UNIVERSIDADE ESTADUAL DO SUDOESTE DA BAHIA
CURSO DE BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO
DEPARTAMENTO DE CIÊNCIAS EXATAS

ALAN TEIXEIRA DE OLIVEIRA

ANÁLISE DAS VULNERABILIDADES DAS REDES SEM FIO NA CIDADE DE VITÓRIA DA CONQUISTA - BA

Vitória da Conquista - BA
2010

ALAN TEIXEIRA DE OLIVEIRA

ANÁLISE DAS VULNERABILIDADES DAS REDES SEM FIO NA CIDADE DE VITÓRIA DA CONQUISTA - BA

Trabalho Monográfico apresentado como requisito para obtenção do título de Bacharel em Ciência da Computação do Curso de Ciência da Computação da Universidade Estadual do Sudoeste da Bahia – UESB.

Orientador: Prof. Me. Stênio Longo Araujo.

Vitória da Conquista – BA
2010

AGRADECIEMENTOS

A Deus, por iluminar os meus caminhos;

Aos meus pais, Aldemar e Marinália, pelo amor, carinho, exemplo e incentivos dados;

A meu irmão, Leonan, pelo companheirismo;

A minha noiva, Daiane, pelo carinho e amor dedicados, além do incentivo e apoio para a conclusão deste trabalho.

Ao meu amigo Erinaldo, por ser grande incentivador e parceiro durante todo o curso;

Ao meu orientador, o Prof. Stênio, pelos ensinamentos, sugestões e críticas.

Aos demais amigos, familiares, colegas e professores que de alguma forma contribuíram para a conclusão desse trabalho.

É graça divina começar bem. Graça maior persistir na caminhada certa. Mas a graça das graças é não desistir nunca.
(D. Hélder Câmara)

RESUMO

As redes sem fio apresentam-se em franco crescimento, seja no uso doméstico ou corporativo. A segurança das mesmas ainda é um desafio, pois detalhes podem influenciar na sua qualidade. Este trabalho visa mapear as redes sem fio em uma determinada região da cidade de Vitória da Conquista - Bahia, com a utilização de equipamentos e softwares específicos para tal fim, com o intuito de fazer uma análise de como as mesmas se apresentam, no que tange a segurança. Boa parte das redes encontradas apresenta-se abertas ou com um tipo de criptografia vulnerável.

Palavras-chave: Redes sem fio. Segurança. Criptografia.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE GRÁFICOS

LISTA DE ABREVIATURAS

IEEE - Instituto de Engenheiros Eletricistas e Eletrônicos

ANATEL – Agência Nacional de Telecomunicações

ARPANET - A*dvanced Research and Projects Agency* (Agência de Pesquisas em Projetos Avançados)

FTP - *File Transfer Protocol* (Protocolo de Transferência de Arquivos)

SMTP - *Simple Mail Transfer Protocol* (Protocolo de Simples Transferência de Email)

DNS - *Domain Name System* (Sistema de Nomes de Domínios)

NNTP - *Network News Transfer Protocol*

FHSS - *Frequency Hopping Spread Spectrum*

OFDM - *Orthogonal Frequency-division Multiplexing*

CSMA - *Carrier sense multiple access* (Acesso múltiplo com sensoriamento da portadora)

CERT - Centro de Estudos para Resposta e Tratamento de Incidentes em Computadores

DOS - *Denial of Service*

TKIP - *Temporal Key Integrity Protocol*

EAP - *Extensible Authentication Protocol*

SSID - *Service Set IDentifier*

ABINEE – Associação Brasileira da Indústria Eletro e Eletrônica

SUMÁRIO

1 Introdução

Com o avanço da internet e as novas tecnologias da informação a interligação entre computadores se tornou cada vez mais necessária. A evolução das redes de computadores fez com que aumentasse a necessidade de comunicação entre os mais distintos dispositivos, não somente entre os dispositivos fixos, mas também entre os dispositivos móveis.

A utilização de cabos de par trançado ou fibras, é a forma mais rápida de transmitir dados, contudo, o custo de sua instalação e manutenção cresce potencialmente de acordo com a quantidade de *hosts* e de distância a ser coberta. Nesse contexto ainda existem casos onde não existe a viabilidade técnica e financeira para a instalação das mesmas, daí surge à necessidade da utilização de algum outro meio que promova a conectividade. As redes sem fio cumprem perfeitamente esta necessidade, permitido flexibilizar e ampliar facilmente o alcance de uma rede (MORIMOTO, 2008 e TANENBAUM, 2003).

Cada vez mais é comum a utilização de dispositivos móveis e portáteis que necessitem de uma infraestrutura de rede.

Além disso, a única diferença entre os sistemas sem fio e os cabeados esta em sua forma de transmissão, possibilitando fácil instalação ou adaptação a redes já existente. No entanto, esta característica pode ser a que trará mais problemas, tanto a usuários quanto a técnicos e demais profissionais da área.

A segurança é o fator fundamental a ser analisado ao ser implementado o sistema de rede sem fio, já que nos sistemas cabeados para que este aspecto seja afetado o atacante deve ter um ponto de acesso à rede. Porém, no contexto das redes sem fio a proteção do sistema deve ser feito através da implementação de protocolos de segurança mais confiáveis, pois as informações trafegam através do ar abertamente, necessitando ao atacante somente esta na área de alcance do sinal emitido por uma das antenas de comunicação da rede.

1.1 Contextualização e Motivação

As redes sem fio são cada vez mais utilizadas para promover a conectividade dentro das instituições e organizações. E a interligação à distância entre empresas, suas filiais e seus clientes. Esta é uma nova conjuntura, com ambiente propicio para que pessoas mal intencionadas possam obter acesso à rede e comprometer os computadores e os sistemas das instituições, transformando-as em um ambiente potencialmente inseguro.

1.2 Problematização

Atualmente, existem muitos protocolos para garantir a segurança e integridade das informações trocadas entre os dispositivos sem fio. Porém, a maioria deles apresenta grades falhas na segurança, sendo possível a invasão e o roubo de informações importantes. Muitas vezes isso ocorre por conta da falta de formação dos técnicos envolvidos em sua implantação ou da inexperiência dos usuários, bem como de falhas nos meios que proveem a integridade de tais informações.

Ataques a essas redes são cada vez mais frequentes, além de serem um alvo em potencial de pessoas mal intencionadas. As redes sem fio disponibilizam inúmeros atrativos como protocolos falhos, dificuldade de detecção do atacante, falta de conhecimento técnico para configuração da rede e facilidade de acesso.

1.3 Objetivo Geral

Mapear as redes sem fio em determinada região da cidade de Vitória da Conquista – BA e verificar os protocolos utilizados para promoção da segurança em tais redes.

1.4 Objetivo Específico

Desenvolver, a partir de um estudo dirigido, um referencial teórico sobre as características funcionais e práticas das redes sem fio bem como dos protocolos de segurança implantadas nas mesmas.

Listar os problemas no que tange a segurança de tais redes, fazendo um teste prático de redes já em funcionamento em uma área da cidade de Vitória da Conquista.

1.5 Justificativa

As redes sem fio despontam como uma das tecnologias que mais cresceram nos últimos anos. Sua implementação desordenada e sem uma necessidade de regulamentação, traz graves problemas a segurança de dados.

Dados do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (Cert) mostram que o número de incidentes envolvendo a questão da segurança da informação é cada vez maior. No ano de 2009 foram registrados 358.343 casos relacionados ao problema, o que representa um aumento de 62,02% em relação ao ano de 2008 com 222.252 casos (CERT, 2010).

Aliada muitas vezes ao despreparo técnico, as redes são instaladas sem a preocupação com a segurança, ou na inexperiência dos usuários que na maioria das vezes apenas mantém as configurações padrões dos aparelhos adquiridos.

Protocolos de segurança confiáveis ainda são um desafio as redes sem fio, mas a tendência, com a expansão das mesmas é que os atuais protocolos sejam melhorados.

1.6 Metodologia

Nesta pesquisa foram realizadas as seguintes etapas:

A) Pesquisa bibliográfica aprofundada, com conceituação teórica sobre o funcionamento de redes sem fio e seus principais protocolos de comunicação. Conceitos importantes como topologia, padrões de redes sem fio e rede locais *ethernet*, bem como

os mecanismos de autenticação e criptografia são estudados para o completo entendimento de suas vulnerabilidades. A revisão bibliográfica consiste na busca de informações a cerca do tema proposto. Com a leitura de material já publicado no que diz respeito ao estudo (WAZLAWICK, 2008).

B) Testes realizados, com auxilio de um *notebook* contendo uma placa de rede sem fio, juntamente com um GPS, para mapeamento dos pontos estudados e elaboração de um mapa, No teste foi utilizado o *software Kismet*, instalada em um sistema LINUX com o objetivo de mapear as redes em funcionamento.

C) Resultados com gráficos, mapas, tabelas e conclusões sobre os dados encontrados, levando em conta as vulnerabilidades avaliadas.

2 Referencial Teórico

2.1 Redes de Computadores

Segundo Tanenbaum (2003) as redes de computadores constituem-se de “um conjunto de computadores autônomos interconectados por uma única tecnologia. Dois computadores estão interconectados quando podem trocar informações”.

Uma rede de computadores consiste em um conjunto de dispositivos interligados entre si para compartilhamento de recursos ou periféricos. Geralmente estes dispositivos são chamados de *hosts* e podem ser representados por computadores, impressoras, *scanners* ou quaisquer dispositivos que possuam uma interface de comunicação comum aos demais (WIKIPEDIA, 2010).

Para que a comunicação seja feita de modo satisfatório entra em cena a figura do protocolo, que consiste em um conjunto de regras necessárias à comunicação entre tais dispositivos. Através da utilização de protocolos é que a comunicação flui e os dados podem trafegar de forma correta entre os nós da rede.

O TCP/IP provê a comunicação entre os dispositivos e controlam o fluxo dos dados, além de fazer a identificação dos equipamentos presentes na rede (MORIMOTO, 2008). O TCP/IP é baseado em camadas, onde cada uma delas desempenha um papel importante no funcionamento da rede e seu entendimento é de fundamental importância para diferenciação entre as redes (TANEBAUM, 2003).

A comunicação entre tais dispositivos não precisa ser feita unicamente através de fios, pode ser via fibra ótica, infravermelho, *Bluetooth*, micro-ondas ou satélites de comunicação. Existe uma infinidade de redes de computadores em diversos tamanhos, aspectos e tecnologias utilizadas, além de poderem ser empregadas as diversas formas de comunicação na interligação de uma mesma rede. Outro aspecto importante a ser observado, é que as redes de computadores são sistemas heterogêneos, ou seja, dentro delas pode existir uma gama de *hosts* diferentes e com *hardwares* diferentes, mas os mesmos se comunicam graças à utilização do mesmo protocolo de comunicação (RUFINO, 2007).

2.2 O modelo OSI

Para se obter um padrão na comunicação e na interconexão entre os dispositivos e alcançar acessibilidade universal, a Organização Internacional de Padronização *(OSI – International Standars Organization)* aprovou no inicio da década de 80, um padrão de referencia, denominado Modelo de Referência OSI. Sua última revisão foi no ano de 1995 (SANCHES, 2007).

O modelo OSI, apresentado na Figura 1, possui sete camadas, a saber: Aplicação, Apresentação, Sessão, Transporte, Rede, Enlace de dados e Física.

> (…) esse modelo nasce da necessidade de uniformizar os elementos que participam da solução do problema de comunicação entre equipamentos de diferentes fabricantes. Esses equipamentos apresentam basicamente as seguintes diferenças: Processador central, Velocidade, Memória, Dispositivos de armazenamento, Interfaces para comunicação, Sistemas operacionais (SANCHES, 2007, p. 215).

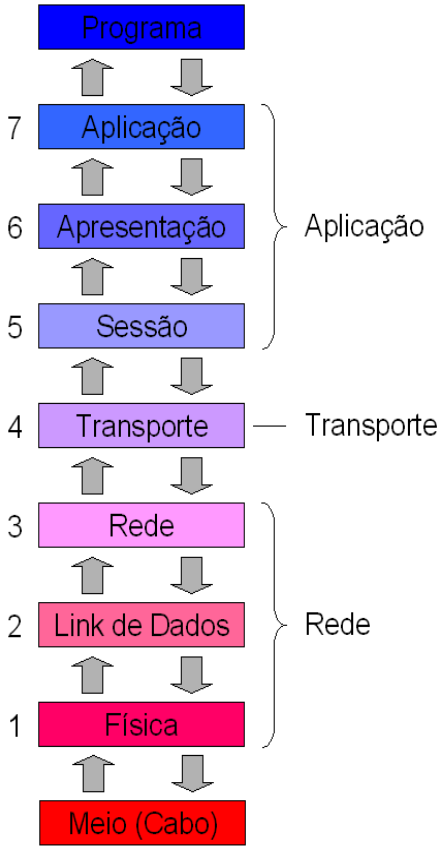


Figura 1 - Modelo OSI
Fonte: (TANEMBAUM, 2003)

O modelo tem o objetivo claro de definir os diferentes aspectos da comunicação entre os mais diversos dispositivos, proporcionando a conexão mesmo em dispositivos

heterogêneos. As camadas do modelo foram definidas de acordo com os seguintes princípios:

1 – A camada deve ser criada onde houver a necessidade de abstração;

2 – Cada camada deve executar uma função específica;

3 – A função de cada camada deve levar em consideração padrões internacionais;

4 – Os limites das camadas devem ser definidos a fim de evitar fluxo de informações nas interfaces;

5 – O número de camadas deve grande o suficiente para que funções diferentes sejam exercidas por camadas diferentes e pequena o suficiente para que sua arquitetura não seja de difícil entendimento e funcionamento (TANEBAUM, 2003).

O modelo estabelece uma estrutura com as seguintes particularidades:

1 – Estrutura Multinível - Foi utilizada uma estrutura de modo que cada nível resolva uma parte do problema, utilizado para tanto, informações de um nível inferior e fornecendo a níveis superiores;

2 – Pontos de Acesso – Em cada camada devem existir pontos de acesso aos serviços;

3 – Dependência dos níveis – Cada nível depende do nível inferior e também do nível superior;

4 – Cabeçalho – Em cada nível um cabeçalho é incorporado, a fim de o nível correspondente no computador receptor fique sabendo que uma informação lhe foi direcionada;

5 – Unidades de Informação – Em cada nível a unidade de informação possui diferentes nomes e estruturas (SANCHES, 2007).

2.2.1 O modelo TCP/IP

O protocolo TCP/IP é usado desde os tempos da remota ARPANET, até a sua atual sucessora, a internet.

> Quando foram criadas as redes de rádio e satélite, começaram a surgir problemas com os protocolos existentes, o que forçou a criação de uma nova arquitetura de referência. Desse modo, a habilidade para conectar várias redes de maneira uniforme foi um dos principais objetivos do projeto, desde o início. Mais tarde, essa arquitetura ficou conhecida como **Modelo de Referência TCP/IP**, graças a seus principais protocolos. Esse modelo foi definido pela primeira vez em Cerf e Kahn (1974). Uma nova perspectiva foi oferecida mais tarde em Leiner *et al.* (1995). A

> filosofia de projeto na qual se baseia o modelo é discutida em Clark (1988) (TANEBAUM, 2003, p. 44).

O TCP foi projetado para proporcionar uma comunicação confiável entre redes não confiáveis. Seu projeto visava à adaptação às mais diversas circunstâncias da rede, como topologias, largura de banda, retardo, tamanho dos pacotes e outras.

> A camada IP não oferece qualquer garantia de que os datagramas serão entregues na forma apropriada; portanto, cabe ao TCP administrar os *timers* e retransmiti-los sempre que necessário(...). O IP foi projetado como o objetivo da interligação entre os computadores, dando uma identificação numérica e diferenciada a cada interface de rede pertencente ao *host* conectado a rede. A tarefa do IP é fornecer a melhor forma possível (...) de transportar datagramas da origem ao destino, independentemente de essas máquinas estarem na mesma rede ou de haver outras redes entre elas (TANENBAUM, 2003, p. 48).

De acordo com Tanenbaum (2003) o protocolo TCP/IP possui cinco camadas (ver Figura 2).

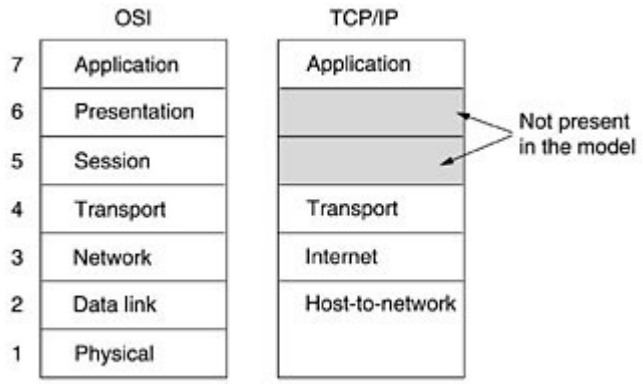


Figura 2 - O protocolo TCP/IP
Fonte: (TANEBAUM, 2003)

Camada host/rede: A primeira camada é onde se encontra um grande vácuo. O modelo de referência TCP/IP não especifica muito bem o que acontece ali, exceto o fato de que o *host* tem de conectar à rede utilizando algum protocolo para que seja possível enviar pacotes IP . É nessa camada onde a comunicação física acontece. É aqui um dos pontos que difere as redes cabeadas, das redes sem fio; o *hardware* e demais equipamentos utilizados para conexão dos dispositivos/*hosts* pertencentes à rede. Ela engloba as características da camada Física e parte da camada de Enlace de dados do modelo de referência OSI (TANEBAUM, 2003).

Camada inter-redes: Comparável à camada de redes no modelo OSI,

responsável pela interconexão entre redes, pela transferência de pacotes entre elas, alem de garantir o tráfego mesmo em redes diferentes e proporcionar que os pacotes cheguem ao seu destino, traçando a melhor rota de entrega, mesmo que em ordens diferentes.

É a camada onde o protocolo IP atua, definindo um formato de pacote padrão, unidade que trafega na rede, mesmo que essa não seja a principal característica dessa camada. Faz o controle de congestionamento pelo descarte dos pacotes excedentes (TANEBAUM, 2003).

Camada de transporte : É a camada localizada acima da camada de inter redes. Tem por fim fazer com que os *hosts* de origem e destino mantenham uma conversação. Dois protocolos são definidos nessa camada: o TCP e o UDP (*User Datagrama Protocol* – Protocolo de datagrama do usuário). O TCP garante a entrega do fluxo de dados do computador de origem a qualquer computar de destino pertencente à rede. Cuida também do fluxo de dados impedindo que um emissor rápido envie muitas informações a um receptor lento ou que esteja envolvido em outra transação (SANCHES, 2003).

O UDP, protocolo de conexão não confiável, destinado a aplicações em que o controle do fluxo das informações é feito pela própria aplicação isentando o protocolo de tal tarefa.

As conexões na camada de transporte podem ser de dois tipos: *half duplex* e *full duplex* . As conexões *full duplex* são mais indicadas pois a comunicação é bidirecional, ou seja, é feita nos dois sentidos, de modo que as aplicações que a utilizam podem enviar receber informações simultaneamente. Já a comunicação *half duplex* a comunicação se dá em um único sentido de cada vez (RUFINO, 2007).

No modelo TCP/IP o transporte pode ser feita de forma “bufferizada”, fazendo um cache dos arquivos a serem transmitidos, aumentando a disponibilidade da rede e agilizando a transferência das informações.

No TCP/IP as camadas de sessão e de apresentação foram suprimidas, pois não se percebeu qualquer necessidade de sua implantação.

Camada de aplicação: Na camada de aplicação ficam localizados os protocolos de nível mais alto.

> (...) O protocolo de terminal virtual (TELNET), o protocolo de transferência de arquivos (FTP), e o protocolo de correio eletrônico (SMTP). (...) Muitos outros protocolos foram incluídos com o decorrer dos anos como o DNS (*Domain Name System*), (...) o NNTP (...) e o HTTP, protocolo usado para buscar páginas na World Wide Web, entre muitos outros (TANEBAUM, 2003, p.47).

2.3 Utilização das redes de computadores

As redes de computadores são utilizadas para os mais diversos fins e em diversas situações. Sua aplicabilidade vai desde tarefas domésticas simples ou grandes aplicações nas indústrias. A maioria das empresas possui um número significativo de computadores, cada um deles até certo ponto funcionam independentemente, mas a certa altura surge a necessidade de conectá-los seja para compartilhamento de uma simples impressora, visando a redução de custos ou até mesmo para um melhor controle de impressões até o compartilhamento de informações importantes, arquivos e até dispositivos físicos como discos rígidos, CD-Roms, aplicativos e dados diversos.

As redes também propiciam a comunicação não só entre computadores que estão próximos, como aqueles situados em um mesmo edifício ou sala, mas também propiciam a comunicação entre distâncias maiores como entre cidades, estados ou até mesmos continentes diferentes, proporcionando grande integração entre filiais espalhadas em diversas localidades. Além do compartilhamento de informações, uma rede de computadores oferece um eficiente meio de comunicação entre indivíduos. Há ainda possibilidade de trabalho cooperado como o desenvolvimento de um relatório ou documento por pessoas localizadas em diferentes locais, mas com acesso à rede corporativa, bem como a realização de reunião por recursos de videoconferências, economizando com despesas de viagens e customizando o tempo; e emissão de pedidos, vendas e compras em tempo real agilizando o processo e mantendo atualizados os registros; e por último a possibilidade do relacionamento direto com os clientes por meio da internet, aproximando-se do cliente, automatizando o atendimento e tendo a loja funcionando ininterruptamente (TANENBAUM, 2003).

O acesso às informações pode ter vários significados dentro do ambiente doméstico. Pode estar relacionado tanto com a obtenção de notícias, bem com a diversão. Os dados disponíveis podem estar relacionados aos mais diversos temas como esportes, ciências, saúde, serviços, histórias, jogos, viagens e muitas outras informações.

O entretenimento também pode ser influenciado pela tecnologia, o compartilhamento de músicas, filmes e todo material multimídia entre os computadores amplia a sua utilização. Jogos despontam como uma grade área dentro da computação e sua jogabilidade e interatividade é expandida através das redes.

O comércio eletrônico facilita a vida das pessoas. Pagamento de contas,

transações bancárias, compras *on-line*, investimentos, e muitas outras atividades podem ser desenvolvidas pela utilização da internet. Sistemas móveis constituem um dos segmentos que mais crescem na indústria da informática. *Notebooks*, PDAs, *smartfones*, e outros dispositivos estão cada vez mais baratos e produzidos em larga escala, o que facilita o acesso de tais equipamentos à um maior número de pessoas. Muitos usuários de computadores domésticos desejam ter acesso às informações localizadas nos mesmos, isso é intermediado através de tais dispositivos (RUFINO, 2007).

A medida que a tecnologia sem fio cresce e os mecanismos para proporcionarem o funcionamento das mesmas novas aplicações podem ser desenvolvidas.

2.4 Redes Sem fio

As redes sem fio ou *wireless*, são constituídas de equipamentos que são interligados por meio de dispositivos que se comunicam sem a necessidade de utilização de cabos; utilizam frequência de rádio, infravermelho ou outro meio onde o tráfego de informações pode acontecer.

A maior diferença entre as redes *sem fio* e as redes cabeadas é o meio de transmissão, e é justamente aí que se encontra o maior problema relacionado à segurança.

2.4.1 Classificação das redes sem fio

As redes *sem fio* podem ser classificas de acordo com a distância de alcance do seu sinal, equipamentos utilizados e meio de transmissão:

WPAN (*Wireless Personal Area Network* – Redes Pessoais Sem Fio) está associada as redes de curta distância geralmente até 10 metros, temos como exemplo as transmissões em infravermelho e *Bluetooth*. É utilizada para conexão de pequenos dispositivos pessoais, como fones de ouvido a equipamentos portáteis, por possuir baixo custo e taxa de transferência limitada. A Figura 3 apresenta o funcionamento da WPAN.

WLAN (*Wireless Local Area Network* – Redes Locais Sem Fio) as redes WLAN, representada na Figura 5 e foco deste trabalho, constituem-se do padrão utilizado atualmente para substituição das redes cabeadas para comunicação entre dispositivos,

compartilhamento de internet e tráfego de dados com velocidades superiores. Pode alcançar grandes distâncias quando associada a transmissores e antenas apropriadas. Sua configuração é simples, e o preço dos equipamentos é cada vez menor devido ao aumento em sua utilização, além do avanço nas tecnologias empregadas.

Figura 3 - Rede WPAN
Fonte: www.dell.com.br

WMAN (*Wireless Metropolitan Area Network* - Redes Metropolitanas Sem Fio), representa na Figura 4, são as redes utilizadas para comunicação dentro do espaço das cidades ou entre cidades e estados diferentes, é apenas uma classificação diferenciada para as WLAN's com um maior raio de alcance. Geralmente é utilizada por provedores e pontos de acesso a serviços ou grandes empresas que têm a necessidade de comunicação com filiais distantes.

WWMAN (*Wireless Wide Metropolitan Area Network* – Redes de Longa Distância Sem Fio) ainda são um novo conceito dentro da área. Trata-se das redes sem fio com grande alcance chegando a países e continentes diferentes. Sua utilidade está no grande crescimento das corporações e a necessidade de interconexão entre as mesmas.

2.4.2 Meios de transmissão

A comunicação entre os dispositivos sem fio pode acontecer de diversas formas e através de diferentes tecnologias como segue:

IrDA (*Infrared Data Association* - Associação de Dados Infravermelho) trata da

comunicação feita através de dispositivos de infravermelho, possui custo reduzido, porém não é muito difundindo, pois, a taxa de transmissão é baixa e a distância de alcance é pequena. O padrão foi criado por uma associação de cerca de 150 indústrias que buscavam uma forma de comunicação barata e de baixo alcance. A comunicação pode ser feita a 115 bps no padrão 1.0 ou a até 4 Mbps no padrão 1.1 e somente em *half duplex* com a transmissão dos pacotes de forma serial.

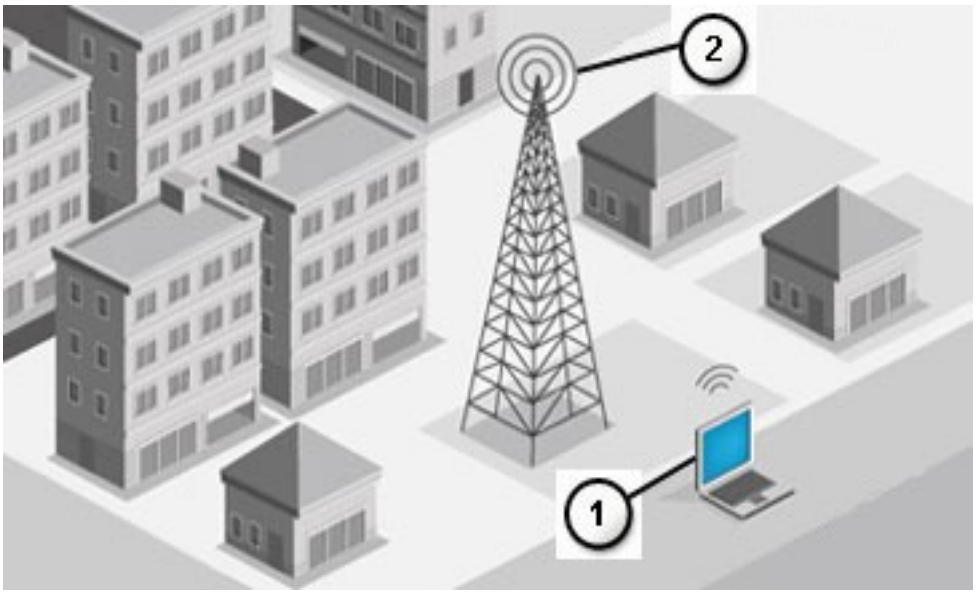


Figura 4 - Rede WMAN
Fonte: www.dell.com.br

Figura 5 - Rede WLAN
Fonte: www.dell.com.br

ZigBee trata do padrão IEEE 802.15.4, ainda em desenvolvimento, muito parecida com o *Bluetooth.* Foi pensada para transmissão em curtas distância de até 70 metros com a velocidade de 250 Kbps. Seu alcance pode ser ampliado se os dispositivos forem colocados em série funcionando como repetidores.

O *Bluetooth,* é um dos padrões mais utilizados para comunicação de dispositivos móveis, como PDAs e celulares. O grande diferencial entre ele e infravermelho é que os dispositivos não precisam estar na linha de visão um do outro, por utilizarem ondas de rádio para comunicação. Possui três classes de operação, a classe 1 que opera a 100mW e tem alcance de aproximadamente 100 metros, a classe 2 com frequência de 2,5 mW e alcance de cerca de 10 metros e a classe 3 com frequência de 1 mW com alcance de 1 metro. Oferece três velocidades distintas: a versão 1.2 com taxa de 1Mbps, a versão 2.0 com taxa de 3 Mbps; e a versão 3.0, ainda em desenvolvimento, com taxa de transmissão de 53 à 480 Mbps. Além disso a comunicação acontece entre dispositivos de mesmo perfil, que são especificações que diferenciam os dispositivos quanto a sua aplicabilidade. A Figura 6 apresentada um dos modelos de adaptador Bluetooth disponíveis no mercado.

WiMax (*Worldwide Interoperability for Microwave Access* - Interoperabilidade Mundial para Acesso de Micro-ondas) corresponde ao padrão IEEE 802.16 publicado em 2002. Especifica a interface de comunicação das redes WMAN. A taxa de transmissão pode chegar a 1GBps e a até 50 km de alcance, com perspectiva de chegar a até 10 GBps. Utilizada para comunicação dos mais diversos dispositivos como PDAs, smartfones, celulares, notebooks, impressoras e outros equipamentos compatíveis.

Figura 6 - Adaptador Bluetooth
Fonte: www.wikimedia.org

Wi-Fi diz respeito à tecnologia de comunicação sem fio mais utilizada atualmente. Inicialmente a marca foi licenciada pela Wi-Fi *Alliance*, mas atualmente este termo é utilizado para descrever um padrão de comunicação sem fio inspirado na norma IEEE 802.11. Ela opera em faixas de frequência que não necessitam de autorização dos órgãos de regulamentação em comunicação, no caso do Brasil, a ANATEL (Agência Nacional de Telecomunicações) , sendo este um dos fatores para o seu crescimento e também um dos motivos causadores de problemas em seu funcionamento. Para ter acesso à rede basta apenas ter uma placa compatível com o padrão. Atualmente a maioria dos *notebooks* já vem de fábrica com placas de comunicação sem fio, caso contrário adaptadores USB ou PCMCIA podem ser encontrados com facilidade e no caso de *desktops*, as placas PCI ou adaptadores USB podem ser utilizados.

2.4.3 Frequências Públicas

De acordo com as convenções internacionais existem três faixas de frequência que podem ser utilizadas para as redes sem fio.

As frequências disponíveis em cada uma das três faixas são:

- 902 - 928 MHz;
- 2,4 – 2,485 GHz (2,4 a 2,5 GHz no Brasil);
- 5,150 – 5,825 GHz (RUFINO, 2007, p. 20)

2.4.3.1 Frequência 2,4 GHz

Dentre as faixas em operação é a mais utilizada pelos equipamentos e serviços sem fio. Alguns a conceituam como poluída ou suja. É utilizada amplamente em telefones sem fio, *Bluetooth,* forno micro-ondas e pelos padrões 802.11b e 802.11g das redes sem fio (RUFINO,2007).

2.4.5 Canais

Alguns dos padrões 802.11 podem operar em vários canais.

> O espectro de radiofrequência é dividido em faixas, que são intervalos reservados, normalmente, para um determinado tipo de serviço, definido por convenções internacionais e/ou por agências reguladoras. Uma faixa é, em geral, subdividido em frequências menores, para permitir a transmissão em paralelo de sinais diferentes em cada uma delas. Essas frequências menores (ou sub frequências) são chamados de canais, que já fazem parte do nosso dia-a-dia há bastante tempo, como os canais de rádio (AM/FM) e televisão (RUFINO, 2007).

Canal	Frequência
1	2,412
2	2,417
3	2,422
4	2,427
5	2,432
6	2,437
7	2,442
8	2,447
9	2,452
10	2,460

Tabela 1 - Canais
Fonte: (RUFINO, 2007)

As agências regulamentadoras dos diversos países definem limites para a potência dos transmissores e do ganho das antenas presentes nos dispositivos, tal limitação tem o intuito de restringir o alcance das redes a fim de permitir que outras redes consigam operar nos mesmos canais (Ver tabela 1) (ROSS, 2003).

2.6 Tipos de transmissão

O modelo de transmissão das informações pode variar de acordo com o padrão de rede adotado. Cada um dos modelos possuem suas particularidades.

2.6.1 *Spread Spectrum*

Nessa tecnologia, o sinal é distribuído de maneira uniforme por toda a frequência consumindo mais banda, mas garantindo a integridade das informações estando menos suscetível a interferências e ruídos gerados por outros equipamentos (RUFINO, 2007).

2.6.2 FHSS (*Frequeny-Hopping Spread-Spectrum)*

O maior problema desse método é a limitação da velocidade a 2 MBps, com mudanças constantes nos canais de comunicação.

> Neste modelo, a banda de 2,4 GHz é dividida em 75 canais, e a informação é enviada utilizando todos esses canais numa sequência pseudoaleatória, em que a frequência de transmissão dentro da faixa vai sendo alterada em saltos. Essa sequência segue um padrão conhecido pelo transmissor e pelo receptor, que uma vez sincronizados, estabelecem um canal lógico (RUFINO, 2007, p. 19).

Esse sistema evita interferências entre os usuários, pois o mesmo utiliza de um sinal com transportador estreito, alterando a sua frequência varias vezes por segundo, proporcionando que a qualquer instante, cada transmissão, provavelmente estará utilizando um subcanal diferente, reduzindo o risco de interferências (ROSS,2003).

2.6.3 DSSS (Direct Sequence Spread Spectrum)

O DSSS é o meio de transmissão utilizando no padrão 802.11b,

> utiliza uma técnica denominada *code chips,* que consiste em separar cada bit de dados em 11 subbits, que são enviados de forma redundante por um mesmo canal em diferentes frequências, e a banda 2,4 GHz é dividida em 3 canais. Essa característica torna o DSSS mais susceptível a ataques diretos em uma frequência fixa e a ruídos que ocupem parte da banda utilizada (RUFINO, 2007, p. 19).

2.6.4 OFDM (*Orthogonal Frequency Division Multiplex/Modulation)*

Trata-se do método de transmissão mais eficiente e mais utilizado nas redes sem fio atualmente, esse modelo é capaz de identificar as faixas que possuem ruídos e isolá-las ou mudar a faixa ou velocidade de transmissão.

2.6.5 Características

Algumas das características são próprias das redes sem fio, principalmente as relacionadas ao *hardware*, ligados a camada 2 e 3 do modelo OSI. Outros são adaptações das redes cabeadas.

2.6.5.1 CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

Em redes cabeadas o mecanismo *Carrier Sense Multiple Acess with Colision Detection* (CSMA/CD) é utilizado para que os pacotes não colidam. Esse modelo permite que os *hosts* verifiquem se o canal de comunicação está livre para que a transação possa ser realizada. Dentro do escopo das redes sem fio tentou-se implementar o mesmo método, porém não se tornou viável a sua aplicação, pois seria preciso a existência de dois canais de comunicação, um para a recepção dos dados e outro para a transmissão, além de outras dificuldades .

Para suprir tal carência o CSMA/CA foi proposto como solução para garantir que quando o canal de transmissão estiver livre, não haja nem outra durante a operação.

A diferença entre o modelo CSMA/CD

> (...) é a geração de retardo para consulta, caso esteja havendo transmissão no momento do pedido. Essas características geram acessos rápidos em redes com tráfego pequeno, os quais passam a ter resposta mais lenta quanto maior for o volume de trafego da rede em questão. (...) quando uma estação não consegue acesso ao meio após um período de aleatório de espera, não recebendo um novo prazo, e, sim entra em uma fila de prioridade. Quando o meio estiver liberado, a fila vai sendo processada, o que permite que estações que estão esperando há mais tempo tenham vantagens de uso do meio, para transmissão, em relação aos pedidos mais recentes (RUFINO, 2007).

2.6.5.2 ESSID (Extended Service Set Identifier)

É a identificação da rede, conhecida tanto pelo concentrador como pelos clientes. É também conhecido como o “nome da rede”. Na maioria das vezes o concentrador envia o nome à área de abrangência, aguardando um pedido de conexão. Quando o ESSID não é propagado pelo concentrador, os clientes devem ter conhecimento prévio do mesmo para poderem solicitar a conexão.

2.6.5.3 BEACON

Os *Beacon frames* são sinais propagados gratuitamente pelos concentradores para que os clientes percebam a sua presença e solicitem conexão. Esse tipo de sinal pode ser facilmente configurado nos concentradores, para que não sejam propagados, ajudando na segurança da rede.

2.7 Padrões Atuais

A norma IEEE 802.11 define as regras para o funcionamento da camada Física e de Enlace de dados na arquitetura OSI.

> (…) reúne uma serie de especificações que basicamente definem como deve ser a comunicação entre um dispositivo cliente e um concentrador ou a comunicação entre dois dispositivos clientes (RUFINI, 2007, p. 25).

Na verdade a 802.11 constitui-se de uma família, que cresce de acordo com as extensões e modificações na norma padrão. Destacam-se os seguintes padrões:

A) Padrão 802.11a

“É o padrão que descreve as especificações da camada de enlace lógico e física para redes sem fio que atuam no ISM de 5 GHz. Apesar de ter sido publicado em 1999 não existem muitos dispositivos que atuam nesta frequência” (DUARTE, 2003, P.19).

Foi definido após o padrão 802.11b, e tem como uma de suas características

principais a velocidade de transmissão de 54 Mbps (108 Mbps em modo otimizado). Possui uma chave de autenticação de 256 bits e comporta até 64 clientes simultâneos. Adota a modulação OFMD, e possui doze canais de comunicação. O principal problema em sua expansão é a não compatibilidade com o padrão 802.11b (RUFINO, 2007).

B) Padrão 802.11b

Foi a primeira extensão do padrão 802.11 a ser criada, utiliza a modulação DSSS, permitindo até 32 clientes em 12 canais de comunicação, dos quais somente 3 podem ser utilizados simultaneamente, pois o padrão exige certo “espaço” entre um canal que está sendo utilizado e outro próximo, o que limita bastante a sua utilização (RUFINO, 2007).

> Descreve a implementação dos produtos WLAN mais comuns em uso atualmente. Este inclui aspectos da implementação do sistema de rádio e também inclui especificação de segurança. Esta descreve o uso do protocolo WEP. Trabalha na ISM de 2.4 GHz e provê 11 Mbps. Foi aprovado em julho de 2003 pelo IEEE (DUARTE, 2003, p. 19).

C) Padrão 802.11g

“Descreve o mais recente padrão para redes sem fio. Atua na banda ISM de 2,4 GHz e provê taxas de transferências de até 54 Mbps” (DUARTE,2003, p. 19).

Permite a coexistência com equipamentos do padrão 802.11b, facilitando sua implantação em sistemas mais antigos. Incorpora as principais características do padrão 802.11a, como a modulação OFDM. Possui compatibilidade com o padrão 802.11b utilizando as mesmas frequências em seus canais (SANCHES, 2007).

D) Padrão 802.11i

Trata-se de um grupo de trabalho que está ativamente definindo uma nova arquitetura de segurança para WLANs de forma a cobrir as gerações de soluções WLAN, tais como a 802.11a e a 802.11g (DUARTE,2003, p 19).

Foi homologado em 2004. Refere-se ao mecanismo de segurança e privacidade, podendo ser implantado em outros padrões já existentes. Um dos principais protocolos definidos é o

> (…) RSN (*Robust Security Network*), que permite meios de comunicação mais seguros que os atuais. Está inserido nesse padrão também o protocolo WPA, que foi desenhado para prover soluções de segurança mais robustos, em relação ao WEP, além do WPA2, que tem por principal característica o uso do algoritmo criptográfico AES (*Advanced Encryption Standard*) (RUFINO, 2007, p. 27).

E) Padrão 802.11n

O padrão ainda está em desenvolvimento e também pode ser conhecido como WwiSE (*World Wide Spectrum Efficiency*), seu principal foco está no aumento da velocidade, que promete chegar a 300 Mbps e no aumento da distância alcançada, com expectativas de chegar a 400 metros *outdoor*. Tem a característica de ser compatível com os padrões existentes e utilizar a modulação MIMO-OFDM (*Multiple input, Multiple Out*-OFDM). O MIMO permite que a placa utilize diversos fluxos de transmissão, utilizando vários conjuntos transmissores, receptores e antenas, transmitindo os dados de forma paralela (RUFINO, 2007).

F) Padrão 802.11x

Este padrão preestabelece a existência de um mecanismo de autenticação centralizado, baseado em um banco de dados ou qualquer servidor de autenticação conhecido. Não foi projetado para as redes sem fio, mas seus conceitos e características são complementares aos demais protocolos existentes, podendo dentre da rede promover um único padrão de autenticação para todos os usuários, estejam eles utilizando os sistemas cabeados ou sem fio. Só estarão aptos a navegar e utilizar os serviços da rede, somente os usuários autenticados no servidor central (RUFINO, 2007).

G) 802.16 (WiMax)

Seu principal uso e finalidade de criação é o alcance de longas distâncias utilizando ondas de rádio, pois a utilização de cabos de rede para implementação de uma rede de dados de alta velocidade a uma distância longa, seja ela entre cidades, em uma residência ou em uma área rural, por exemplo, pode elevar os custos e estar ao alcance financeiro de poucos. Procurando desenvolver um padrão para atender esta demanda, o IEEE cria o padrão 802.16 (ENGST e FLEISHMAN, 2005).

Sua primeira especificação trabalhava na faixa de frequência de 10 a 66 GHz, ambas licenciadas como não licenciadas. Porém, com um pouco mais de trabalho surgiu o 802.16a, que abrange um intervalo de utilização compreendido entre 2 e 11 GHz, incluindo assim a frequência de 2,4 GHz e 6 GHz dos padrões 802.11b, 802.11g e 802.11a. A sigla utilizada para denominar o padrão 802.16 é o WiMax, que por sua vez, diferentemente de sem fio, possui um significado real: *Wireless Interoperability for Microwave Access* (Interoperabilidade sem fio para acesso micro ondas), criado pela Intel® e outras empresas líderes na fabricação de equipamentos e componentes de comunicação. A velocidade de transmissão de uma rede WiMax pode chegar até 34,4 Mbps em bandas licenciadas e até 75 Mbps em redes não licenciadas (ENGST e FLEISHMAN, 2005).

2.8 Configurações e modos de operação

Nos sistemas de comunicação existem três tipos de modos de operação diferentes: *Simplex*, Semiduplex (*Half Duplex*) e *Duplex* (*Full Duplex*).

No modo *Simplex* a transmissão da informação é feita de forma unidirecional, ou seja os dados trafegam em apenas um sentido de cada vez.

No modo *Half Duplex*, o sistema transmite os dados no dois sentidos, porém utilizando o mesmo canal de comunicação, trafegando a informação em um sentido apenas de cada vez.

Já no modo *Full Duplex*, a informação trafega nos dois sentidos, e em canais diferentes, a transmissão é bidirecional e simultânea (SANCHES, 2007). Os três modelos são apresentados na Figura 7.

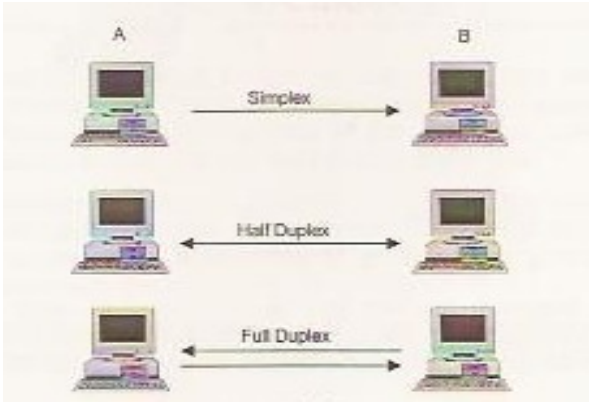


Figura 7 - Modos de Operação
Fonte: RUFINO, 2007

2.8.1 Topologias de rede

Em uma rede sem fio, os dispositivos presentes são chamados de estações ou *hosts*. Eles podem estar configurados de três maneiras distintas: Ad-Hoc, segundo o qual as estações se falam diretamente; modo infraestrutura onde existe um ponto de acesso intermediando a comunicação; e o modo *Wireless Distribution System* onde os dispositivos funcionam como repetidores do sinal (SANCHES, 2007).

2.8.1.1 Ad-Hoc

Nesta topologia, representada pela Figura 8, os equipamentos se comunicam diretamente uns com outros, analogamente as redes constituídas por cabos, porém no caso dos cabos coaxiais quando ocorria o rompimento de um dos cabos, a rede como um todo parava de funcionar. Já nas redes sem fio, quando isso acontece, apenas o *host* com problemas é que fica de fora das transações (RUFINO,2007).

Sua montagem é simples bastando apenas que duas ou mais estações possuam uma placa ou dispositivo de rede sem fio.

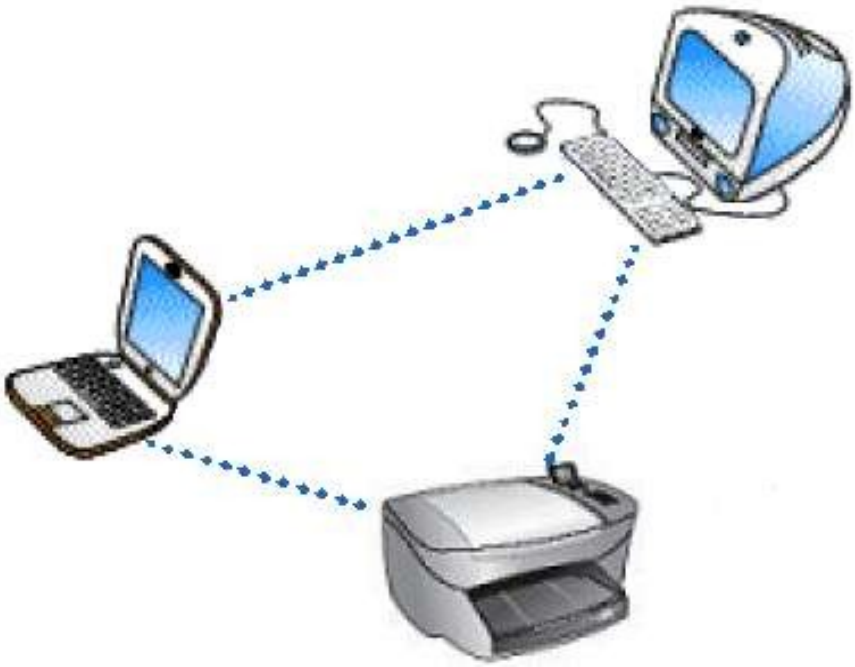


Figura 8 - Rede Ad-Hoc
Fonte: www.hp.com

2.8.1.2 Infraestrutura

Quando a rede está operando em modo infraestrutura, os *hosts* estão interconectados utilizando um concentrador de conexões e todas as informações devem trafegar por ele. O concentrador pode ser uma máquina convencional ou outro tipo específico de equipamentos como por exemplo o *Acess Point* (AP). Quando uma estação precisa se comunicar com outra estação, ela deve fazer esta solicitação ao concentrador enviando os pacotes a ele, para que o mesmo retransmita os dados à estação de destino (SANCHES, 2007).

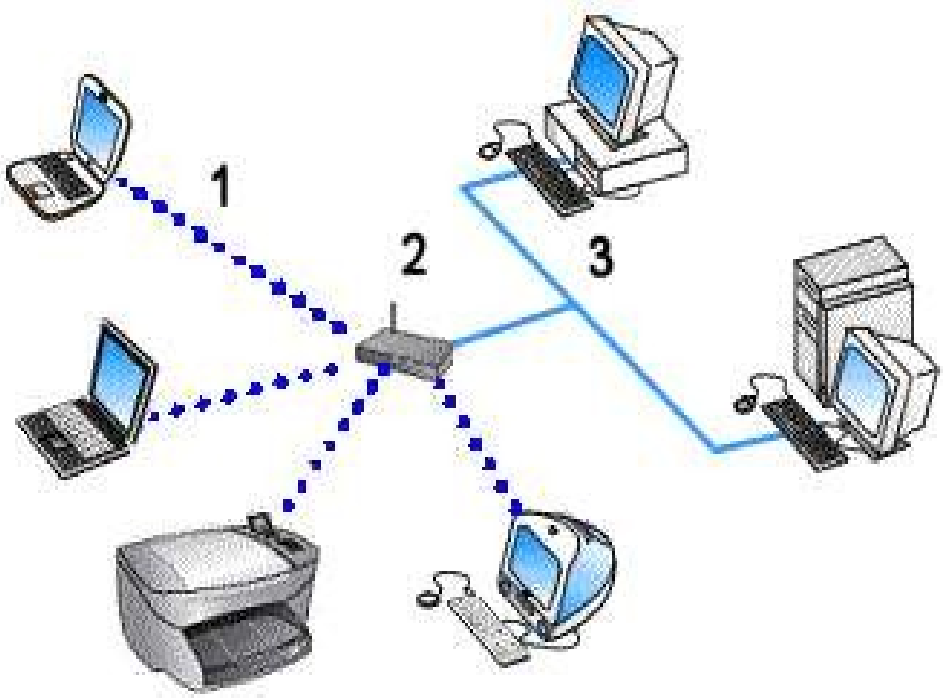


Figura 9 - Rede infraestrutura
Fonte: www.hp.com

2. 9 Equipamentos

Os equipamentos são os dispositivos pelas quais a comunicação se torna possível, eles são responsáveis pelo envio e recepção do sinal. Destacam-se:

- ***Access Points***

Os *Access Points*, apresentado na Figura 10, também conhecidos como AP's, são equipamentos utilizados como concentradores de rede, eles recebem o sinal da rede cabeada e irradia o sinal para os demais equipamentos, na maioria das vezes também funciona como autenticador, provendo segurança, ou pode funcionar como repetidor de sinal (MORIMOTO,2008).

Figura 10 - Access Point
Fonte: www.linksys.com

- **Placas e adaptadores de rede sem fio**

As placas de rede sem fio são as responsáveis pela recepção do sinal nas máquinas clientes, sejam elas máquinas *desktops* ou *notebooks*, quando *desktops* elas na maioria das vezes tem conexão PCI, já quando associada a notebooks elas podem ser com conexão PCMCIA ou USB (MORIMOTO, 2008) (ver Figuras 11 e 12)

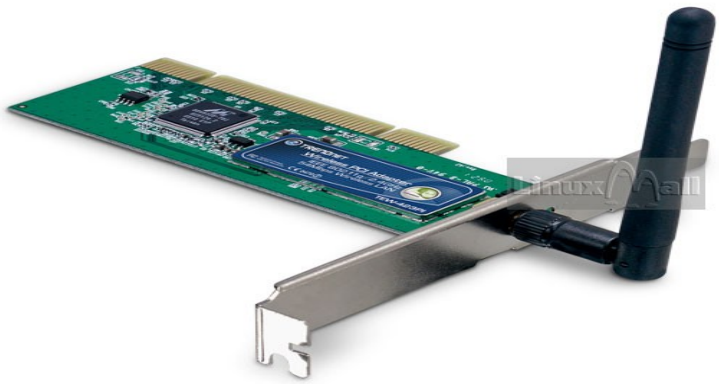


Figura 11 - Placa de rede sem fio
Fonte: www.linuxmall.com.br

Figura 12 - Receptor sem fio PCMCIA
Fonte: www.linksys.com

- **Antenas**

As antenas são utilizadas para aumentar o alcance das redes sem fio, a combinação delas com os equipamentos, faz com que a rede tenha um poder de alcance maior.

As antenas podem ser do tipo Omni (ver Figura 13), que irradiam o sinal no ângulo de 360º, são indicadas para ambientes abertos é que tenham clientes com raio de alcance circular, assim como a irradiação do sinal (SANCHES, 2007).

Figura 13 - Antena Omni-direcional
Fonte: www.aquario.com.br

Também podem ser direcionais, quando irradiam o sinal em apenas uma direção, a irradiação do sinal pode ser curto e amplo, ou longo e estreito. Dentre as antenas direcionais temos as parabólicas (ver Figura 14), que são aplicadas quando o alcance a ser atingido é longe, seu sinal pode chegar de 40 km a 50 km.

Figura 14 - Antena Parabólica
Fonte: www.wirelessip.net

Elas podem ser do modelo setorial (ver Figura 15), com raio de alcance de 3 km a 8 km, são geralmente utilizadas em espaços urbanos, para compartilhamento e conexão a internet.

Figura 15 - Antena Setorial
Fonte: www.wirelessip.net

Ou podem ser do tipo Yagi (ver Figura 16), geralmente usadas em ambientes com difíceis condições de operação, como ventos fortes, chuva pesada e até mesmo gelo, podem ter um alcance de até 30 km.

Figura 16 - Antena Yagi
Fonte: www.wirelessip.net

3 Mecanismos de segurança e vulnerabilidades

A busca de segurança é um fator que ultrapassa os limites da produtividade e funcionalidade. Velocidade e eficiência representam uma vantagem competitiva nos negócios, contudo a falta da segurança nesse ambiente pode resultar em prejuízos e perca de oportunidades (NAKAMURA e GEUS, 2007).

A manutenção da confidencialidade dos dados dentro das organizações surge com a utilização em grande escala dos sistemas de processamento de dados. O uso de redes para o compartilhamento de recursos, traz consigo algumas vulnerabilidades. Para garantia de que apenas usuários autorizados tenham acesso à rede, existe uma gama de mecanismos, características e funcionalidades que podem ser aplicados (STALLINGS, 2008).

O desenvolvimento de novas aplicações que valorizam a mobilidade das redes sem fio, como as voltadas para a internet, comercio eletrônico, diversão faz com que a segurança seja um ponto crucial em seu desenvolvimento, demandando discussão, entendimento e soluções (NAKAMURA e GEUS, 2007).

Em redes cabeadas para que o equipamento esteja conectado a rede, ele precisa necessariamente de um ponto de acesso. No entanto, nas redes sem fio basta apenas que ele tenha um meio de receber o sinal. Surge daí a necessidade do ocultamento das informações trafegadas. A criptografia é um modo de ocultar e proteger as informações. A codificação dos dados envolve um algoritmo que aplica um conjunto de instruções ao dado a ser transmitido juntamente com uma chave de criptografia. Antes de transmitir os dados, tanto os AP quanto os clientes codificam as informações, daí as informações podem ser lidas apenas por equipamentos que possuam a mesma chave (RUFINO, 2007).

3.1 Endereçamento de MAC

Cada equipamento pertencente a rede, possui um número de identificação, conhecido como endereço físico de *hardware* ou também chamado de MAC. O MAC possui um código hexadecimal de 12 dígitos definido por seu fabricante e controlado pelo *Institute of Eletrical and Electronics Engineers* (IEEE). Esse número é único e cada dispositivo de rede possui o seu independente de fornecedor ou marca (RUFINO,2007).

Uma maneira de evitar que usuários indesejados tenham acesso à rede é fazendo com que o concentrador de rede apenas aceite conexões de dispositivos cujo número de MAC esteja cadastrado em uma lista de endereços permitidos.

O maior problema desse tipo de técnica é que se a rede possuir uma alta rotatividade de *hosts,* ou seja, a inserção e remoção de máquinas da rede for alta, o administrador da rede vai ter um pouco de trabalho para mantê-la sempre atualizada, pois a adição e remoção de MAC's deve ser manual, por isso tal método é apenas indicado para pequenas redes. Mesmo o endereço MAC pertencendo a apenas um equipamento, existem técnicas que permitem através de softwares específicos descobrir um número de MAC que esteja na lista de endereços permitidos e fazer com que o equipamento não autorizado passe a fazer parte da rede, identificando o mesmo com um endereço cadastrado (RUFINO, 2007).

3.2 WEP (*Wired Equivalent Privacy*)

O WEP é uma das técnicas utilizadas para prover a segurança, nele são utilizados algoritmos simétricos, fazendo com que a chave deva ser compartilhada.

> Os critérios que foram levados em consideração para o desenho do protocolo:
>
> - **Suficientemente forte**: algoritmo deve ser adequado às necessidades do usuário.
> - **Auto-sincronismo**: deve permitir a um equipamento entrar na área de cobertura ou em hardware com a mínima eu nenhuma intervenção manual.
> - **Requerer poucos recursos computacionais**: pode ser implementado por software ou em hardware e por equipamentos com pouco poder de processamento.
> - **Exportável**: deve poder ser exportado dos Estados Unidos e também passível de importação para outros países (no momento da elaboração do padrão, havia restrições para a exportação de criptografia; hoje essas limitações estão limitadas a alguns países).
> - **De uso opcional:** o mesmo (RUFINO, 2007, p. 33-34).

WEP opera na camada de enlace de dados, baseia-se no modelo criptográfico RC4 e utiliza CRC-32 (*Cyclic Redundancy Check*) para fazer a verificação da integridade da mensagem transmitida, protegendo os dados de alterações não autorizadas. A criptografia RC4 é simétrica, a chave utilizada para a criptografia é a mesma é utilizada para a

descriptografar os dados. Este padrão criptográfico utiliza uma cifra chamada *Stream Cipher,* que faz com que cada mensagem seja criptografada com uma chave diferente. Isto acontece, pois é adicionado um elemento novo elemento à chave criptográfica. Quanto uma mensagem é criptografada pelo algoritmo RC4, existem duas informações que são inseridas no processo de criptografia. A palavra chave e um valor randômico conhecido como vetor de iniciação . Este vetor que caracteriza o *Stream Cipher* no algoritmo (SANCHES, 2007).

Porém o vetor de inicialização no WEP é muito pequeno, ele é alterado a cada pacote, começando do zero até o valor máximo de 2^{24}. Supondo que a rede trafegue a 5.5 Mbps e sabendo que o vetor de inicialização possui 24 bits, o que gera 16 milhões de possibilidades, em apenas 11 horas a quantidade possível de vetores estará exaurida. Basta ao atacante utilizar destes programas que rapidamente terá acesso à rede (SANCHES, 2007).

Apesar do WEP esta presente na maioria dos equipamentos sem fio atuais, ela já não consiste em um modelo de segurança adequado à maioria dos cenários onde as redes sem fio são aplicadas. Existe um grande número de ferramentas capazes de quebrar as chaves criptografadas pelo protocolo, podem ser citados nesta lista dois dos mais conhecidos que são o *AirCrack-NG*[1] e o *WEPCrack*[2].

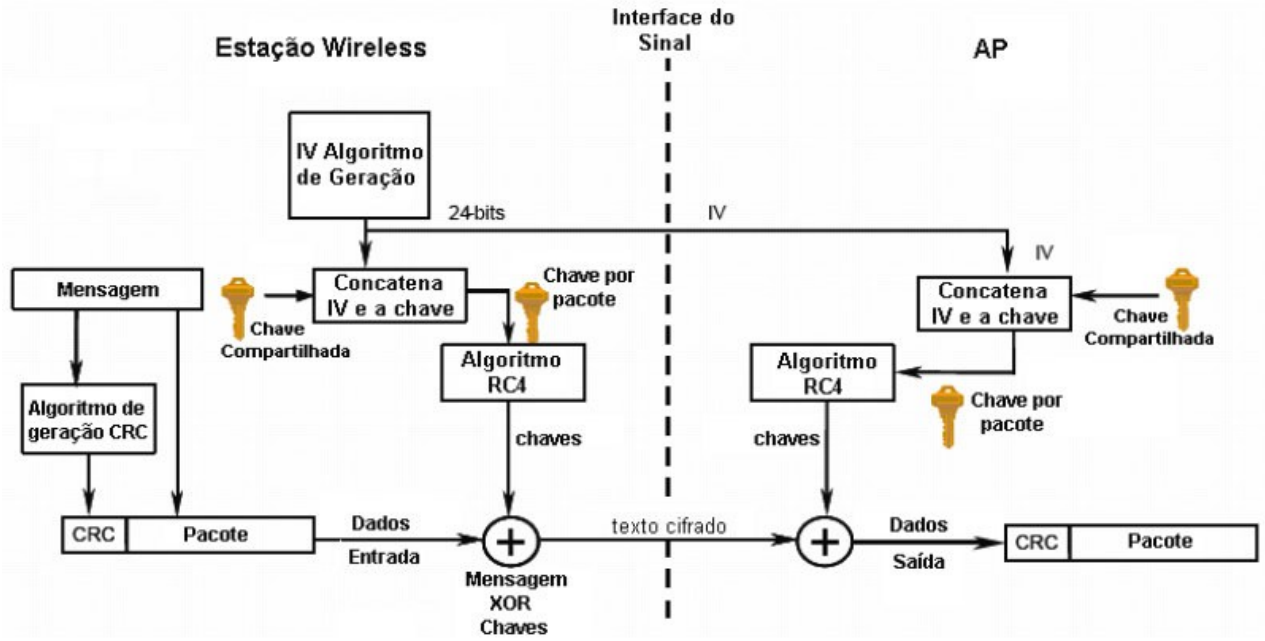


Figura 17 - Processo de autenticação do protocolo WEP
Fonte: www.vivasemfio.com.br

1 Aircrack-ng é um detector de redes, aplicativo de quebra de WEP e ferramenta de análise para redes locais sem fios , disponível em http://www.aircrack-ng.org/

2 WEPCrack é uma ferramenta open source para quebrar chaves WEP, disponível em http://wepcrack.sourceforge.net/

3.3 WPA (*Wi-Fi Protected Access*)

O WPA surgiu como proposta para solução dos problemas do WEP. Ele implementa a maioria das funcionalidades do padrão IEEE 802.11i, e foi liberado como medida paliativa até que o novo padrão seja completado.

Em sua versão I, não esta disponível a conexão entre dispositivos no modo *Ad-Hoc*, pois a tecnologia WPA utiliza-se de um concentrador para que a autenticação de *hosts* seja efetuada.

A WPA foca-se em duas melhorias em relação a WEP. Uma tratando da criptografia dos dados, garantindo a ocultação das informações, e a outra em relação a autenticação dos usuários utilizando 802.1x e EAP (*Extensible Authentication Protocol*) (RUFINO, 2007).

Tendo em vista a grande possibilidade de utilização das redes sem fio, sendo elas passiveis de utilização em ambientes domésticos, públicos e corporativos, pensou-se em algo que pudesse ser flexível a tais espaços com diferentes modelos de segurança. Em ambientes cuja viabilidade de implementação de um servidor específico é baixa, no caso de residências e pequenos escritórios, com um nível de segurança menor, pode ser utilizado o esquema de chave pré-compartilhada, chamado PSK (*Pre-Shared Key*). Neste modo, a senha deve ser inserida individualmente e manualmente nos clientes e no ponto de acesso para a autenticação e em caso de alteração existe a necessidade de alteração manual em todos os *hosts.* A vantagem é que exige um menor investimento e é de fácil instalação e configuração.

O WPA pode operar também com servidor de autenticação (RADIUS em sua maioria), distribuindo chaves diferentes para cada usuário, indicado para redes maiores e que dependam de um nível maior de segurança, além da possibilidade de utilização de uma utilização de infraestrutura de chaves públicas (ICP), no caso de utilizar certificados digitais para autenticação de usuários.

A informação é criptografada utilizando um vetor de inicialização de 48 bits, que no WEP é de 24 *bits*, em conjunto com uma chave de 128 *bits*, através do Protocolo de Integridade de Chave Temporária (TKIP – *Temporal Key Integrity Protocol*), responsável pelo gerenciamento das chaves temporárias, fazendo a substituição da chave dinamicamente de acordo com a utilização do sistema, podendo ser configurado para a mudança de chave ser feita a cada pacote, sessão ou período, evitando ataques de

recuperação de chaves, como no protocolo WEP, preservando as informações trafegadas e a integridade da rede. Quanto mais rápida for a troca de chaves for feita, menor será a possibilidade de descoberta dos valores do vetor de inicialização em conjunto com a chave.

Em conjunto com à autenticação e criptografia, o WPA também melhora a qualidade da verificação da integridade dos dados é utilizado o MIC (*Message Integrity Check*). O MIC possui uma função matemática na qual emissor e receptor de dados fazem uma comparação e avaliam a integridade dos dados.

O WPA trabalha com sessões, após o cliente se autenticar é gerada uma chave mestra para a transmissão dos dados. O TKIP envia a chave ao cliente e ao AP, fazendo com que o sistema gere dinamicamente apenas uma chave de criptografia, utilizadas em todos os pacotes da sessão.

A Tabela 2 apresenta um comparativo entre o WEP e WPA.

Tabela 2 - Comparativo entre WEP e WPA.

	WEP	WPA
Criptografia	Quebrada por cientistas e *hackers.*	Dificulta as falhas do WEP.
	Chave estática, utilizada por todos na mesma rede.	Chave de sessão dinâmica – por usuário, por sessão, por chave de pacote
	Distribuição de chave manualmente – Necessidade de digitar a chave em todos os dispositivos.	Distribuição das chaves automaticamente.
	Chave de 40 bits	Chave de 128 bits
Autenticação	Quebrada, uso da chave WEP para autenticação.	Autenticação de usuário mais forte, utilizando 802.1x e EAP.

Fonte: (SANCHES, 2007).

3.4 802.1x

O 802.1x é o modelo de autenticação e acesso ao meio de redes com e sem fio baseado em porta, podendo ser a porta um ponto de acesso fixo, como nas redes cabeadas ou uma porta lógica no caso das redes sem fio. Apesar de ter sido projetado para redes cabeadas o padrão foi adaptado para a utilização em redes sem fio. Ele provê a necessidade de autenticação antes que seja enviado qualquer pacote, identificando o usuário por meio de certificados, senhas, biometria, etc..

Com a homologação do padrão 802.1x, o protocolo CCMP também foi adicionado ao WPA aumentando a segurança, já que o mesmo utiliza o algoritmo AES para encriptação dos dados em forma de blocos, e não a cada *byte*. Com a incorporação do algoritmo AES o protocolo passou a ser conhecido também como WPA2.

O padrão define o seguintes termos:

PAE (*Port Access Entity*): Entidade de Acesso à Porta é uma entidade lógica que é associada a uma porta, ela pode fazer o papel de solicitante, autenticador ou ambos.

Autenticador: É uma porta LAN que exige autenticação do cliente antes de disponibilizar o serviço que oferece. Em redes cabeadas pode ser um *switch* ou roteador e em redes sem fio pode ser um AP operando em modo infraestrutura que solicitem autenticação.

Solicitante: O solicitante trata-se de um dispositivo da rede que solicita um serviço da rede ao autenticador. Ele associa-se a rede e depois faz a autenticação. Tanto nas redes sem fio quanto nas cabeadas o solicitante e o autenticador estão conectados por um segmento ponto a ponto lógico e físico.

Servidor de autenticação: Para que a autenticação seja feita, o servidor de autenticação verifica os dados do solicitante no lugar do autenticador e responde a ele, comprovando se o solicitante realmente está autorizado a acessar os serviços. O servidor de autenticação pode ser de dois tipos:

Um componente do Ponto de Acesso: o AP deve ser configurado com todos as autorizações de acesso dos usuários correspondentes.

Uma entidade distinta: nesse modelo, o AP envia os dados para a autenticação a um servidor que não esteja ligado diretamente a rede (SANCHES,2007) .

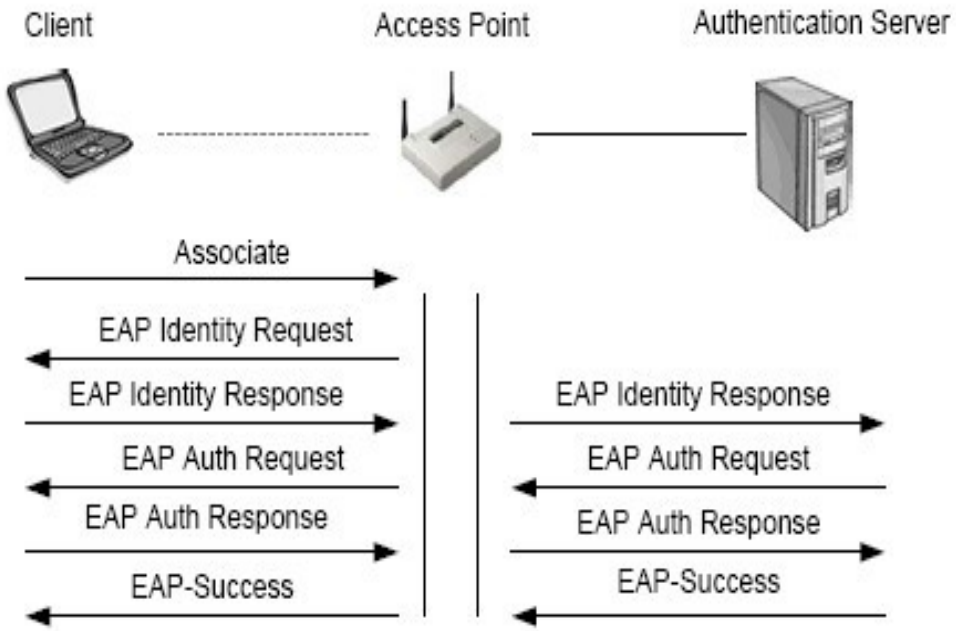


Figura 18 - Autenticação 802.1x
Fonte: www.vivasemfio.com.br

Toda a autenticação no protocolo é feita através de EAP (*Extensive Authentication Protocol*). O EAP controla a autenticação dos usuários através de senhas, certificados ou outro modelo que garanta a identificação do usuário.

3.5 RADIUS (*Remote Access Dial-In Service*)

O RADIUS – Serviço de Autenticação Remota de Usuários Discados - é utilizado para disponibilizar acesso a usuários da rede pelo protocolo AAA (*Autorization, Authentication and Accounting)* de cliente-servidor para uso quando o cliente fizer *login* ou *logoff* no servidor de acesso que pode ser autenticado tanto por usuário, através de senhas e certificados, quanto por sistema, através de endereçamento MAC.

A autenticação é feita quando o usuário tenta se conectar a rede envia-se a informação com nome de usuário e senha. O servidor RADIUS verifica as informações e autoriza o acesso do cliente, caso contrário, o acesso é negado.

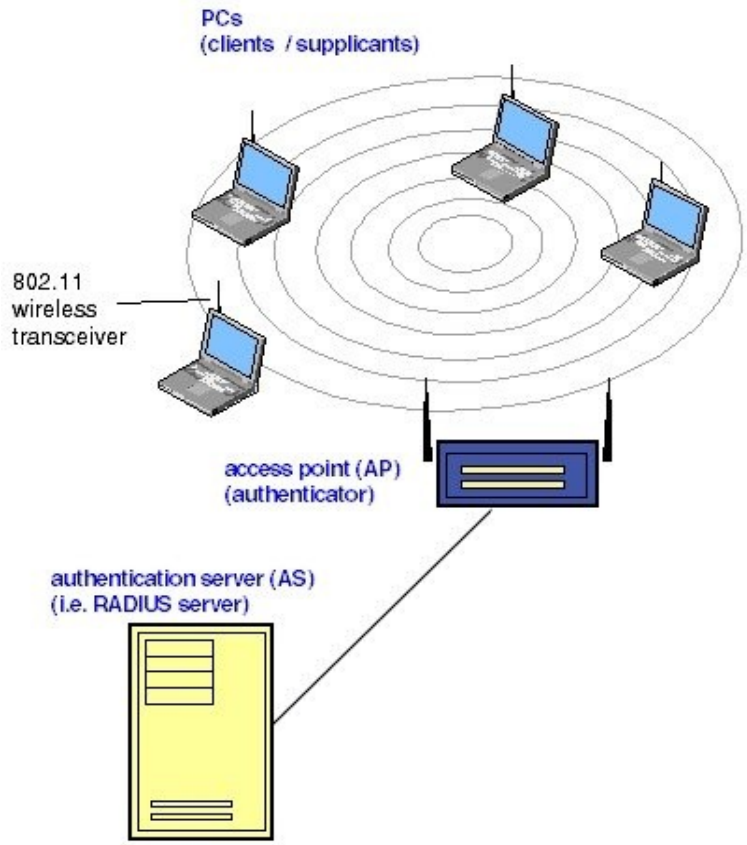


Figura 19 - Autenticação RADIUS
Fonte: Fonte: www.wirelessip.net

A autenticação é promovida em três fases:

Fase de autenticação: Verifica o nome de usuário e senha no banco de informações.

Fase de autorização: Determina se o acesso será aceito ou não, um endereço é atribuído ao cliente se o acesso for autorizado.

Fase de contabilidade: Coleta informações sobre o acesso, contabilizando informações importantes sobre a sessão.

3.6 Ocultamento de ESSID

Pontos de acesso são identificados com um ESSID, que não é nada mais que o identificador da rede ou ID de rede. O SSID (*Service Set Identifer*) é um tipo de ESSID que é utilizado para identificação dos dispositivos presentes na rede.

Para que a conexão entre dispositivos e pontos de acesso seja estabelecida é

preciso que o SSID dos dispositivos envolvidos seja o mesmo e que seja conhecido por eles. Cada fabricante utiliza um valor padrão de identificação e pode ser utilizado como um mecanismo de fragilidade da rede, para tanto é preciso que precauções sejam tomados para que tal mecanismo possa ser utilizado a favor da segurança:

Valor padrão: Como os valores de ESSID ao serem adquiridos possuem um valor pré-definido por seus fabricantes é preciso que esse valor seja modificado para que a sua identificação seja mais difícil para o atacante.

Ocultamento de ESSID: A maioria dos dispositivos possui o recurso de "*broadcast* ESSID", que faz com que o valor do ESSID seja propagado periodicamente pela rede fazendo com que os dispositivos no raio de alcance possam identificar facilmente o ponto de acesso, sem a necessidade de um conhecimento prévio do valor. Ao deixar o recurso ativado o usuário esta abrindo mão desse mecanismo de segurança, porém estará optando por uma rede mais flexível.

3.7 Riscos e vulnerabilidades

3.7.1 Segurança Física

Os cuidados com o ambiente e localização das redes sem fio na maioria das vezes não é levada em consideração. Precações deste tipo em sua maioria são mais consideradas quando se faz referência as redes cabeadas. Porém esse pensamento é equivocado, pois as redes sem fio tem um poder de alcance físico muito maior que o de redes cabeadas. Em redes cabeadas a segurança esta voltada para a proteção do acesso físico direto a rede por meio de um ponto de acesso à rede ou de salas com equipamentos necessários ao seu funcionamento. No que se refere as redes sem fio além dos itens citados, deve-se levar em consideração o alcance do sinal, pois este pode ser captado a dezenas ou centenas de metros de sua origem. O posicionamento dos pontos de acesso deve ser bem analisado, além de serem considerados velocidade e desempenho (RUFINO,2005).

3.7.2 Localização e alcance do sinal

A localização dos AP também pode influenciar na segurança das informações que trafegam no meio, além da área de abrangência do sinal. O mal posicionamento dos pontos de acesso podem fazer com que o sinal chegue a locais ou ambientes não desejados, já que o sinal é propagado em todas as direções, quanto mais no centro do ambiente o dispositivo de propagação estive melhor será o aproveitamento do sinal. A potência dos equipamentos utilizados também deve ser observada pois ampliam os limites de alcance da rede, em conjunto com a associação de equipamentos amplificadores ou antenas (ver Figura 20). O projetista ou administrador deve estar atento a tais fatores a fim de ajustar os equipamentos. Um teste de propagação de sinal pode ser feito a fim de verificar os valores (RUFINO, 2005).

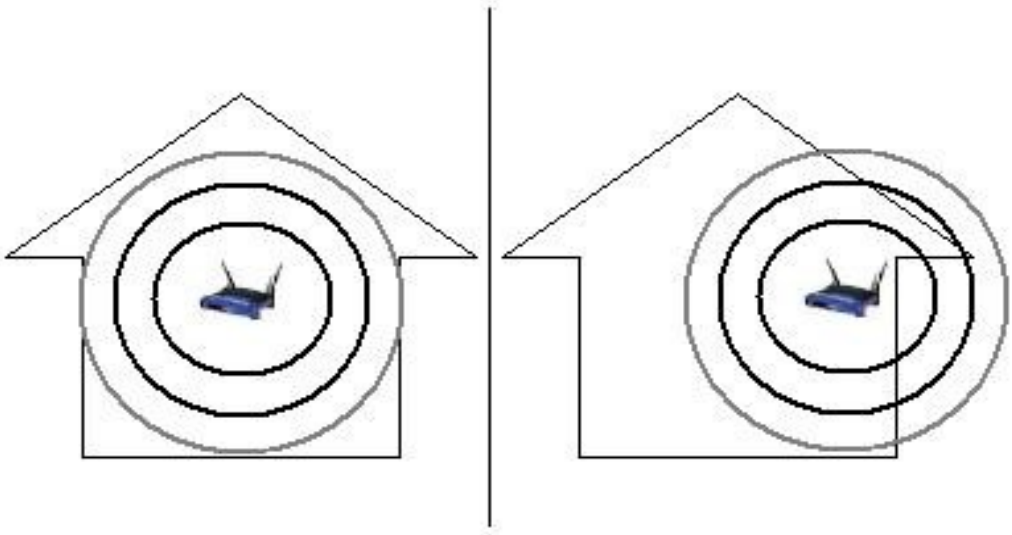


Figura 20 - Posicionamento do equipamento
Fonte: (RUFINO, 2007)

3.7.3 Configuração Padrão

Desde a concepção das redes sem fio a sua segurança foi pensada, no entanto com sua evolução a adaptação dos novos padrões a padrões antigos faz com que alguns aspectos sejam mantidos a fim de promover a compatibilidade entre padrões diferentes.

Equipamentos novos saem de fábrica com configurações básicas ou valores padrões de senhas, ESSID, criptografia. Equipamentos neste estado são alvos fáceis de ataques, tais valores são conseguidos facilmente em manuais ou sites da internet. Administradores de redes, técnicos e usuários finais, não levam essas características em consideração e colocam os equipamentos em funcionamento sem qualquer alteração.

A maioria dos equipamentos saem de fábrica com senhas e endereços de IP padrão, sem que uma mudança seja feita o atacante pode ter fácil acesso à rede e as configurações do equipamento, podendo até alterá-las, trazendo transtornos aos demais usuários.

Qualquer informação pode ser útil ao atacante, alguns detalhes podem facilitar a descoberta do fabricante e modelo do equipamento. Alguns AP vem com serviços de SNMP e de acesso remoto habilitados, podendo o atacante utilizar deste mecanismo para adentrar na rede, as vezes mesmo sem conhecer usuários e senhas do sistema. (RUFINO, 2005)

Mesmo administradores com experiência em redes cabeadas acabam encontrando dificuldades na implantação de redes sem fio, por conter alguns itens voltados a segurança que diferem totalmente nesta variante.

Como já citado os valores de SSID e o *broadcast* do mesmo também devem ser alterados a fim de dificultar ao atacante a identificação da rede (DUARTE, 2003).

3.7.4 Redes Mistas

Na maioria das implementações de redes está característica está presente. As redes mistas são aquelas onde o acesso pode ser feito dos dois modos, sem fio ou cabeado.

A inserção de redes sem fio em redes cabeadas preexistentes podem trazer riscos. Empresas investem em equipamentos, material, treinamento para que a segurança das informações seja completa. Um planejamento da agregação da rede sem fio deve ser muito bem analisado e estudado, mesmo que a qualidade na proteção cabeada seja alta, o invasor que conseguir acesso sem fio, terá acesso a toda rede, já que as mesmas estão interligadas (ver Figura 21) (AMARAL e MAESTRELLI, 2004).

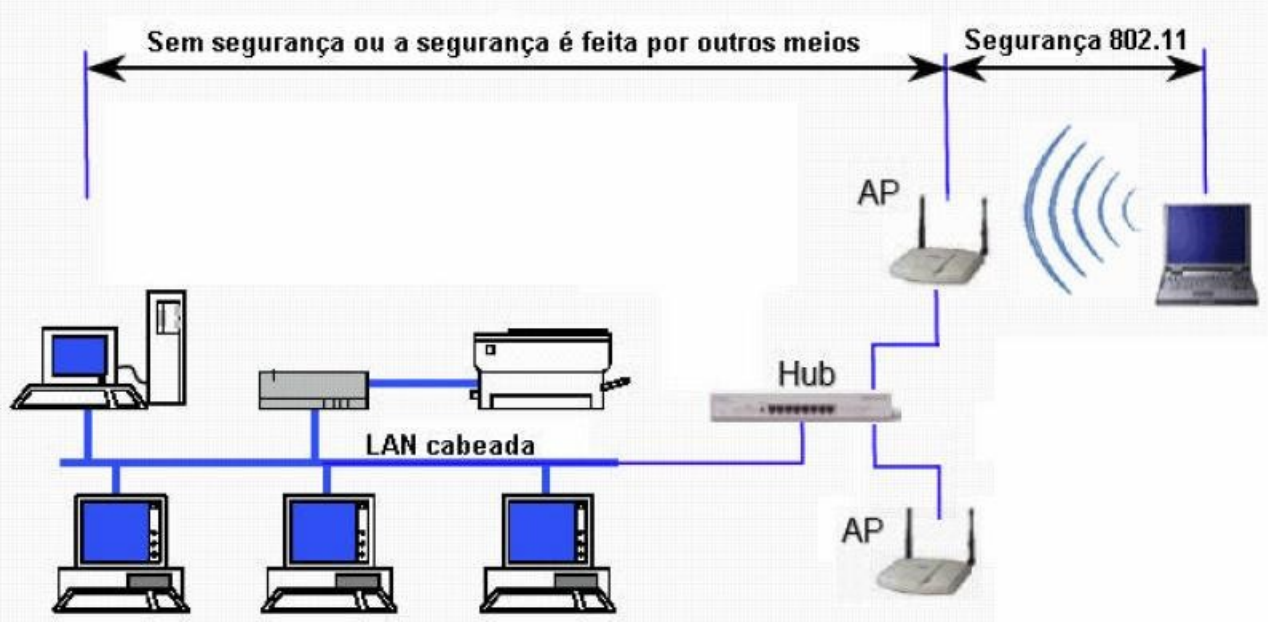


Figura 21 - Exemplo de redes mistas
Fonte: www.vivasemfio.com.br

3.8 Tipos de ataque

3.8.1 Escuta de Trafego

A escuta de tráfego pode ser feita em qualquer tipo de rede, seja ela cabeada ou sem fio, que não esteja utilizando qualquer tipo de cifragem dos dados para sua transmissão. Ferramentas específicas não são necessárias, é possível utilizar o Tcpdump[3] que é uma ferramenta tradicional, capaz de colher muitas informações do tráfego de uma rede (RUFINO, 2007).

Estas ferramentas, assim como outras existentes, são também conhecidas como *Sniffers*[4], as quais possuem funções maléficas ou benéficas. Os benefícios de tais ferramentas é que auxiliam a analisar o tráfego da rede e identificar possíveis falhas na rede. Os malefícios é que são utilizadas para capturar senhas, informações confidenciais de clientes e para abrir brechas na segurança da rede.

3 Tcpdump é uma ferramenta utilizada para monitorar os pacotes trafegados numa rede de computadores. Ela mostra os cabeçalhos dos pacotes que passam pela interface de rede, disponível em http://www.tcpdump.org/.
4 Um *sniffer* é um programa que consegue capturar todo o tráfego que passa em um segmento de uma rede

3.8.2 Ataque Homem-do-meio

Esta forma de ataque é conhecida por homem do meio por ser feito a um concentrador que está posicionado no meio de uma conexão de rede sem fio. Normalmente este ataque é feito clonando-se um concentrador já existente ou criando outro para interpor-se aos concentradores oficiais, recebendo assim as conexões dos novos clientes e as informações transmitidas na rede (RUFINO, 2007).

3.8.3 Negação de Serviço (DoS)

Este tipo de ataque não necessita que o invasor necessariamente tenha que ter invadido a rede e nem ter acesso à mesma, porém pode causar grandes problemas. Isso ocorre porque os administradores de rede, na maior parte dos casos, se preocupam muito em proteger a rede de invasores e esquecem de colocar nos seus mapas de riscos este tipo de ataque, por imaginar que isso não ocorrerá em suas redes (RUFINO, 2007).

Este ataque consiste no envio de inúmeros pacotes de requisição à rede alvo. A rede atacada não é invadida, o ataque consiste em fazer com que a rede apresente indisponibilidade de serviço (SOLHA; TEIXEIRA; PICCOLIN, 2000).

3.8.4 Endereçamento MAC

Neste modelo, o ataque é feito clonando o endereçamento MAC da placa de rede de um dos clientes da rede, fazendo-se passar pelo mesmo. Algumas medidas de segurança utilizadas funcionam com um cadastramento dos endereços dos clientes, a fim de evitar que dispositivos não cadastrados façam uso da rede. O uso do método é simples, a alteração do endereço MAC das interfaces é simples em qualquer dos sistemas operacionais atuais (RUFINO, 2007).

3.8.5 Mapeamento

Uma das primeiras coisas que o atacante faz é um mapeamento da região a ser

explorada, buscando identificar locais em potencial para serem atacados. Com isso ele obtêm uma gama de informações necessárias para que o ataque seja bem sucedido. Neste trabalho será utilizada a mesma técnica, porém tendo como fim esclarecer e mapear tais vulnerabilidades.

3.8.5.1 Mapeamento Ativo

Este é o método onde o atacante pode obter informações sobre equipamentos em operação, e permite identificar as vulnerabilidades nos equipamentos ou no sistema, além de informações importantes para se agregarem a rede e fazerem o ataque direto. Para que este tipo de mapeamento ocorra é necessário esta conectado a rede (RUFINO, 2007).

Existem inúmeros programas que são utilizados em tal técnica. Um programa que pode ser utilizado é o *THC-rut*[5], que permite identificar o endereço MAC das máquinas associadas a rede, bem como seus respectivos fabricantes, podendo fazer o ataque direto a máquina alvo. Além da possibilidade de utilização de outros programas para obtenção de outras informações importantes como o *Nmap*[6] que permite descobrir quais serviços estão em execução no endereço, bem como as portas lógicas em que eles atuam (RUFINO,2007).

3.8.5.2 Mapeamento Passivo

Essa técnica permite que os equipamentos e redes em operação sejam mapeadas sem que o mapeamento seja notado. Softwares de redes cabeadas podem ser utilizados, basta esta na área de cobertura do sinal. A exemplo o *p0f,* que permite ao atacante selecionar qual dispositivo da rede esta mais vulnerável ao ataque, tendo maior chance de sucesso (RUFINO, 2007).

5 *Software* que permite identificar os endereços MAC em uso na rede e os seus respectivos fabricantes. http://thc.org/thc-rut/

6 Nmap é uma ferramenta de código aberto para exploração de rede e auditoria de segurança. Ela foi desenhada para escanear rapidamente redes amplas, embora também funcione muito bem contra hosts individuais. http://nmap.org/

3.8.5.3 Softwares para mapeamento

Existem inúmeras ferramentas disponíveis para tal procedimento além dos já citados que permitem obter informações como:

- SSID da rede: identificação da rede, o qual é necessário para a conexão a rede;
- ESSID: identificação do concentrador de rede;
- Criptografia: que tipo de segurança esta sendo utilizada;
- Potência do Sinal: identifica a amplitude do sinal emitido;
- Canal: identifica em qual canal a rede esta operando;

Dentre as ferramentas utilizadas para o mapeamento destacam-se:

NetStumbler que foi uma das primeiras ferramentas criadas para o sistema operacional *Windows*, ele opera nas redes 802.11 a/b/g, com comparatibilidade com a maioria das placas do mercado, além de integração com equipamentos GPS, possibilitando além da identificação da rede e suas características, a sua localização (ver Figura 22). Arquivos de log podem ser salvos para posterior análise. Com ela é possível identificar o nome das redes, endereços de MAC e outras informações. Porém ela não permite captura de trafego e quebra de WEP (RUFINO,2007).

O *Kismet* (ver Figura 23)*,* é uma das ferramentas mais completas do mercado, além de novas funcionalidades serem acrescentadas constantemente, é compatível com a maioria dos chipsets do mercado e esta disponível para os sistemas Linux, FreeBSD, Mac OS X ,Net BSD, OpenBSD e demais sistemas no padrão Unix, além de cliente *Windows*, permite identificar redes em modo infra-estrutura e *Ad-Hoc* e obter informações detalhadas sobre as redes como:

- SSID – nome da rede;
- nível do sinal;
- criptografia utilizada;
- canal;
- clientes conectados;
- MAC das maquinas da rede;
- bloco de endereços IP da rede;

quantidade de pacotes transmitidos;

Todas as informações obtidos por ele são gravadas em arquivos, para consulta posterior, informações sobre os equipamentos da rede e trafego são guardados. Com o

arquivo de trafego é possível ter acesso aos arquivos que trafegam na rede.

Permite a integração com aparelhos de GPS. A integração é feita por meio de outro software, o "*GPS daemon*" (GPSD), que estabelece a comunicação entre o equipamento e o *Kismet* . De acordo as redes são identificadas um arquivo de log com a extensão .GPS é gerada com informações sobre a rede e a localização das mesmas. Uma desvantagem é a não possibilidade de continuação de arquivo anterior, ou seja a cada sessão iniciada, um novo arquivo é gerado (RUFINO,2007).

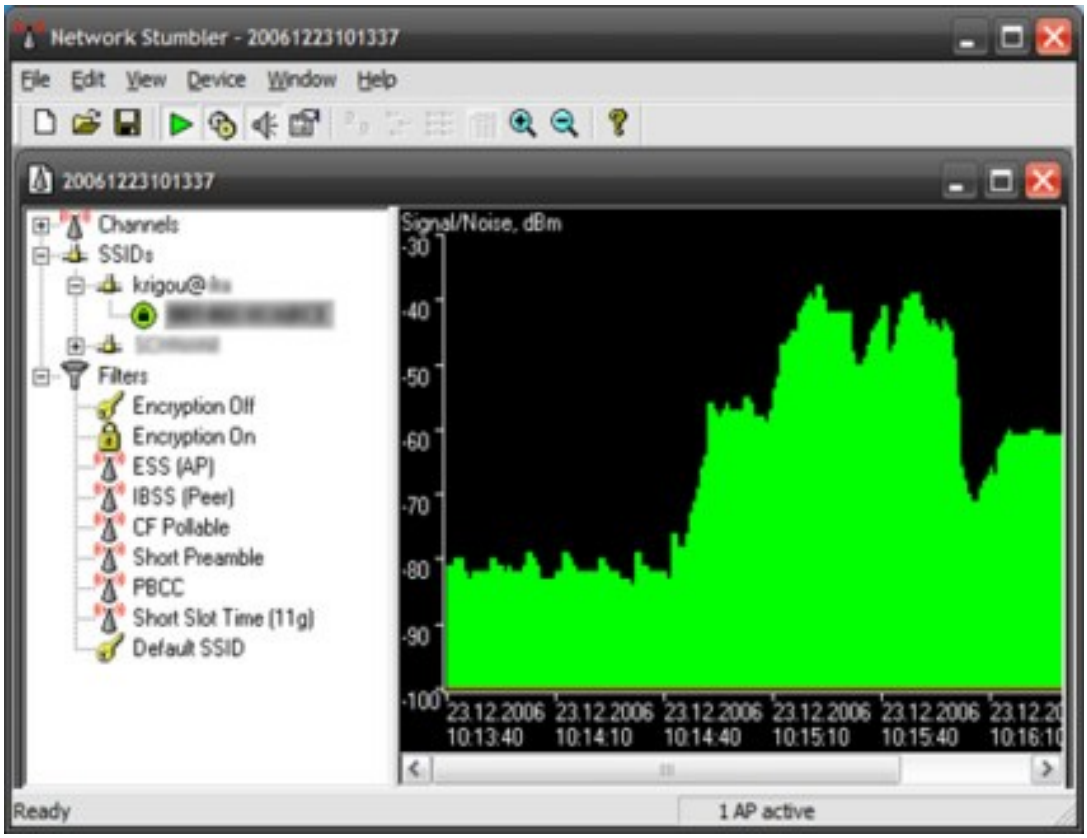


Figura 22 - Netstumbler em Operação
Fonte: www.clubedowarchalking.com.br

Com as informações geradas é possível gerar um mapa com a localização das redes através das coordenadas obtidas pelo GPS e as informações da rede obtidas pelo *Kismet.* Este mapa é gerado pelo Gpsmap, *software* responsável pelo *download* dos mapas e desenho da localização das redes.(ver Figuras 23 e 24)

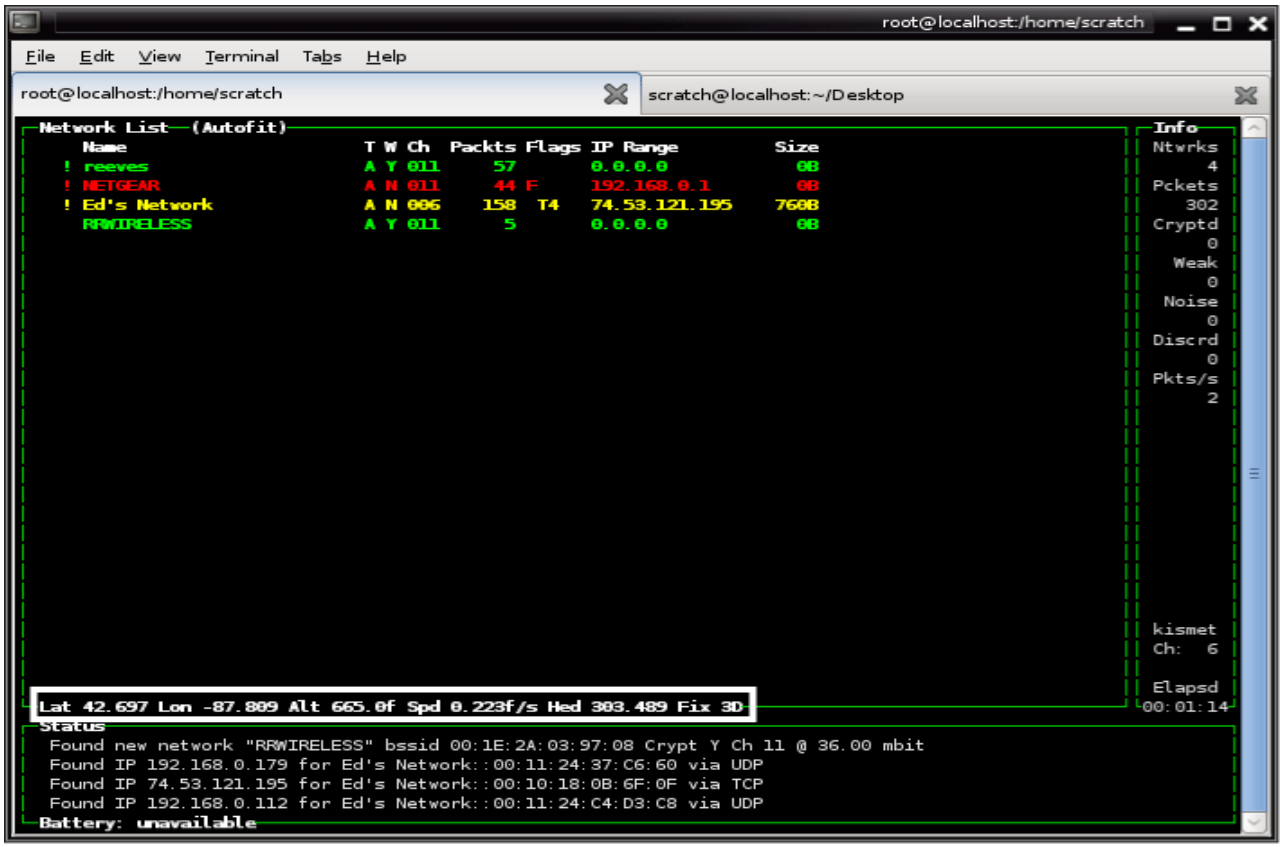


Figura 23 - Kismet operando com GPS
Fonte: www.scratchdrive.com

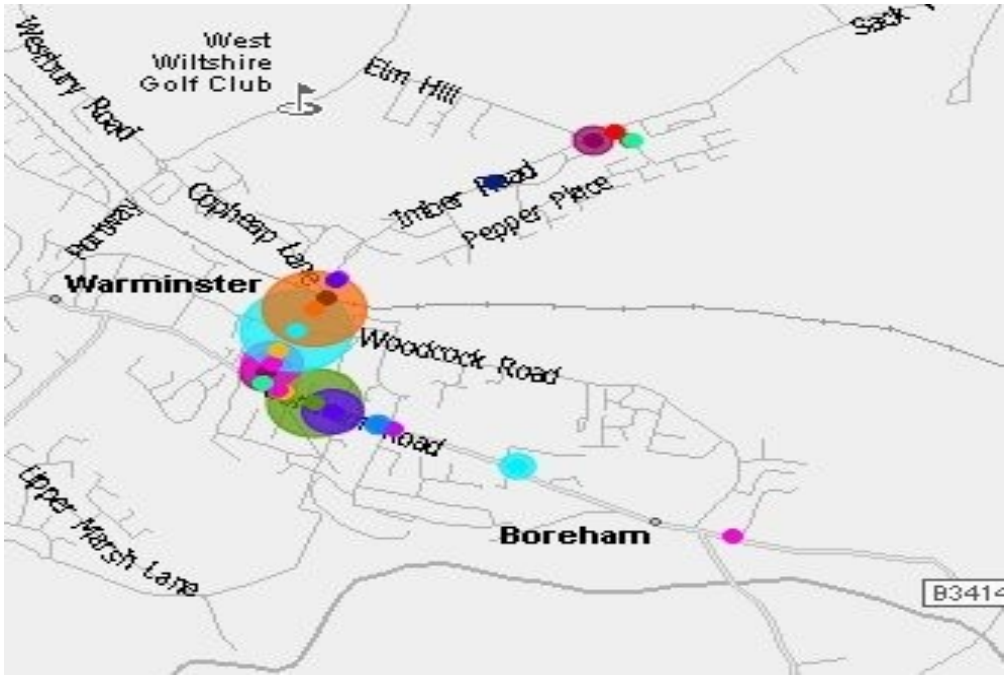
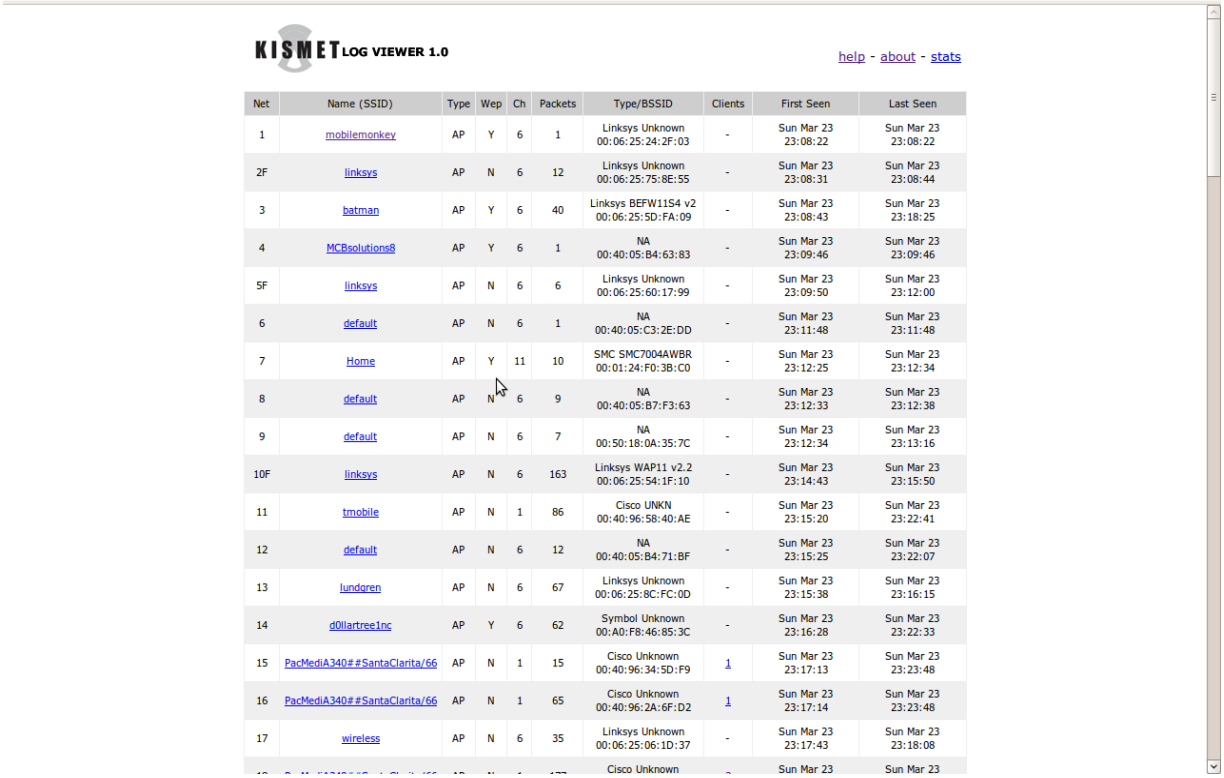


Figura 24 - Mapa gerado pelo Gpsmap
Fonte: www.wirelessdefence.com

Além do *Kismet*, do GPSD e do Gpsmap, o *Kismet log viewer* (KLV) (ver Figura 25), que responsável por facilitar a visualização das informações geradas pelo *Kismet*,

gera arquivos no formato HTML, facilmente visualizado em navegadores web.



KISMET LOG VIEWER 1.0

help - about - stats

Net	Name (SSID)	Type	Wep	Ch	Packets	Type/BSSID	Clients	First Seen	Last Seen
1	mobilemonkey	AP	Y	6	1	Linksys Unknown 00:06:25:24:2F:03	-	Sun Mar 23 23:08:22	Sun Mar 23 23:08:22
2F	linksys	AP	N	6	12	Linksys Unknown 00:06:25:75:8E:55	-	Sun Mar 23 23:08:31	Sun Mar 23 23:08:44
3	batman	AP	Y	6	40	Linksys BEFW11S4 v2 00:06:25:5D:FA:09	-	Sun Mar 23 23:08:43	Sun Mar 23 23:18:25
4	MCBsolutions8	AP	Y	6	1	NA 00:40:05:B4:63:83	-	Sun Mar 23 23:09:46	Sun Mar 23 23:09:46
5F	linksys	AP	N	6	6	Linksys Unknown 00:06:25:60:17:99	-	Sun Mar 23 23:09:50	Sun Mar 23 23:12:00
6	default	AP	N	6	1	NA 00:40:05:C3:2E:DD	-	Sun Mar 23 23:11:48	Sun Mar 23 23:11:48
7	Home	AP	Y	11	10	SMC SMC7004AWBR 00:01:24:F0:3B:C0	-	Sun Mar 23 23:12:25	Sun Mar 23 23:12:34
8	default	AP	N	6	9	NA 00:40:05:B7:F3:63	-	Sun Mar 23 23:12:33	Sun Mar 23 23:12:38
9	default	AP	N	6	7	NA 00:50:18:0A:35:7C	-	Sun Mar 23 23:12:34	Sun Mar 23 23:13:16
10F	linksys	AP	N	6	163	Linksys WAP11 v2.2 00:06:25:54:1F:10	-	Sun Mar 23 23:14:43	Sun Mar 23 23:15:50
11	tmobile	AP	N	1	86	Cisco UNKN 00:40:96:58:40:AE	-	Sun Mar 23 23:15:20	Sun Mar 23 23:22:41
12	default	AP	N	6	12	NA 00:40:05:B4:71:BF	-	Sun Mar 23 23:15:25	Sun Mar 23 23:22:07
13	lundgren	AP	N	6	67	Linksys Unknown 00:06:25:8C:FC:0D	-	Sun Mar 23 23:15:38	Sun Mar 23 23:16:15
14	d0llartree1nc	AP	Y	6	62	Symbol Unknown 00:A0:F8:46:85:3C	-	Sun Mar 23 23:16:28	Sun Mar 23 23:22:33
15	PacMediA340##SantaClarita/66	AP	N	1	15	Cisco Unknown 00:40:96:34:5D:F9	1	Sun Mar 23 23:17:13	Sun Mar 23 23:23:48
16	PacMediA340##SantaClarita/66	AP	N	1	65	Cisco Unknown 00:40:96:2A:6F:D2	1	Sun Mar 23 23:17:14	Sun Mar 23 23:23:48
17	wireless	AP	N	6	35	Linksys Unknown 00:06:25:06:1D:37	-	Sun Mar 23 23:17:43	Sun Mar 23 23:18:08
						Cisco Unknown		Sun Mar 23	Sun Mar 23

Figura 25 - Imagem do Kismet Log Viewer
Fonte: Banco de dados do autor.

4 Desenvolvimento

A pesquisa tem por objetivo a observação da qualidade das redes sem fio em funcionamento na cidade de Vitória da Conquista - BA. A utilização das redes sem fio é crescente, e este trabalho pode servir como fonte de informação para implantação de redes deste tipo no futuro. Foi feita uma coleta passiva dos dados, que são difundidos publicamente pelas redes sem fio em determinado bairro da cidade de Vitória da Conquista - BA. A coleta de dados proporcionou uma visão da situação dessas redes, como nível de segurança, qual tipo de segurança foi implantada e o nível de exposição das mesmas.

4.1 Equipamentos utilizados

Para esta pesquisa foi utilizada a técnica conhecida como *war driving* , que consiste na varredura de uma determinada área geográfica em busca de redes sem fio e suas vulnerabilidades. Tal procedimento, se trata de uma sondagem passiva, apenas obtendo dados que estão sendo propagados no ambiente. Não caracterizando uma invasão.

Para a captura dos dados foi utilizada como base um *notebook* da marca Intelbras®, modelo i39, como processador Intel® Dual Core com *clock* de 1.86 GHz, memória RAM de 1GB, com o sistema operacional Ubuntu, versão 8.10 com versão do *kernel* 2.6.27.10, compilado para maquina genérica. Para utilização de antena externa foi utilizado, conforme Figura 1, um adaptador sem fio USB, marca Gi-link, modelo WL-2407 USB IEEE 802.11 b/g , com *chipset* Zydas WLA-54L Wi-Fi, com conector SMA para antena externa.

O *software* base para captura dos dados foi o Kismet, já descrito, com versão 2008.05.R1, operando com a placa em modo passivo.

Foi utilizada uma antena de base magnética para fixação em superfícies metálicas, neste caso o teto do veículo, com pouco mais de 20 cm, cabo de 1m com conector SMA, frequência de 2,4 GHz a 2.5 GHz e impedância de 50 ohms, de irradiação omini-direcional, com ganho de 5dbi e potencia admitida de 1W, fabricada pela TP-LINK® sob modelo TL-ANT2405C (ver Figura 26).

Para registro da localização das redes foi utilizado um equipamento GPS, conforme

Figura 27, da marca Garmin® modelo Etrex H, que faz a comunicação com o PC através de uma porta serial, que para utilização no *notebook*, foi utilizada em conjunto com um cabo adaptador Serial/USB da marca Leadership®. Em conjunto com o GPSD que captura os dados pelo protocolo NMEA e disponibiliza os dados por uma porta TCP para leitura no *Kismet*.

Figura 26 - Antena com adaptador utilizados para captação dos dados
Fonte: Banco de dados do autor.

Para melhor visualização dos relatórios foi utilizado o *Kismet log viewer,* software que utiliza dos arquivos gerados pelo *Kismet*, e cria arquivos HTML, facilitando a visualização das informações e proporcionando um melhor entendimento. O KLV ainda possui alguns *scripts* incorporados que auxiliam na fusão dos dados referentes as coletas.

Figura 27 - GPS com cabo para conexão
Fonte: Banco de dados do autor.

4.2 Região Pesquisada

A coleta dos dados foi realizada em uma região residencial da cidade de Vitória da Conquista. Foi escolhido esta área por sua localização e grande concentração de edifícios, possuindo um maior índice populacional que outras áreas da cidade, consequentemente mais usuários. A área compreende a Av. Olivia Flores, do seu início a partir da Av. Rosa Cruz, até o cruzamento com a Av. Luiz Eduardo Magalhães, passando pela Estrada Velha de Barra do Choça, até encontrar novamente a Av. Rosa Cruz conforme Figura 28.

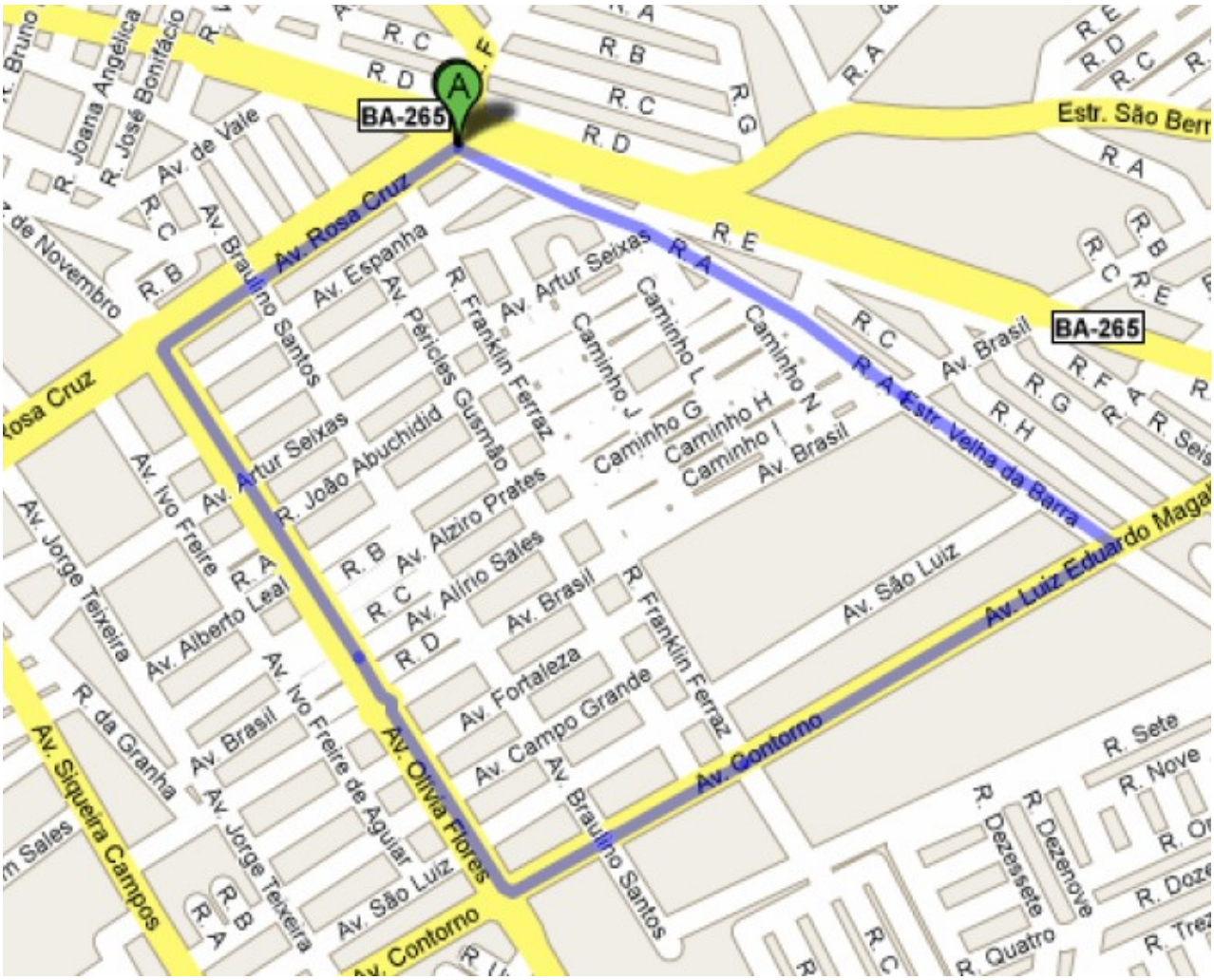


Figura 28 - Limites da área a ser pesquisada.
Fonte: www.google.com/maps

A pesquisa foi feita percorrendo a área descrita em seus limites e as ruas em seu interior.

Foram feitas duas coletas de dados. A primeira captação dos dados foi feita nos dias 9 e 10 de dezembro de 2008 , por volta das 10h30min da manhã até as 11h20min, com um total de 50 minutos em cada coleta. A segunda coleta foi realizada nos dias 20 e 21 de novembro de 2010, por volta das 14h00min até ás 14h50min, com um total de 50 minutos. A escolha de um fim semana se deu pela maior presença das pessoas em suas residências, proporcionando um maior uso das redes ali instaladas.

Algumas imagens da região pesquisada são apresentadas nas Figuras 29 e 30.

Figura 29 - Imagem da região pesquisada
Fonte: Banco de dados do autor.

Figura 30 - Imagem da região pesquisada
Fonte: Banco de dados do autor.

5 Resultados e discussões.

Dentro da área pesquisada, na primeira coleta de dados, foram encontradas 484 (quatrocentas e oitenta e quatro) redes em operação. Na segunda coleta foram localizadas 1022 (mil e vinte e duas) redes. Das quais, nos dois momentos, a maioria estava operando no modo infraestrutura, ou seja, com um concentrador de rede, onde um equipamento é responsável pela proliferação do sinal e conexão dos *hosts*.

As tabelas 3 e 4, seguidas do respectivo gráfico, ilustram com detalhes os dados sobre o modo de operação das redes.

Tabela 3 - Demonstrativo dos modos de operação das redes na coleta I.

Total		Modo Infraestrutura		Ad-Hoc	
Quantidade	Porcentagem	Quantidade	Porcentagem	Quantidade	Porcentagem
484	100,00%	481	99,38%	3	0,62%

Tabela 4 - Demonstrativo dos modos de operação das redes na coleta II.

Total		Modo Infraestrutura		Ad-Hoc	
Quantidade	Porcentagem	Quantidade	Porcentagem	Quantidade	Porcentagem
1022	100,00%	1019	99,71%	3	0,29%

O crescimento das redes sem fio, levando-se em conta a comparação das duas coletas de dados, o grande salto em seu número de 484 para 1022, pode ser caracterizada pelo aumento na venda de *notebooks* e dispositivos portáteis. Nos três primeiros meses do ano de 2010 foram comercializados 1,362 milhões de *notebooks* e *netbooks*, uma alta de 70% se comprado com os dados de 2009 (R7, 2010). Informações da Associação Brasileira da Indústria de Elétrica e Eletrônica (Abinee) e da consultoria IT Data revelam que as vendas de computadores portáteis já representam 52% dos computadores vendidos para o consumidor final do mercado brasileiro (IG, 2010).

Espera-se que os *notebooks*, ao fim do ano de 2010, representem 55% das vendas do setor. O que reflete a convergência para as plataformas móveis. Em 2009 as vendas de *desktops* caíram 6,4% enquanto as de *notebooks* e *netbooks* aumentaram 19%. (R7, 2010).

A partir da análise dos dados pode-se verificar a grande incidência de redes no modo infraestrutura, caracterizando em sua maioria um ponto de acesso à rede, em sua grande maioria para o compartilhamento de internet. Nesse modo de operação temos um equipamento como ponto centralizador da rede, onde a comunicação é distribuida entre os diversos clientes (RUFINO, 2007). Outra característica deste modelo é que o mesmo é utilizado em provedores de internet, foram encontradas redes com mais de 100 *hosts* conectados.

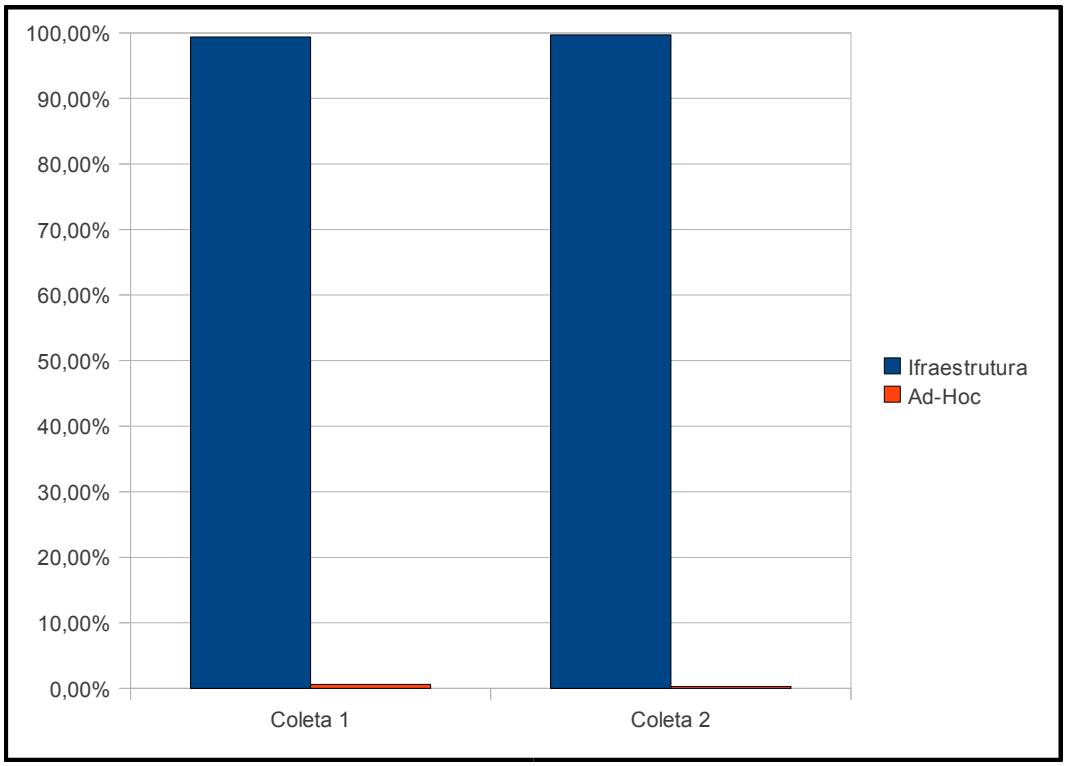


Gráfico 1 - Modos de operação das redes.

Um grande problema na implantação das redes sem fio, é que muitas vezes os usuários apenas retiram os equipamentos de suas embalagens e os põem em operação, sem que nenhuma alteração seja feita em sua configuração, facilitando assim o acesso de terceiros da rede em questão.

A tabela 5, seguida do seu respectivo gráfico ilustra a situação das redes encontradas com essa característica. Apenas 11 redes (2,27%) apresentavam tal característica. Já a tabela 6 que representa a segunda coleta, demonstra que não foi encontrada nenhum equipamento operando com a configuração padrão de fábrica.

Tabela 5 - Tabela das redes operando com configuração de fábrica na coleta I.

Total		Conf. de Fábrica		Conf. Alteradas	
Quantidade	Porcentagem	Quantidade	Porcentagem	Quantidade	Porcentagem
484	100,00%	11	2,27%	473	97,73%

Tabela 6 - Tabela das redes operando com configuração de fábrica na coleta II.

Total		Conf. de Fábrica		Conf. Alteradas	
Quantidade	Porcentagem	Quantidade	Porcentagem	Quantidade	Porcentagem
1022	100,00%	0	0,00%	1022	100,00%

A manutenção das configurações implica em uma menor eficiência, no que diz respeito a segurança da rede. O atacante apenas deverá esta na área de cobertura da para que consiga o acesso.

Todos os equipamentos a venda atualmente no mercado são acompanhados de manual de instruções com informações sobre a configuração dos dispositivos e na maioria dos casos o equipamento é acompanhado por um CD, que guia o utilizador, de maneira simples e interativa a fazer uma configuração do equipamento.

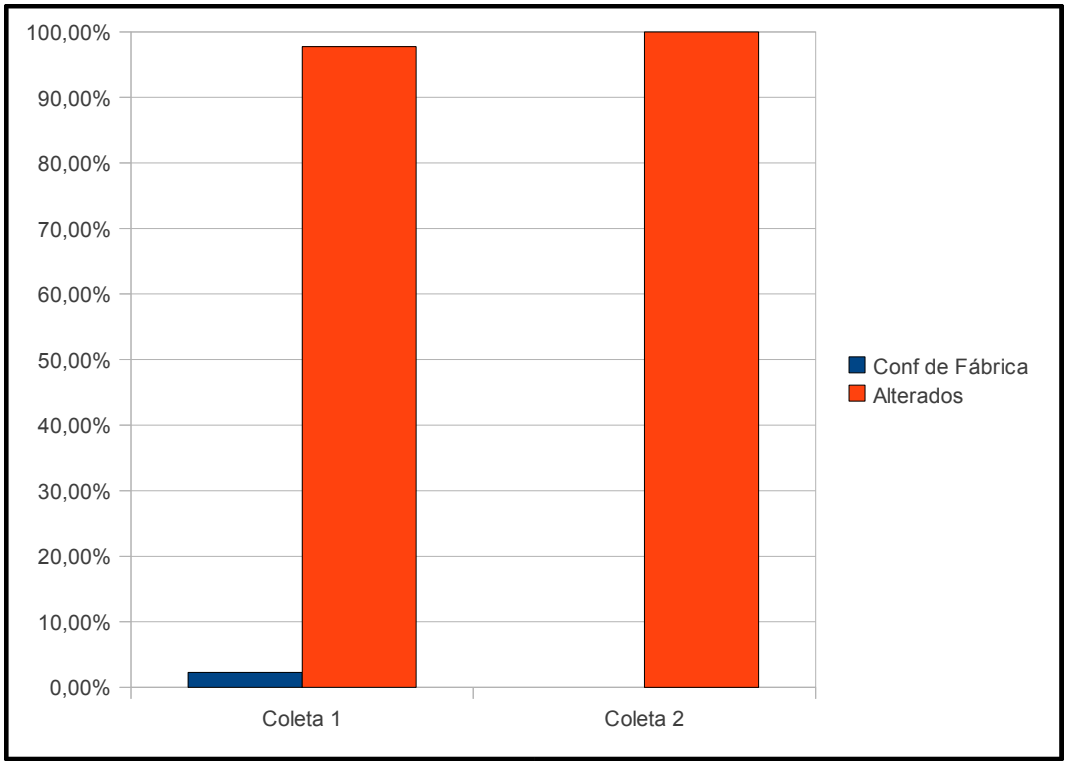


Gráfico 2 - Alterações nas configurações de fábrica

Um dos mecanismos para prevenção de ataques é o ocultamento da rede, pois evita que o SSID ou nome da rede seja difundido via *broadcast*, para que os clientes identifiquem facilmente a rede para conexão, de acordo com a tabela 7, essa medida de segurança estava presente em apenas 2,07% das redes encontradas.

Tabela 7 - Redes SSID Oculto na coleta I.

Total		SSID Oculto		SSID Visível	
Quantidade	Porcentagem	Quantidade	Porcentagem	Quantidade	Porcentagem
484	100,00%	10	2,07%	474	97,93%

A tabela 8 juntamente com gráfico 3, demonstra que no segundo momento, nenhuma rede utilizava de tal mecanismo. Esse tipo de medida, em sua maioria, é tomada por empresas prestadoras de serviços, que vendem o serviço de internet. O ocultamento da SSID evita que clientes indesejados tentem entrar na rede, além de aumentar o nível de segurança.

Tabela 8 - Redes SSID Oculto na coleta II.

Total		SSID Oculto		SSID Visível	
Quantidade	Porcentagem	Quantidade	Porcentagem	Quantidade	Porcentagem
1022	100,00%	0	2,07%	1022	97,93%

Esse tipo de configuração pode ser feito em qualquer equipamento atual, a não utilização do mesmo, pode esta associado a maior dificuldade de configuração de acesso às redes nos clientes. Quando o SSID não esta sendo propagado pelo concentrador, os clientes tem que ter uma configuração prévia da rede que será utilizada (RUFINO, 2007).

Outro fator que deve ser levado em consideração é o tipo de criptografia utilizado. Na pesquisa foram encontradas redes com três características. A tabela 6 ilustra os dados encontrados. O maior problema encontrado é que a maioria das redes não apresenta nenhum tipo de segurança ou utiliza o protocolo WEP, 233 redes (48,14%) não possuem nenhum tipo de segurança, estão com acesso totalmente liberado; 163 redes (33,68%) utilizam o protocolo WEP, que provê certo nível de segurança, mesmo considerando que protocolo é o mais simples de ser quebrado, e somente 88 delas (18,18%) utilizam o protocolo WPA, este considerando o mais seguro dentre os três encontrados.

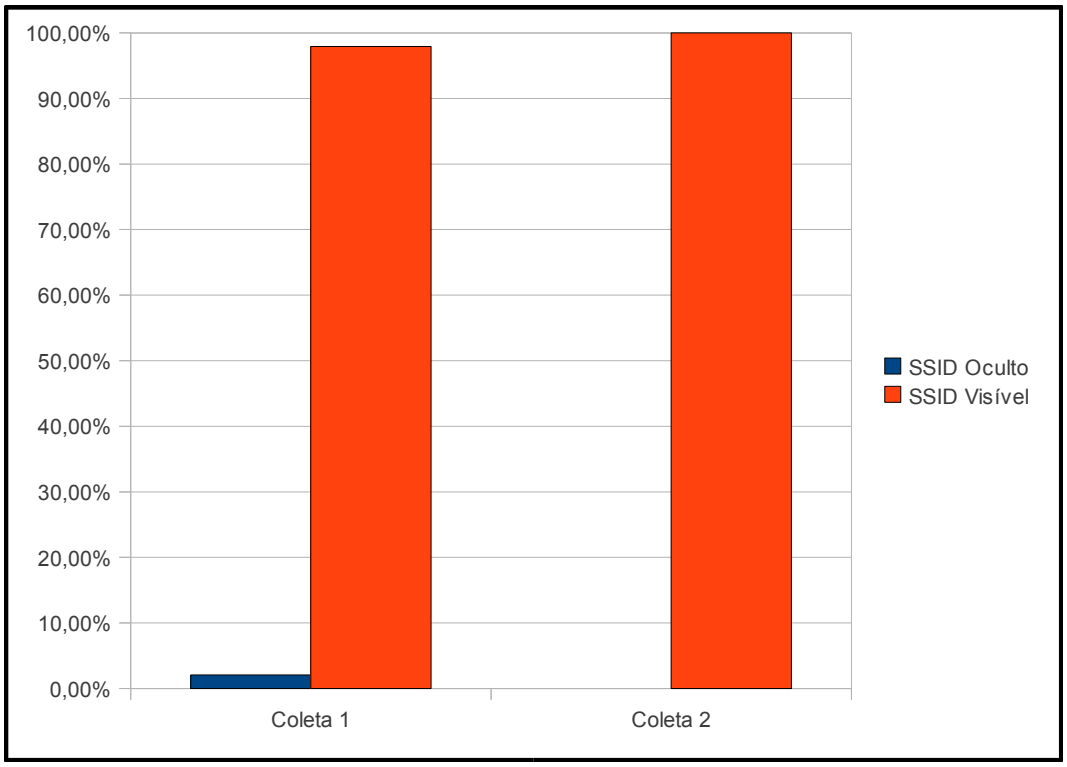


Gráfico 3 - Apresentação de SSID

Tabela 9 - Tabela das configurações de segurança na coleta I.

Total		Sem Criptografia		WEP		WPA	
Quantid.	Porcent.	Quantid.	Porcent.	Quantid.	Porcent.	Quantid.	Porcent.
484	100,00%	233	48,14%	163	33,68%	88	18,18%

No segundo momento, verifica-se um aumento no uso de algum tipo de criptografia na rede, anteriormente 51,86% das redes utilizavam algum tipo de criptografia, posteriormente o índice já representa 68,78% dos quais a utilização de WPA já representa 42,07% do total o que demonstra um aumento no uso da criptografia WPA.

Tabela 10 - Configurações de segurança na coleta II.

Total		Sem Criptografia		WEP		WPA	
Quantid.	Porcent.	Quantid.	Porcent.	Quantid.	Porcent.	Quantid.	Porcent.
1022	100,00%	319	31,21%	273	26,71%	430	42,07%

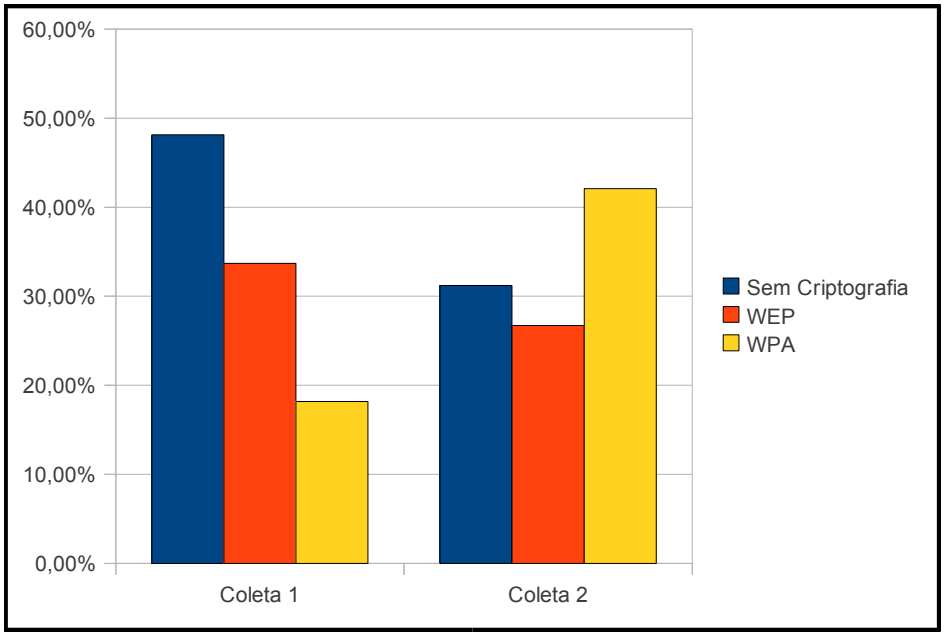


Gráfico 4 - Uso de Criptografia nas redes.

Os dados revelam que apesar dos números representarem um aumento significativo no uso da segurança, a quantidade daqueles que ainda fazem a utilização de configurações simples ainda é grande. Porém, com a convergência digital, e o uso cada vez maior da internet como meio de informação o nível de conhecimento e de entendimento das pessoas quanto a necessidade de preservação das informações tende a aumentar.

A Figura 31 apresenta o mapa gerado a partir dos dados coletados e produzidos pelo *Kismet* em conjunto a localização fornecida pelo GPS. A ferramenta possibilita a geração de mapas com três opções diferenciadas para localização das redes, uma exibindo as redes de acordo com o canal de operação, uma segunda opção de acordo com o modelo de criptografia dos dados, e uma terceira opção apenas para a localização das redes.

O nome das redes foi ocultado a fim de preservar as mesmas. Na Figura 33 a disposição das redes de acordo com a operação de cada canal.

Figura 31 - Mapa das redes encontradas, em vermelho as redes com presença de criptografia, em verde as redes abertas e em azul as redes com configurações padrão de fábrica.

Fonte: Banco de dados do autor.

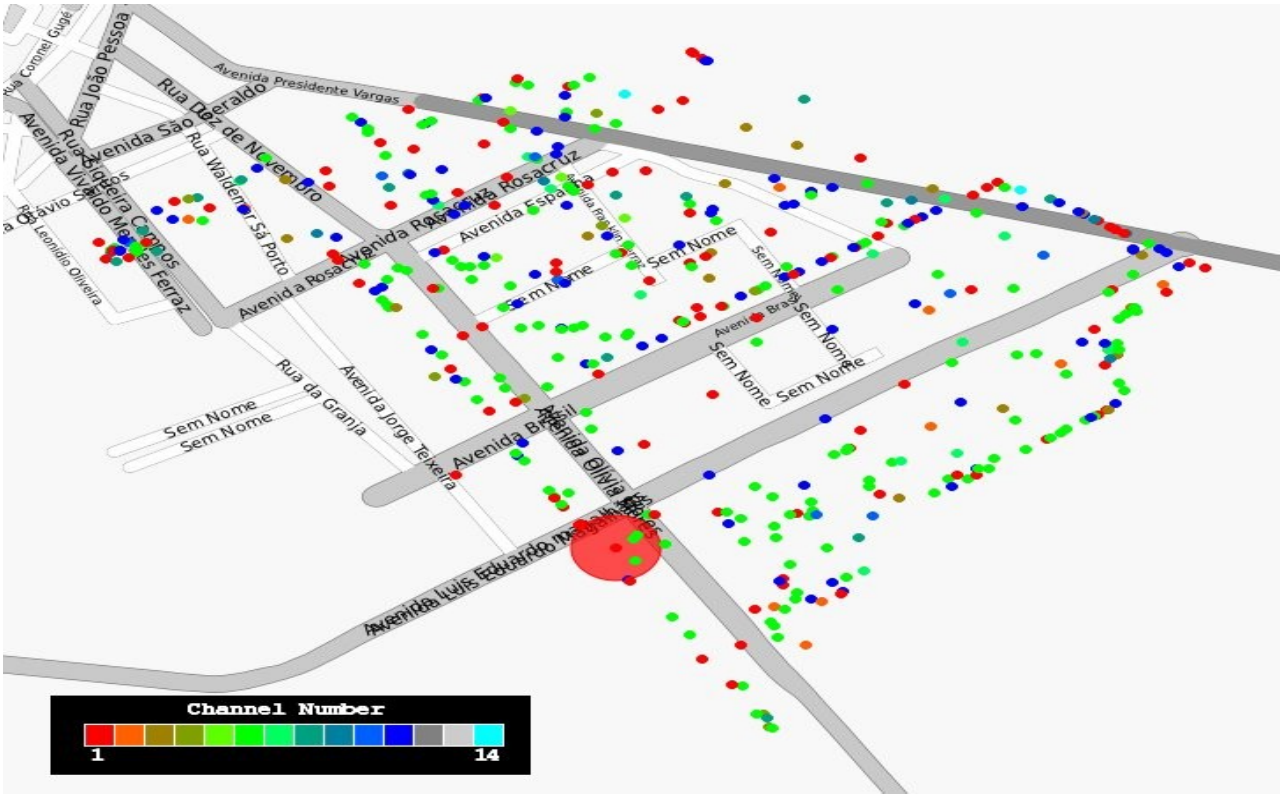


Figura 32 - Mapa das redes por canal de operação.
Fonte: Banco de dados do autor.

6 Trabalhos Relacionados

Foram produzidos dois artigos semelhantes com o intuito de fazer a análise de redes nas cidades de São Paulo – SP e Lajeado – RS. Nos dois trabalhos foram utilizadas as mesmas ferramentas, salvo algumas alterações nas especificações de *hardware* dos *notebooks* utilizados. Ambos apresentam apenas uma análise da presença ou não de criptografia nas redes. Um comparativo é apresentado na tabela 11.

Tabela 11 - Comparativo das redes sem fio encontradas em São Paulo – SP , Lajeado – RS e Vitória da Conquista – BA (Adaptado de CASIAN, A. et al., 2004 e HAUSCHILD.; STOLL; JÚNIOR, 2007).

	Redes Encontradas	Com Criptografia	Sem Criptografia
São Paulo	316 (100%)	104 (33%)	212 (67%)
Lajeado	212 (100%)	161 (76%)	51 (24%)
Vitória da Conquista I	484 (100%)	251 (52%)	233 (48%)
Vitória da Conquista II	1022 (100%)	730 (69%)	319 (31%)

As datas em que as coletas foram realizadas são um pouco que distantes, em São Paulo o trabalho foi realizado no ano de 2004, em Lajeado no ano de 2007 e em Vitória da Conquista a primeira coleta foi realizada no ano de 2008 e a segunda coleta no ano de 2010.

O trabalho em Lajeado foi realizado com duas ferramentas o *Kismet,* mesmo sistema utilizado nas pesquisas em São Paulo e Vitória da Conquista, e o *Network Stumbler,* alem de fazer dois tipos de captura, uma em movimento e outra parado. Para efeitos comparativos foram utilizados apenas as informações coletadas pelo *Kismet* e em movimento.

Analisando cronologicamente as coletas, nota-se que a utilização de criptografia nas redes aumentou com o passar do tempo. Dado esse que pode ser justificado pela maior facilidade de acesso às informações, no que se refere a segurança das redes sem fio, além dos fatores já citados no desenvolvimento do trabalho. Um destaque deve ser dado a cidade de Lajeado onde foi constatado a utilização de mecanismo de segurança em 76% das redes encontradas, já em Vitória da Conquista em um primeiro momento a utilização de tais mecanismos era de 52% e no segundo momento de 69% o que demonstra um aumento significativo.

7 Conclusão e Trabalhos Futuros

As redes de computadores são uma realidade tanto nos ambientes domésticos quanto corporativos, aliados a elas milhares de informações trafegam em todos os sentidos. A segurança dessas informações é uma premissa importantíssima dentro da atual conjuntura da sociedade, principalmente no ambiente corporativo. Métodos para assegurar que as informações não serão perdidas ou roubadas estão cada vez mais eficientes.

Dentro do contexto das redes, as redes sem fio, são uma tendência e já são de significativa representação no mercado, a exemplo da pesquisa realiza, em uma pequena área geográfica cerca de 1000 redes operando sem fio foram encontradas. A segurança destas redes ainda é um desafio.

A qualidade, no que se refere a segurança, destas redes obteve um aumento considerável, considerando-se as duas coletas realizadas. O aumento no uso da segurança nas redes reflete o aumento da preocupação dos indivíduos com a proteção das suas informações.

Este trabalho teve como objetivo analisar a atual situação das redes na cidade de Vitória da Conquista, buscando analisar e listar as suas falhas. Os riscos, ameaças e vulnerabilidades apresentadas afetam as redes em qualquer ambiente onde estejam em funcionamento. A observação das medidas de segurança pode reduzir drasticamente o nível de exposição das informações.

Vale lembrar, que o atacante bem motivado, após muitas tentativas pode obter sucesso em seu objetivo. O trabalho serve como fonte de dados para adesão de algumas políticas de segurança que podem ser adotadas.

O Gráfico 4, que traz um resumo da coleta realizada, apresenta um aumento expressivo do uso da criptografia nas redes sem fio em operação. Sobretudo do modelo WPA que proporciona uma melhor qualidade da proteção dos dados. Contudo as redes sem fio em operação que não apresentam nenhuma segurança ainda é grande, o acesso às redes esta totalmente aberto, facilitando o uso das mesmas para a copia de informações ou uso dos serviços disponíveis nas mesmas.

A busca de melhorias nos protocolos de segurança, e atenção dos administradores de rede e dos usuários também influencia na qualidade da segurança das informações.

O mundo das redes sem fio é um ambiente muito dinâmico e cativante. Como

propostas para trabalhos futuros algumas sugestões:

Verificação do ambiente em que as redes sem fio operam, residências, escritórios, empresas, e analise de que modelo de segurança as mesmas utilizam.

Verificar o nível de conhecimento e qualificação técnica dos indivíduos envolvidos na instalação e configuração das mesmas.

Fazer a coleta em outra região da cidade a fim de fazer comparativos com dados aqui descritos.

A segurança sempre será um fator de grande importância nos ambientes computacionais, a busca por um maior qualidade da mesma deve sempre esta relacionadas com profissionais capacitados e equipamento de qualidade.

REFERÊNCIAS

CANSIAN, A. et al. Falhas em políticas de configuração: uma análise do risco para as redes sem fio na cidade de São Paulo. In: SIMPÓSIO DE SEGURANÇA EM INFORMÁTICA. 4., 2004, São José dos Campos. **Anais**. São José dos Campos: SBC, 2004. Disponível em: <http://www2.acmesecurity.org/publicacoes/artigos/acme-artigo-ssi-2004-wlan.pdf>. Acesso em: 13 ago. 2008.

CERT. **Estatísticas dos Incidentes Reportados ao CERT.br.** Disponível em <http://www.cert.br/stats/incidentes/>. Acesso em: 12 nov. 2010.

DUARTE, Luiz Otávio. **Análise de Vulnerabilidades e Ataques Inerentes a Redes Sem Fio 802.11x** . Monografia. Título de Bacharel em Ciência da Computação . UNESP : São José do Rio Preto - São Paulo, p. 55, 2003.

FLEISHMAN, Glenn e ENGST, Adam. Kit do Iniciante em Redes Sem Fio. 2. ed. Editora Makron Books, São Paulo: 2005.

HAUSCHILD, F.; STOLL, R.; JÚNIOR, W.D.B. **Uma análise da segurança de redes sem fio na cidade de Lajeado**. UNIVATES, Lajeado: 2007.

IG. **Venda de notebooks cresce 70% no trimestre.** Disponível em: <http://economia.ig.com.br/empresas/industria/venda+de+notebooks+cresce+70+no+trimestre/n1237636179604.html>. Acesso em: 12 nov. 2010.

MORIMOTO, Carlos Eduardo. **Redes, guia prático**. Porto Alegre: Sul Editores, 2008.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. **Segurança de redes em ambientes corporativos**. São Paulo: Novatec Editora, 2007.

R7. **Venda de computadores cresce 32% no primeiro semestre, segundo IDC.** Disponível em <http://noticias.r7.com/tecnologia-e-ciencia/noticias/venda-de-computadores-cresce-32-no-primeiro-semestre-segundo-idc-20100827.html>. Acesso em 12 de novembro de 2010.

ROSS, John. Wi-Fi – instalação, configuração e utilização de redes wireless. Rio de Janeiro: Alta Books, 2003.

RUFINO. Nelson Murilo de Oliveira. **Segurança em redes de computadores**: aprenda a proteger suas informações em ambientes Wi-Fi. 2. ed. São Paulo: Novatec Editora, 2007.

SANCHES, Carlos Alberto. **Projetando redes WLAN**. 2. ed. São Paulo: Érica, 2007.

SOLHA, L. E. V. A. ; TEIXEIRA, R. C.; PICCOLIN, J.D.B. **Tudo que você precisa saber sobre os ataques DdoS,** 2000. Disponível em: <http://www.rnp.br/newsgen/0003/ddos.html>. Acesso em 2: dez. 2010.

STALLINGS, William. **Criptografia e segurança de redes**. 4. ed. São Paulo: Pearson Prentice Hall, 2008.

WAZLAWICK, Raul Sidnei. **Metodologia de pesquisa para ciência da computação**. Rio de Janeiro: Elsevier: 2008.

TANENBAUM, Andrew S. **Redes de computadores**. 4. ed. Rio de Janeiro: Elsevier, 2003.

WIKIPEDIA. **Rede de computadores**. Disponível em: <http://pt.wikipedia.org/wiki/Rede_de_computadores>. Acesso em: 07/07/2010.