



UNIVERSIDADE CÂNDIDO MENDES

**COORDENAÇÃO DE PÓS-GRADUAÇÃO E ATIVIDADES
COMPLEMENTARES**

DEPARTAMENTO DE PESQUISA E PÓS-GRADUAÇÃO

COORDENADORIA DE CURSOS DE PÓS-GRADUAÇÃO LATO SENSU

Emerson Barros de Meneses

REDE WIRELESS: UMA SOLUÇÃO SEM FIOS

Trabalho de Conclusão de Curso

Rio de Janeiro

Dezembro/2009

EPÍGRAFE

“Um telégrafo sem fio não é difícil de entender. O telégrafo normal é como um gato muito longo. Você puxa o rabo em New York e ele mia em Los Angeles. A tecnologia sem fio é a mesma coisa, só que sem o gato”.
(EINSTEIN, Albert)

SUMÁRIO

RESUMO	05
1. INTRODUÇÃO	06
2. BREVE HISTÓRICO	08
3. EQUIPAMENTOS MAIS COMUNS	14
4. COMO FUNCIONA	04
5. IMPLEMENTAÇÃO	20
6. MIGRAÇÃO	25
7. GASTOS	27
8. SEGURANÇA	29
9. CONCLUSÃO	33
REFERÊNCIAS BIBLIOGRÁFICAS	34

1 Introdução

Esta monografia é constituída pela pesquisa do uso, implementação e vantagens das redes wireless (sem fios) assim como na definição do assunto e dos principais tópicos relacionados a ela.

Segundo a SYMANTEC (2003), o uso das redes sem fio está se multiplicando cada vez mais à medida que a qualidade das mesmas vai melhorando e os preços dos equipamentos vão se tornando mais acessíveis.

Com uma rede cabeada, ou seja, computadores interligados por meio de fios, faz-se necessário mudanças físicas, obras e arrumações. Os problemas estruturais do local como a alteração de layout de móveis, salas, divisórias e salões de reunião. E cabos aparentes espalhados por todo local.

Ao expandir novos pontos de rede emergenciais ou simplesmente ampliar a rede de forma a acomodar os funcionários, onde quer que eles estejam, os fios novamente atrapalham.

Ou ainda prédios tombados pelo patrimônio histórico, atende uma determinada área onde a execução de obra civil ou simplesmente um furo através da parede é expressamente inviável e proibido por lei.

Havendo a necessidade de alocar/disponibilizar um ambiente de informática para um projeto de curta duração, onde colocá-los sem alterar na estrutura física e cabos.

A importância deste tema se deve ao interesse de varias empresas/usuários terem demonstrado dificuldades quanto a esse assunto em implantar, manter e/ou ampliar redes cabeadas tomando assim as redes wireless muito mais viável.

O objetivo principal deste trabalho de conclusão de curso é demonstrar a importância que deve ser dada ao assunto assim como auxiliar nos processos referentes a implementação/migração de redes em fio. E demonstrar de forma simples e objetiva as vantagens em utilizar sistemas de comunicação sem a necessidade de cabos interligando computadores. Onde a conectividade da rede é feita de forma rápida, fácil e a custos acessíveis, com acesso seguro e altamente funcional para qualquer tamanho de empresa,

escritório e residências, tanto para novos prédios como para lugares temporários. Possibilitando constantes mudanças de layout e um ambiente tecnologicamente moderno e visualmente atrativo.

A metodologia utilizada resumiu as propostas de uma pesquisa bibliográfica incluindo livros, artigos, apostilas e matérias de internet. Esta pesquisa também é qualitativa, buscando adquirir conhecimento para se associar aos conceitos pesquisados.

Desta forma, o trabalho está organizado em 8 capítulos. No primeiro, trata-se de uma introdução ao trabalho, onde o assunto é tratado como um todo. Mostrando sua contextualização, problematização, importância do tema, objetivo principal, e metodologia utilizada para o levantamento de dados. No segundo capítulo, breve histórico sobre o assunto, o que são as redes sem fio, seus padrões e componentes. No terceiro, é apresentado alguns equipamentos mais comuns utilizados em redes wireless. No quarto, uma passagem rápida de como ela funciona aos olhos do computador. No quinto capítulo, forma de implementar e pontos a serem levados em conta antes de montar uma rede sem fios. No sexto, como migrar de uma rede por cabos para uma sem fios. No sétimo, gastos médios estipulados. No oitavo é demonstrado pontos importantes sobre a segurança do sistema de redes wireless. No nono e último capítulo, a conclusão geral do trabalho de conclusão de curso.

2 Breve Histórico

Os primórdios do que hoje chamamos de tecnologia wireless, ou tecnologia que utiliza ondas de rádio para transmissão de dados entre dispositivos, ocorreu no final do século passado, e envolveu uma série de descobertas e avanços científicos que foram sendo desenvolvidos, onde o resultado final é uma rede de comunicações global e uma imensa malha de redes disponíveis em variados espaços públicos, empresas, e já na casa de muitas pessoas, inclusive aqui no Brasil.

Há muitas versões sobre o início da tecnologia wireless, sendo que cada busca enfatizar uma visão do que trata a tecnologia e do que o conceito wireless representa. O início mais focado por livros e cursos é o envio de códigos Morse por Marconi em 1901, mas vários outros marcos são utilizados, como a descoberta da indução eletromagnética por Faraday em 1831 e a demonstração pública de Tesla em 1893, e podem ser citados como sendo início dessa tecnologia, portanto estaremos traçando uma linha do tempo, com uma análise posterior de onde o início do wireless poderia ser posicionado.

1831 – Michael Faraday descobre os princípios da indução eletromagnética.

1842 – Joseph Henry descobre que uma faísca elétrica entre dois condutores pode ser utilizada para induzir magnetismo entre agulhas, esse efeito é detectado a uma distância de 30 metros.

1858 – Feddersen descobre o caráter oscilatório das faíscas elétricas.

1867 – James Clarck Maxwell desenvolve sua teoria do eletromagnetismo e prediz a existência de ondas elétricas no éter.

1870 – Von Bezold descobre a interferência com descargas de compensadores.

1875 – Thomas Edison nota um fenômeno que denominou “força etérica”, mas abandonou a idéia quando Elihu Thompson, dentre outros, ridicularizaram a idéia.

1879 – David E. Hughes descobre que um tubo de arquivamentos férreos fica condutivo por ação à distância através de faíscas elétricas, ele faz um sinal audível em um fone em uma distância de 500 metros, mas parou suas experiências, pois Sir George Stokes julgou que os acontecimentos demonstravam indução simples.

1882 – Graham Bell e William H. Preece transmitem sinais de Telégrafo Wireless através do mar por meios de indução, entre a Inglaterra e a Ilha Wight.

1887 – Heinrich Rudolph Hertz, professor privado em Kiel, descobre que o efeito de faíscas elétricas está baseado nos fenômenos das ondas no éter. Ele confirmou a teoria de Maxwell, onde as ondas viajam pela mesma velocidade de luz.

1890 – Branly chama a atenção às propriedades de tubos com arquivamentos férreos que foram redescobertos e desenvolve o primeiro coherer para detectar ondas de rádio.

1892 – Preece sinaliza no canal de Bristol com seu sistema de indução.

1893 – Tesla demonstra publicamente a comunicação wireless via rádio em St. Louis, descrevendo em detalhes os princípios da comunicação via rádio.

1894 – Ledge repete os testes de Herz com um coherer.

1895 – em seqüência, Tesla encontra sinais de recebimento das telegrafias de seu laboratório em Nova Iorque em West Point, Marconi transmite o primeiro telégrafo, e Popoff constrói um receptor para ondas elétricas naturais onde tenta descobrir temporais.

1896 – Marconi demonstra a telegrafia wireless ao escritório de telégrafo inglês, após um ano testando na Itália. Ele prova as possibilidades de telegrafia sem fios com um coherer.

1897 – Marconi adquire a patente do telégrafo wireless e estabelece a primeira "Estação Marconi" em Needles (Ilha Wight), esta estação envia um sinal à costa inglesa a mais de 22 km.

1898 – em 3 de junho é enviado a primeira telegrafia wireless paga, enviada de Needles, e em 20 julho, a primeira mensagem de jornal é enviada de um navio para o Daily Express sobre os resultados de uma competição de navegação.

1901 – Marconi usa sintonia entre os receptores e transmissores, e em 12 e 13 dezembro, primeiros sinais são enviados pelo Oceano Atlântico de Poldhu para New Foundland (2800 km).

1902 – Marconi desenvolve o detector magnético, e há a primeira comunicação bidirecional através do Atlântico.

1903 – Schlömilch desenvolve o detector eletrolítico, Poulsen descobre a transmissão de ondas contínuas com um arco elétrico, e surge o primeiro serviço de notícias para navios em mar, o "Serviço Marconi" wireless de Londres para o "Handelsblad" holandês. (...)

1971 – Primeira rede wireless, a Alohanet, na Universidade do Hawaii.

O prêmio Nobel da física de 1909 e a patente foram conferidas à Marconi, porém a descoberta do rádio ocorreu no mesmo ano que um russo, Popoff, fazia experimentos para a detecção de tempestades utilizando a mesma tecnologia, e há um impasse sobre a descoberta, mesmo sendo universalmente aceita como sendo dos EUA.

Além disso, em 1983, Tesla demonstrara publicamente uma transmissão via rádio. Devido esses fatos, e ao do governo dos EUA não desejar pagar pela utilização das patentes de Marconi na Primeira Guerra Mundial, em 1943 a patente foi transferida para Tesla, poucos anos após sua morte.

Diversos livros e cursos apresentam uma história bem descrita no final da linha do tempo, mas pobre em seu início, e falham em descrever como a comunicação wireless começou. Aqui podemos ver que as comunicações wireless datam de bem antes da primeira rede, a Alohanet, ter sido formada, ou da primeira comunicação via celular, que aconteceu em 1946 pela NTT do Japão.

Partindo da definição de wireless, que é a de dados se propagando via ondas de rádio, as descobertas e testes de transmissão via indução não podem ser considerados, e as teorias sobre o a aplicação do rádio não podem ser utilizadas, até terem sua aplicação confirmada para o fim proposto no significado. Assim, partimos direto para a utilização das ondas de rádio.

A aplicação de Tesla em 1983, no Franklin Institute of Philadelphia e no National Electric Light Association, continha todos os elementos antes da invenção da válvula de osciloscópio. Tesla foi o primeiro a aplicar o mecanismo da condução elétrica para finalidades wireless. Ele utilizou receptores eletromagnéticos, que eram versões

anteriores dos cohereres utilizados por Marconi em tempos mais recentes. Após essa demonstração, os princípios da comunicação via rádio (envio de sinais de rádio para serem captados por receptores) ficaram comprovados e amplamente conhecidos.

As redes sem fio, segundo ADAM ENGST E GLENN FLEISHMAN (2005) iniciou-se de um projeto que ligou as universidades do Havaí em 1971, que conectavam os computadores de quatro ilhas. Elas entraram para o uso da computação pessoal em 1980, quando a idéia de compartilhar dados entre computadores começava a se tornar popular.

As primeiras redes sem fio baseadas em ondas de rádio ganharam notoriedade no início dos anos 90, quando os processadores se tornaram mais rápidos a ponto de suportar tal aplicação. As redes existentes na época eram patenteadas e incompatíveis, por isso, no meio da década de 90 as atenções se voltaram para o novo modelo do IEEE (*Institute of Eletrical and Eletronic Engineers*), o 802.11. (ENGST & FLEISHMAN, 2005)

Em 1999 o IEEE finalizou o padrão 802.11b (11Mbps a 2,4GHz). Em 2002, foi distribuído ao mercado o 802.11a (54Mbps a 5GHz), que é incompatível com o padrão 802.11b. No mesmo ano, foi ratificado o padrão 802.11g (54Mbps a 2,4GHz), que opera na mesma velocidade do 802.11a e na mesma freqüência do 802.11b. (ENGST & FLEISHMAN, 2005)

Concluí-se que a história do wireless trata de descobertas que iniciou no século passado, e envolve a contribuição de vários pesquisadores, que não são menos ou mais importantes umas quanto às outras, e não deveriam ser ignoradas ou simplificadas a ponto de obscurecer a trajetória de vários desses notáveis pesquisadores em detrimento da aplicação comercial por Marconi, que foi importante, mas de forma alguma a única.

Atualmente este tipo de rede já se tornou bem popular, e seu futuro parece ser ainda mais difundido do que no atual presente.

Apesar da facilidade de uso deste tipo de rede, suas vulnerabilidades devem ser tratadas de forma a melhorar a proteção da rede.

3 Equipamentos mais Comuns

Segundo ARTHAS (2004), a topologia de uma rede IEEE 802.11 é composta pelos seguintes elementos:

BSS - *Basic Service Set* - corresponde a uma célula de comunicação *wireless*.

STA - *Stations* - são as estações de trabalho que comunicam-se entre si dentro da BSS.

AP - *Access Point* - funciona como uma *bridge* entre a rede *wireless* e a rede tradicional. Coordena a comunicação entre as STA dentro da BSS. Existem APs que também atuam como roteador, possibilitando o compartilhamento de *Internet* pelos outros micros da rede. Eles vêm de fábrica como servidores DHCP (*Dynamic Host Configuration Protocol*), facilitando a obtenção de um endereço IP na rede. Também conhecido como concentrador.

Bridge - Faz a ligação entre diferentes redes, por exemplo, uma rede sem fio para uma rede cabeada convencional..

ESS - *Extended Service Set* - consiste de várias células BSS vizinhas que se interceptam e cujos AP estão conectados a uma mesma rede tradicional. Nestas condições uma STA pode movimentar-se de um BSS para outro permanecendo conectada à rede. Este processo é denominado *Roaming*.

Dois modos de operação são previstos:

Infrastructure mode - quando existe a presença de um AP coordenando a comunicação entre as estações de uma célula (BSS). (ARTHAS, 2004)

Ad-Hoc mode - quando não existe AP e as estações se comunicam entre si diretamente. Este modo não é recomendado pelo padrão. (ARTHAS, 2004)

Existem vários tipos de hardwares para acessar uma rede sem fio, como placas USB (externas), placas PCI(internas), Mini PCI (internas para notebooks), PCMCIA (internas para notebooks) e adaptadores de placas *Ethernet*.

4 Como Funciona

Segundo ENGST & FLSIESHMAN (2005), palavra *Wireless* significa SEM FIO, ou seja, são redes cujos cabos são substituídos por ondas de rádio. Sua utilização é muito simples, assim como sua instalação, o que ajuda a proporcionar seu crescente uso nos dias de hoje.

Existem vários tipos e padrões de redes *wireless*, como por exemplo, o *WiMax*, *Bluetooth*, *Wi-Fi*(*Wireless Fidelity*), *InfraRed*(Infravermelho). (ARTHAS, 2004)

Uma rede *wireless* é reconhecida por ser sem fio, pois o transmissor e o receptor estão se comunicando sem a presença de fios, no nosso caso, por ondas de rádio. (ENGST & FLEISHMAN, 2005)

Encaixam-se nessa categoria os seguintes tipos de rede: Locais Sem Fio ou WLAN (*Wireless Local Area Network*), Redes Metropolitanas sem Fio ou WMAN (*Wireless Metropolitan Area Network*), por exemplo o WiMAX (*Worldwide Interoperability for Microwave Access*), 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*). (ARTHAS, 2004)

Segundo TEIXEIRA (2005), o WiMAX, que utiliza o padrão IEEE 802.16, foi ratificado em Dezembro de 2001, estava focando basicamente as faixas de frequências situadas entre 10GHz e 66GHz considerando sempre aplicações com linha de visada, obtendo até 34Mbps.

Conforme ENGST & FLSIESHMAN (2005), a grande vantagem em instalar uma rede sem fio é a mobilidade. Há alguns anos, um cenário onde permitia-se que as pessoas pudessem desfrutar da conectividade de uma rede sem a necessidade de fios era um tanto quanto futurista. Hoje a realidade mudou.

As redes sem fio nos proporcionam a mesma conectividade de uma rede cabeada comum dentro do perímetro de alcance da rede, tornando possível que aquele e-mail que não poderia esperar por resposta possa ser respondido no meio de uma reunião ou até mesmo no meio do almoço.

Segundo publicado na revista INFO Exame (Coleção 2005 – *Wi-Fi*) pela jornalista Débora FORTES (2005), algumas empresas, como a CISCO, estão adotando novas políticas de uso para este tipo de rede, como manter os *laptops* fechados durante uma reunião.

Segundo ARTHAS (2004), quando se discute a configuração de uma WLAN existem alguns padrões, desenvolvidos ou em desenvolvimento pelo IEEE (*Institute of Electrical and Electronic Engineers*) que devem ser considerados:

IEEE 802.11a: é o padrão que descreve as especificações da camada de enlace e física para redes sem fio que atuam na frequência de 5GHz. Apesar de ter sido firmado em 1999 não existem muitos dispositivos que atuam nesta frequência.

IEEE 802.11b: descreve a implementação dos produtos WLAN mais comuns em uso atualmente. Este inclui aspectos da implementação do sistema de rádio e também inclui especificação de segurança. Esta descreve o uso do protocolo WEP (*Wired Equivalency Privacy*). Trabalha na ISM de 2.4 GHz e prove 11 Mbps. Foi aprovado em julho de 2003 pelo IEEE.

IEEE 802.11g: descreve o mais recente padrão para redes sem fio. Atua na banda ISM de 2.4 GHz e provê taxas de transferências de até 54 Mbps.

IEEE 802.11i: trata-se um grupo de trabalho que está ativamente definindo uma nova arquitetura de segurança para WLANs de forma a cobrir as gerações de soluções WLAN, tais como a 802.11a e 802.11g.

IEEE 802.11e: fornece melhoramentos ao protocolo 802.11, sendo também compatível com o 802.11b e 802.11a. Os melhoramentos incluem a capacidade multimídia feita possível com a adesão da funcionalidade de qualidade de serviços (QoS – *Quality of Service*), como também melhoramentos em aspectos de segurança. 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*). 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.

Segundo ARTHAS (2004), os grupos do IEEE que estão desenvolvendo outros protocolos são:

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 802.11f – 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.

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.

5 Implementação

Nos últimos anos, verificou-se um crescimento explosivo das “Wireless LANs”, devido ao enorme marketing feito pelos fabricantes baseando-se no principal triunfo que é a mobilidade. Outra vantagem seria, em adição àquela é a facilidade de instalação. Entretanto, para se implementar uma rede local sem fio deve-se ficar atento a diversos fatores. É necessário um projeto bastante detalhado.

O planejamento de uma rede sem fio pode durar poucos dias ou mesmo semanas, dependendo da complexidade e funcionalidades exigidas pelo seu cliente. Esse é um processo passo a passo, em que o projetista da rede deve descobrir/pesquisar características que podem ser divididas em seis grupos:

Análise do ambiente – Primeiramente deve se analisar o ambiente em será implementada a rede sem fio. Pode-se citar um escritório em que 20 pessoas farão uso da rede, uma residência com poucos computadores, um aeroporto, ou mesmo um hospital que se caracteriza como o mais complexo ambiente para a instalação de uma rede sem fio devido aos equipamentos radiológicos, portas de incêndio, longos corredores, elevadores e usuários móveis. Além da diferença do tamanho da rede, deve-se levar em conta a quantidade de usuários existentes na rede, nível mínimo de segurança exigido, largura de banda desejada, impacto que a rede terá sobre o ambiente, etc.

Infra-estrutura existente – Há uma rede (cabada ou sem fio) existente no local? O projetista deve ter muita atenção nesse item pois se houver uma rede já existente, uma documentação detalhada deve existir contendo itens como o hardware utilizado, a frequência que está sendo usada (caso seja uma rede sem fio), número de usuários, política de segurança implementada, sistema operacional de rede em uso, convenção de nomenclatura dos equipamentos, topologia da rede, etc.

Localização do ambiente – Após uma análise do ambiente, já se sabe em que local será instalada a rede. Será em um ambiente “indoor”, “outdoor” ou ambos. Em ambientes “outdoor” como ligação entre prédios, pode-se ter inúmeras situações e obstáculos que dificultem a instalação e manutenção de uma rede sem fio. Obstáculos como: árvores, montanhas, prédios, e condições climáticas desfavoráveis como: fortes chuvas, ventos e neve podem enfraquecer ou mesmo eliminar o sinal de transmissão. Pode-se fazer o uso de uma torre para superar tais obstáculos, requerendo um projeto de engenharia, um estudo do local onde será instalada a torre, assim como a permissão de órgãos especializados dependendo da altura necessária. Em ambientes “indoor” como escritórios, fábricas e galpões a implementação da rede sem fio torna-se mais fácil por não possuir obstáculos naturais e pela limitação nas distâncias.

Finalidade do negócio – A instalação de uma rede sem fio deve atender as necessidades de negócio do cliente. Portanto, é de crucial importância saber a finalidade da implementação da rede sem fio. Pode-se citar dois exemplos. Primeiro, a criação de um escritório temporário para conectividade dos jornalistas na cobertura de uma Olimpíada. Nesse caso, a rede deve ser de alta velocidade (802.11a) com taxa de transmissão de até 54 Mbps, devido à enorme quantidade de informação que irá trafegar assim como o grande número de usuários se beneficiando da rede ao mesmo tempo. Segundo exemplo, um escritório em que somente trafegariam na rede: arquivos, imagens, emails, etc, não necessitando de uma rede sem fio de alta velocidade. Enfim, deve-se analisar quais aplicações serão utilizadas pelos usuários.

Recursos disponíveis – A cada dia, o preço dos equipamentos de rede sem fio vem caindo gradativamente, isso faz com que mais empresas invistam na implementação das redes sem fio. Entretanto, na fase de planejamento, é viável e necessário saber do cliente quais recursos estão disponíveis. Recursos financeiros, profissionais qualificados e tempo alocado para a execução do projeto são os mais importantes.

Nível de segurança – A segurança é um dos fatores que mais influenciam na decisão de se adotar uma nova tecnologia. E com as redes sem fio, essa preocupação não é diferente. Pelo contrário, deve se utilizar todas as ferramentas disponíveis para se

obter o nível mínimo de segurança. O projetista deve explicar ao cliente que as redes sem fio são mais vulneráveis que as redes cabeadas por não possuírem fronteiras de transmissão das ondas de rádio. Baseado nisso, é viável seguir a política de segurança empregada na empresa como a utilização de rede virtual privada.

Após um levantamento detalhado das necessidades do cliente, o projetista deve ter em mãos toda a documentação da análise realizada. Esse documento servirá como um mapa para a implementação da rede e também para uma futura referência aos técnicos e administradores. Caso o planejamento de uma rede sem fio seja feito de forma inapropriada, a rede pode não funcionar adequadamente e o cliente pode gastar muito dinheiro em hardware e software e não ter suas necessidades atendidas. A fase de planejamento pode demorar mas é o passo mais importante na implementação de uma rede sem fio.

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 à 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 frequência 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 uma verdadeira barreira.

* Microondas

A lógica é a mesma dos aparelhos de telefone sem fio. Os microondas também usam a disputada frequência 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 e as máquinas 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.

6 Migração

Para migrar de uma rede com fios para uma wireless deve-se observar alguns fatos para somente depois iniciar a implementação.

- Quantos desktop e notebooks terão acesso sem fio a rede

- Qual a área a ser coberta. O responsável do local já possui planta baixa impressa desta área. Caso positivo, o projetista deve ter muita atenção nesse item, uma documentação detalhada deve existir contendo itens como o hardware utilizado, número de usuários, política de segurança implementada, sistema operacional de rede em uso, convenção de nomenclatura dos equipamentos, topologia da rede, etc. Caso negativo, é interessante avaliar estes pontos a partir do início.

- Se já houver um local pré-definido para a colocação do ponto de acesso, verificar a existência de tomada elétrica estabilizadora e ponto de rede de dados neste local específico.

- Definir um dos padrões a utilizar: 802.11a, 802.11b ou 802.11g

- Ter em mente que, dependendo da potência da antena no apartamento, a rede doméstica pode abranger uma área muito maior que apenas a da casa. Com isto a rede pode ser utilizada sem o conhecimento ou ter o tráfego capturado por vizinhos ou pessoas que estejam nas proximidades da casa. Alterar configurações padrão que acompanham o seu ponto de acesso. Alguns exemplos são:

- Alterar as senhas. Usar senhas difíceis, 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 ponto de acesso. 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);

- Desligar o ponto de acesso 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.

7 Gastos

A primeira coisa à enfatizar é, “O que é preciso, exatamente?” Muitas pessoas migram para Rede sem fios por sua relação custo-benefício comparada a uma rede cabeada. Em algumas instâncias uma rede cabeada é cara demais para ser instalar. Embora uma rede de Rede sem fios tenha bom custo-benefício, há assuntos que precisam ser considerados como alcance de sinal, velocidade de rede e interferência.

Com ponto de partida para os gastos foi levado em conta equipamentos básicos para montar uma rede 802.11b/g de 11/54Mbps, em uma pequena e objetiva pesquisa de mercado atual levando em consideração as marcas e modelos mais conhecidos e usados.

- Access Point

Preço: R\$ 320,00

- Placa de Rede Wireless PCI

Preço: R\$ 190,00

- Cartão Pcmcia 11mbps 802.11b 2.4GHz

Preço: R\$ 198,00

- Adaptador Wi-Fi USB 802.11g USB

Preço: R\$ 129,00

8 Segurança

Este tipo de rede, por ser realizada através de ondas de rádio, não se limita ao perímetro onde se encontra o ponto de acesso, atravessando paredes o sinal pode chegar a alcançar a área externa do estabelecimento, facilitando o acesso indevido. Para se evitar que um computador alheio obtenha acesso indevido a rede ou capture as informações ali trafegadas, este capítulo demonstra os métodos e ações que podem ser implementados em busca de assegurar uma maior confiabilidade e autenticidade, se utilizando, por exemplo, de criptografia como o WEP (*Wired Equivalency Privacy*) ou o WPA (*Wi-Fi Protected Access*), assegurando a confiabilidade das informações. Para assegurar a autenticidade dos usuários, utilizar um servidor RADIUS (*Remote Authentication Dial-In User Server*), autenticando os usuários que podem acessar a rede.

Devido à simplicidade de uso e de configuração, a segurança tem sido o elemento mais preocupante neste tipo de rede, pois uma pessoa mal intencionada pode obter acesso de modo fácil utilizando uma antena, por exemplo, feita com uma lata tubular com papel alumínio e softwares específicos para cada situação.

Uma rede wireless utilizando, por exemplo, o padrão IEEE 802.11g obtém velocidade nominal de 54mbps com um alcance, também nominal, de 100m.

Para se estabelecer uma rede sem fio é preciso no mínimo, no modo estruturado, um Access Point (AP) e um dispositivo (USB, PCI, PCMCIA) que acesse o AP.

Este tipo de rede é excelente para locais onde uma rede cabeada comum não se encaixaria, obrigando a mudar todo o layout do local.

Mobilidade é a palavra chave que caracteriza este tipo de rede.

Porém, é um novo ambiente, onde novos tipos de ataques surgem, forçando então a criação de mecanismos de defesa para esta aplicação.

É aconselhável evitar que o sinal da rede sem fio ultrapasse os limites físicos do local onde ela opera, evitando que um atacante se posicione fora dos limites físicos do local, aumentando assim o conforto do mesmo.

Para evitar que o sinal saia dos limites físicos a posição do AP é essencial, existem locais onde não há como evitar este tipo de falha, mas é uma precaução a ser estudada.

Para uma rede sem fio caseira ou de um escritório pequeno, é indicado utilizar o primeiro padrão de criptografia desenvolvido, o WEP.

O WEP trabalha com chaves simétricas, ou seja, a mesma chave é sempre utilizada para encriptar e desencriptar as informações que serão trafegadas na rede.

Sua principal desvantagem é exatamente esta, pois um atacante que deseja ter acesso à rede pode, por meio de escuta, obter a chave, tornando possível a desencriptação dos dados da rede.

Outra desvantagem significativa é que a chave deve ser conhecida por todos aqueles que acessam a rede, o que pode facilitar a disseminação ilegal da mesma.

Para corrigir as vulnerabilidades apontadas no WEP, foi criado o WPA, protocolo de criptografia mais robusto do que o anterior.

No WPA existe um protocolo chamado TKIP, que é responsável pelo gerenciamento das chaves temporárias, podendo alterar as chaves a cada pacote, dificultando ainda mais a escuta do tráfego da rede.

No WPA existe também um protocolo chamado EAP, responsável por permitir uma autenticação de usuário. Utilizando um servidor RADIUS para autenticar usuários a rede fica restrita apenas às pessoas que possuem uma conta cadastrada no servidor.

A segurança aumenta com a autenticação de usuários, porém, por utilizar novos recursos, como bancos de dados e servidores, aumenta-se a possibilidade de um ataque diretamente em cada recurso separadamente.

A criptografia tem como meta proteger as informações trafegadas na rede, mas, existem outros modos de se melhorar a segurança de uma rede sem fio, que devem ser utilizados em conjunto com a criptografia para se obter maiores níveis de segurança.

Alguns APs possuem um servidor DHCP (Dynamic Host Configuration Protocol) incluso, fazendo com que qualquer pessoa que tente entrar na rede obtenha um endereço IP válido, permitindo seu acesso.

Desabilitar o envio do SSID (Nome da Rede), deste modo, uma pessoa que queira se conectar a rede é obrigada a saber o SSID do AP para então estabelecer uma conexão. Este recurso não é efetivo por si só, já que uma pessoa interessada em atacar pode capturar pacotes e identificar a rede.

Listar os endereços MAC permitidos é um recurso que pode ser utilizado em paralelo com todos os outros já citados, ele autentica apenas o aparelho que utiliza a rede, tornando possível que qualquer pessoa utilize a rede por meio de um aparelho permitido.

Existem meios de se alterar um endereço MAC de uma placa, após um atacante escutar o tráfego e obter um endereço MAC válido ele consegue alterar o endereço de sua placa e obter o acesso a rede.

Após associar todas as formas de segurança já citadas, a rede sem fio se torna mais segura internamente, porém, ainda vulnerável a ataques externos vindos do meio público (Internet).

Para bloquear conexões indevidas, utiliza-se um firewall na saída da rede ou mesmo em cada dispositivo que utiliza a rede. Deste modo, dificulta-se o acesso indevido pelo meio externo.

Utilizar um antivírus sempre atualizado, para evitar que pragas virtuais possam se instalar na rede e abrir portas para intrusos remotos. Um antivírus evita também que um programa de código malicioso faça com que a rede seja comprometida de forma a contaminar arquivos vitais dos sistemas operacionais.

Utilizar VPN nas ligações externas da rede evita que o tráfego que sai dos AP seja capturado por um atacante.

Proteger apenas a rede sem fio em seu ambiente interno não é o suficiente para se garantir a privacidade dos dados trafegados, pois, os dados entram e saem do ambiente seguro, tornando o ambiente externo como foco para ataques.

9 Conclusão

Este trabalho conclui que uma rede sem fio é de extrema facilidade de uso e configuração, possibilitando uma mobilidade excelente que pode ser utilizada como diferencial para as empresas e residências.

Sua implantação é simples, descartando a necessidade de grandes reformas onde uma rede cabeada precisaria estar passando fios por paredes ou canaletas especiais, devido a esta facilidade, o uso deste tipo de rede atrai cada vez mais usuários.

Como todo ambiente lógico não é totalmente seguro, as redes sem fio têm suas vulnerabilidades, atualmente existem vários processos que ajudam a tornar um ambiente Wireless seguro, mesmo não garantindo que a rede seja totalmente segura.

Esta pesquisa não encontrou motivos para não utilizar uma rede sem fio, elas são versáteis e úteis em muitos casos, desde que se faça uso de seus métodos e ações para garantir a privacidade e qualidade das informações transitadas e aumentar a sensação de que o ambiente sem fio é seguro.

Utilizando os métodos explanados no capítulo 5 ao 8, ou seguindo as orientações do fabricante é possível se obter um nível satisfatório de qualidade e segurança, respeitando as limitações técnicas e econômicas do usuário.

Referências Bibliográficas

ARTHAS, Kael. **Tutorial Wireless**. 2004. Disponível em:

<http://www.babooforum.com.br/idealbb/view.asp?topicID=269602> . Acessado em: 25/12/2009

BABOO, Fórum. **5. Ataques às Redes Sem Fio**. 2005. Disponível em:

<http://www.babooforum.com.br/idealbb/view.asp?topicID=335352> . Acessado em: 14/12/2009.

CERT. **Práticas de Segurança para Administradores de Redes *Internet***, 4.13.6.

Monitoração da Rede *Wireless*. 2003. Disponível em: <http://www.cert.br/docs/seg-adm-redes/seg-adm-redes.html#sec1> . Acessado em: 01/11/2009

ENGST, Adam; FLEISHMAN, Glenn. **Kit do Iniciante em Redes Sem Fio: O guia prático sobre redes *Wi-Fi* para Windows e Macintosh**. 2ª ed.: São Paulo. Ed.: Pearson Makron Books. 2005

PATRICK. **História e Perspectivas, O Início da Tecnologia Wireless**. 2006. Disponível em <http://www.mundowifi.com.br/forum/thread63.html> . Acessado em 25/12/2009

TEIXEIRA, Edson Rodrigues Duffles. **Tutoriais: Banda larga e VOIP**. 2005. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialwimax/default.asp> . Acessado em: 04/10/2009.