UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
ESCOLA DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELETRÔNICA E COMPUTAÇÃO

Análise da Viabilidade de Uso de um Sistema de Acesso Wireless para Banda Larga (IBL)

Autor:

_____

Luiz André de Carvalho

Orientador:

_____

DSc. Ricardo Rhomberg Martins

Examinador:

_____

MSc. Mauros Campello Queiroz

Examinador:

_____

DSc. Fernando Antônio Pinto Barúqui

DEL
Agosto/2004

Dedicatória

Dedico este projeto a todos que de alguma forma me ajudaram a concluir esta etapa da minha vida sem que eu me preocupasse com mais nada além dos estudos. Principalmente minha família.

Agradecimento

É com imenso prazer que venho expressar o meu agradecimento a todas as pessoas que contribuíram para a realização deste projeto, ajudando-me a concluir o meu curso superior.

Agradeço a todos os professores de DEL, que me ajudaram no decorrer deste projeto, orientando-me em todas as partes do seu desenvolvimento.

E ao meu professor orientador, Ricardo Rhomberg Martins, que me ajudou a concluir esta etapa da minha vida.

Resumo

Este trabalho analisa a viabilidade de um sistema de acesso Wireless para banda larga. O projeto inclui uma breve teoria sobre a tecnologia, abrangendo também os recursos, equipamentos, vantagens, desvantagens, infra-estrutura do projeto, tipos de ligação, e uma análise sobre segurança e plano de atribuição,destinação e distribuição de faixas de freqüências no Brasil.

Palavra-Chave:

- Conceito de Redes
- Conhecimento em projetos de sistema de Antenas
- Fundamentos de leis de espectros de frequência
- Lógica digital
- Interface Hardware/Software

Índice

Capítulo 1 - Introdução

As redes broadband ou de banda larga já são uma realidade nos países com telecomunicações ditas do primeiro mundo. A demanda por grandes volumes de informações entregues a enormes velocidades e, uma exigência cada vez maior oriunda do mundo dos negócios, da mídia, dos governos, das redes cientifica e tecnológicas e da Internet, tem estimulado o crescimento dessas redes e o desenvolvimento das mais variadas tecnologias nestas áreas.

Como conseqüência, inúmeras redes estão sendo construídas, utilizando tecnologias desenvolvidas para broadband como MMDS, LMDS, satélites em suas bandas mais altas, cabos coaxiais e de fibra óptica, Digital Home Platform transmitidas por emissoras de tv Digital e outros.

No Brasil, a utilização de transmissão em broadband ainda caminha devagar. Seu crescimento esta sendo estimulado pelo aparecimento dos primeiros modelos de parcerias entre provedores de acesso de Internet de alta velocidade e de conteúdo de broadband bem como ao crescimento da demanda de Pay TV, e o crescimento das redes corporativas de grande porte.

A curto e médio prazo além do crescimento das redes de Pay TV e das redes corporativas, o maior crescimento se dará no mercado de Internet de alta velocidade com a oferta de inúmeros serviços como sites coorporativos, serviços de informações, e-commerce e outros.

Sendo um mercado recém criado, ainda em fase de implantação, ninguém espera colher resultados antes de 2 anos quando se espera estar implantada uma base sólida de assinantes para estes serviços.

As redes de transmissão e distribuição de conteúdo broadband utilizado no Brasil utilizam técnicas de wireless e de rede fixa. As redes wireless utilizam na sua rede de transmissão Sistemas de Microondas de alta capacidade ou transponders de Satélites e nas redes de distribuição utilizam sistemas MMDS, LMDS, Satélites DTH (direct to home) e mais recentemente sistemas digitais de radiodifusão de som e imagem.

As redes wireless broadband tem tendência a um grande crescimento inicial mas vão encontrar limites no futuro para a sua expansão. Apesar da recente abertura de novos canais na faixa mais alta do espectro de radio freqüência, bem como o aumento considerável dos canais de radiodifusão com a introdução da TV digital, isto se dara

pela natural limitação física da capacidade das faixas e canais disponíveis no espectro de radio freqüência.

Tal tendência não acontece com as redes físicas de transmissão e distribuição constituídas de cabos ópticos. Com o desenvolvimento da nova tecnologia DWDM - wavelenght Division Multiplex -multiplexação dos sinais ópticos por comprimentos de onda, cada fibra óptica do cabo passa a contar com inúmeras freqüências portadoras, constituindo cada freqüência portadora um novo canal (fibras virtuais). Isto possibilita ampliação da capacidade do cabo de fibras ópticas a níveis enormes, proporcionais ao desenvolvimento desta tecnologia, (aumento do numero de freqüências portadoras e das janelas de transmissão da fibra óptica) tornando o aumento da capacidade da rede broadband enorme mas difíceis de quantificar na atualidade pois vai depender do estado da arte.

Ou seja o aumento da capacidade de transmissão e distribuição das fibras ópticas através de suas janelas de transmissão fica dependente dos equipamentos terminais e repetidores mas as instalações físicas permanecem as mesmas.

Como conseqüência as empresas que querem rapidamente acessar o mercado constroem primeiro a sua rede broadband na forma wireless, dada a velocidade de instalação e inicio de operação; enquanto paralelamente constroem a sua rede óptica de grande extensão, para depois integrar as duas de acordo com a sua conveniência e demanda do mercado no momento.

A velocidade de construção dessas redes físicas, pode ser entretanto retardada por dificuldades na obtenção dos direitos de passagem, em áreas de propriedade de terceiros ou pelo não uso de infra-estruturas adequadas existentes ao longo das rotas. Tal utilização reduz enormemente os recursos em investimentos necessários bem como o tempo de construção da rede.

Há 3 anos, as concessionárias públicas estatais, obtinham o direito de passagem em áreas privadas a custa de desapropriação da faixa da propriedade pelo estado, ou a sua compra pela operadora; e a utilização da infraestrura de outra concessionária publica de qualquer serviço por simples e rápidos acordos.

Após a privatização dessas concessionárias públicas o enfoque dos novos proprietários, passou a ser maximificar a utilização de sua infra-estrutura, alugando o excedente de sua capacidade, ou investindo para ingressar através de subsidiarias no setor de serviços de telecomunicações; tendo em vista a política governamental de iniciar no Brasil a partir do ano 2001 o processo de competição global, na área.

A Legislação de telecomunicações é clara. As subsidiárias dessas empresas podem atuar no mercado de telecomunicações, desde que construam suas redes e solicitem uma licença de serviço a Anatel.

A vantagem na construção de Redes Broadband por detentores de infra-estrutura apropriada ou direito de passagem é enorme. Aproximadamente de cada 1 milhão de dólares investidos na rede, 700 mil são gastos em obras civis e apenas 300 mil refere-se a custos de instalação de cabos. Assim essas empresas podem constituir redes com custos 70% inferiores; o que os demais detentores de concessões de serviços de redes e que estão construindo suas redes próprias consideram uma competição desleal.

Com aumento da demanda, os preços de utilização desses domínios subiram e as restrições veladas à cessão da infra-estrutura aumentaram. Os conflitos entre as partes se iniciaram, reduzindo a velocidade de implantação de novas redes de telecomunicações.

Assim em novembro de 1999, visando a reduzir esses conflitos e acelerar o processo em suas áreas a ANATEL (Agência Nacional de Telecomunicações) a ANEEL (Agência Nacional de Energia Elétrica) e pela ANP (Agência Nacional de Petróleo), elaboram um regulamento, cujo objetivo foi estabelecer as diretrizes para o compartilhamento de infra-estrutura dos setores de energia elétrica, telecomunicações e petróleo. O Regulamento pretende garantir às operadoras de telecomunicações o acesso isonômico, e a preços justos, a postes, dutos, torres e meios de transmissão.

É uma idéia difícil de colocar em pratica porque as empresa dos setores elétricos, de petróleo e de gás e mesmo as concessionárias de rodovias e ferrovias privadas, que detém infra-estrutura ou direitos de passagem tem estratégias próprias para atuar no mercado de telecomunicações. Algumas estão ocupando a sua infra-estrutura, na prática seja porque há espaço limitado em algumas delas, ou seja porque estão chegando primeiro para que, com suas próprias redes, atender à demanda futura do mercado de broadband.

O regulamento para o compartilhamento de infra-estrutura, emitido pelos três órgãos reguladores do governo em novembro de 1999 define os itens passíveis de compartilhamento em três classes: Servidões administrativas, dutos e torres, e cabos coaxiais e fibras não ativadas. Com relação ao compartilhamento, este se dará pela utilização da capacidade excedente do detentor da infra-estrutura ou da servidão que o manterá sob seu controle e gestão.

O compartilhamento só poderá ser negado por razões de limitação na capacidade, segurança, estabilidade, confiabilidade, violação de requisitos de engenharia ou de cláusulas pré-estabelecidas.

O regulamento estabelece também alguns itens do contrato a ser estabelecido entre as partes, entre outros: condições da cessão, proibição de sub locação da infra-estrutura ou de sua utilização para fins não previstos no contrato sem a prévia anuência do Detentor, bem como as condições técnicas relativas à implementação, segurança dos serviços e qualidade.

Os preços a serem cobrados e condições comerciais, podem ser negociados livremente pelos agentes, observados os princípios da isonomia e da livre competição. Os custos de adaptação ou modificação na infra-estrutura compartilhada são de responsabilidade das partes que se beneficiarem da modificação.

Os segmentos rodoviários e os Municípios, até a pouco ausentes da questão e que dispunham de uma excelente boa vontade na cessão de sua infra-estrutura ou direitos de passagem, em face da crescente demanda, passaram também a emitir as suas regulamentações, no sentido de comercializar a cessão ou aluguel de seus domínios.

O Departamento Nacional de Estradas de Rodagem DNER emitiu uma portaria em 1999 que isenta, provisoriamente, as concessionárias de outros serviços públicos do pagamento de licença para a travessia de alguns tipos de redes pelas rodovias federais. Por outro, com relação à utilização (e não travessia) da faixa de domínio, outras portarias de 1999 estabelecem a cobrança de licença a concessionárias de telecomunicações de serviços públicos e privados. Estas portarias publicam uma tabela com os valores de cobrança pela cessão ou aluguel da faixa de domínio.

Também alguns departamentos estaduais de Estradas de rodagem emitiram portarias similares como o Departamento Estadual de Estradas de Rodagem de São Paulo e o Departamento de Estradas de Rodagem do Estado do Paraná.

Com relação aos Municípios; o "pioneiro" nesta questão é o Município de São Paulo , capital do Estado, que emitiu um decreto estadual em meados de 1999. Este Decreto, dispõe sobre a permissão de uso de vias públicas e obras nos domínios do Município de São Paulo, para implantação, instalação e passagem de equipamentos urbanos destinados à prestação de serviço de infra-estrutura. Ele estabelece condições de pagamento proporcionais a área utilizada (espaço aéreo ou enterrado), o valor dos equipamentos utilizados, a utilidade pública dos serviços a serem prestados e o valor imobiliário do logradouro.

As redes de banda larga via wireless, são mais simples, não ficam presas numa rede burocrática como foi citada acima, e é uma resposta ao problema da democratização da Internet, pos permite via rádio, acesso aos mais distantes localidades no Brasil.

Capítulo 2 – Características e Definições

2.1 Projeto conceitual

Esta fase envolve a definição de todo o projeto, detalhando o objetivo de cada parte e destacando sua funcionalidade. A interligação entre as áreas será também elaborada.

- **Wireless**

O nome wireless vem do inglês, significando "**sem fio**" (**wire**=fio, **less**=sem), sendo comumente utilizado no meio da informática para designar as tecnologias que permitem comunicação sem conexão física direta entre os equipamentos.

O sistema de acesso Wireless (via rádio) é a maneira mais eficiente de acesso à Internet por banda larga. Podem ser obtidas as velocidades de 64Kbps, 128Kbps, 256Kbps e 512Kbps podendo chegar a 11 Mbits.

O funcionamento do sistema wireless é muito simples. Podemos compará-lo ao do celular da seguinte maneira: existe uma antena num ponto central e estratégico. Esta antena está conectada à rede local de um provedor, que se conecta diretamente ao backbone Internet. A antena emite um sinal na freqüência de 2.4 GHz (freqüência livre para operação), utilizando o sistema chamado Direct Sequence Spread Spectrum (DSSS) . Este sinal é captado por uma antena instalada na casa ou empresa do usuário e é levada até uma placa especial que é instalada dentro de seu computador (esta placa substitui seu FAX Modem) e, a partir daí, o usuário estará conectado à Internet. Basta ligar seu computador para a conexão estar ativa. Estas placas são baseadas no padrão IEEE 802.11b Wi-Fi de alta velocidade, sendo que existem hoje no mercado placas que permitem o acesso rápido às redes wireless com a utilização de rádios plug-and-play que operam faixa de 2.4 GHz e não necessitam de licença especial. Com o mesmo

cartão PCMCIA o usuário pode conectar-se a Internet a uma velocidade de 11Mbps em empresas, residências, pequenos escritórios, hotéis, aeroportos, entre outros.

O Wireless IP é uma conexão contínua e permanente, via transmissão de rádio freqüência.

A solução Wireless IP (WIP) provê um acesso bidirecional full duplex de alta velocidade à Internet e entre filiais e matriz, sem a necessidade de utilização de linhas telefônicas ou linhas privadas (LP).

Toda a transmissão e recepção de dados passam pelos hubs e por um sistema Wireless IP. Os computadores da empresa podem ficar ligados 24 horas por dia à Internet, em alta velocidade, sem nenhum custo adicional de linhas privadas ou discadas.

O sistema WIP suporta encriptação Wired Equivalente Privacy (WEP) com chave de até 128 bits. Todo o tráfego de rede passa por uma VPN (Virtual Private Network) utilizando o protocolo IPSec (IP Secure) com chave de 1024 bits, garantindo proteção à rede contra ataques externos.

O sistema é ligado através de uma antena e um transmissor, sem a necessidade de aquisição de nenhum tipo de equipamento, como roteadores ou cable modems.

Fig. 2.1 - Torre para acesso à Internet em Minas Gerais

Montada no pico da Mina do Pau Branco, a torre acima, esta a 25,4 km de Belo Horizonte e 1,8 km de um centro comercial , a torre disponibiliza os recursos para que todos os condomínios da região possam ter acesso rápido e seguro à Internet. Para uma

região como a Barra por exemplo, cercada de condomínios, ela poderia estar situada no prédio mais alto, cobrindo uma vasta área da região.

Devido à distância da rede de energia elétrica, os equipamentos montados na torre são alimentados por um sistema fotovoltaico com tensão de saída alternada, monofásica, de 115 V/60 Hz e potência de saída de 150 VA. A tensão do banco de baterias é 12 V e potência nominal do gerador fotovoltaico de 159 Wp acoplados a um banco de baterias de 185 Ah (12 V). Todo o sistema foi dimensionado para suprir a carga do rádio transmissor, consumindo uma corrente de 0,117A durante 24 h/dia. Dentro das cidades, ela poderia aproveitar a rede de energia elétrica existente.

2.2 IEEE 802.11b

Esta é a tecnologia de rede sem fio mais difundida atualmente e a que tem maiores chances de tornar-se padrão nos próximos um ou dois anos, passando a rivalizar com as redes Ethernet que já estão tão bem estabelecidas.

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; Existem tanto placas PC-Card, que podem ser utilizadas em notebooks e em alguns handhelds, quanto placas para micros de mesa.

Não existe mistério na instalação das placas. Basta deixar que o Windows detecte o novo hardware e forneça os drivers da placa, ou executar o utilitário de configuração. O Windows XP possui drivers para algumas placas, facilitando a tarefa. As placas 802.11b são detectadas como placas Ethernet, apenas uma forma que os fabricantes encontraram para facilitar a compatibilidade com os vários sistemas operacionais.

Existem muitos casos de fabricantes que optaram por produzir apenas placas PC-Card (presumindo que a maior parte das vendas seria feita para usuários de notebooks) e que oferecem como complemento um adaptador opcional que pode ser usado para encaixar os cartões em micros de mesa. Lembre-se que o padrão PC-Card dos notebooks e o barramento PCI dos desktops são muito semelhantes, por isso basta um adaptador simples.

O Hub é chamado de ponto de acesso e tem a mesma função que desempenha nas redes Ethernet: retransmitir os pacotes de dados, de forma que todos os micros da rede os recebam.

- **Ponto de Acesso**

Não existe limite no número de estações que podem ser conectadas a cada ponto de acesso mas, assim como nas redes Ethernet, a velocidade da rede decai 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 a 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 a rede e sincronizasse os dados necessários. No caso das escolas a principal utilidade seria fornecer acesso a Web aos alunos. Esta já é uma realidade em algumas universidades e pode tornar-se algo muito comum dentro dos próximos anos.

- **Vamos então às especificações e aos recursos desta arquitetura.**

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 a 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.

fig. 2.2 - Ponto de acesso.

Mas, existe a possibilidade de combinar o melhor dos dois mundos, conectando um ponto de acesso 802.11b a uma rede Ethernet já existente. No ponto de acesso da foto abaixo pode-se notar que existe um conector RJ-45:

fig. 2.3 - Ponto de acesso com conector RJ-45.

Isto adiciona uma grande versatilidade à rede e permite diminuir os custos. O usuário 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. Se o usuário colocar o ponto de acesso próximo da janela da frente da sua casa por exemplo, provavelmente um vizinho distante dois quarteirões ainda vai conseguir se conectar a sua rede.

O usuário 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. O utilitário lhe fornecerá um gráfico com a potência e a qualidade do sinal.

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.

As redes sem fio, sejam baseadas no 802.11b ou em qualquer outro padrão, apresentam um grande potencial para o futuro. Uma mudança mais interessante é o estabelecimento de pontos de acesso a Web em lojas, supermercados, shoppings, restaurantes, escolas, etc. onde o acesso a Web será oferecido como conveniência aos clientes armados com notebooks e palmtops, que dentro dos próximos anos se tornarão muito mais populares e já virão com interfaces de rede sem fio. Será uma forma de acesso muito mais barata (e mais rápida) que a através dos celulares 2.5G ou mesmo 3G e ao mesmo tempo será algo muito barato de implantar para os comerciantes que já tiverem um PC com acesso a Web.

Já que na maior parte do tempo em que não estamos em casa ou no trabalho estamos em algum destes lugares, estas pequenas redes públicas diminuirão em muito a necessidade de usar o acesso via celular, que mesmo com o 2.5G continuará sendo caro, já que não haverá mais cobrança por minuto, mas em compensação haverá tarifação pela quantidade de dados transferidos. Será uma grande conveniência, já que o usuário poderá acessar a Web em praticamente qualquer lugar. O velho sonho de muitos

educadores de escolas onde cada aluno tem um computador conectado à rede da escola também poderá tornar-se realidade mais facilmente.

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.

- **Variantes do 802.11 estão a caminho.**

Apesar de as redes Wi-Fi, ou 802.11b, ganharem popularidade rapidamente, existem outros padrões. Já chegaram no Brasil o 802.11a. Pelo menos um fabricante, a D-Link, lançou equipamentos nesse padrão em abril de 2003. As letras a e b identificam duas variantes da especificação 802.11 que foram publicadas ao mesmo tempo mas acabaram se materializando em momentos diferentes. Enquanto o 802.11b opera a 2,4 GHz, o 802.11a trabalha a 5 GHz. O 802.11a tem uma velocidade máxima de 54 Mb/s, cerca de cinco vezes a do Wi-Fi. Em compensação, a distância máxima de conexão por 802.11a fica em torno de 20 metros, um quinto do alcance do 802.11b. Uma área que pode ser interligada com um ou dois pontos de acesso Wi-Fi exigiria cerca de dez pontos de acesso 802.11a. Isso significa que, pelo menos no ambiente corporativo, as redes 802.11a sempre serão mais caras. O 802.11a é incompatível com o Wi-Fi, mas há fabricantes desenvolvendo interfaces multipadrão, o que vai amenizar esse problema. Mesmo assim, há quem ache que o 802.11a tem poucas chances de sucesso no mercado. O padrão 802.11g, ainda em desenvolvimento, vai ser uma espécie de Wi-Fi 2.0. Vai operar a 22 Mb/s, mas mantendo a compatibilidade com o 802.11b. Outro que está sendo elaborado é o 802.11e. Vai acrescentar gerenciamento de banda e melhor imunidade a interferências tanto ao Wi-Fi como ao 802.11a. Há um quinto padrão em estudos, o 802.11i, que deve melhorar a segurança das redes sem fio.

A padronização 802.11 garante a interoperabilidade entre produtos de diferentes fabricantes, como ocorre hoje com o Ethernet (padrão IEEE 802.3). Abordaremos a seguir diversos aspectos das WLANs (Wireless Local Area Networks).

- **Componentes**

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 se comunicam 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

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.

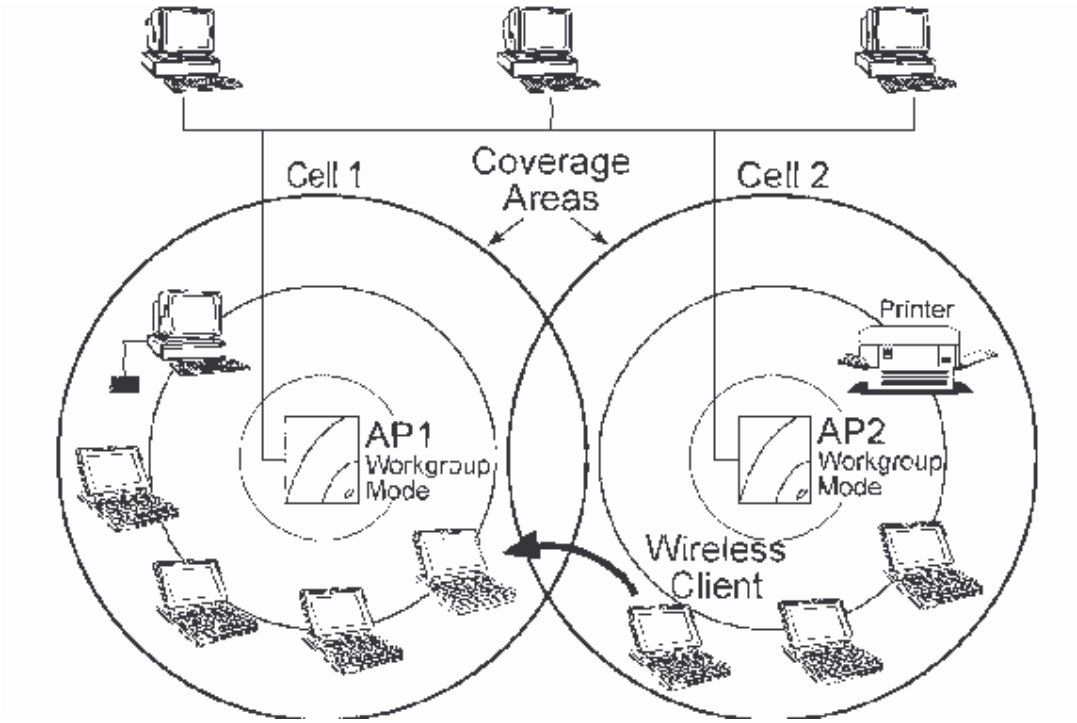


fig. 2.4 - Roaming.

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).

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

➢ Arquitetura

O IEEE 802.11 estabelece a padronização das camadas física e de enlace para redes sem fio.

A camada física é implementada através de 3 diferentes especificações:

FHSS - Frequency Hopping Spread Spectrum

DSSS - Direct Sequence Spread Spectrum

IR - Infrared

As especificações FHSS e DSSS operam na freqüência de 2,4 GHz denominada banda ISM (Industrial Scientific and Medical) cujo uso é liberado sem necessidade de licenciamento.

Para o DSSS, seguindo a regulamentação do FCC (Federal Communications Commission) dos Estados Unidos, são disponíveis 11 canais na banda ISM sendo a potência máxima permitida de 4W. Estes 11 canais são parcialmente sobrepostos, de forma que em um mesmo site são possíveis até 3 diferentes canais vizinhos operando sem interferência.

A subcamada MAC (Media Access Control) da camada de enlace é implementada via mecanismo CSMA/CA (Carrier Sense Multiple Access Collision Avoidance). Dois métodos são previstos:

No primeiro método, semelhante ao mecanismo utilizado nas redes Ethernet, as estações que desejam transmitir "escutam" o meio. Quando o canal está livre a estação transmite, caso esteja ocupado ela aguarda a transmissão em andamento finalizar-se, espera um tempo aleatório e repete o procedimento de escutar o meio. Após transmitir a estação aguarda uma confirmação ACK (Acknowledgement) da estação receptora. Caso receba um ACK a transmissão ocorreu com sucesso, caso contrário haverá retransmissão.

No segundo método denominado Virtual Carrier Sense, a estação antes de transmitir reserva o meio por um determinado período de tempo através de um pacote RTS (Request to Send) que é confirmado via pacote CTS (Clear to Send), o qual faz com que todas as estações da rede atualizem seus NAV (Network Allocation Vector) de forma a reservar o meio para a estação solicitante pelo intervalo de tempo estipulado. A partir deste ponto a estação efetua a transmissão e aguarda confirmação - ACK - da recepção.

- **Velocidade**

O padrão IEEE 802.11 original prevê velocidades de operação de 1 e 2Mbps. A nova versão denominada IEEE 802.11b (High Rate), prevê velocidade de operação de até 11Mbps, com fall back automático para 5.5 , 2 e 1 Mbps baseado na qualidade do sinal.

- **Segurança**

Dois métodos de segurança são previstos:

Autenticação - método que consiste na verificação de autorização de cada estação antes de ter acesso à rede.

Criptografia - método através do qual as mensagens são criptografadas utilizando algoritmo RC4 PRNG da RSA Data Security. Este método, denominado WEP (Wired Equivalent Privacy) , é destinado a prover às redes sem fio o mesmo nível de segurança das redes tradicionais.

- **ROAMING**

O roaming entre diferentes células é definido de forma superficial no padrão, deixando para cada fabricante os detalhes de implementação. Desta forma, para tornar possível à interoperabilidade do roaming entre equipamentos de diferentes fabricantes, foi definido o IAPP (Inter-Access Point Protocol) adotado por um grupo de empresas.

- **Aplicações**

As soluções baseadas no padrão IEEE 802.11 destinam-se à implementação de redes locais sem fio, bem como interligação de redes locais através de enlaces de rádio.

Diversas áreas podem beneficiar-se da tecnologia WLAN: hospitais, eventos, escritórios temporários, construções antigas ou tombadas pelo patrimônio histórico, salas de treinamento, escolas, interligação entre prédios na mesma região metropolitana, etc.

➢ **Mercado**

Com a padronização do IEEE, o mercado de produtos e soluções wireless está em franco desenvolvimento, com previsões de crescimento de US$ 210 milhões em 1997 para US$ 1.4 bilhões em 2004. Paralelamente os custos das soluções WLAN estão bastante atraentes e em tendência de queda.

2.3 A Solução Enterasys [10]

RoamAbout.
ENJOY THE FREEDOM OF WIRELESS NETWORKING

A solução da Enterasys Networks para redes sem fio, denominada Roam About Wireless LANs é aderente ao padrão IEEE 802.11b.

A tecnologia utilizada é a DSSS (Direct Sequence Spread Spectrum), operando na faixa de freqüência de 2,4GHz, com 11 canais disponíveis conforme padronização do FCC. A velocidade de comunicação é de 11Mbps com fallback automático para 5,5Mbps, 2Mbps e 1Mbps de acordo com a qualidade do sinal (relação sinal-ruído).

A solução implementa mecanismo de segurança WEP (Wire Equivalent Privacy), roaming aderente ao IAPP e suporta gerenciamento SNMP e RMON.

Dois modos de operação estão disponíveis: Ad-Hoc mode e Infrastructure mode. Neste último modo, o mesmo Access Point pode ser configurado para operação em rede interna, denominada configuração Workgroup (indoor), ou para interligação entre redes localizadas em prédios distintos, denominada configuração Build-to-Build (outdoor).

➢ **ROAMABOUT INDOOR**

A solução indoor é composta dos seguintes itens:

Access Point - equipamento com uma porta Ethernet e um slot PCMCIA para placa de rede sem fio, que funciona como bridge (ponte) entre a rede Ethernet tradicional e a rede sem fio.

Wireless Cards - cartão PCMCIA de rede sem fio utilizado no Access Point e nas estações da rede. Já vem com antena embutida e leds de link e tráfego.

ISA ou PCI Adapter - adaptador opcional para uso em PC's que não possuem slot PCMCIA.

Indoor Antena - pequena antena opcional para ser utilizada no Access Point quando este é colocado dentro de um rack ou em PCs de forma a aumentar o alcance do sinal.

Ethernet Adapter - adaptador com uma porta Ethernet 10BaseT e um Wireless Card. Utilizado para conectar um dispositivo que já possua placa de rede (PC, notebook, impressora etc…) à rede sem fio.

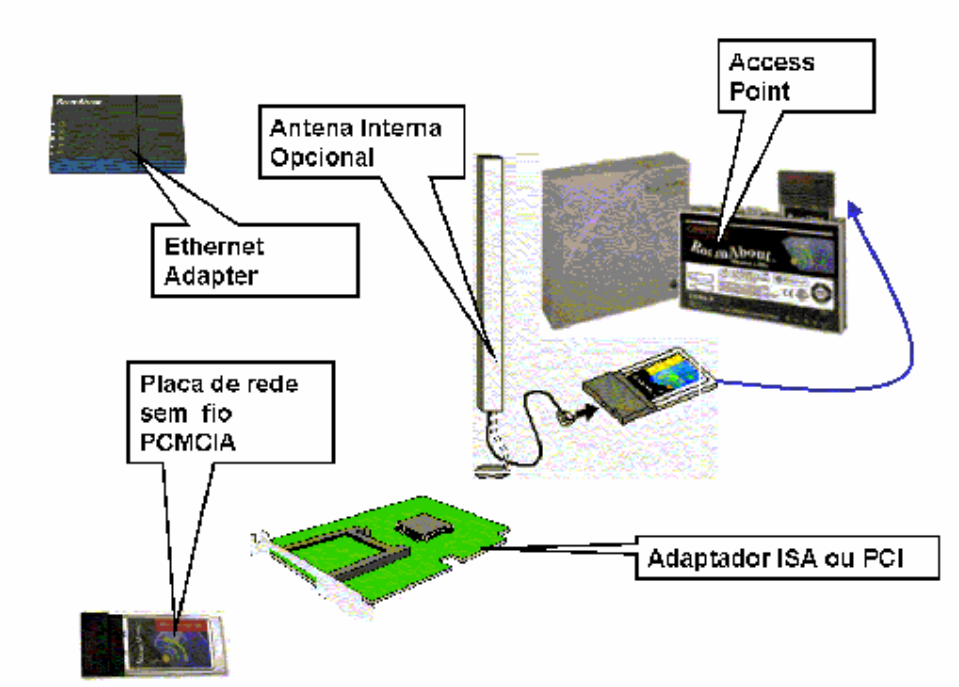


Fig. 2.5 - Componentes de uma solução indoor.

O Access point coordena a comunicação na rede sem fio criando uma esfera com raio de até 171m de alcance em ambiente aberto e 53m de alcance em ambiente semi-aberto, de forma que as estações com placas de rede sem fio comunicam-se entre si dentro deste perímetro via Access Point.

Adicionalmente o Access Point funciona como bridge entre a rede sem fio e a rede Ethernet tradicional da empresa, implementando ainda mecanismos programáveis de filtragem de pacotes de forma a não saturar a rede sem fio.

Cada Access Point pode atender até 200 estações, sendo recomendável um número de até 50 estações por Access Point de forma a manter adequado o nível de

utilização da rede. O equipamento é acompanhado de um poderoso e amigável software de configuração e monitoramento executável em Windows, suporta gerenciamento SNMP e RMON. Os Wireless Cards são acompanhados de drivers para MS Windows 95, 98, NT, CE e 2000, Macintosh, Linux e Novell 3.x e 4.x. O produto vem ainda com software utilitário para monitorar a intensidade do sinal e nível de ruído na comunicação via rede sem fio.

- **A tabela a seguir apresenta as relações de alcance x velocidade da solução indoor**.

DISTâNCIAS RoamAbout Indoor (raio da esfera em torno do AP) 11 Mbps (com fall back automático para 5.5, 2, e 1 Mbps)

VELOCIDADE (Mbps) | ALCANCE (m)

	Ambiente aberto|	Ambiente semi-aberto|	Sensibilidade do receiver
11Mbps	66m	28m	-84dBm
5.5Mbps	91m	35m	-87dBm
2Mbps	125m	43m	-90dBm
1Mbps	171m	53m	-93dBm

- **ROAMABOUT OUTDOOR**

A solução outdoor utiliza os mesmos Access Point e Wireless Cards da versão indoor, acrescidos de antenas para uso externo. Duas versões estão disponíveis:

Versão B2B (Build to Build) - destinada à interligação entre prédios, utiliza um par de antenas direcionais Yagi de 14dBi operando em 2,4Ghz. Na configuração B2B uma antena é colocada em cada prédio e ambas são direcionadas uma para outra em linha de visada.

Versão Móvel - destinada à interligação de veículos móveis, utiliza uma antena omnidirecional central de 7dBi operando em 2,4Ghz e antenas para veículos.

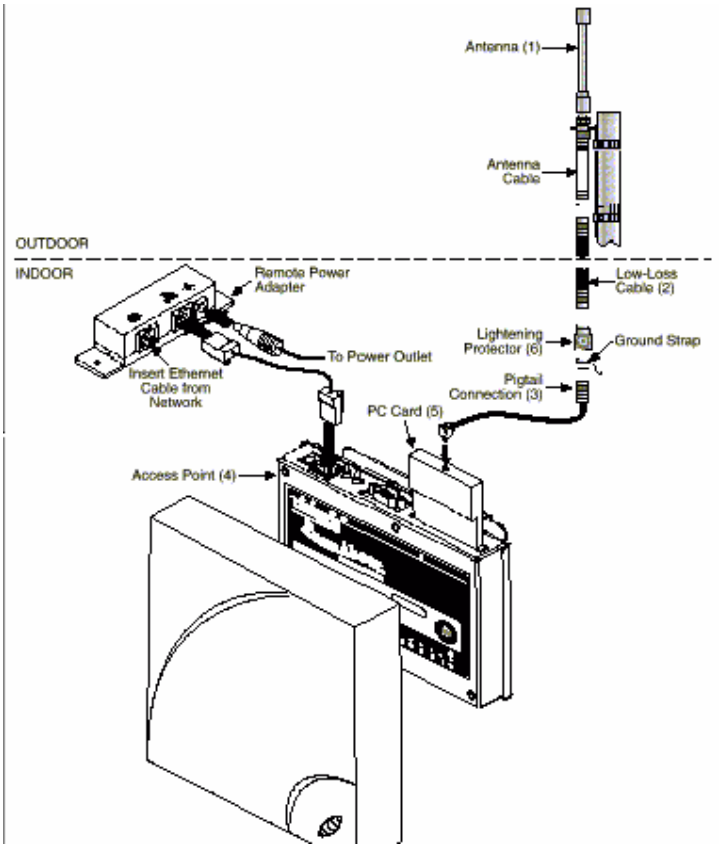


fig. 2.6 Antena omnidirecional

A tabela abaixo relaciona o alcance x velocidade da solução Outdoor com antena direcional (14dBi) e Omnidirecional (7dBi).

DISTâNCIAS RoamAbout Outdoor |	VELOCIDADE
14dBi Yagi p/14dBi Yagi	14dBi Yagi p/7dBi Omni
11 Mbps	
2.5 km	2.5km
5.5 Mbps	
7.9 km	3.5 km
2 Mbps	
11.2 km	5 km
1 Mbps	
15.8 km	7.1 km

A Enterasys possui ainda um novo modelo de Access Point (**RoamAbout R2**) desenvolvido para o padrão IEEE 802.11a com velocidade de operação de 54Mbps.

2.4 Como Montar Uma Rede Sem Fio Padrão 802.11b

Montar uma rede Wi-Fi peer-to-peer envolve muitos passos, mas nenhum muito complicado. Para conectar dois micros de mesa, um Pentium III de 866 MHz e um Celeron 900 MHz, ambos com 128 MB e Windows 98, o INFOLAB[14] usou duas placas PCI de rede sem fio da Compaq. Essa placa é uma interface PCI/PC Card que vem com um cartão PC Card Wi-Fi para ser encaixado nela. Vamos instalar primeiro a placa e depois o cartão. Certifique-se de ter o CD do Windows 98 à mão. Ele vai ser requisitado em vários momentos. Para começar, desligamos o micro, abrimos o gabinete, encaixamos a placa sem o cartão num conector PCI e apertamos o parafuso de fixação. Em seguida, fechamos o gabinete e ligamos o micro. O Windows detecta a nova placa e instala o programa controlador. Em seguida, inserimos no drive o CD que vem com a placa e instalamos o Client Manager, programa de gerenciamento da Compaq.O próximo passo é encaixar o cartão PC Card na placa adaptadora, o que pode ser feito com o micro ligado. O Windows 98 reconhece o cartão e instala o programa controlador para ele. No caso do cartão da Compaq, durante a instalação é exibida uma tela para configuração. Depois de clicar em Edit Configuration, damos um nome para a rede, que deverá ser o mesmo em todos os micros. No menu da direita, escolhemos peer-to-peer Group. Para habilitar a criptografia, clique em Enable Data Security e digite uma senha com 13 caracteres. Essa senha também deverá ser a mesma em todos os micros. Interfaces 802.11b de qualquer marca deveriam ser compatíveis entre si. Mas o INFOLAB[14] verificou que pode ser necessário desabilitar a criptografia para que cartões de fabricantes diferentes possam se comunicar.

- **Configuração do Windows**

Terminada a instalação da interface, ativa-se os serviços de rede do Windows 98. Clicar em Iniciar/Configurações/Painel de Controle e, em seguida, dá-se um duplo clique em Rede. Na aba Configuração, aparece os componentes instalados. Verifique se o protocolo TCP/IP está entre eles e se aparece associado à interface sem fio (neste caso, Compaq WL 110 PC Card). Se não estiver, clica-se em Adicionar. Escolha Protocolo e clique novamente em Adicionar. Selecioná-se o fabricante Microsoft e o protocolo TCP/IP e clique em OK. Novamente na aba Configuração, verifique se o

Compartilhamento de Arquivos e Impressoras está instalado. Se não estiver, clique no botão correspondente a essa opção, abaixo, para configurá-la.Abra o Windows Explorer e escolha a pasta ou disco que quer compartilhar com os demais micros. Clique com o botão direito e escolha Compartilhamento. Na janela que se abre, assinale Compartilhado e, se quiser, digite uma senha alfanumérica de preferência para acesso. Para compartilhar a impressora, clique em Iniciar/Configurações/Impressoras. Clique com o botão direito na impressora e escolha Compartilhamento. Tanto a instalação das placas e cartões Wi-Fi como a configuração do Windows deverão ser feitas em cada um dos micros. Para instalar o driver de impressora no micro cliente (aquele que não tem a impressora conectada diretamente), clique em Iniciar/Configurações/Impressoras e, em seguida, dê um duplo clique em Adicionar Impressora. Vá clicando em Avançar. Escolha Impressora de Rede. Quando o Windows pedir o caminho de rede, clique em Procurar. Navegue até encontrar o micro que tem a impressora, selecione-a e continue clicando em avançar.

- **Acesso à Internet**

Terminada a configuração da impressora, já é possível transferir arquivos de um micro para outro, e ambos podem imprimir. Dando um duplo clique no ícone Ambiente de Rede, podemos ver os micros conectados e os discos e pastas compartilhados. O próximo passo é configurar o acesso à Internet. O INFOLAB[14] empregou uma conexão por cable modem nessa rede. O cabo que vem do cable modem é ligado a uma interface Ethernet num dos micros. Nesse micro, vamos configurar o compartilhamento.Para isso, abra o Painel de Controle e dê um duplo clique em Adicionar ou Remover Programas. Na aba Instalação do Windows selecione Ferramentas para a Internet. Clique no botão Detalhes, selecione Internet Connection Sharing e clique em OK. O Windows vai instalar esse programa e iniciar um assistente. Siga as instruções da tela e, quando solicitado, coloque um disquete no drive. O Windows vai gravar nele o programa que deve ser rodado nos demais micros para configurá-los. Terminada essa etapa, todos os micros devem ser capazes de acessar a Internet.

- **Proteção contra intrusos**

Falta instalar o antivírus e o firewall, sem os quais nenhuma rede de respeito pode existir. Nesta rede, instala-se o PC Cillin, da Trend Micro. Trabalhando com dois micros, não vale a pena usar um antivírus específico para rede, que é muito mais caro. Optá-se por duas licenças da versão para uso pessoal. O firewall ZoneAlarmPro é instalado apenas no micro que está ligado ao cable modem.Embora esse software tenha uma versão gratuita, ela não suporta o compartilhamento de conexão. Por isso, usá-se a versão paga. Quando o instalador perguntar se o usuário quer dar permissão ao navegador para acessar a Internet, diga sim assinalando essa opção. Na tela configuring your ICS/NAT, assinale a opção This Computer is the Gateway. Nessa mesma tela, digite o endereço IP do micro.Para obtê-lo, clique em Iniciar/Executar, digite winipcfg e clique em OK. Na tela que aparece, selecione a interface sem fio no menu à direita. Copie o endereço IP (exemplo: 192.168.0.1) para a tela de instalação do ZoneAlarm. No teste do INFOLAB[14], o software funcionou bem sem nenhum ajuste adicional.

2.5 Sistema de Antenas

Identificação das antenas, quais as mais utilizadas, especificando cada uma, de acordo com os modelos encontrados no mercado.

- **Aumentando o alcance.**

Assim como em outras tecnologias de transmissão via rádio, a distância que o sinal é capaz de percorrer depende também da qualidade da antena usada. As antenas padrão utilizadas nos pontos de acesso, geralmente de 2 dBi são pequenas e práticas, além de relativamente baratas, mas existe a opção de utilizar antenas mais sofisticadas para aumentar o alcance da rede.

Fig. 2.7 - Ponto de acesso com as antenas padrão

Alguns fabricantes chegam a dizer que o alcance dos seus pontos de acesso chega a 300 metros, usando as pequenas antenas padrão. Isto está um pouco longe da realidade, pois só pode ser obtido em campos abertos, livres de qualquer obstáculo e mesmo assim o sinal ficaria tão fraco que a velocidade de transmissão mal chegaria a 1 megabit.

Mesmo assim, a distância máxima e a qualidade do sinal (e conseqüentemente a velocidade de transmissão) podem variar bastante de um modelo de ponto de acesso para outro, de acordo com a qualidade do transmissor e da antena usada pelo fabricante.

Existem basicamente três tipos de antenas que podem ser utilizadas para aumentar o alcance da rede.

As antenas Yagi, são as que oferecem um maior alcance, mas em compensação são capazes de cobrir apenas a área para onde são apontadas. Estas antenas são mais úteis para cobrir alguma área específica, longe do ponto de acesso, ou então para um usuário em trânsito, que precisa se conectar a rede. Em ambos os casos, o alcance utilizando uma antena Yagi pode passar dos 500 metros.

Fig. 2.8 Antena Yagi

A segunda opção são as antenas ominidirecionais, que, assim como as antenas padrão dos pontos de acesso, cobrem uma área circular (ou esférica, caso o ponto de acesso esteja instalado acima do solo) em torno da antena. A vantagem é a possibilidade de utilizar uma antena com uma maior potência. Existem modelos de antenas ominidirecionais de 3dbi, 5 dBi, 10 dBi ou até mesmo 15 dBi, um grande avanço sobre as antenas de 2 dBi que acompanham a maioria dos pontos de acesso.

Fig. 2.9 Antenas ominidirecionais

Assim como as Yagi, as antenas ominidirecionais podem ser usadas tanto para aumentar a área de cobertura do ponto de acesso, quanto serem instaladas numa interface de rede, em substituição à antena que a acompanha, permitindo captar o sinal do ponto de acesso de uma distância maior.

Mais uma opção de antena são as mini-parabólicas, que também captam o sinal em apenas uma direção, como as Yagi, mas em compensação podem ter uma potência ainda maior, dependendo do modelo usado.

Fig. 2.10 Mini-Parabólica

Estas antenas podem custar de 30 a mais de 200 dólares, dependendo da potência. As antenas Yagi estão entre as mais caras, vendidas por US$ 150 ou mais. Além do problema do preço, existe um aumento no risco de uso indevido na rede, já que o sinal irá propagar-se por uma distância maior, mais uma razão para reforçar a segurança.

2.6 Interligação dos Sistemas

Nesta etapa será descrita a rede de interligação de todas as áreas do projeto, detalhando a especificação dos recursos, equipamentos, infra-estrutura e tipos de ligação.

- **Recursos**

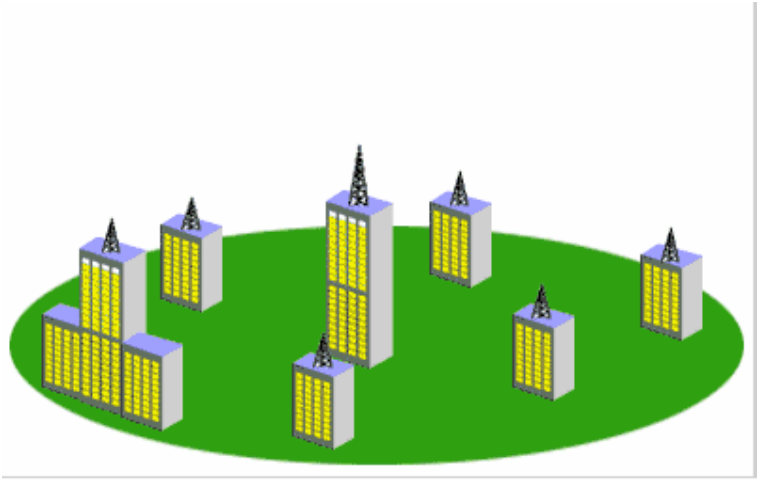


Fig. 2.11 - exemplo de interligação

Soluções tecnológicas, estratégias de marketing, idéias de novos negócios e mensagens à diretoria não podem cair nas mãos da concorrência.

Por outro lado, todos sabemos que vencer no mercado competitivo e globalizado sem a rápida comunicação de dados entre matriz, filiais e parceiros é quase impossível. A conclusão é simples: qualquer empresa precisa de uma rede que deve ser, em primeiro lugar, confiável.

O Wireless IP é uma tecnologia que permite aos usuários implantarem uma rede de comunicação completa entre computadores, sem a utilização de fios ou cabos. Como solução externa e usando antenas adequadas, podem-se atingir distâncias de mais de 12 Km dependendo da topografia da região, interligando matriz e filiais.

As soluções Wireless IP oferecem flexibilidade e mobilidade, por permitir o acesso à rede em qualquer lugar. Permite também que sua empresa preserve seu investimento em caso de futuras expansões ou mudança física de local. É muito rápido e fácil mover a antena para outro endereço.

- **Equipamentos**

Fig. 2.12 - Exemplos de equipamentos

Com os acessórios para Wireless, é possível montar estruturas de rede à distância, com velocidade de até 11Mbit/s de transmissão. Para os computadores e periféricos conectados a conexão "wireless" fica totalmente transparente e a configuração é como uma placa de rede normal. A rede wireless é transparente também para o protocolo, TCP/IP, IPX, NetBEUI ou outros podem trafegar e existir ao mesmo tempo na mesma rede.

- **Infra-estrutura**

Controle e monitoração total sobre os serviços disponibilizados. Este é o compromisso de uma empresa com seus clientes. A infra-estrutura da solução Wireless IP fundamenta-se em hubs distribuídos pela região metropolitana de uma cidade. De cada hub, faz-se uma visada próxima ao cliente. Cada cliente sai pela Internet usando balanceamento de cargas entre 2 backbones.

O **diagrama da rede** representado na figura contém a infra-estrutura da rede, os equipamentos e as configurações da rede. Este é um serviço que uma empresa utiliza visando melhorar a qualidade da solução Wireless IP. Através desse serviço cada equipamento é monitorado, indicando se ele está ou não respondendo. Desta forma é possível verificar a origem de algum problema.

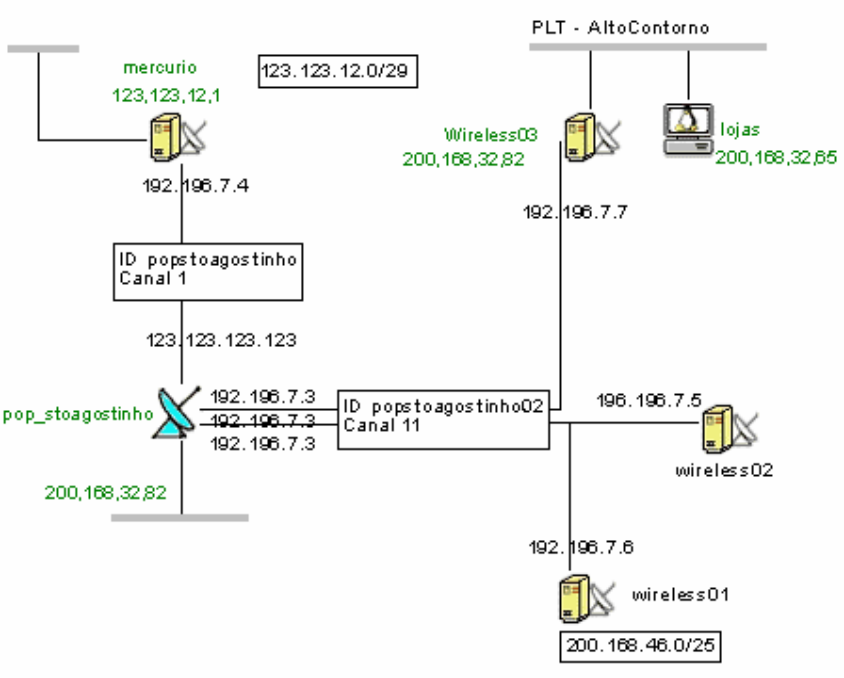


Fig. 2.13 - Exemplo de monitoramento de um sistema de wireless

Monitoramento dos equipamentos e dos serviços de cada servidor - É possível verificar os serviços do servidor que estão no ar.

Data do teste: Wed Aug 7 08:45:01 BRT 2002 - Atualizado a cada 5 minutos

OK Problema Serviço não monitorado

Servidor	ping	www	dns	smtp	pop3	proxy	ftp	radius	ssh	imap
embratel										
diveo										
argos										
gemini										
enterprise										
soho										
viking										
wireless01										
wireless02										
wireless03										

Fig. 2.14 - Monitoramento do sistema

Níveis de sinal Wireless - Mostram a qualidade das conexões wireless. São indicados níveis de sinal, ruído, qualidade do sinal e velocidade.

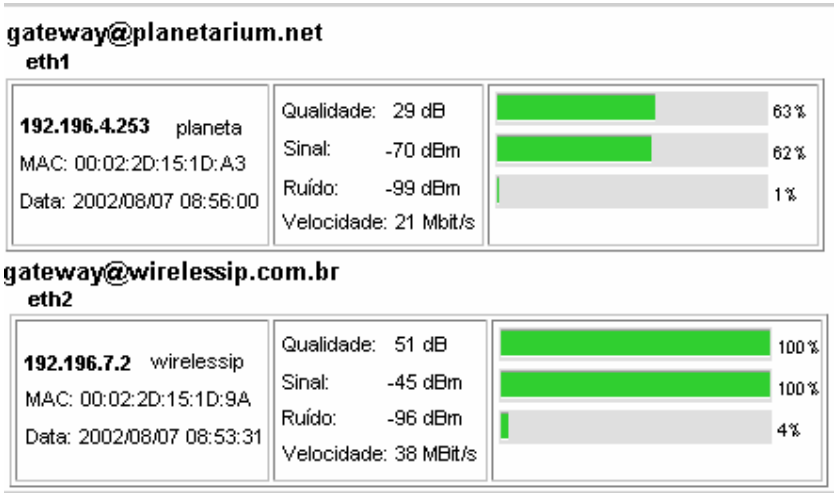


Fig. 2.15 - Controle de sinal

Sinal Médio - Os principais sinais emitidos e recebidos pelos rádios de cada cliente é monitorado. Os logs são tratados e é disponibilizado para cada cliente um gráfico de sua situação durante as 24 horas do dia.

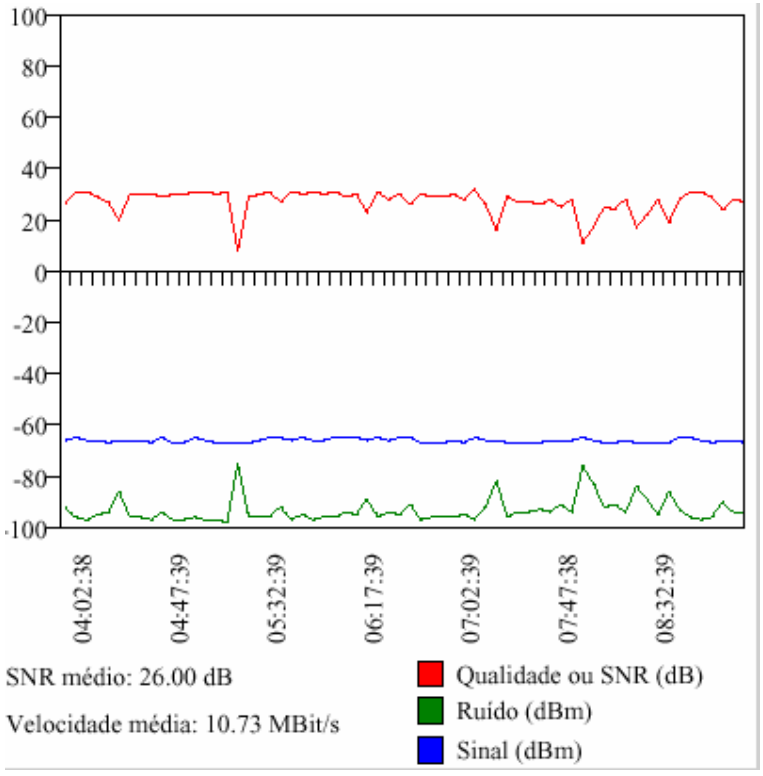


Fig. 2.16 - Controle de Sinais

Gráfico de Tráfego de Rede - O cliente sabe exatamente a situação do seu link. Através de gráficos que representam os bytes que entram e saem de sua rede a monitoração é feita em horas do dia, dias da semana, semanas do mês e meses do ano. O cliente sabe se a banda contratada está realmente sendo realmente disponibilizada para seu uso.

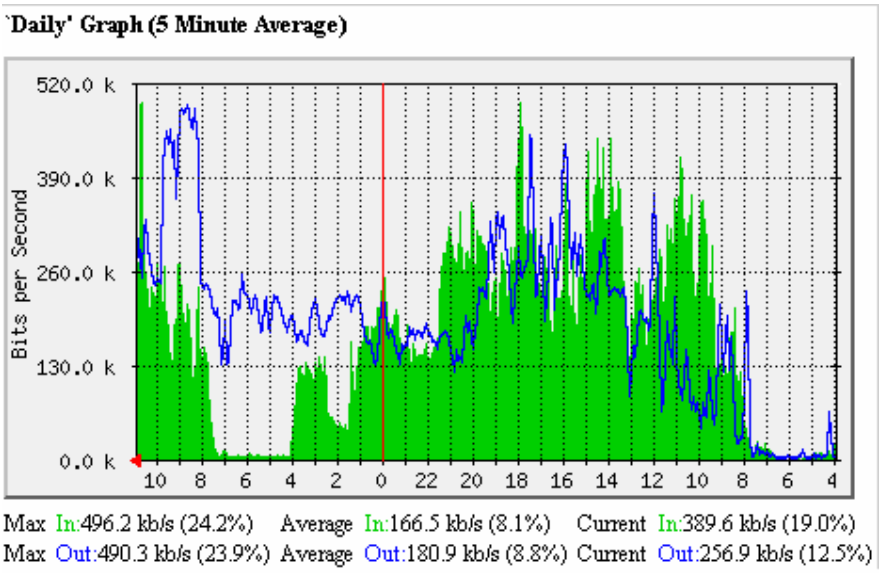


Fig. 2.17 - Gráfico de tráfego de Rede

- **Tipos de Ligação**

- **1- Rede interna**

Esse tipo de ligação (conforme mostrado na figura abaixo) é utilizado em ambientes internos e apresenta as seguintes vantagens:

Mobilidade – Alcance de até 150 m

Flexibilidade – É possível utilizar redes sem fio em lugares fisicamente impossíveis de se ter uma rede cabeada.

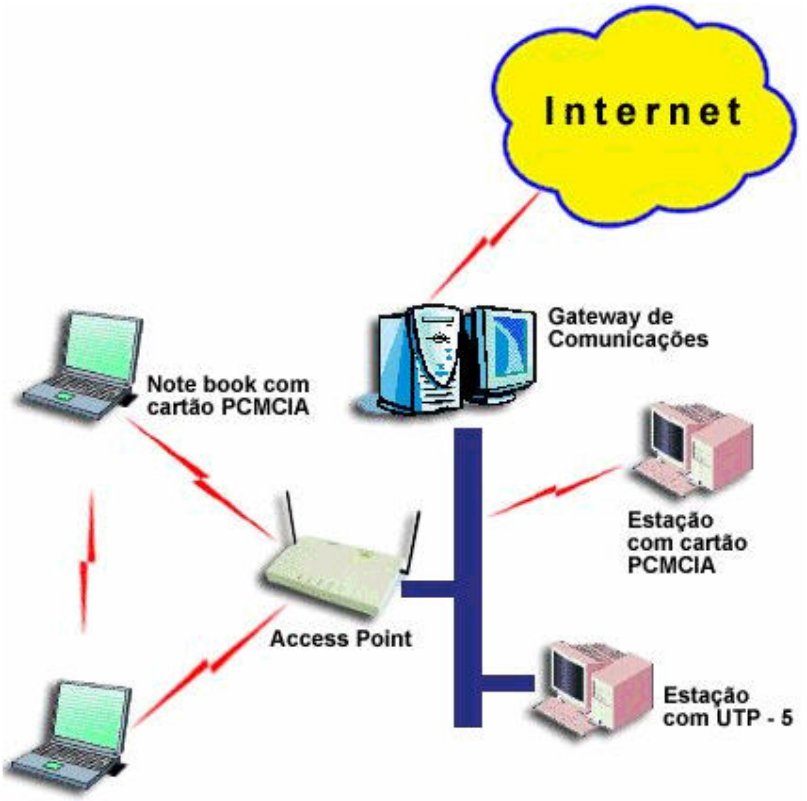


Fig. 2.18 - Tipo de Ligação interna

- **2- Rede externa**

- **2.1 Conexão ponto-a-ponto**

Os equipamentos são os mesmo utilizados em uma rede interna, porém conectam a uma antena externa. Este tipo de conexão é utilizado para:

- Interligação de LANs em alta velocidade sem custos fixos mensais.
- Possibilidade de VOIP

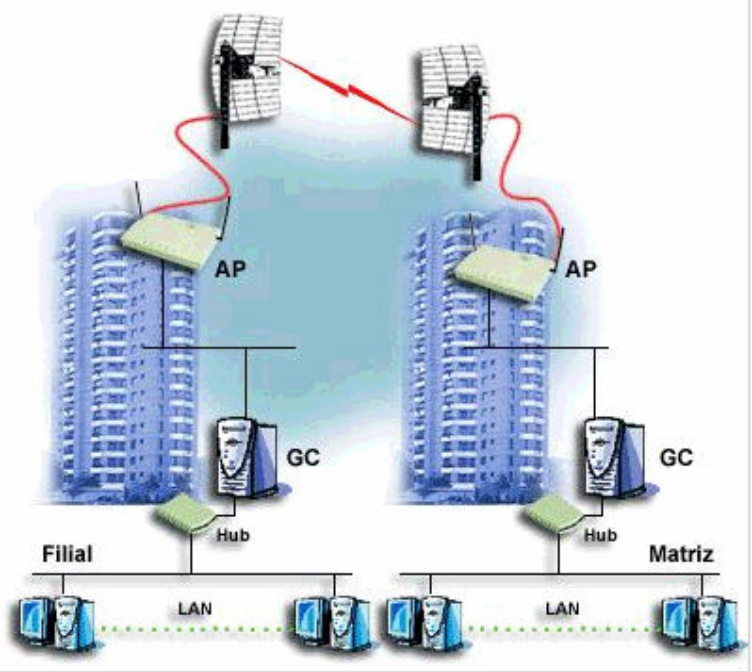


Fig. 2.19 - Tipo de Ligação Externa

➢ 2.2 Conexão Multiponto

Na conexão multiponto, um ponto central irradia o sinal para vários pontos. Pode ser usada para:

Interligação de empresas.

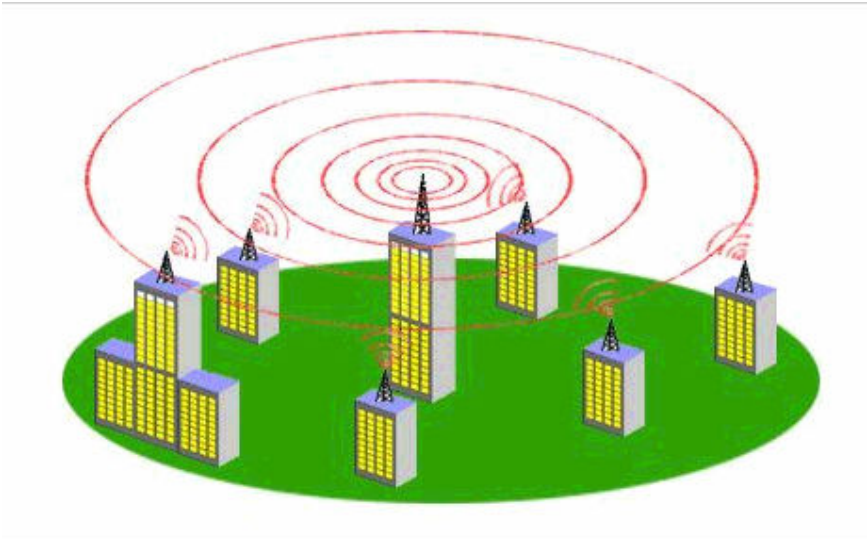


Fig. 2.20 - Exemplo de uma Conexão Multiponto

2.7 Vantagens e Desvantagens

Aqui serão detalhadas as vantagens e desvantagens na realização deste projeto.

- **Vantagens**

Mobilidade

Sistemas de redes locais sem fio podem prover aos usuários acesso à informação em tempo real em qualquer lugar.

Não Usa o Telefone

A linha telefônica fica livre enquanto o usuário navega na Internet. Não existe tarifação de impulso telefônico.

Instalação rápida e simples

Instalação de uma antena externa e um rádio no servidor. Essa instalação é feita em até 15 dias.

Flexibilidade

Tecnologia sem fio permite que as redes cheguem aonde cabos não podem ir.

Baixo Custo de manutenção

O custo fixo mensal de um link wireless é menor do que aquele fornecido por uma empresa de telecom, com a mesma velocidade. Além disso, não necessita de roteadores.

Alta imunidade a ruídos

Os rádios utilizados operam na frequência 2,4 GHz. Eles trabalham num sistema de espalhamento de frequência ou frequence hope, o que reduz drasticamente a possibilidade de interferências, garantindo a qualidade do sinal e a integridade das informações. Assim, como é utilizada uma freqüência muito alta, microondas, o sistema é imune a chuvas, raios e outras interferências de fenômenos metereológicos.

Conexão Permanente

Com o WIP, a sua conexão com a Internet é permanente. O usuário permanece on-line 24 horas por dia, 7 dias por semana.

Escalabilidade

Acessos sem fio podem ser configurados segundo diversas topologias de acordo com as necessidades da empresa. As configurações podem ser facilmente alteradas e as distâncias entre as estações adaptadas desde poucos usuários até centenas.

Segurança

O sistema WIP suporta encriptação Wired Equivalente Privacy (WEP) com chave de até 128 bits. Todo o tráfego de rede passa por uma VPN (Virtual Private Network) utilizando o protocolo IPSec (IP Secure) com chave de 1024 bits, garantindo proteção à rede contra ataques externos.

Interligação entre matriz e filiais.

Com a VPN (Rede Privada Virtual) é possível conectar matriz a filiais através da Internet, de forma segura, garantindo autenticação, privacidade e integridade.

- **Desvantagens**

Custo de implantação

Adaptadores Ethernet de alta velocidade são, em geral, 10 vezes mais baratos que adaptadores para redes sem fio. A implementação de redes sem fio reduz significativamente os custos mensais de telecomunicações o que proporciona uma rápida recuperação do capital investido nestes equipamentos.

Soluções proprietárias

Devido ao lento procedimento de padronização, muitas empresas precisam apresentar soluções proprietárias, oferecendo funções padronizadas mais características adicionais (tipicamente uma taxa de transmissão mais rápida utilizando uma tecnologia de codificação patenteada). Porém, estas características adicionais funcionam apenas em um ambiente homogêneo, isto é, quando adaptadores do mesmo fabricante são utilizados em todos os nós da rede. Deve-se seguir sempre uma mesma padronização, sendo que a utilizada é a 802.11b.

Restrições

Todos os produtos sem fio precisam respeitar os regulamentos locais. Várias instituições governamentais e não-governamentais regulam e restringem a operação das faixas de freqüência para que a interferência seja minimizada. Um grande empecilho para o uso destes equipamentos é necessidade de visada direta entre os pontos.

- **O Espectro de freqüência das telecomunicações. [1]**

Com o avanço das comunicações por meio de ondas eletromagnéticas tornou-se necessário à criação de uma regulamentação de utilização das freqüências. Há tantas emissões radioelétricas no éter que se não se colocasse em ordem seria praticamente impossível escutar. O espectro radioelétrico (ou espectro de freqüências para as telecomunicações) caracteriza-se como um bem universal finito, requerendo uma ordenação para o progresso de sua utilização na sociedade. Ao administrar essa ordem

são evitados os desperdícios do bem finito, momento em que se incorporam técnicas que aliam a qualidade de seu uso com a tecnologia existente.

A cobrança feita pela Anatel sobre a utilização do espectro, iniciada recentemente (Até pouco tempo atrás sua utilização era gratuita), têm como variáveis o tamanho da faixa de freqüência da concessão, a área a ser atingida pela transmissão e a população que ela beneficia, e ainda o tipo de serviço prestado pela concessionária.

O uso do espectro radioelétrico brasileiro é disciplinado por Normas e Padrões Internacionais e regido pela Legislação das Telecomunicações Brasileiras, cuja responsabilidade da aplicação recai sobre o Ministério das Comunicações e a Agência Nacional de Telecomunicações - ANATEL.

Mesmo assim, existe uma desordem generalizada e as maiorias das bandas estão saturadas de emissões. A disposição das bandas de rádio se produz sob a jurisdição da UIT (União Internacional de Telecomunicações). A UIT, devido às características especiais de cada zona do mundo, dividiu este em três regiões. A maioria do espectro radioelétrico está organizada de maneira parecida, todavia são suas diferenças regionais que obrigam a criar as três regiões:

Região 1:	Europa, África e Norte da Ásia.
Região 2:	América do Norte, América do Sul e Groelândia.
Região 3:	Pacífico e o Sul da Ásia.

- **O espectro radioelétrico está dividido nas seguintes freqüências:**

VLF. Ondas muito largas. (3 kHz - 30 kHz).
OL (LF). Ondas largas (30kHz - 300 kHz).
OM (MF). Ondas Médias (300 kHz - 3 MHz).
OC (HF). Ondas Curtas (3 MHz - 30 MHz).
MAF (VHF). Freqüências Muito Altas (30 MHz - 300 MHz).
UHF. Freqüências Ultra Altas (300 MHz - 3 GHz).

A partir dos 3 Ghz o uso das freqüências se profissionaliza, utilizando-se, sobretudo em radiomedicina, radioastronomia, etc. Para realizar comunicação em freqüências superiores, necessitaríamos de parabólicas gigantescas.

- **As Utilizações do espectro:**

VLF. 3 kHz a 30 kHz .

As três regiões coincidem em sua distribuição. Os serviços que se podem encontrar são de estações utilitárias (serviços de radionavegação e marítimos). Em 20 kHz se encontram estações de sinal horário e freqüências padrão. O espectro compreendido entre 0 kHz e 9 kHz não está distribuído. Grupos muito especializados de dexistas monitorizam as freqüências abaixo de 10 kHz para escutar o que se chama "Rádio Natural" que são as emissões radioelétricas naturais associadas a fenômenos do planeta (tormentas, terremotos, auroras boreais, eclipses, etc.).

OL (LF). 30 kHz - 300 khz.

As três regiões coincidem em sua maioria ainda que na região 1 há uma diferença substancial. Os serviços comuns seguem correspondendo às estações utilitárias (Serviços Marítimos, radionavegação e radiofarol diversos) Somente na região 1, os 60 kHz estão distribuídos às comunicações internas nas partidas de Rúgbi (fundamentalmente Grã Bretanha) e desde os 148,5 aos 255 kHz se encontra a banda de radiodifusão (estações BCB) de Onda Larga.

OM (MF). 300 kHz - 3 MHz.

As três regiões coincidem em todo. As freqüências entre 300 kHz-526,5 kHz, 1611 kHz – 1810 kHz, 2000 kHz – 2300 kHz e 2498 kHz – 3000 kHz, estão destinados a estações utilitárias (Radiofarol, chamadas de emergência, telegrafia marítima, radiolocalização, chamadas seletivas, estações governamentais, e ainda que nos pareça mentira, os próprios telefones que temos em nossas casas. As freqüências mais emblemáticas são os 500 kHz (chamada marítima de socorro telegráfico), os 518 kHz (serviço NAVTEX), os 2182 kHz (chamada marítima de socorro em fonia) e as estações horárias em 2500 kHz. Encontramos também banda de radiodifusão entre os 526,5 kHz e os 1611 kHz (região 1 em passos de 9 kHz e regiões 2 e 3 em passos de 10 kHz); embora no Norte da América expandiram esta banda até os 1700 kHz. A Segunda banda de radiodifusão é a compreendida entre 2300 kHz e os 2498 kHz (120 m), que na região 1 se utiliza basicamente os serviços marítimos e estações fixas-móveis. As freqüências compreendidas entre os 1810 kHz e os 2000 kHz se reservam para a banda de 160 m de radioamadores.

OC (HF) 3 MHz - 30 MHz.

No amplo espectro das Ondas Curtas encontraremos os seguintes serviços (agrupados abaixo):

Bandas de Radioamadores:

80m (3500 kHz - 3800 kHz)

40m (7000 kHz - 7100 kHz)

30m (10100 kHz - 10150 kHz)

20m (14000 kHz - 14350 kHz)

17m (18068 kHz - 18168 kHz). Distribuição recente.

15m (21000 kHz - 21450 kHz)

12m (24890 kHz - 24990 kHz). Nova distribuição

11m (27600 kHz - 28000 kHz). Faixa cidadão

10m (28000 kHz - 29700 kHz)

- **Serviços de Radiodifusão (Estações BCB):**

Banda Tropical de 90m (3230 kHz - 3400 kHz)

Banda Tropical de 75m (3950 kHz - 4000 kHz)

Banda Tropical de 60m (4750 kHz - 4995 kHz y 5005 kHz - 5050 kHz)

Banda de 49m (5950 kHz - 6200 kHz). Radiodifusão Internacional - Tropicais

Banda de 41m (7100 kHz - 7300 kHz). Radiodifusão Internacional - Tropicais

Banda de 31m (9500 kHz - 9900 kHz). Radiodifusão Internacional

Banda de 25m (11650 kHz - 12050 kHz). Radiodifusão Internacional

Banda de 22m (13600 kHz - 13800 kHz). Distribuição recente

Banda de 19m (15100 kHz - 15600 kHz). Radiodifusão Internacional

Banda de 16m (17550 kHz - 17900 kHz). Radiodifusão Internacional

Banda de 13m (21450 kHz - 21850 kHz). Radiodifusão Internacional

Banda de 11m (25670 kHz - 26100 kHz). Radiodifusão Internacional

O resto da banda corresponde a estações e serviços utilitários. Compreendem entre outros: Comunicações aeronáuticas, estações fixas-móveis, radiomedicina, resgate e socorro espacial, serviços meteorológicos, estações horárias (freqüências e Standard em 5000, 10000, 15000 e 20000 kHz), telefonia, estações móveis de terra, radioastronomia, investigações científicas, radiofaróis, satélites, etc.

Os usos são múltiplos e a teoria da União Internacional de Telecomunicações (UIT) está muito longe da prática da escuta, onde podemos encontrar quase que qualquer emissão em qualquer freqüência.

MAF (VHF) 30 MHz - 300 MHz.

Se há uma parte do espectro radioelétrico em que impera a lei do mais forte, este é o das MAF (VHF). A facilidade para conseguir equipamentos, a facilidade de sua instalação e seu tamanho cada vez mais compacto, faz dessa faixa uma desorganização impressionante. Há diferenças entre as três regiões:

30 MHz - 47 MHz (Operações espaciais, serviços fixos terrestres e radioastronomia)

47 MHz – 68 MHz Região 1 (Banda de TV-Radiodifusão em FM). Só se irradia FM comercial nos países do leste europeu.

54 MHz – 72 MHz Região 2 (Banda de Tv-Radiodifusão em FM). Usualmente compartilhada com outros serviços. Entre 50 MHz e 54 MHz se encontra a banda de 6 m de radioamadores, nas regiões 2 e 3. Na região 1 se reduz de 50 MHz a 52 MHz. (se ampliará em breve)

70 Mhz - 70’5 MHz. Somente na região 1 (Banda de 4m de radioamadores)

70’5 MHz - 87’5 MHz (Estações Utilitárias). Região 1 e 3

72 MHz - 76 MHz (Estaciones Utilitárias) Região 2

76 MHz - 108 MHz (Banda de Radiodifusão em FM). Região 2

87’5 MHz - 108 MHz (Banda de Radiodifusão em FM). Região 1 e 3

108 MHz -144 MHz Estações Utilitárias diversas (ILS, VOR, Banda Aérea, Satélites, estações espaciais, etc...)

144 MHz - 146 MHz (Banda de 2 m de Radioamadores). Região 1. nas Regiões 2 e 3 de 144 MHz a 148 MHz A partir de aqui, nas Regiões 1 e 3 temos:

De 146 a 174 MHz, serviços diversos dos comentados anteriormente, incluindo serviços privados e públicos de comunicações. De 174 a 230 MHz se localiza uma Banda de Radiodifusão utilizada para emissão de TV (bandas de vídeo e áudio) e que se compartilha com usos privados fixos e móveis. De 230 a 300 MHz se escutam serviços privados y públicos diversos.

Na região 2 existem algumas diferenças: De 148 a 174 MHz encontramos emissões como as ditas anteriormente para a região 1. A Banda de Radiodifusão se estende aqui entre os 174 e os 216 MHz. De 216 a 220 MHz se volta a repetir os

serviços de radiolocalização e estações fixas-móveis marítimas. aqui encontramos uma banda adicional de radioamadores que se estende desde os 220 aos 225 MHz. A partir de aqui, e até os 300 MHz escutamos as estações privadas e públicas de diversa índole.

UHF 300 MHz - 3 GHz.

Os serviços que encontramos aqui são diversos. Na maioria do espectro temos comunicações de estações fixas e operadores móveis, radioastronomia, aeronavegação, sinais horários por satélites, satélites de observação direta, ajudas meteorológicas, GPS e telefonia móvel. Aqui há também bandas de radioamadores, que são:

Banda de 70cm (430 MHz - 440 MHz)

Banda de 33cm (902 MHz - 928 MHz)

Banda de 23cm (1240 MHz - 1300 MHz)

Banda de 13cm (2320 MHz - 2450 Mhz)

As bandas de Radiodifusão (que também existem aqui) se encontram nas seguintes freqüências: De 470 a 608 MHz, de 614 a 890 Mhz, y de 942 a 960 MHz.

O Direito a utilização do espectro no Brasil era livre de cobrança, mas hoje em dia a Anatel é responsável por fazer licitações e controlar a utilização do espectro.

- **Segurança e privacidade**

A interface de rádio aberta é muito mais fácil de ser burlada do que sistemas físicos tradicionais. Para solucionar deve-se sempre utilizar a criptografia dos dados através de protocolos tais como WEP ou IPsec.

- **Segurança.**

A maior dúvida sobre o uso de redes sem fio recai sobre o fator segurança. 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? Como disse acima, 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.

Alguns kits permitem ainda conectar antenas Yagi, ou outras antenas de longo alcance nas interfaces de rede, o que aumenta ainda mais o alcance dos sinais, que com

as antenas especiais pode chegar a mais de 500 metros. Veremos isto com mais detalhes logo adiante.

Para garantir a segurança, existem vários sistemas que podem ser implementados, apesar de nem sempre eles virem ativados por default nos pontos de acesso.

Neste caso, qualquer PC da rede (um intruso que se conecte a ela) pode acessar a ferramenta de configuração. Para se proteger o usuário deve alterar a senha de acesso default e se possível também alterar a porta usada pelo serviço. Assim o usuário terá duas linhas de proteção. Mesmo que alguém descubra a senha ainda precisará descobrir qual porta o utilitário está escutando e assim por diante.

Em outros casos será necessário instalar um programa num dos micros da rede para configurar o ponto de acesso, mas vale as mesmas medidas de alterar a senha default e se possível a porta TCP utilizada pelo serviço.

Dentro do utilitário de configuração o usuário 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. Vamos então às configurações:

- **ESSID**

A primeira linha de defesa é o ESSID (Extended 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 o usuário 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 ESSID". Ao ativar esta opção o ponto de acesso envia periodicamente o código ESSID 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". O usuário não precisará mais configurar manualmente o código ESSID 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**

Apenas o ESSID, oferece uma proteção muito fraca. Mesmo que a opção broadcast ESSID esteja desativada, já existem sniffers que podem descobrir rapidamente o ESSID 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 ESSID 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.

O WEP [2] usa o algoritmo de criptografia simétrica RC4. O RC4, a partir da junção da sua chave fixa de 40 bits, com uma seqüência de 24 bits variável conhecida como vetor de inicialização (IV), cria uma seqüência de bits pseudoaleatórios que é, através de ou-exclusivo (XOR), operados aos dados que serão criptografados. O IV

também é transmitido junto com cada pacote criptografado. E a norma do padrão sugere que esse IV seja variado a cada pacote enviado.

O receptor, que também conhece a chave fixa, recebe o pacote, retira o IV dalí e aplica o processo inverso usando a mesma operação de XOR, para descriptografar o pacote e revelar a mensagem.

O RC4 é um algoritmo de fluxo, isto é, o algoritmo criptografa os dados à medida que eles são transmitidos, o que faz com que o RC4 seja um algoritmo de alto desempenho. O RC4 pouco foi criticado, e aqueles que o criticaram tiveram que, posteriormente, remover as suas críticas. Talvez porque o RC4 seja um algoritmo realmente bom e muito simples, ou talvez pela força do seu autor, o respeitado Ron Rivest, um dos sócios da RSA Security e professor do MIT.

Segundo [12], infelizmente o WEP não foi submetido à revisão de um número suficientemente grande de outros pesquisadores. O preço dessa imprudência é que várias falhas foram inseridas no protocolo então novo. Dinheiro e trabalho foram jogados fora, pois o mercado, ansioso pelas novas aplicações que poderia vender com a nova tecnologia, investiu muito.

- **Reutilização do vetor de inicialização**

Como o IV tem 24 bits, ele assume valores entre 0 e 16M, e normalmente ele sempre começa do 0 e é incrementado a cada envio de pacote. Chegará um momento que o IV assumirá novamente os mesmos valores. Podemos calcular quanto tempo vai demorar para esse IV voltar a assumir o valor 0 novamente: imagine uma conexão cuja banda seja de 5Mbits/s.

$$(5Mbits/8)*1500 \cong 416 pac/s$$
$$2^{24} pac/416 \cong 40.329 seg \; ou \; 11h12m$$

Ou seja, numa conexão de 5Mbits/seg, o IV voltará a assumir o mesmo valor em menos de meio dia. Se a implementação assumir que o IV terá valores aleatórios teremos a repetição de um IV em menos tempo. E é a partir dessa repetição de IV que o WEP pode ser quebrado. A chave, K, é fixa, e foi configurada nos clientes que estão se comunicando, logo o par <K,IV> repetir-se-á sempre que o IV se repetir. E sempre que eles se repetirem, gerarão a mesma cadeia pseudo-aleatória, que iremos referenciar como RC4(K,IV).

Imagine dois textos legíveis distintos P_1 e P_2, que são criptografados através da mesma cadeia pseudo-aleatória RC4(K,IV) em C_1 e C_2.

$$C_1 = P_1 \otimes RC4(K, IV)$$
$$C_2 = P_2 \otimes RC4(K, IV)$$
$$C_1 \otimes C_2 = (P_1 \otimes RC4(K, IV)) \otimes (P_2 \otimes RC4(K, IV)) = P_1 \otimes P_2$$

Pelas propriedades do XOR (ou-exclusivo), podemos dizer que de posse de dois textos criptografados e um texto legível é possível descobrir o outro texto legível, pois:

$$C_1 \otimes C_2 \otimes P_1 = P_1 \otimes P_2 \otimes P_1 = P_2$$

- **CRC32 linear**

Outra grande fraqueza do WEP é o seu algoritmo de garantia da integridade (ICV - integrity check value), que é o CRC32.

O CRC32 é linear, isto é,

$$c(x \otimes y) = c(x) \otimes c(y)$$

para qualquer valor de x e y. Essa propriedade serve para qualquer tipo de algoritmo CRC.

Uma conseqüência dessa propriedade é a possibilidade de se fazer modificações controladas no pacote, sem que sejam detectadas por qualquer um dos dispositivos transmissores ou receptores. Veremos que é possível alterar o conteúdo dos pacotes apenas com o conhecimento da string de valores pseudo-aleatórios.

Vamos lembrar como é formado o texto criptografado C, que corresponde ao texto legível P. M é a mensagem a ser criptografada.

$$C = RC4(IV, K) \otimes \langle M, c(M) \rangle$$

Vamos imaginar um outro texto criptografado, C', que seja a imagem da encriptação de um outro texto legível, M', onde M'=MÄD, onde D é a alteração controlada que se deseja fazer. Veja só o desenvolvimento da fórmula a seguir.

$$C' = RC4(IV, K) \otimes \langle M', c(M') \rangle$$
$$C' = RC4(IV, K) \otimes \langle M \otimes D, c(M \otimes D) \rangle$$
$$C' = RC4(IV, K) \otimes \langle M \otimes D, c(M) \otimes c(D) \rangle$$
$$C' = RC4(IV, K) \otimes \langle M, c(M) \rangle \otimes \langle D, c(D) \rangle$$
$$C' = C \otimes \langle D, c(D) \rangle$$

Ou seja, pode-se interceptar o pacote, fazer a alteração, corrigir o ICV, e a alteração não será detectada, pois o sistema de manutenção de integridade foi perfeitamente burlado.

- **Gerenciamento de chaves**

O padrão IEEE 802.11 não especifica como deve ser a distribuição das chaves. Ele é baseado num mecanismo externo de distribuição global da chave em um vetor de 4 chaves.

Cada mensagem contém um campo de identificação de chave para especificar o índice do vetor da chave que está sendo usada. Na prática, a maioria das instalações utiliza a mesma chave para todos os dispositivos.

Isso traz problemas profundos à segurança dessas instalações, uma vez que a chave é compartilhada com vários usuários, fica muito complicado manter o segredo. Alguns administradores de rede tentam amenizar o problema não revelando a chave secreta ao usuário final, configurando, eles mesmos, os dispositivos. Mas isso não traz a solução, pois as chaves continuam guardadas nos dispositivos remotos.

A reutilização de uma única chave por vários usuários também aumenta as chances da colisão do IV. A chance de uma colisão aleatória aumenta proporcionalmente ao número de usuários.

Uma vez que a troca de chaves requer que cada usuário reconfigure o seu dispositivo, as atualizações dos drivers controladores dos cartões de rede (NIC) serão cada vez mais raros. Na prática, a troca demorará meses ou anos para acontecer, dando mais tempo para os intrusos analisarem o tráfego.

- **Não autentica do ponto de acesso**

Com o WEP, a interface de rede pode se autenticar no ponto de acesso, mas não há previsão para que o ponto de acesso se autentique junto à interface de rede. O

resultado é que é possível para um hacker desviar os dados que vão para os pontos de acesso para um terceiro ponto, fazendo um caminho alternativo (Man in the Middle).

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 o usuário 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.

Um detalhe interessante foi a partir do início de 2002 é que os pontos de acesso começaram a suportar o uso de chaves de encriptação dinâmicas, que não exigem configuração manual. Ao adquirir um ponto de acesso agora é importante verificar se ele pode ser atualizado via software, para que mais tarde o usuário possa instalar correções e suporte a novos padrões e tecnologias.

- **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, o usuário 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 o usuário estará pagando também pela camada extra de encriptação.

- **Permissões de Acesso.**

Além da encriptação é necessário 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 ou ainda o Linux, via Samba, 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.

- **Como os dados são transmitidos e interferência.**

As redes 802.11b transmitem sinais de rádio na faixa dos 2.4 GHz utilizando um modo de transmissão chamado Direct Sequence Spread Spectrum, onde o transmissor escolhe uma freqüência onde não existam outras transmissões e se mantém nela durante o período de operação, a menos que o nível de interferência atinja um ponto crítico. Neste caso os transmissores procurarão outra freqüência disponível. O padrão 802.11b utiliza freqüências entre 2.4 e 2.48 GHz, com um total de 11 canais disponíveis (2.412, 2.417, 2.422, 2.427, 2.432, 2.437, 2.442, 2.447, 2.452, 2.457 e 2.462 GHz).

Os transmissores podem utilizar qualquer uma das faixas em busca da banda mais limpa, o que já garante alguma flexibilidade contra interferências. Apesar disso, as redes 802.11b possuem pelo menos quatro inimigos importantes: os transmissores bluetooth, telefones sem fio que operam na faixa dos 2.4 GHz, aparelhos de microondas e outros pontos de acesso 802.11b próximos.

Em nenhum dos quatro casos existe o risco da rede chegar a sair fora do ar (mesmo em casos extremos), mas existe a possibilidade de haver uma degradação de desempenho considerável.

O Bluetooth costuma ser o mais temido, pois também é um padrão de redes sem fio e também opera na faixa dos 2.4 GHz. Mas, na prática, o Bluetooth é o menos perigoso dos quatro, pois utiliza um modo de transmissão diferente do 802.11b, chamado Frequency Hop Spread Spectrum, onde os transmissores mudam constantemente de freqüência, dentro do conjunto de 79 canais permitido pelo padrão.

Esta é uma forma de evitar interferência com outros transmissores Bluetooth próximos, já que a seqüência é conhecida apenas pelos dispositivos envolvidos e, em conseqüência, também evita uma interferência direta com transmissores 802.11b.

Na prática, os transmissores Bluetooth podem causar uma pequena perda de desempenho nos momentos em que tentarem transmitir na mesma freqüência dos transmissores 802.11b. Mas, como o chaveamento é muito rápido, isto só chega a ser um problema nas transmissões de vídeo ou outros tipos de mídia via streaming, onde qualquer pequena pausa já atrapalha a visualização.

Os modelos de telefone sem fio que operam na faixa dos 2.4 GHz são um pouco mais perigosos, já que ao contrário do bluetooth operam a uma freqüência fixa. Neste caso o telefone pode invadir a freqüência utilizada pela rede, prejudicando a velocidade de transmissão enquanto estiver sendo usado.

Os aparelhos de microondas também utilizam ondas de rádio nesta mesma faixa de freqüência e por isso também podem atrapalhar, embora apenas caso fiquem muito próximos dos transmissores. Caso o microondas fique a pelo menos 6 metros, não haverá maiores problemas.

Finalmente, chegamos ao problema final. O que acontece caso todos os seus vizinhos resolvam utilizar redes 802.11b, ou caso o usuário precise utilizar vários pontos de acesso na mesma rede?

Como disse acima, os dispositivos de cada rede podem utilizar qualquer um dos 11 canais permitidos pelo padrão. Mas existe um porém: dos 11, apenas 3 canais podem ser utilizados simultaneamente, pois os transmissores precisam de uma faixa de 22 MHz para operar.

Se existirem até 3 transmissores na mesma área, não haverá problemas, pois cada um poderá utilizar um canal diferente. Com 4 ou mais pontos de acesso o cliente terá perda de desempenho sempre que dois tentarem transmitir dados simultaneamente.

Na prática, o cenário é parecido com o que temos numa rede Ethernet. Como o Hub encaminha todos os pacotes para todas as estações, apenas uma estação pode transmitir de cada vez. Sempre que duas estações tentam transmitir ao mesmo tempo, temos uma colisão de pacotes e a rede fica paralisada por alguns milessegundos, até que as estações possam voltar a retransmitir, uma de cada vez.

No 802.11b temos um cenário parecido. Com vários pontos de acesso operando no mesmo canal, as transmissões precisam ser feitas de forma alternada. Na melhor das hipóteses, o usuário não terá 11 megabits para cada um, mas 11 megabits para todos.

Naturalmente isso só se aplica nos momentos em que ambos transmitirem ao mesmo tempo.

Mais uma curiosidade é que é possível aproveitar os três canais simultâneos para utilizar dois ou três pontos de acesso no mesmo local, como uma forma de aumentar a performance da rede (no caso de redes muito movimentadas, com muitas estações), dividindo os usuários entre os pontos de acesso disponíveis. Existem alguns casos de pontos de acesso que trabalham simultaneamente nas três freqüências, como se fossem três pontos de acesso distintos.

2.8 Elaboração de orçamento e viabilidade de instalação.

O mercado de redes sem fio ainda está em expansão. Existe um grande interesse por parte dos fabricantes em popularizar a tecnologia pois os periféricos para redes Ethernet já estão tão baratos que a margem de lucro dos fabricantes, mesmo dos que vendem soluções mais caras, como a Intel e 3Com é irrisória. Além disso, eles só conseguem vender novos componentes para quem ainda não tem redes, já que placas de rede e Hubs são componentes bastante duráveis, na maioria das vezes aproveitados em vários upgrades.

As redes sem fio são a chance de conseguir convencer os usuários a trocar boa parte da base instalada. Enquanto escrevo (Agosto de 2004) os pontos de acesso ainda custam de 150 e 250 dólares e as interfaces de rede custam de 100 a 150 dólares, em média. Nos EUA os valores já estão um pouco mais baixos que isto e no Japão os pontos de acesso e interfaces chegam a serem vendidos por 100 e 60 dólares respectivamente.

Sem dúvida, os componentes para redes sem fio vão continuar sendo mais caros que os para redes Ethernet por muito tempo. Além dos controladores existem os transmissores e as antenas, que aumentam bastante o custo total do conjunto. Mas o futuro parece promissor.

Conforme a tecnologia for se popularizando e os fabricantes começarem a produzir os componentes em maior quantidade, os preços devem cair para algo próximo de 70 dólares pelos pontos de acesso e 50 dólares pelas interfaces de rede ao longo de 2004.

Outro detalhe importante é que vários fabricantes de placas mãe vêm apresentando projetos de placas com interfaces 802.11b onboard. A primeira foi a Intel, com uma placa de referência apresentada durante a Comdex (a Americana) em Novembro de 2001.

As placas com interfaces onboard serão sem dúvidas muito mais baratas do que o conjunto de placas mãe e uma placa 802.11b separada e passarão a representar uma percentagem considerável do total de placas vendidas, o que poderá ser decisivo para a popularização da tecnologia.

Mas, como vimos, as redes sem fio podem ser usadas como complemento para as redes cabeadas que já existem. Esta é a aplicação ideal, considerando que a velocidade é mais baixa e o custo é mais alto. O melhor custo benefício seria então usar uma rede cabeada para interligar todos os desktops, ligar um ponto de acesso ao hub e usar placas wireless apenas nos notebooks e outros aparelhos portáteis. Se a preocupação for à segurança, é possível incluir ainda um firewall entre a rede cabeada e a rede sem fio.

Mas, não existe garantia que o 802.11b seja mesmo o padrão definitivo. O maior concorrente é o 802.11a, que é menos susceptível a interferências é mais rápido.

Imagine uma cidade onde um cliente entra em um café, abre o notebook ou aciona qualquer outro dispositivo wireless e começa a navegar pela web, consultar e-mails e trocar mensagens instantâneas com amigos e colegas de trabalho. Depois, chegado o horário do compromisso, ele entra no táxi e, sem perder a conexão, continua o trabalho. Ao final do dia, um cliente que está longe de casa senta-se no bar ou no lobby do hotel para um drink e mais uma atualização de compromisso, resposta de mensagens e troca de informações com o sistema corporativo.

Não, não se trata de uma cidade norte-americana ou européia, regiões aonde a febre das redes locais sem fio vem tomando proporções superiores aos casos de pneumonia viral. Estamos falando de Brasil, mais especificamente de São Paulo, onde falta apenas a conexão com a rede pública de telefonia celular para que um executivo possa resolver as suas pendências sem precisar de um ponto de acesso fixo.

Com investimento da ordem de US$ 1 milhão, a Pointer Networks nasceu com o objetivo de se tornar um prestador de serviços Wi-Fi e, desde fevereiro de 2002, construiu 21 redes móveis sem fio com padrão 802.11 (hotspots) nos aeroportos do País.

Roberto Ugolini Neto, presidente da empresa, informa que tem 2000 assinantes dos serviços e contratou links da Embratel para acesso à Internet depois de fechar

contrato com a Infraero. Pelo acesso, são cobrados R$ 50 mensais sem limites no volume de bits trafegados nem tempo de uso.

O nome Pointer Networks também assina o projeto da rede Fran's Café. Cinco lojas já oferecem o serviço em São Paulo e até o final do ano os 80 pontos de venda da rede – São Paulo, interior e litoral, além de outras praças como Rio de Janeiro, Recife e Curitiba – serão equipados com solução Wi-Fi. "É uma forma de oferecermos conveniência aos nossos clientes", define Laura Modé, gerente de negócios da empresa de franquias. "Quando toda a rede estiver coberta, o cliente vai escolher o Fran's Café também levando em conta que terá acesso fácil à Internet", determina.

Outra iniciativa foi ativada pela rede de hotéis do grupo Accor. A companhia selou parceria com a operadora de serviços móveis Oi, do grupo Telemar, para a instalação de hotspots nos 110 hotéis e flats do grupo no País.

O Oi Hotspot, serviço que permite acesso público à Internet sem fio, foi lançado durante a Telexpo, evento que aconteceu em São Paulo no final de março de 2003. A previsão é que sejam instalados de 80 a 100 hotspots nos hotéis Accor este ano. O projeto começa pelo Sofitel Rio de Janeiro, na capital carioca, e pelo Mercure Grand Hotel São Paulo Ibirapuera, em São Paulo, unidades que possuem uma alta ocupação de executivos – mais de 90% dos hóspedes.

- **Pesquisas e Projeções**

Apesar do amadurecimento das iniciativas, fornecedores, operadoras e consultorias ainda têm muito trabalho a enfrentar para elevar, no Brasil, as redes locais sem fio (WLAN) aos patamares que essas soluções têm galgado nos Estados Unidos. Segundo levantamento conduzido pelo Yankee Group, 65% das companhias não vêem necessidade de implementação da tecnologia e apenas 21% declaram ter projetos para permitir que seus empregados tenham acesso a dados por meio de redes wireless de larga cobertura (WLAN).

O estudo, feito com 504 corporações médias e grandes em todas as regiões do País, constata também que, mesmo afirmando baixo interesse por rede de dados sem fio, a maioria das empresas (59%) tem contratos firmados com operadoras para fornecer celulares, trunkings ou pagers a seus profissionais.

Também é inversamente proporcional o requisito que essas empresas estabeleceriam para contratar um serviço. Ao serem questionados sobre a capilaridade

do prestador de serviços, os entrevistados disseram que precisam de: cobertura em toda cidade; na cidade e em regiões do interior; e na cidade e nas principais capitais do País.

Entre os interessados no acesso por redes públicas sem fio, 71% disseram considerar o serviço importante em aeroportos, 47% em hotéis e centros de convenções; 18% em casa; e 12% afirmaram já ter acesso contratado. "As empresas estão atentas a soluções sem fio como as WLANs, mas o retorno do investimento ainda não é claro. Isso mostra que os benefícios prometidos são difíceis de quantificar e, conseqüentemente, de se justificar", avalia Luís Minoru Shibata, analista sênior do Yankee Group no Brasil.

Segundo ele, a migração das redes de celulares para tecnologias que permitam a transmissão de dados em alta velocidade deve estimular o surgimento de novas aplicações e o aumento do interesse por parte das corporações. E é nisso que apostam os precursores da tecnologia no País. O modelo de tarifação tanto da rede Fran's Café quanto dos hotéis Accor ainda não está definido. Nas lojas de café, os usuários terão acesso à Internet sem custo por tempo indeterminado. "É certo que teremos, inicialmente, o serviço pré-pago e posteriormente o pós", informa Alberto Blanco, diretor de marketing da Oi, sobre o projeto Accor.

"O novo serviço deverá atender a executivos, médicos, estudantes e outros profissionais que precisam checar e-mails, conectar-se com seus escritórios ou fazer qualquer tipo de serviço quando estão na rua. Eles saberão que podem se conectar em qualquer unidade do Fran´s", afirma Lupércio de Moares, sócio-diretor do Fran´s Café.

- **Para pequenas e médias**

A Brasil Telecom inaugurou uma iniciativa para ampliar a sua participação no segmento de pequenas e médias empresas. Trata-se do pacote de serviços Smart Wi-Fi, voltado a usuários de demandam mobilidade e praticidade.

Ao optar pelo pacote, o cliente assina contrato com o provedor BrTurbo e compra os equipamentos Wi-Fi com preços até 25% inferiores aos do mercado, graças à parceria entre a operadora e a fabricante de equipamentos de conectividade U.S. Robotics.

➢ Wi-Fi no mundo

Como nos EUA, no Canadá já oferece AcessZone, um programa piloto que visa disseminar a instalação de redes Wi-Fi em parques públicos, estações ferroviárias, aeroportos, universidades e até hospitais. A previsão é de que 40 mil pontos de acessos públicos à Internet de alta velocidade sejam instalados no país nos próximos quatro anos.

Na Europa, o quadro e otimismo com o Wi-Fi são semelhantes. Em 2003, o Parlamento Europeu aprovou uma diretriz no sentido de que todos os países do "velho continente" adotem as medidas necessárias para ampliar em curto prazo o acesso a web em banda larga. E o wi-fi, segundo os parlamentares europeus, é o caminho mais rápido, inovador e promissor para que todos os cidadãos europeus tenham acesso a serviços públicos por conexões em alta velocidade, complementando outras formas de acesso e infra-estrutura existentes.

As primeiras propostas para implantação de redes públicas wi-fi foram apresentadas em junho de 2002, durante um congresso mundial de rádio comunicação. O parlamento europeu espera que milhares de redes para conexão à Internet via rádio estejam implantadas antes de 2005. Depois, é só chegar com o notebook e se conectar sem o risco de ficar sem o equipamento.

No Brasil, por enquanto, as Wi-Fi são conhecidas apenas por uma pequena minoria, mas algumas redes de lanchonete já começam a adotá-las com objetivos comerciais ou numa forma eficiente de marketing. É o começo. Mas a disseminação só vai deslanchar (sem trocadilhos) quando assumida por quem de direito. Não precisa fazer. Deixa que "a gente faz". Mas precisa dizer que quer fazer. E criar o caldo de cultura necessário à sua disseminação.

➢ Wi-Fi na sua vida

Redes sem fios, sem cabos, sem complicação. E mais: a um custo muito inferior ao da infra-estrutura tradicional

Para todos aqueles de alguma forma envolvidos com tecnologia, fiquem atentos a duas tendências muito quentes: Wi-Fi e TV Digital. A primeira já está chegando por aí. A segunda ainda demora um pouco, mas com certeza terá grande impacto por aqui, já que o Brasil tem uma das maiores penetrações de televisão do mundo. E como o

projeto se trata de Wi-Fi, e as coisas andam muito depressa, vamos falar logo antes que a próxima bolha estoure sem discutirmos o assunto.

Como tudo em nossa área começa por uma sigla, vamos a ela: Wi-Fi quer dizer Wireless Fidelity, que poderia ser traduzido como fidelidade sem fio, o que quer que isso queira dizer. Na realidade, a denominação genérica mais adequada seria WLAN – Wireless Local Area Network, ou seja, a nossa conhecida e tão valiosa rede local, agora em versão totalmente sem fio. E sabem onde eu vi a primeira WLAN? Não foi em nenhuma empresa de alta tecnologia, mas na casa de um amigo meu, que instalou a sua rede familiar. Sem fios, sem cabos, sem complicação. Mas o melhor de tudo é o baixo custo: algo entre 100 e 400 dólares são suficientes.

Se funciona em casa, claro que é bom também para as empresas. Mais que isso, as novas possibilidades de negócio que estão surgindo são imensas. Veja bem, se um usuário chega em casa com o seu notebook e pode ser autenticado na rede local, por que não fazer o mesmo em qualquer lugar público, como um aeroporto ou restaurante? E mais, qualquer dispositivo móvel, como um handheld, pode também ser autenticado e ingressar no maravilhoso mundo da Internet. Claro que tudo isso pressupõe conexões de alta velocidade, que já são realidade no mundo wireless.

Aí entra em cena a Wi-Fi Alliance (www.wi-fizone.org). Trata-se de uma associação internacional, formada em 1999 com o objetivo de certificar a interoperabilidade de produtos WLAN. Essa conexão, sendo sem fio, significa um sinal de rádio que transmite num raio de cerca de 100 metros. Todo as empresas imagináveis estão lá: 3Com, Avaya, Cisco, Dell, Ericsson, HP, IBM, Intel, Lucent, Microsoft, Motorola, NEC, Nokia, Nortel, Palm, Siemens, Sony, Toshiba e VeriSign, só para citar alguns dos 183 membros.

Desde Março de 2000 já são 741 produtos certificados pela Wi-Fi Alliance. O padrão adotado é o IEEE 802.11, em três vertentes, que não necessariamente falam entre si. O mais comum é o 802.11b, que opera numa freqüência de 2,4 GHz e permite velocidades de até 11 Mbps. O padrão 802.11g e atinge até 54 Mbps. E, finalmente, o 802.11a, que surge como o mais promissor, opera em 5,6 GHz a até 54 Mbps. Foi criado também o selo Wi-Fi Zone, para validar os locais de conexão, chamados hot spots. O site da Alliance mostra inclusive alguns endereços no Brasil.

Três pontos para meditar: o Wi-Fi vai acontecer em breve e quem pegar a onda no começo vai se dar bem. Mas lembre-se que tudo o que sobe muito, depois cai. Segundo: os aspectos de segurança ainda estão longe de serem resolvidos, o que

também significa novas oportunidades de negócio. Finalmente, os modelos de negócio, envolvendo muitos fabricantes, provedores, operadoras, hot-spots, etc. Ainda não está claro para saber quem é que vai ganhar ou perder dinheiro.

Resumindo com 400 dólares ou menos,e um prazo de 10 á 15 dias um usuário monta sua rede wi-fi, quanto ao custo de equipamentos, a concorrência e a disseminação da tecnologia vem barateando os custos com o passar dos anos, sendo que as grandes empresas apostam nesta nova tecnologia, para acabar com a estagnação no mercado, e o principal é que o cliente tendo conhecimento do assunto, pode montar sua rede sozinho.

Capítulo 3 – Desenvolvimento

Colocar uma rede Wi-fi para funcionar é muito complicado. O sinal do Wi-fi trafega pelo ar, e são tantas as variáveis ao longo do caminho que não dá para ter certeza de que tudo vai funcionar até que se faça a prova do ambiente final. Isso porque a tecnologia sem fio mais usada, o 802.11b, é a que mais pode sofrer interferências e quedas na potência do sinal. Uma simples parede de concreto, um forno de microondas ou grande recipiente de água no caminho das ondas de rádio podem se transformar em verdadeiras barreiras.

3.1– Característica do Projeto

• Transmissão de dados por ondas de Rádio
• Modulação do sinal sobre uma onda portadora
• Visada
– Ambientes externos
• Requer visada direta
– Ambientes internos
• NÃO requer visada direta

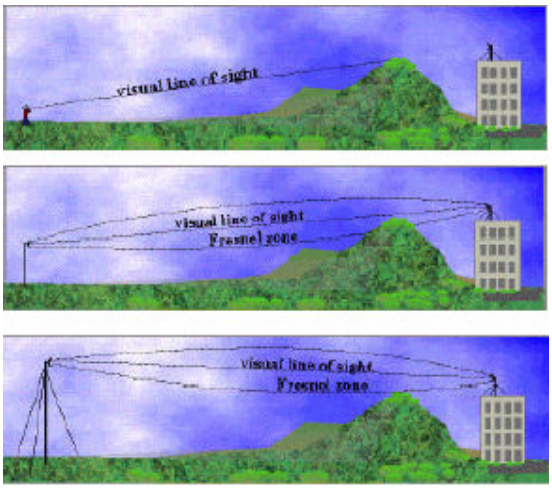


Fig. 3.1 - visada

3.2– Tipo de Transmissão

• Direct Sequence Spread Spectrum (DSSS)

• Frequency Hopping

• CSMA/CA

• Funcionamento

– Ambiente externo

• Ponto a ponto

– Ambiente Interno

• Multiponto

3.3 - Padrões

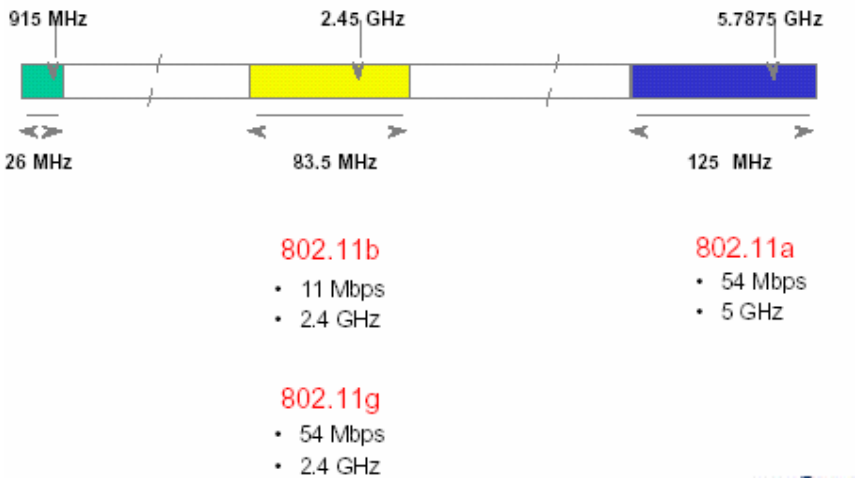


Fig.3.2 - Padrões 802.11

➢ **Relação Freqüência, Potência e Padrão**

Localização	Faixa de freqüência (MHz)	Potência de saída máxima	Padrão
Europa	2400 ~ 2483.5 5150 ~ 5350 5470 ~ 5725	10 mW/MHz 200 mW/MHz 1000 mW/MHz	IEEE 802.11b, HomeRF, Bluetooth HIPERLAN/2 IEEE 802.11a
US, Canada, America Latina	2400 ~ 2483.5 5150 ~ 5250 5250 ~ 5235 5725 ~ 5825	1000 mW/MHz 2.5 mW/MHz 12.5 mW/MHz 50 mW/MHz	IEEE 802.11b HomeRF, Bluetooth HIPERLAN/2 IEEE 802.11a, BWIF IEEE 802.16
Japão	2400 ~ 2497 5150 ~ 5250	10 mW/MHz 200 mW/MHz	IEEE 802.11b HomeRF, Bluetooth HIPERLAN/2 IEEE 802.11a Wireless Home-link

Fig. 3.3 - Tabela de escolha de Padrão

3.4 – Padrão Escolhido 802.11b

• Padrão estabelecido em setembro de 1999
• Velocidade de até 11 Mbps
• Utiliza freqüência de 2.4 GHz
• Conectividade robusta
• Padrão mais utilizado de comunicação sem fio
• Também conhecido como Wi-Fi (Wireless Fidelity)

No Brasil, por enquanto, apenas a tecnologia 802.11b está homologada pela Anatel, a Agência Nacional de Telecomunicações.

- **Padrão Escolhido 802.11a**

• Padrão "Fast Ethernet" para redes sem fio
• Velocidades de até 54 Mbps
• Padrão estabelecido em 2002/2
• Ainda em aceitação pelo mercado
– Diversos produtos disponíveis
• Vantagens
– Alta velocidade
– Menor nível de interferência que o 2.4 GHz
• 2.4 GHz utilizado pelo Bluetooth, Telefones sem fio, Celulares
e formos de microondas
• Desvantagens
– Menor alcance
– Necessidade de maior número de Access Points (4 x).
– Não está homologada pela Anatel.

- **Padrão Escolhido 802.11g**

• Outro padrão de alta velocidade
• Visto como uma evolução do 802.11b
• Velocidades de até 54 Mbps

• Funciona em 2.4 GHz

• Vantagens

– Compatibilidade com o 802.11b

– Melhor alcance que o 802.11a

Conforme os preços dos dispositivos g caiam, a tendência é que vá havendo uma migração natural para essa tecnologia, e o b acabe desaparecendo com o tempo.

• Desvantagens

– Não está homologada pela Anatel.

➢ **Padrão Escolhido 802.11e**

• Padrão em estudo para as redes sem fio

• Implementa

– QoS para redes 802.11b

– Melhor gerência de banda

– Melhor imunidade a interferências

• Detecta interferências e tenta mudar a freqüência de funcionamento.

• Desvantagens

– Não está homologada pela Anatel.

3.5 – Elementos de Hardware

• Placa de rede sem fio

• Access Point (AP's)

• Antena

• Cabo

• Amplificador de potência

3.6 – Placas de Redes

• Faz a interface entre a estação de trabalho e a rede

• Cartão PCMCIA

• Adaptador PCI

• Silver x Gold

– Tamanho da chave de criptografia

Fig. 3.4 - Placa de Rede

No caso dos notebooks e dos handhelds, há modelos que já têm a tecnologia Wi-fi embutida no próprio processador (caso dos laptops 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.

3.7- Access Point

• Conecta a rede cabeada a rede sem fio

– Função de bridge

– Pode assumir a função de roteador

• Configuração da freqüência dos canais

• Permite roaming entre células

– Se área de cobertura dos APs for sobreposta

– APs devem estar em canais diferentes

• Gateway entre 802.11a e 802.11b

O ideal é colocá-lo numa área central da casa ou do escritório. Quanto mais perto os equipamentos estiverem dele, melhor a potência do sinal. Se o usuário 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 que dão acesso a rua, que podem fazer o sinal vazar para áreas estranhas e comprometer a segurança). Depois de instalar o ponto de acesso, teste a potência em diferentes áreas.

Dá para encontrar no mercado brasileiro, diversas opções e modelos de marcas tão diversas quanto Linksys, D-Link, 3Com, Trendware, UsRobotics e NetGear, por preços que começam na faixa dos 300 reais.

Fig. 3.5 - Access Point

3.8 – Gerenciamento

• Implementa o gerenciamento da rede sem fio
• Monitora
– Erros
– Tráfego
– Nível de sinal
– Acessos não autorizados

3.9 – Configuração

• Interface de configuração
• HTTP, Telnet, SNMP ou Interface serial
• Parâmetros de segurança
• SSID: Service Set Identifier
• WEP: Wired Equivalent Privacy
• EAP: Extensible Authentication Protocol
• Parâmetros de rede

• DHCP: Dynamic Host Configuration Protocol

• NAT: Network Address Translation

3.10 – Antenas

• Parte fundamental para o bom funcionamento do sistema sem fio

• Tipos

– Interna / Externa

– Direcional / Omnidirecional

➢ **Antenas Direcionais**

• Concentra o sinal em uma única direção

• Modelos

– Grade

– Semi-parabólica

– Yagi

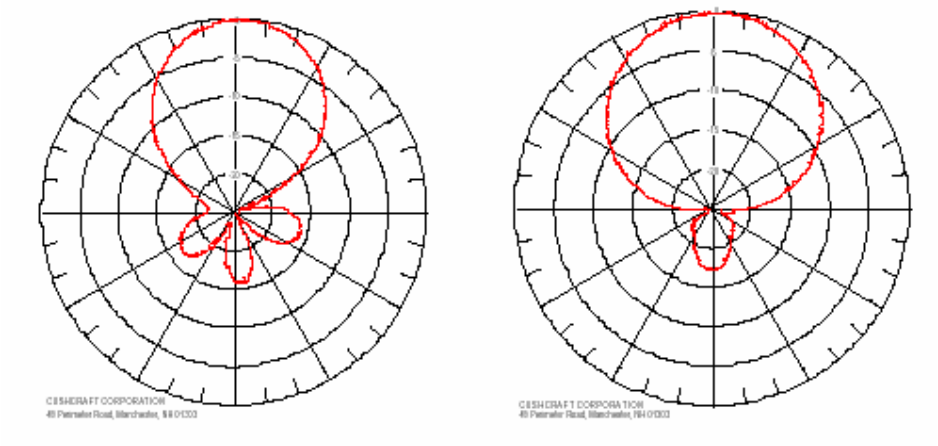


Fig. 3.6 - Diagramas de Irradiação de Antenas Direcionais.

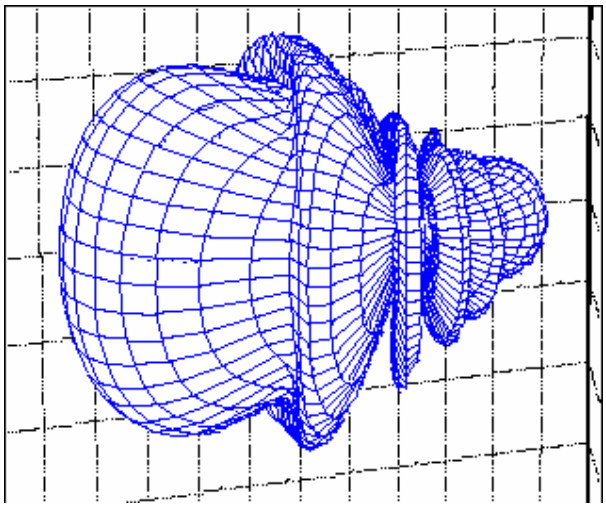


Fig. 3.7 - Diagrama de Irradiação de Antenas Direcionais

- **Antenas Omnidirecionais**

• Transmitem 360 graus em torno do seu eixo

• Também conhecidas como Dipolo

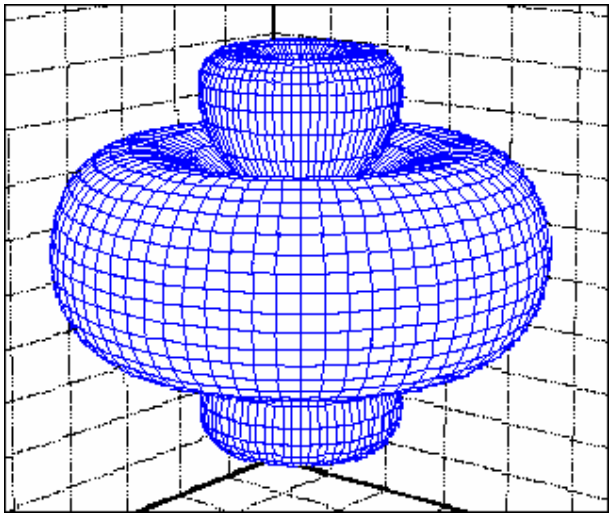


Fig. 3.8 - Diagrama de Irradiação de Antenas Omnidirecionais

3.11 – Polarização

• Define a orientação da onda eletromagnética

• Deve ser igual entre as antenas transmissoras e receptoras

3.12 - Conectores

Conector “N”

Fig. 3.9 - Conector “N”

Conector Lucent

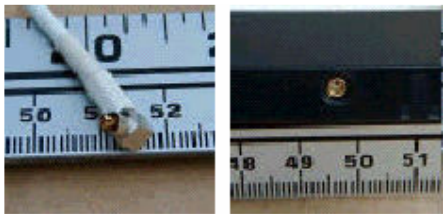


Fig. 3.10 - Conector Lucent

3.13 – Diversos

• Cabo

– RGC213

Fig. 3.11 - Cabo RGC213

• Patch cord

Fig. 3.12 - Patch cord

• Amplificador de potência

Fig. 3.13 - Amplificador

• Protetor de surto

– Surge protector

Fig. 3.14 - Protetor de Surto

➢ **Ambiente Externo – Instalação típica**

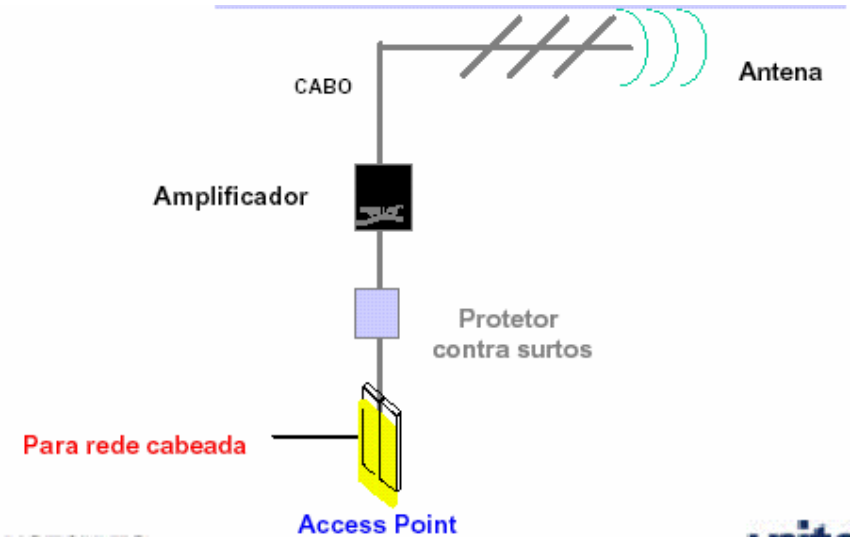


Fig. 3.15 - Ilustração de uma Instalação típica em Ambiente Externo

3.14 – Situando o Projeto

• Análise prévia do ambiente (Site Survey)
• Medida das distâncias entre dispositivos sem fio
• Avaliação das possíveis fontes de interferências

➢ **Site Survey**

• Etapa mais importante na elaboração dos projetos de wireless.
• Atividades.
– Análise do lay -out ou planta do local a ser atendido pela rede wireless.
– Identificar a quantidade de células e Access Points.
– Uso de ferramentas (softwares) para análise de intensidade
de sinal e fontes de interferências
• Baseado no levantamento podemos especificar
– Equipamentos e acessórios necessários
• Antenas
• Access Points
• Quantidade de cabo

• Conectores
• Amplificadores

3.15 – Identificar Interferências

• Fontes mais comuns
– Fornos de microondas
– Telefones sem fio na mesma freqüência
– Alarmes de segurança na mesma freqüência
– Equipamentos Bluetooth
– Motores elétricos
– Outros equipamentos sem fio operando na mesma faixa de freqüência.

➢ **Forno de Microondas**

• O Magnetron dos fornos de microondas tem a freqüência central de funcionamento em 2450~2458 MHz
– Interfere com 802.11b/g
• Intensidade de sinal de 18 dBm
– Medida a 3 metros de distância
• Soluções
– Tentar utilizar canais diferentes
– Aumentar a distância entre o forno e os equipamentos sem fio
– Utilizar materiais bloqueadores de RF
– Utilizar 802.11a

➢ **Materiais ou Situações que Causam Interferência no Sinal da Rede.**

1- Antenas Baixas

Quanto mais altas as antenas estiverem posicionadas, menos barreiras o sinal encontrará no caminho até os computadores. Trinta centímetros podem fazer enorme diferença.

2- Telefone Sem Fio

Nas casas e nos escritórios, a maioria dos telefones sem fio opera na freqüência de 900Mhz. Mas há modelos que já trabalham na faixa de 2,4Ghz, justamente a mesma usada pelos equipamentos 802.11b e 802.11g. Em ambientes com estes tipos de telefones, ou próximos a áreas com ele, a qualidade do sinal do Wi-fi pode ser afetada. Mas isso não acontece necessariamente em todos os casos.

3- Concreto e Trepadeira

Eis uma péssima combinação para o Wi-fi. 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...

4- Micro no chão

O princípio das antenas dos pontos de acesso – quanto mais altas, melhor – também valem para as plaquinhas 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.

5- Água

Grandes recipientes de água, como aquários e bebedouros, são os inimigos da boa propagação do sinal Wi-fi. Evite que esse tipo de material possa virar uma barreira no caminho entre o ponto de acesso e as máquinas da rede.

6- Vidro e Árvore

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

3.16 - Segurança

Segurança em redes *wireless* ainda é um assunto tratado de forma muito delicada, tanto pelos que são usuários da tecnologia, quantos pelos os fabricantes de equipamentos. Segurança, apesar de ser um item fundamental em qualquer projeto de rede, ainda é tratada com certo descaso por aqueles que estão montando uma pequena rede. Apesar dos recursos de segurança atual não serem 100% invioláveis, é sempre bom garantir, ao máximo, que seu ambiente e possíveis dados estejam bem guardados.

A segurança é o calcanhar de Aquiles das tecnologias *wireless* atuais, principalmente o Wi-Fi. Se já era difícil garantir e proteger redes convencionais, imagine conseguir essa façanha com informações voando pelo ar, de um lado para outro. Por ainda não ser uma tecnologia 100% segura, todas medidas de segurança adicionais, mesmo que simples, são bem-vindas.

Qualquer pessoa, sem muito conhecimento avançado sobre o assunto, pode adotar medidas básicas para melhorar a segurança de uma rede *wireless*, o que muitas vezes acaba não acontecendo, criando assim, um verdadeiro paraíso para curiosos e intrusos, muitas vezes conhecidos como *hackers*.

Para dificultar ao máximo, invasões indesejadas em sua rede particular e manter vizinhos bisbilhoteiros longe dos seus arquivos, o usuário pode tomar algumas precauções que veremos a seguir.

3.16.1) Habilite e configure a encriptação de dados.

Utilizar a encriptação de dados é a melhor coisa que um usuário pode fazer para começar a melhorar sua segurança. O método de encriptação mais comum é o WEP (*wired equivalent privacy*), que lhe permite criar chaves de 64, 128 ou 265 bits. Outros métodos, como o WPA (*Wi-Fi Protected Access*), também podem ser utilizados, sempre levando em consideração que a encriptação, apesar de ser um item fundamental, não é a garantia de uma rede impenetrável. O novo protocolo Wi-Fi 802.11i especificado pelo IEEE há pouco tempo , além das chaves convencionais, também traz o sistema AES (Advanced Encryption Standard) que demonstra ser um grande avanço no que diz respeito ao Wi-Fi e seu futuro. Sem dúvidas, uma rede com dados encriptados,

provavelmente espantará 99% dos curiosos de plantão, já que a quebra de chaves de 256 bits ainda não é uma tarefa para qualquer um.

3.16.2) Defina um SSID.

SSID (*service set identifier*) é o nome do seu ponto de acesso, que equipamentos visitantes precisam saber para conectar-se a ele. Pontos de acesso costumam vir com SSIDs padrão de fábrica: nomes como Linksys, Default, 3Com, são alguns dessa longa lista. Um SSID padrão como esses pode ser uma informação bastante útil para quem está tentando invadir uma rede *wireless*, afinal, sabendo qual a marca e modelo de determinado aparelho, fica fácil arriscar e tentar encontrar o endereço IP, usuário e senha do mesmo. Um SSID padrão geralmente significa que a rede foi configurada por alguém com muita pressa e/ou pouco conhecimento.

3.16.3) Mude a senha de administrador do seu *hotspot*.

Uma vez com o SSID padrão em mãos, é muito simples chegar ao endereço IP, pelo qual é possível ter acesso ao módulo de administrador do aparelho. Cada fabricante tem um padrão de endereço IP que é configurado de fábrica, ou quando é dado *reset* no aparelho, por isso é importante habilitar a senha do módulo administrador do seu ponto de acesso. Com a senha habilitada, mesmo que o invasor consiga o número IP do seu ponto, ele não terá como ir adiante e entrar no módulo de administração, conseguindo informações valiosas para quem está atacando.

3.16.4) Configure o servidor.

Se possível, defina no hotspot quais são os endereços MAC das máquinas autorizadas a se conectar. (muitos equipamentos permitem isso) Também limite o número de endereços IPs fornecidos pelo servidor DHCP do seu ponto.

3.16.5) Desligue o *broadcast* do SSID.

O envio do nome SSID pelo sinal é bastante útil nos casos onde o acesso é aberto ao público, pois quem se conecta precisa saber o nome do SSID para efetuar a

conexão. Em redes sem visitantes (apenas computadores que raramente mudam) é possível desligar o envio do SSID pelo sinal, informando manualmente esse nome aos dispositivos autorizados a conectar-se ao ponto. Dessa forma, um estranho pode até saber que a sua rede está ali, mas terá isso como um desafio a mais na hora de invadir o seu ambiente. Caso a sua opção de *broadcast* de SSID estiver habilitada, o ideal então é não manter o nome padrão.

3.16.6) Regule a intensidade do sinal.

Este talvez seja o ponto onde a maioria acaba por pecar ao instalar uma rede particular. A maior parte dos aparelhos permite que o usuário configure a força do sinal, reduzindo ao máximo os sinais que ultrapassam os limites físicos da sua rede/ambiente, impedindo que ele chegue ao alcance do vizinho ou curioso. O ideal é ir baixando aos poucos e testando nos vários pontos da casa ou ambiente. Assim, o usuário dificulta ao máximo uma invasão via rádio, já que a grande maioria não vai estar equipada com antenas direcionais de alto ganho.

3.16.7) Para completar, instale uma *firewall*.

Todos os pontos acima estão relacionados aos estágios a serem vencidos antes de alcançar seu computador. A instalação de um software de firewall no computador reforça ainda mais a segurança, impedindo o acesso de pessoas indesejadas, mesmo que elas tenham vencido todos os estágios anteriores. Os mais conhecidos são da Zone Alarm, McAfee e Norton.

Caso a sua rede *wireless* precise de um nível de segurança maior que a alcançada através das medidas acima, isso indica que ela precisa ser desenhada e implementada por especialistas. Redes para escolas, locais públicos, médias e grandes empresas, condomínios, etc. precisam ser muito bem projetadas. O projeto de uma rede com tamanha importância ou proporções leva em conta fatores como clima e topografia, tarefa que é executada por empresas especializadas.

Capítulo 4 – Pré-Projeto e conclusão

A primeira fase contempla a implementação da solução de uma rede *wireless*; a criação de um sistema de autenticação dos usuários que permita a mobilidade entre dos mesmos dentro de uma escola Virtual; a webização dos processos dentro da Escola de forma a interligar alunos, professores e serviços previamente definidos neste pré-projeto, bem como, a respectiva instalação das plataformas aplicacionais e a disponibilização dos serviços mínimos associados e acordados.

4.1) Implementação da solução de rede wireless

Identifique em planta e por grau de prioridade (1- Imprescindível, 2- Necessário, 3- Desejável, 4- Acessório), os locais onde pretende oferecer conectividade, bem como o número de Acess Points (AP).

Local	Prioridade	Nº Usuários	Nº de Ap's
Biblioteca (ex)	**1**	**500**	**1**
Salas de aula			
Laboratórios			
Gabinete de Prof's			
Auditório			
Secretaria			
Átrio			
Corredores			
Cantina/Bares			
Estudante			
Reitoria			
Espaços Abertos			
Outros			

4.2) Criação de um sistema de autenticação

Identifique a solução pretendida e demonstre com um modelo esquemático.

4.3) Serviços e Aplicações

Identifique os serviços que pretende disponibilizar em cada tipo de perfil:

	Armazenamento e partilhamento de arquivos	**Impressão**	**WWW**	**E-mail**	**FTP**
Alunos não graduados (ex)	**não**	**não**	**sim**	**Sim**	**não**
Alunos graduados					
Professores					
Outro pessoal da instituição					
Outro pessoal acadêmico					
convidados					
público					

4.4) Previsão dos Encargos/Orçamentação

Deverá ser referida uma previsão dos encargos, de acordo com elegibilidade exigida no edital da Escola, que contemple nomeadamente os seguintes aspectos:

4.4.1) Instalação da rede e pontos de acesso Wi-Fi:

1. Site Survey – Normalmente é feito sem custos por fornecedores de antenas Wi-Fi.
2. Aquisição das antenas Wi-Fi e respectiva instalação nos locais.
3. Configuração das redes Wi-Fi.
4. Sistema de segurança/autenticação das redes Wi-Fi.
5. Routers.

4.4.2) Aplicações, Serviços e Conteúdos:

Aplicações e Serviços:

1. Hardware (servidores) – referencial 5% do valor total.
2. Software – referencial (compra de software/licenças 40%, Desenvolvimento 20%).
3. Integração de Sistemas – referencial 35%.

Plataforma de gestão de conteúdos:

1. Hardware (servidores) – referencial 5% do valor total.

2. Software – referencial (compra de software/licenças 60%, Desenvolvimento 30%).

3. Integração de Sistemas – referencial 5%.

4.5) Exemplo: Pré-projeto Escola Virtual

Número de alunos: 500

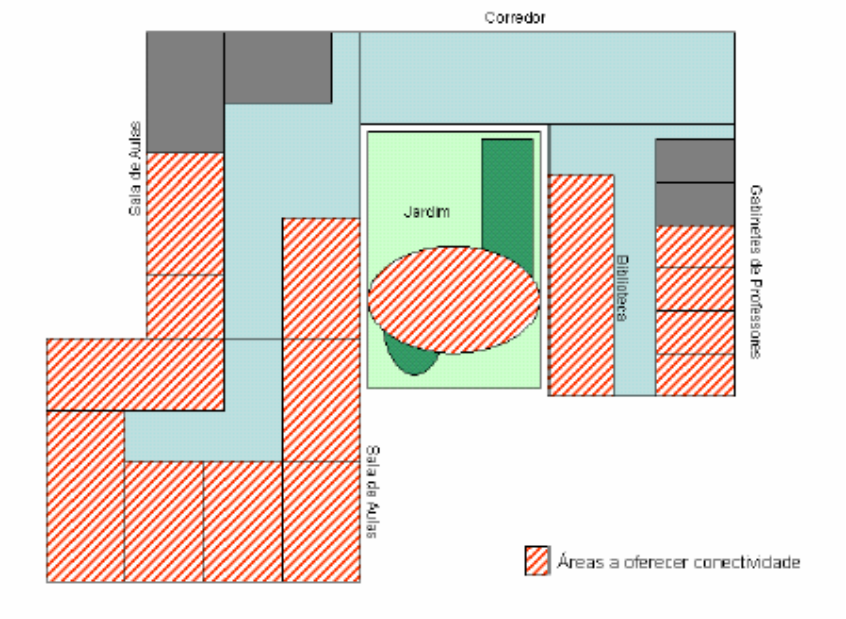
Número de professores: 50

Sites: 1

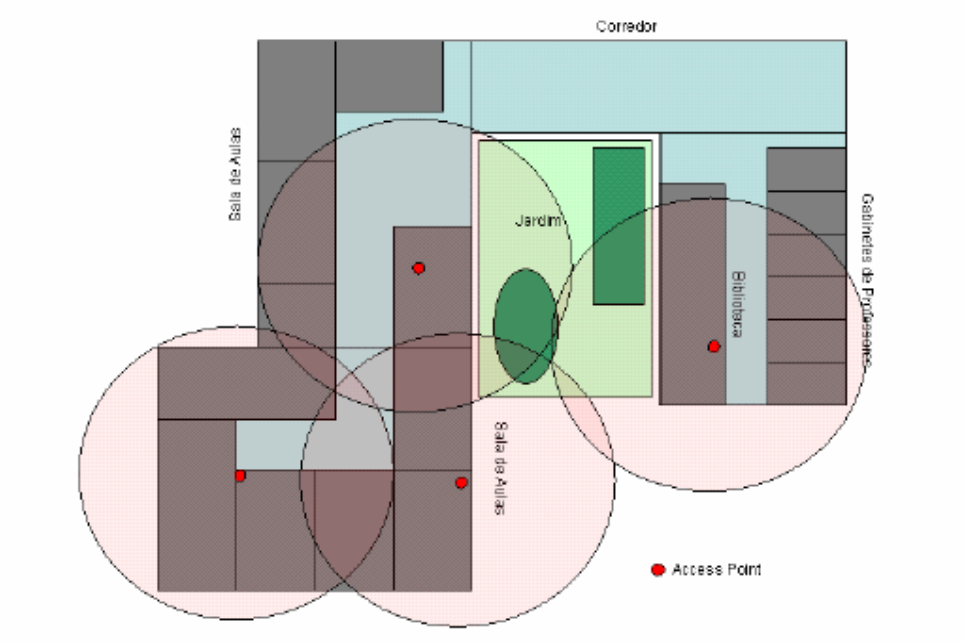
4.5.1) Rede Wi-Fi

Indicação das áreas a cobrir em planta:

- Salas de aula
- Jardim (área comum)
- Biblioteca
- Gabinete de professores



Através de um site survey consegui-se quantificar o número de equipamentos a instalar por forma a permitir oferecer conectividade nas áreas desejadas. A localização determinada para os Access Points foi a seguinte:



4.5.2) Requisitos de equipamento (ver capítulo 3):

X Access point (802.11b/g)

y PC Linux com Apache

z VPN Concentrator

xxxxm Cabo Ethernet

Período de instalação: A infra-estrutura será instalada em 15 dias.

4.5.3) Serviços e aplicações

Definição dos serviços a desenvolver.

4.5.3.1) Fase I

Período: A fase I será desenvolvida em até 2 meses.

4.5.3.1.1)Serviços wireless

Disponibilização de informação bilingue sobre as ligações wireless disponíveis na escola, áreas de cobertura, como se ligar/configurar, aplicações de ligação, informação para utilizadores de fora.

4.5.3.1.2) Serviços pessoais

Pretende-se disponibilizar contas de email e área de arquivos para cada usuário (alunos e professores) com os seguintes perfis:

25MB para alunos

50MB para professores

Estarão disponíveis on-line diversas informações em páginas personalizadas geradas automaticamente. Os conteúdos a disponibilizar nesta fase são:

4.5.3.1.3) Serviços Administrativos

Dados Pessoais – possibilidade de acrescentar e alterar dados.

Horário do Professor.

Agenda Comum (listagem automática de todos os eventos).

4.5.3.1.4) Serviços por Cadeira

Horário das cadeiras com salas de aula.

Horário dos exames/ vigilâncias / atendimento aos alunos.

Programa, bibliografia, métodos de avaliação, calendarização.

Mapa de exames mini-testes e entregas de trabalhos.

Avaliação.

Sumários das aulas.

Aulas eletrônicas (Word ou gravadas- com politica de acesso aos conteúdos conforme presença na aula ou não).

Trabalhos.

Links para artigos ou referências para leitura, problemas propostos, exercícios.

Resolução dos Exames atuais e de anos anteriores.

4.5.3.1.5) Serviços de Biblioteca

Listagem e Motor de pesquisa de livros.

Possibilidade de fazer a reserva online / consultar disponibilidade.

Disponibilização de alguns documentos (pdf).

Horário de funcionamento/ contacto.

4.5.3.1.6) Serviços de Reprografia

Listagem das lições.

Horário de funcionamento.

4.5.3.1.7) Serviços de Pesquisa

Motor de busca de material da instituição, usando a plataforma XML para indexação dos dados.

Plataforma:

Hardware: 3 servidores Pentium 4 @ 2GHz, 1GB RAM, 5TB HD.

SO Linux.

Aplicações base: Apache, sendmail.

O Desenvolvimento será feito com base em módulo open -source disponíveis on-line e módulos de gestão fornecidos pela rede acadêmica.

Todos os conteúdos serão disponibilizados on-line às outras instituições que o desejem através do esquema XML adotado.

4.5.3.2) Fase II

Período: A fase II será desenvolvida em até 6 meses.

4.5.3.2.1) Serviços por Cadeira

Distribuição do serviço docente.

Serviço de aviso aos alunos inscritos.

Reserva de salas de aulas.

Fórum de discussão para temas/trabalhos.

Ver reclamação de notas.

Publicação de ebooks e epapers.

4.5.3.2.2) Serviços de Biblioteca

Disponibilização de todos os documentos (pdf)

4.5.3.2.3) Serviços de Reprografia

Possibilidade de aluno encomendar/pagar on-line as lições que deseja e ir levantar mais tarde.

4.5.3.2.4) Serviços de Pesquisa

Extensão do motor de busca para pesquisas de material das outras instituições ensino, usando a plataforma XML comum.

4.6 - Conclusão

O desafio das redes wireless ainda é ser tão seguras quanto as cabeadas.Uma limitação natural das versões do Wi-fi é o alcance restrito de sinal. Tecnicamente, a explicação está em algo conhecido como campo de visada: uma antena precisa olhar para outra. Isso põe por terra os planos mais ambiciosos de ligar, sem fios, prédios separados por dezenas de quilômetros.

Quanto ao lado positivo, ela é mais prática que as redes cabeadas, podendo atender escolas, hospitais, prédios tombados, regiões dispersas no país, etc. O principal, é que as grandes empresas continuam apostando nesta tecnologia, lançando no mercado, freqüentemente novas tecnologias e produtos.

Apesar dos problemas de segurança, o sistema é totalmente viável e tende a melhorar com lançamento de novos produtos no mercado.

Capítulo 5 – Complementação do Texto

4.1 Bibliografia

[1] www.anatel.gov.br

[2] www.gta.ufrj.br

[3] Data sheet access point

[4] Data sheet wireless cards

[5] The Wireless LAN Association site

[6] Wireless Ethernet Compatibility Alliance site

[7] www.dcc.ufmg.br

[8] www.fernadosenra.hpg.ig.com.br

[9] www.astroamador.hpg.ig.com.br

[10] Enterasys wireless tecnologies

[11] www.3Com.com

[12] BARNES, D. Network America: Wireless security? Read it and Wep. June 27, 2002. URL: http://www.vnunet.com/Features/1133066.

[13] VERISSIMO, F. Segurança em Redes Sem Fio. Monografia do curso de Tópicos Especiais em Redes de Faixa Larga . Janeiro de 2001.

[14] www.infolab.com.br