem técnicas de gerenciamento de rede capazes de minimizar ou eliminar a interferência de WLANs sobrepostas.

- Todos os produtos WLAN (802.11 e 802.11b) são interoperáveis?

Não. As WLANs 802.11b certamente permitirão interoperações com outros produtos WLAN 802.11b, mas as WLANs 802.11b não operarão com WLANs que utilizam outras técnicas de modulação (Frequency-Hopping Spread Spectrum). Os produtos normalmente têm certificação da WECA, assegurando a interoperabilidade com outros produtos WLAN 802.11b.

- Em quais mercados e segmentos-alvo os produtos WLAN são vendidos?

Os mercados verticais foram os primeiros a adotar o uso de WLANs, mas a utilidade da WLAN se difundiu em aplicações horizontais de uso comum. Os produtos do padrão de alta velocidade IEEE 802.11b são desenvolvidos para utilização em todos os segmentos do mercado - corporações, empresas pequenas, armazenagem, varejo, educação, atividades domésticas, acesso público etc. - praticamente todos os usuários de redes já são beneficiados com a utilização de redes locais sem fio.

COMO MONTAR UM PROVEDOR DE ACESSO VIA RÁDIO

Reprodução de artigo publicado pela ABRANET - http://www.abranet.com.br/

A Abranet possui um grupo de trabalho em formação que vai atuar diretamente nesta área, não somente nas questões de SCM, mas de outras pertinentes a regulamentação, quanto ao SCM.

1 As empresas que comercializam serviços de Telecom atuam basicamente em duas frentes:
Serviços de Telefonia (STFC - Serviço de Telefonia Fixa Comutada)
Serviços de dados
Nas concessões de STFC, que é um serviço de interesse público as empresas compradoras (tanto as "incumbents" quanto as "espelhos"), receberam autorizações de operar serviços de dados, estas operadoras, portanto podem realizar conexões dedicadas, ligando o “ponto A com ponto B” por quaisquer meios, utilizando radiofreqüência ou não.
- O Serviço de transmissão de dados, em caráter privado, contava com várias denominações (SRTT / SLE etc...) com a Lei 9472 de 06 de julho de 1997 criou-se o SCM - Serviço de Comunicação Multimídia que veio a englobar todas estas atividades (mais informações sobre a Lei 9472 podem ser visualizadas no site da ANATEL - www.anatel.gov.br)

2 Mas o que tem haver isto com nosso negocio de Provedor de acesso?

- É necessário desenvolver em paralelo, para que possamos entender as dicotomias e onde na verdade estes temas, Provedor de acesso x SCM se encontram.

- Com a insatisfação dos clientes, principalmente dos heavy users com a banda estreita, o mercado banda larga começou a crescer, e tivemos um movimento de crescimento deste serviço, nas grandes cidades o ADSL tomou conta de certa maneira deste mercado, mas um movimento diferente, na realidade não muito programado pelas teles começou a surgir, principalmente, nas pequenas/médias cidades onde as redes ADSL não estavam contempladas a “priori”, o ACESSO VIA RADIO 2.4 Ghz, no inicio com um custo razoável e agora relativamente barato.

- Os provedores não só criaram/adaptaram uma tecnologia, (inicialmente puramente indoor) para operar outdoor como começaram a desenvolver ferramentas, como controle de banda, cachês, roteamentos alternativos que fizeram com que as redes de rádio 2.4 Ghz, começassem a ter QoS (Nível de Qualidade) superior as redes ADSL.

- Vejamos, portanto o inicio da invasão rádio 2.4 (anterior ao efetivo conhecimento e aplicação da Legislação SCM), mas os legisladores de certa maneira, visionaram esta invasão.

- Gostaríamos de frisar, que a outorga SCM, a priori, não tem nada a haver com operação de rádio freqüência, uma empresa outorgada pela Anatel pode, ou não, utilizar este meio (rádio freqüência) para ligar o “ponto A ao ponto B”, (pois se utilizar fibra ótica, par trancado, coaxial) não irá necessitar desta autorização, quando uma empresa tem a outorga ela tem a prerrogativa de pedir ou não, uso de rádio freqüência, no caso para rádio freqüência licenciada exclusiva ou não.

- Um erro comum, que vamos esclarecer á seguir e a confusão á despeito de ser as freqüências de 2.4 e 5.8 freqüências "Livres" portanto, livres de licença para operação,

3 Freqüência Licenciada divide-se em:
Exclusivas - Basicamente de operadoras celulares, ou seja, elas adquirem via leilão, estas freqüências, serão proprietárias na exploração deste serviço, tem território delimitado e são onerosas.
Não exclusivas – Citamos um exemplo: A “Telecom A” pode operar um enlace a 15 Ghz em Manaus para atender um cliente de 4 Mbs e a “ Telecom B” pode estar usando esta mesma freqüência pra atender um outro em Curitiba, as estações tem de estar registradas e pagam a Anatel uma taxa de otimização de rádio freqüência

(IPPUR) (que é calculado via uma fórmula que se encontra no site da Anatel), ou seja, geram custos em toda a sua utilização.
Freqüências 'Livres “ou não”Licenciadas”.
Copiados do FCC (órgãos americanos), são nomeados ISM (Industrial and Service Mode) foram estabelecidas para que organismos como polícia, bombeiros etc, tivessem acesso a comunicação de uma maneira menos "burocrática", sua característica principal e a necessidade de estarem homologadas, cadastradas no órgão regulador, mas, não pagam pela otimização deste espectro.
- Na realidade o que queremos ressaltar, é que quando a Anatel “lacra”, (e estão lacrando!), seu provedor por estar prestando serviço de rádio, o foco não é na freqüência e sua utilização, está na permissão ou não de sua empresa em prestar Serviço de Telecomunicação.

- A Lei de SCM vem a regular a relação entre o ISP e seu cliente, com a ANATEL ele tem somente duas; uma regulatória que se exaure no momento que o órgão concede a licença, e outra fiscalizatória, em que o cerne da questão (esta somente se à parte básica da rede estiver ok).

- Finalizando, toda empresa que liga “ponto A ao ponto B”, para acesso IP (Internet) ou dados privados tem que estar regular (SCM) para prestar este serviço.

Perguntas mais Freqüentes

1 -E muito caro?

A outorga custa R$9.000,00 (nove mil reais), o pagamento é efetuado para a ANATEL via um boleto, quando da publicação no diário oficial da união, pode ser utilizada em todo o território nacional.

2 - O que preciso?

A empresa deve estar:

• Constituída segundo as leis Brasileiras com sede e administração no País;
• Com todas as condições de idoneidade perante o Poder Público (seja quanto a licitações, impostos ou permissões).

Documentos necessários:

• Contrato Social com o objeto compatível com a autorização
• Cópia do CNPJ
• Inscrição Municipal
• Inscrição Estadual
• Registro no CREA, assinado por um responsável técnico que seja engenheiro eletrônico, eletricista ou engenheiro de telecomunicações.
• Certidões Negativas da Fazenda Federal, Estadual e Municipal
• Prova de regularidade Junto ao INSS e FGTS

3 – Como proceder?

Inicialmente você vai precisar elaborar um projeto muito simples, com auxílio de um engenheiro de confiança.

5 - Mas meu serviço de rádio é pequeno, será que compensa SCM só pra regularizá-lo?

O SCM não é só pra regularizar rádio, (leia a íntegra da lei no site da Anatel) e verá que ele abre um leque enorme de serviços hoje e no futuro, além de ter descontos em links e outros serviços junto as Teles, por ser uma empresa de Telecom também.

COMO MONTAR UM PROVEDOR

Rede
Reprodução de artigo publicado pela ABRANET - http://www.abranet.com.br/
São necessárias poucas peças para se tornar um ISP. Dividindo-se a infra-estrutura de um ISP em três áreas distintas, consegue-se ver facilmente onde cada peça se encaixa.
1. Rede Central - Esta parte é responsável pela conexão com a WAN. Isso resume a Internet, sendo uma rede de redes, ela é apenas uma simples conexão entre um ISP com outro ISP.
2. Rede de Distribuição - Aqui é onde os serviços Backbone se conectam a rede de acesso. A Ethernet define o backbone do ISP e mantém tudo unido.
3. Rede de Acesso - Aqui é onde os serviços de acesso são adicionados, por exemplo, esses podem ser os Servidores de Acesso Remoto (RAS), para modems dial up ou DSL para conexões de linhas dedicadas.

A primeira peça do equipamento a se considerar é o switch Ethernet. Assim como o backbone do ISP, a Ethernet é o denominador comum que permite que equipamentos de diferentes fabricantes se interconectem. A partir do ponto de distribuição, um ISP pode adicionar serviços de acesso, assim como, largura de banda adicional.
A rede de acesso do ISP é o ponto onde os usuários se conectam ao serviço. A forma mais comum é através de modems discados. Antes, os modems de mesa e os servidores de terminal eram a forma padrão para se conectar. Hoje, com a queda de preço das linhas E1 e dos modems V.90, um único equipamento integrado oferece a melhor solução. Esse equipamento é chamado Servidor de Acesso Remoto (RAS).
O RAS se conecta à companhia telefônica local através de um linha E1, e ao switch Ethernet local. Quando os usuários fazem uma chamada para se conectar ao provedor , o RAS responderá a chamada com um de seus modems. Após conectar o usuário, o RAS pegará os pacotes IP e os enviará para a Internet.

O RAS opera da seguinte maneira:
1. Um usuário disca o número do telefone de acesso do ISP usando seu modem e o RAS responde a ligação através de um modem.
2. Após conectar os modems, inicia-se uma sessão PPP entre o usuário e o RAS.
3. Através do PPP, o RAS obtém o nome de usuário e a senha.
4. O RAS pesquisa um servidor RADIUS e autentica o usuário.
5. Sendo um usuário válido, o RAS lança automaticamente um endereço IP para o usuário e termina a configuração da conexão. O usuário está pronto para navegar pela Internet e enviar e-mails.

A próxima peça é o roteador. Ele conectará a rede do ISP ao provedor upstream. É através deste provedor que se conecta a outras redes e hosts, ou em outras palavras à Internet. O provedor upstream, nada mais é do que um ISP que se conecta diretamente à rede mundial e vende serviço de acesso a ISP's menores alocando sub redes.
Em seguida são necessários os servidores. Os serviços básicos que qualquer ISP precisa para prover acesso, são:
1. DNS - Resolução de nome de domínio primário/secundário
2. RADIUS - Autenticação de usuário e contas

3. WWW - Servidor Web
4. E-mail - Provedor de serviços POP3/IMAP4 e SMTP

DNS - é o método pelo qual os computadores traduzem nomes como www.blackbox.com.br em um endereço IP. Isso é feito porque todo tráfego na Internet é baseado em endereços IP e os nomes são mais fáceis para os seres humanos memorizarem.
RADIUS (Remote Authentication Dial In User Service) - Serviço de autenticação remota de usuários discados. É o protocolo de autenticação, onde um cliente, como por exemplo um RAS, requer ao servidor RADIUS a validação de um usuário. Os nomes de usuários e senhas, assim como parametros adicionais são mantidos em um banco de dados centralizado. O registrador RADIUS rastrea as transações de autorização e autenticação e captura as estatísticas de cada sessão. Existem muitos servidores RADIUS gratuitos disponíveis na Web, e muitos sistemas tarifadores ISP incorporam suporte a RADIUS em seus pacotes.
E-mail e hospedagem Web são as mais básicas e importantes partes do portifólio de serviços do ISP. Esses servidores enviam e armazenam os e-mails endereçados para os assinantes do ISP. Atualmente, a hospedagem Web é tão comum que ela é freqüentemente incluida no pacote de acesso básico. Todos os softwares necessários estão disponíveis gratuitamente na Web e normalmente vem pré-instalado com o sistema operacional. Opcionalmente, serviços de e-mail/www/FTP podem ser feitos com um servidor especial.
Todos os quatro serviços podem ser executados em um único servidor, contudo, as modernas engenharias de rede difunde a distribuição entre dois ou três servidores. Isso permite o back-up de serviços em servidores alternados. Afinal, os assinantes querem serviços 24 horas por dia sem interrupções
Como pode ser observado, hoje, a Internet representa um novo mercado de serviço de comunicação. Recurso de massa e baixo custo facilitaram a construção de um provedor de Internet. Com poucos equipamentos e alguns softwares gratuitos, ficou muito fácil montar um ISP.

Versão 04/2005 revisão (ALEDEGUI)