UNIVERSIDADE SAGRADO CORAÇÃO

ANDREA LUISA DE MATOS

ESTUDO DE REDES SEM FIO NAS EMPRESAS DE BAURU - SP

BAURU

2010

ANDREA LUISA DE MATOS

ESTUDO DE REDES SEM FIO NAS EMPRESAS DE BAURU - SP

Trabalho de conclusão de curso apresentado ao Centro de Ciências Sociais Aplicadas como parte dos requisitos para obtenção do titulo de bacharel em Ciência da Computação, sob orientação do Prof. Dr. Kelton Augusto Pontara da Costa.

BAURU

2010

ANDREA LUISA DE MATOS

ESTUDO DE REDES SEM FIO NAS EMPRESAS DE BAURU - SP

Trabalho de conclusão de curso apresentado ao Centro de Ciências Sociais Aplicadas como parte dos requisitos para obtenção do titulo de bacharel em Ciência da Computação, sob orientação do Prof. Dr. Kelton Augusto Pontara da Costa.

Banca examinadora:

_____

Prof. Dr. Kelton Augusto Pontara da Costa
Universidade Sagrado Coração

_____

Prof. Esp. Henrique Pachioni Martins
Universidade Sagrado Coração

_____

Prof. Esp. André Luiz Ferraz de Castro
Universidade Sagrado Coração

Bauru, 28 de junho de 2010.

Dedico este trabalho aos meus
pais e minhas irmãs.

AGRADECIMENTOS

Agradeço principalmente a Deus por estar concluindo este curso.

Aos meus pais e minhas irmãs pelo carinho compreensão e incentivo.

Especialmente a minha mãe, Valdelice, que me deu incentivo e o ânimo necessário para seguir em frente nos momentos mais dificies nesses 5 anos de curso.

A todos os professores e meus amigos de faculdade Alexandre e Hareton pelo apoio.

Ao Professor Doutor Kelton Costa, pela orientação.

A todos que de alguma forma colaboraram, direta e indiretamente para realização deste trabalho.

RESUMO

As redes sem fio têm sido amplamente adotadas por corporações, instituições e até mesmo em residências. Uma vantagem deste tipo de rede é a flexibilidade oferecida. Sem a necessidade de cabos, os usuários estão livres para se moverem livremente enquanto conectados á rede. No entanto, essa tecnologia virou alvo (na maioria das vezes) fácil de usuários mal intencionados e bem informados comprometem tanto a confidencialidade de dados, quanto a autenticidade de dispositivos. Este trabalho visa apresentar os protocolos de redes sem fio, os mecanismos de segurança, vulnerabilidades nos protocolos, os tipos de ataques e ferramentas de defesa. Entender, analisar e avaliar a segurança de redes sem fio nas empresas de Bauru – SP, identificando as vulnerabilidades e apontar meios para a solução das mesmas.

Palavras Chave: Redes sem fio, Vulnerabilidades, questionário sobre segurança de redes sem fio.

ABSTRACT

Wireless networks have been widely adopted by corporations, institutions and even in homes. One advantage of this type of network is the flexibility offered. Without the need for cables, users are free to move about freely while connected to the network. However, this technology became a target (mostly) easy to malicious users well informed and committed both data confidentiality, and authenticity of devices. This paper presents protocols for wireless networks, security mechanisms, vulnerabilities in the protocols, the types of attacks and defensive tools. Understand, analyze and evaluate the security of wireless networks in enterprises of Bauru - SP, identifying vulnerabilities and point out ways to solve them.

Keywords: Wireless networks, , defense tools, the questionnaire on security of wireless networks.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURA E SIGLAS

AES	Advanced Encryption Standart
AP	Access Point
ARP	Address Resolution Protocol
CBC-MAC	Cipher Block Chaining Message Authenticity Check
CCMP	Cipher Block Chaining Message Authentication Code Protocol
CRC-32	Cyclic Redundancy Check
DFS	Dynamic Frequency Selection
DHPC	Dynamic Host Configuration Protocol
DoS	Negação de Serviço
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EAP-TLS	EAP-Transport Layer Security
EAP-TTLS	EAP-Tunneled Transport Layer Security
ESSID	Extentended Service Set Identifier
GHz	Gigahertz
GPS	Global Positioning System
HTTP	HyperText Transfer Protocol
IBSS	Independent Basic Service Set
ICV	Integrity Check Value
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IV	Inicialization Vector
LAN	Local Area Network
LMDS	Local Multipoint Distribution System
MAC	Media Access Control
MHz	Megahertz
MIMOOFDM	Multiple Input, Multiple OutOFDM

MIC	Message Integrity Check
MSK	Master Session Key
NETBEUI	NetBIOS Extended User Interface
OFDM	Orthogonal Frequency Division Multiplexing
PDA	Personal Digital Assistants
PEAP	Protected Extensible Authentication Protocol
PMK	Pair-wise Master Key
PRNG	Pseudo Random Number Generator
PSK	Phase Shift Keying
QOS	Quality of service
RADIUS	Remote Authentication Dial-In User Service
RC4	Route Coloniale 4
RFC 3748	Request for Comments
RSN	Robust Security Network
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TA	Transmitter Address
TPC	Transmite Power Control
TK	Temporal Key
TKIP	Temporal Key Integrity Protocol
TPC	Transmite Power Control
TTAK	Temporal and Transmitter Address Key
WEP	Wired Equivalent Privacy
WI-FI	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Networks
WMAN	Wireless Metropolitan Area Networks
WPA	Wi-fi Protected Access
WPAN	Wireless Personal Área Networks

WWAN	Wireless Wide Area Network
XOR	Exclusive OR

SUMÁRIO

1 INTRODUÇÃO

Com o crescimento dos computadores e do acesso a internet nas ultimas décadas resultou na expansão da utilização de redes sem fio.

As redes sem fio fornecem informações em tempo real, flexibilidade e maior mobilidade, tornando-se assim, sem duvida, mais populares e indispensáveis, sendo utilizados em lugares como, aeroportos, cyber cafés, hotéis, domicilio, universidades e até mesmo interligando empresas. Além de serem utilizadas pra prover a conectividade dentro de instituições, e criar links á distancia entre organizações, suas filiais e clientes.

Este é um novo cenário, em que a rede sem fio esta ganhando mercado, estando assim presente cada vez mais na vida das pessoas por causa da sua agilidade. Mas com tanta evolução, uma grande preocupação começou a surgia nesse ambiente: A Segurança.

Com a facilidade de instalação e configuração de equipamentos, tornam-se as redes sem fio cada vez mais um alvo frequente de ataques de crackers e pessoas mal-intencionadas. Mas isto não implica em falar que as redes sem fio não são seguras, é que com a facilidade de instalação, aspectos como segurança não são verificados durante a configuração da rede sem fio, também como qualquer outra tecnologia de rede esta possui suas vulnerabilidades e falhas.

A adoção da tecnologia de redes sem fio por empresas pode trazer muitas vantagens, chegando a certos casos em ser imprescindível, entretanto, a falta de conhecimento da tecnologia, falta de segurança e planejamento, pode trazer grandes riscos de segurança para essas empresas.

A instalação e configuração correta dos equipamentos, uso de mecanismos de segurança mais eficiente, uso da ferramenta de monitarização mais eficaz evita e minimiza as vulnerabilidades da tecnologia.

1.1 Objetivos Gerais

Este trabalho tem a finalidade de estudar os protocolos de redes sem fio, os mecanismos de segurança, vulnerabilidades nos protocolos e os tipos de ataques e ferramentas de defesa.

1.2 Objetivos Específicos

Entender, analisar e avaliar a segurança de redes sem fio em algumas das empresas de Bauru – SP, identificando as vulnerabilidades e apontar meios para a solução das mesmas.

1.3 Justificativa

As redes sem fio, por ser uma tecnologia recente, muitas vulnerabilidades podem ser encontradas e outras ainda serão descobertas.

Ataques direcionados às redes sem fio além de comprometer os recursos destas, podem comprometer os recursos de outras redes com as quais esta se interconecta. Outro fator determinante da segurança em redes sem fio é relacionado com a origem dos ataques. Estes podem ser originados de qualquer posição dentro da área de cobertura da rede em questão, o que dificulta a tarefa de localização precisa da origem do ataque.

Assim sendo, a segurança tornou uma das principais necessidades das empresas.

1.4 Estrutura do Trabalho

Para melhor compreensão do trabalho, o mesmo foi organizado em seis capítulos:

O primeiro capítulo apresenta uma breve introdução sobre o assunto a ser abordado, referenciando a importância da segurança da rede sem fio em algumas empresas, apresentando os objetivos gerais, específicos e a justificativa bem como a estrutura do trabalho. Já o segundo capítulo aborda sobre as tecnologias utilizadas em redes sem fio, bem como meios de transmissão, tipos, modos de operação, padrões, segurança de redes sem fio, riscos, vulnerabilidades, ataques e as ferramentas de defesa. No terceiro capítulo apresenta um estudo de caso realizado em algumas empresas da cidade de Bauru sobre redes sem fio, estudo que tem o objetivo verificar a segurança das redes sem fio. O quarto capítulo descreve os matérias e métodos utilizados para elaboração do trabalho bem como o cronograma do trabalho. No quinto capítulo descreve as principais conclusões sobre o trabalho, apresentando os resultados obtidos das pesquisas realizadas. No sexto capítulo descreve as referências bibliográficas utilizadas no trabalho.

2 FUNDAMENTOS DA REDE SEM FIO

Atualmente as redes de computadores sem fio são uma peça indispensável para um grande conjunto de empresas e instituições. Estas redes permitem a transmissão das informações em redes sem fio, proporcionando a facilidade de dispositivos e flexibilidades de conexões.

A mobilidade facilita na transmissão de informações dentro de uma empresa/instituição, sem perder o acesso ao sistema e aos dados da rede.

A flexibilidade é a facilidade física na sua instalação, sem a necessidade de uma estrutura de fios e cabos.

Segundo Martins (2005), o termo redes sem fio começou a ser usado no Reino Unido, e significa uma rede interligada sem fios, ou seja, são canais de comunicação alternativos (radiofreqüência, infravermelho e laser).

As redes sem fio estão se tornando uma tecnologia atraente e promissora, pois serve como meio de acesso a internet através de locais remotos como um escritório, um parque, um aeroporto, um bar, e até mesmo em casa.

Para Kurose e Ross (2006, p. 393) dizem que “independente do crescimento futuro de equipamentos sem fio para internet, já ficou claro que redes sem fio e os serviços moveis relacionados que elas possibilitam, vieram para ficar”.

2.1 Conceitos de redes sem fio

Segundo Prado (2006 apud Sguarezi, 2007, p.21), na terminologia de redes sem fio, as estações bases são chamadas de concentradores de acesso (ou Access points), e interligam estações sem fio entre si, à Internet ou a uma rede tradicional, havendo a possibilidade de ataques bem sucedidos à rede caso a configuração destas estações base não seja cuidadosamente realizada. Tais ataques se tornam ainda mais graves quando estas redes estão sendo implementadas de forma descuidada em locais de maiores concentrações de acesso, como grandes empresas e hospitais, expondo informações confidenciais.

2.1.1 Vantagens e Desvantagens das redes sem fio

Segundo Colunga (2005), as redes sem fio apresentam as seguintes vantagens:

- **Flexibilidade:** permite a comunicação dentro da área de cobertura, sem nenhuma restrição. Além disso, permite que a rede alcance lugares onde os fios não poderiam chegar.
- **Facilidade:** não é necessária passagem de cabos através de paredes, forros, a instalação é rápida, portanto uso mais eficiente do espaço físico. Redução do custo agregado: mesmo mais dispendiosa que uma rede cabeada, está agregada.
- **Diversas topologias:** as configurações podem ser facilmente alteradas, tem uma facilidade de expansão e a manutenção é reduzida

Para o mesmo autor, em contrapartida, apresentam as seguintes desvantagens:

- **Qualidade de serviço:** a qualidade de serviço é menor do que as redes cabeadas, pois há limitações de radio transmissão e alta taxa de erros por causa da interferência.
- **Custo:** o preço dos equipamentos de Redes sem Fio é mais alto que os equivalentes em redes cabeadas.
- **Segurança:** com o uso das ondas de radio na transmissão pode interferir outros equipamentos. E podem acarretar perda de dados e alta taxa de erros na transmissão
- **Baixa transferência de dados:** embora a taxa de transmissão das Redes sem Fio esteja crescendo rapidamente, ela ainda é muito baixa se comparada com as redes cabeadas.

2.2 Ponto de acesso

Segundo Sguarezi (2007), o ponto de acesso é o principal componente para efetuar a conexão de redes sem fio, assim os usuários enviar e receber dados entre si. Essa transmissão é feita a partir de um sinal de uma ou duas antenas em um ponto de acesso. Como mostra a figura 1:

Figura 1 – Exemplo de aparelho de ponto de acesso

Fonte: SGUAREZI, 2007, p. 26

Os usuários podem acessar notebooks, PDas, em residências comerciais e residenciais, que estão equipados com placas de comunicação wireless e um dispositivo centralizador que é o ponto de acesso. (Sguarezi , 2007).

Segundo INFOEXAME (2004, págs. 54-55 apud Sguarezi, 2007, p.26), o ideal é posicionar o ponto de acesso num lugar mais alto que puder, para ter um bom aproveitamento do aparelho, mas existem barreiras tais como:

- “Antena baixa - Um dos cuidados descritos em manuais de instalação de antenas se refere à localização do equipamento devido à transmissão de sinais”;
- “Telefone sem fio - A maioria dos telefones sem fio opera na freqüência de 900 MHz, porém existe modelo que opera na de 2,4 GHz, ou seja, em ambientes com esse tipo de telefone, ou próximo deles, pode comprometer a qualidade do sinal do wireless, porém não acontece necessariamente em todos os casos”;
- “Concreto e trepadeira - Juntos tornam-se uma barreira a ponto de prejudicar totalmente o sinal”;
- “Microondas - Assim como o telefone sem fio, os aparelhos que transmitem microondas usam a freqüência de 2,4 GHz, sendo o ideal ficarem isolados do ambiente onde está a rede”;
- “Micro no chão - Como dito sobre o posicionamento dos pontos de acesso, quanto mais alto melhor a freqüência, e essa regra vale também para as placas e os adaptadores colocados no micro”;
- “Água - Recipientes com água como aquário, bebedouro, podem considerar uma barreira para a boa propagação do sinal”;
- “Vidro e árvore - O vidro pode prejudicar a qualidade do sinal, porém na presença de árvores dividindo os ambientes, como por exemplo, primeiros andares de dois prédios da mesma companhia, a influência negativa aumenta entre as duas antenas”

A tabela 1 mostra os exemplos de materiais com influencia no sinal

Tabela 1 – Exemplo de materiais com influência no sinal

BARREIRAS	CRITICIDADE	EXEMPLOS
Ar	Mínimo	
Madeira	Baixa	Divisórias, portas
Gesso	Baixa	Paredes Internas
Material sintético	Baixa	Divisórias
Vidros	Baixa	Janelas
Água	Média	Madeiras úmidas, aquário
Tijolos	Média	Paredes internas e externas
Concreto	Alta	Pisos, paredes
Metal	Muito Alta	Mesas, divisórias de metal

Tabela 1 – Exemplo de materiais com influência no sinal

Fonte: SGUAREZI, 2007, p. 27

> Existem limitações de máquinas que podem ser atendidos por um AP, 128 máquinas, porém é aconselhada a utilização de 40 máquinas concorrentes devido à queda de performance, pois a banda total é dividida pelo número de equipamentos ativos no momento da operação. Para não afetar o desempenho pode-se utilizar mais AP's em uma configuração chamada Agrupamento de Células, onde cada agrupamento atende no máximo 40 máquinas concorrentes, formando grupos que coexistem em um mesmo ambiente. (SGUAREZI, 2007, p. 27).

De acordo com Sguarezi (2007), existem limitações de máquinas que podem ser atendidos por um AP, 128 máquinas, porém é aconselhada a utilização de 40 máquinas concorrentes devido à queda de performance, pois a banda total é dividida pelo número de equipamentos ativos no momento da operação. Para não afetar o desempenho pode-se utilizar mais AP's em uma configuração chamada Agrupamento de Células, onde cada agrupamento atende no máximo 40 máquinas concorrentes, formando grupos que coexistem em um mesmo ambiente, como mostrado na Figura 2.

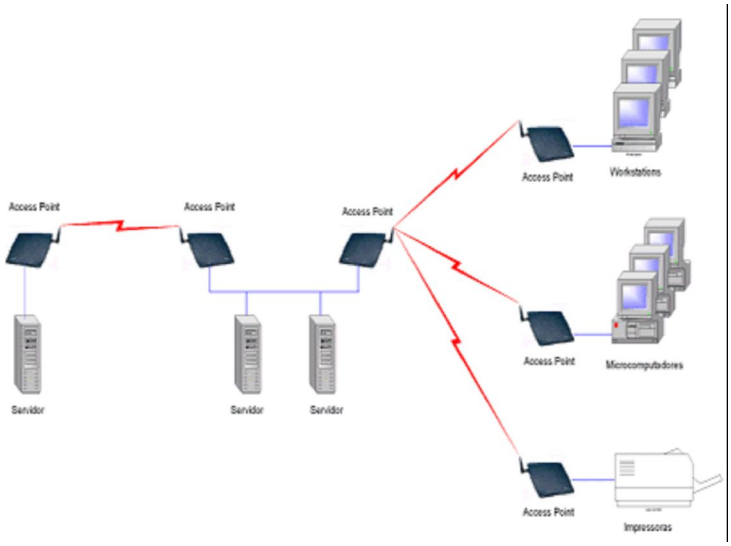

Figura 2 – Pontos de acesso em funcionamento

Fonte: SGUAREZI, 2007, p. 28

2.3 Tipos de redes sem fio

"Assim como as redes tradicionais, as redes sem fio podem ser classificadas em diferentes tipos com base nas distâncias através das quais os dados podem ser transmitidos". (MICROSOFT, 2010).

2.3.1 WLAN

Para Maia (2003), as redes locais sem fio WLAN ou Wireless LAN, são redes que oferecem uma pequena dispersão geográfica e altas taxas de transmissão. Além de oferecer grande flexibilidade para seus usuários, principalmente os que utilizam computadores portáteis e PDAs.

Segundo RNP (2004 apud Bezerra et al., 2004, p. 24), as redes locais sem fio WLAN constituem se basicamente em redes locais cabeadas, conforme representado na Figura 3, fornecendo as mesmas funcionalidades, mas com grande flexibilidade e conectividade em ambientes prediais ou de campus. Combinando mobilidade e conectividade a elevadas velocidades, podem atingir distâncias de até 18 metros de acordo com alguns casos.

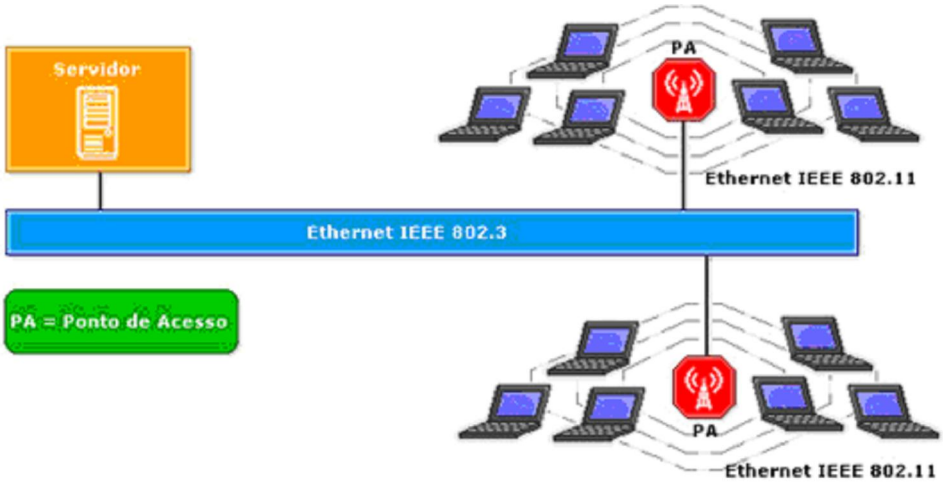

Figura 3 – Rede WLAN

Fonte: BEZERRA, 2004, p. 24.

Para Tanenbaum (2003) complementa que WLAN ou LAN sem fio são sistemas usados em computadores que tem um modem de radio e uma antena e que podem se comunicar. Para isso existe uma antena que chega a 18 metros e permite a comunicação.

De acordo Kurose e Ross (2006, p. 423) argumentam que,

> Presentes no local de trabalho, em casa, em instituições educacionais, em cafés, aeroportos e esquinas as LANs sem fio agora são uma das mais importantes tecnologias de rede de acesso a internet de hoje. Embora muitas tecnologias e padrões de LANs sem fio tenham sido desenvolvido na década de 1990, uma classe particular de padrões surgiu claramente como vencedora: a LAN sem fio IEEE 802.11.

Até pouco tempo atrás, este tipo de LAN era pouco usada, devido a fatores como exigência de licença para uso de radiofreqüência, baixa capacidade, preocupações com segurança, altos preços e baixa taxa de transmissão de dados. Uma vez que estes empecilhos têm sido amenizados, a popularidade deste tipo de rede local vem crescendo. (ANGELO; BARBOSA, 2003).

2.3.2 WPAN

As Redes WPAN estão associadas ao *Bluetooth.*

Segundo Ângelo e Barbosa (2003), o surgimento de outros padrões de redes sem fio, como o Bluetooth foi criada na década de 1990.

> Algumas empresas se uniram para projetar uma rede sem fio de alcance limitado chamada Bluetooth, a fim de conectar esses componentes sem a utilização de fios. A rede Bluetooth também permite a conexão de câmeras digitais, fones de ouvido, scanners e outros dispositivos a um computador, simplesmente trazendo-os para dentro do alcance da rede. Nada de cabos, nada de instalação de drives; basta juntá-los, ligá-los e eles funcionarão. Para muitas pessoas, essa facilidade de operação uma grande vantagem. (TANENBAUM, 2003, p. 33)

As redes pessoais sem fio WPAN são voltadas, principalmente, para a conexão de um computador a dispositivos periféricos, como impressoras, PDAs e telefones celulares, eliminando a necessidade de cabos, cobrindo pequenas distâncias oferecendo baixas velocidades. (MAIA, 2003).

"A transmissão de dados é feita através de radiofreqüência, permitindo que um dispositivo detecte o outro independente de suas posições, desde que estejam dentro do limite de proximidade". (ALECRIM, 2008).

Conforme Tanenbaum (2003), a unidade do sistema é normalmente o mestre, comunicando-se com o mouse, o teclado etc., que atuam como escravos. O mestre informa aos escravos que endereços usar, quando eles podem transmitir, por quanto tempo podem transmitir que freqüências podem usar e assim por diante. Como mostra a figura 4.

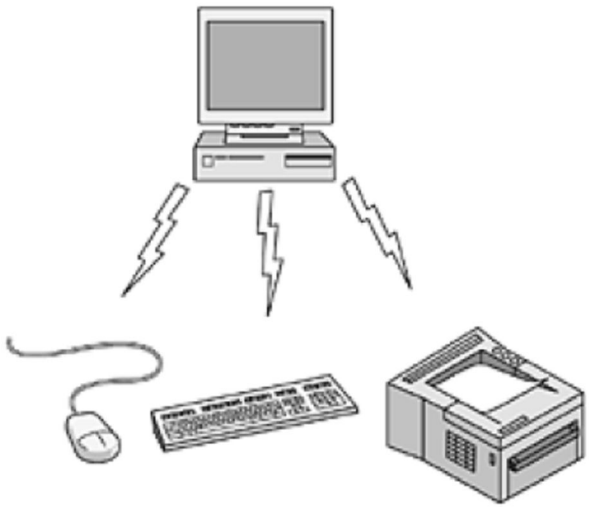

Figura 4 – Configuração da Bluetooth

Fonte: TANENBAUM, 2003, p. 34.

Para Ângelo e Barbosa (2003), o alcance médio dos dispositivos Bluetooth está em torno dos 10 metros e a taxa de dados, 1 Mbps. A principal característica é a facilidade de comunicação quando colocados dois dispositivos um alcance do outro. Se o usuário desejar, pode-se montar uma pequena rede doméstica usando Bluetooth. Há inclusive adaptadores USB/Bluetooth à venda no mercado.

A tabela 2 mostra para que seja possível atender aos mais variados tipos de dispositivos, o alcance máximo do Bluetooth foi dividido em três classes.

Tabela 2 – Potência e alcance das classes

Classes	**Potencia Máxima (mW)**	**Área cobertura (metro)**
Classe 1	100	100
Classe 2	2,5	10
Classe 3	01	01

Fonte: ALECRIM, 2008.

2.3.3 WMAN

As redes metropolitanas sem fio WMAN oferecem uma cobertura geográfica maior que as WLANs e altas taxas de transmissão (MAIA, 2003).

Segundo Shammas (2010), as redes WMAN permitem a comunicação em diferentes locais em uma área metropolitana, como: em edifícios, escritórios e cidade. Sem os custos elevados de instalar cabos e fibras ópticas.

Segundo Ono (2004 apud Alves, 2009, p. 24), o seu funcionamento sucede de forma idêntica aos sistemas de redes celulares, onde existem estruturas (como as TV's via satélite) localizadas próximas aos clientes que recebem o sinal, transmitidas pelas estações base e depois disso fazem um roteamento através de uma conexão Ethernet padrão diretamente ligadas aos clientes.

Uma das tecnologias usadas para esse tipo de rede é a WiMAX cuja o objetivo é promover compatibilidade e inter-operabilidade entre equipamentos baseados no padrão IEEE. 802.16. Usa as freqüências de freqüências de 2 GHz a 11 GHz para criação das redes metropolitanas com velocidade de até 75 Mbps. (Shammas, 2010).

2.3.4 WWAN

Para Maia (2003), as WWAN são uma tecnologia voltada para aplicações móveis como telefones celulares e alguns serviços de dados. São redes com grande dispersão geográfica. Com o crescimento de banda larga são transmitidos e-mail, textos, imagens e sons via celular, com a mesma velocidade e qualidade dos dispositivos ligados por fios.

Segundo Shammas (2010), a velocidade de transmissão é bastante limitada quando comparadas ao WiMAX.

2.4 Modos de operação

Segundo Alves (2009), as redes móveis sem fio são sistemas de comunicação onde as estações, que são moveis, se comunicam por meio de enlaces de radio. Esse tipo de rede pode ser classificadas em dois tipos: as redes infra-estruturadas, e as redes ad hoc.

2.4.1 Ad-Hoc

Para Alves (2009), as redes ad hoc, ou IBSS, são compostas por estações independentes, sendo criadas de maneira espontânea por estes dispositivos. Este tipo de rede se caracteriza pela topologia altamente variável, existência por um período de tempo determinado e baixa abrangência.

De acordo com Rufino (2005), a rede ad-hoc funciona a partir de um ponto central da conexão. Os equipamentos se conectam-se diretamente uns aos outros. As antigas redes feitas com cabo coaxial, onde um único cabo interligava vários equipamentos, assim permitia a comunicação de um ponto com qualquer outro ponto da rede. Mas a analogia não é perfeita, pois quando ocorria um rompimento ou mau contato, a comunicação da rede inteira era prejudicada. Diferente do modo Ad-Hoc, onde apenas o equipamento com problema deixa de se comunicar com o restante. A Figura 5 ilustra essa topologia

Figura 5 – Topologia de rede no modelo Ad-Hoc

Fonte: RUFINO, p. 9.

Junior e Duarte (2003, p. 2) afirmam que,

> Nas redes ad hoc, os nós são responsáveis por desempenhar as funções que antes eram desempenhadas pelo ponto de acesso, logo, cada nó da rede se torna um roteador, e é responsável por reencaminhar as mensagens de outros nós que desejem se comunicar com um nó que esteja fora da sua área de alcance. Como os nós podem se mover aleatoriamente, alterando dinamicamente a topologia da rede, os protocolos de roteamento utilizados nas redes ad hoc devem ser adaptativos e capazes de encontrar rotas nesse cenário de alta mudança de conectividade.

Para Tanenbaum (2003), nas redes Ad-Hoc os computadores se comunicam diretamente uns aos outros. Um exemplo típico é de duas ou mais pessoas juntas em uma sala não equipada com uma LAN sem fio, fazendo seus computadores se comunicarem diretamente.

Flickenger et al (2005) consideram que, no modo Ad-Hoc não existe um único nó máster ou ponto de acesso, e sim uma rede multiponto-para-multiponto, onde cada cartão se comunica diretamente com os vizinhos. Os nós devem estar ao alcance para que se comuniquem e devem estar de acordo quanto ao nome da rede e o canal utilizado.

2.4.2 Infra estrutura

De acordo com Rufino (2005), o equipamento central de uma rede que utiliza a topologia de infra-estrutura é o concentrador. O concentrador é rodeado de vários clientes,

assim todas as configurações de seguranças fiquem concentradas no concentrador. Os itens de (autorização, autenticação, controle de banda, filtros de pacote, criptografa etc.) são controlados em um único ponto. A vantagem é facilitar a interligação de redes cabeadas com a internet, já que o concentrador desempenha o papel de ponto ou gateway.

A figura 6 abaixo ilustra o modelo de infra-estrutura.

Figura 6 – Topologia de rede no modelo infra-estrutura

Fonte: RUFINO, p. 9.

Junior e Duarte (2003) concordam que, a característica das redes infra-estruturadas é a presença de um terminal centralizador, chamado de ponto de acesso. O ponto de acesso é o responsável por centralizar certas funções da rede, como o roteamento e o controle de acesso ao meio.

Flickenger et al. (2006) afirmam que,

> Modo master (também chamado de AP ou modo de infra-estrutura) é usado para criar um serviço que se parece com um ponto de acesso tradicional. O cartão wireless cria uma rede com um nome específico (chamado SSID) e canal, oferecendo serviços de rede nele. No modo master, os cartões wireless gerenciam toda a comunicação relativa à rede (autenticando clientes wireless, tratando da contenção do canal, repetindo pacotes, etc). Cartões wireless em mod o master podem apenas comunicar-se com cartões associados a ele em modo gerenciado.

2.5 Padrões

Para Tanenbaum (2003), o IEEE é a maior organização profissional do mundo. Publicam uma série de jornais e promovem várias conferências a cada ano. Um grupo de padronização afim de desenvolver padrões nas áreas de informática e engenharia elétrica.

> O Institute of Electrical and Electronics Engineers (IEEE) formou um grupo de trabalho com o objetivo de definir padrões de uso em redes sem fio. Um desses grupos de trabalho foi denominado 802.11, que reúne uma série de especificações que basicamente definem como deve ser a comunicação entre um dispositivo cliente e um concentrador ou a comunicação entre dois dispositivos clientes. (RUFINO, 2005, p. 25)

O IEEE 802.11 é o primeiro padrão firmado para redes sem fio e reconhecida pela IEEE, provê no máxima uma taxa de transmissão de 2Mbps. (Cozer, 2006).

2.5.1 Padrão 802.11a

Segundo Duarte (2003 apud Alves, 2009, p. 27), O padrão 802.11a surgiu em 1999, contudo não é muito utilizado atualmente por não ter muitos dispositivos que opera nessa faixa de freqüência.

De acordo com Tanenbaum (2003), a LAN 802.11a foi a primeira das LANs sem fio de alta velocidade e utiliza OFDM.

O padrão 802.11 tem na sua segundo versão o padrão 802.11a, onde são disponibilizados oito canais por ponto de acesso o que possibilita maiores taxas de transmissão de até 54mbps, suporta até 64 clientes conectados simultaneamente. Permite um número maior de conexões em relação ao 802.11b, utiliza o protocolo de segurança WEP de até 256bits. (COZER, 2006).

Para Rufino (2005), o padrão 802.11a tem como principal característica o aumento de velocidade para um máximo de 54 Mbps (108 Mbps em modo turbo), porém podendo operar em velocidades mais baixas. A diferença é a operação na faixa de 5 GHz, numa faixa com poucos concorrente, mas com menor área de alcance.

> O principal problema relacionado à expansão deste padrão tem sido a inexistência de compatibilidade com a base instalada atual (802.11b), já que esta utiliza faixas de freqüência diferentes. A despeito disso, vários fabricantes têm investido em equipamentos neste padrão, e procedimento similar começa a ser usado em redes novas, onde não é necessário fazer atualizações nem há rede sem fios preexistentes. (RUFINO, 2005, p. 27)

2.5.2 Padrão 802.11b

Segundo Rufino (2005), o padrão 802.11 foi ratificado em 1999. Sendo ainda hoje o mais popular e com maior base instalada, com mais produtos e ferramentas de administração mesmo tendo limitações em termos de utilizações de canais

A tabela 3 abaixo descreve as limitações do padrão 802.11b com relação à utilização dos canais e as respectivas freqüências.

Tabela 3 – Associação Entre Canal e Respectiva Freqüência

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	2,457
11	2,462
12	2,467
13	2,472
14	2,484

Fonte: ALVES, 2009 p.29

Para Rufino (2005) e Tanenbaum (2003), a velocidade de operação do 802.11b É quase sempre igual a 11 Mbps. Mas podem operar a velocidades mais baixas.

O 802.11b opera na freqüência de 2,4 GHz e usa somente o patrão DSSS. Permite um número máximo de 32 clientes conectados. (Rufino, 2005).

Tanenbaum (2003, p.233), “Embora o 802.11b seja mais lento que o 802.11a, seu alcance é cerca de 7 vezes maior, o que é mais importante em muitas situações”.

2.5.3 Padrão 802.11d

Segundo Filho (2005 apud Sguarezi, 2007, p. 35), padrão desenvolvido para áreas fora dos cinco países regulatórios (EUA, Canadá, Europa, Japão e Austrália), o 802.11d tem um quadro estendido que inclui campos com informações, parâmetros de freqüências e tabelas com parâmetros de cada pais, o que permite a habilitação do hardware de 802.11 operar em vários países onde ele, por problemas de compatibilidade, não poderia operar. Por exemplo, o 802.11a não opera na Europa.

2.5.4 Padrão 802.11e

Segundo Mello (2006, p.14),

> O 802.11e agrega qualidade de serviço (QoS) às redes IEEE 802.11. Em suma, 802.11 permite a transmissão de diferentes classes de tráfego, além de trazer o recurso de Transmission Oportunity (TXOP), que permite a transmissão em rajadas, otimizando a utilização da rede.

2.5.5 Padrão 802.11f

Para Fagundes (2006), o padrão 802.11f são recomendações praticas que descrevem os serviços dos access points, os protocolos, as primitivas e os conjuntos de funções devem ser compartilhados pelos múltiplos fornecedores para operarem em rede.

2.5.6 Padrão 802.11g

Segundo Tanenbaum (2003), em novembro de 2001 o 802.11g foi aprovada como uma versão aperfeiçoada do 802.11b, depois de muitas disputas sobre qual tecnologia seria usada.

Cozer (2006) complementa que, o padrão 802.11g trabalha na freqüência de 2,4GHz e taxas de transmissão de até 54 Mbps.

O 802.11g utiliza a técnica OFDM para transmissão de dados. A técnica DSSS é utilizada quando se faz a comunicação com qualquer dispositivo do 802.11b. (ALECRIM, 2008).

2.5.7 Padrão 802.11h

Segundo Mello (2006, p.15),

> O patrão 802.11h é a atualização 802.11a (Wi-Fi) que vai ao encontro com algumas regulamentações para a utilização de banda de 5 GHz na Europa. O padrão 11h conta com dois mecanismos que otimizam a transmissão via rádio: a tecnologia TPC permite que o rádio ajuste a potência do sinal de acordo com a distância do receptor; e a tecnologia DFS, que permite a escolha automática de canal, minimizando a interferência em outros sistemas operando na mesma banda.

2.5.8 Padrão 802.11i

Para Rufino (2005), o padrão 802.11i foi homologado em junho de 2004, os mecanismos de autenticação e privacidade podem ser implementados em vários aspectos e protocolos existentes.

Segundo o mesmo autor, o RSN é o principal protocolo deste padrão, que permite meios de comunicação mais seguros. O protocolo WPA também esta inserido nesse protocolo definido para resolver problemas de seguranças mais robustas, em relação padrão WEP, além do WPA2, que tem por principal característica o uso do algoritmo criptográfico AES.

2.5.9 Padrão 802.11k

Segundo Sguarezi (2007), este padrão padroniza diversos tipos de informação sobre características e troca de mensagens do radio 802.11. Os principais objetivos da extensão 802.11k são:

- Permitir que as estações realizem mediações de parâmetros específicos do radio 802.11
- Padronizar mensagens de requisição e de relatório com resultado das mediações.
- Disponibilizar o acesso a estas informações para as camadas superior da pilha de protocolos.

2.5.10 Padrão 802.11n

Moreira e Malheiros (2006) dizem que, o padrão 802.11n tem pouca diferença dos padrões atuais, uma modificação chamada MIMOOFDM (Multiple Input, Multiple OutOFDM) que traz maior eficiência na propagação do sinal e ampla compatibilidade reversa com demais protocolos.

Já Moreira e Malheiros (2006, p.6) dizem que, "as redes 802.11n operam na faixa de 2,4 GHz e 5 GHz, podendo trabalhar com canais de 40 MHz e, também, manter compatibilidade com os 20 MHz atuais, mas neste caso as velocidades máximas oscilam em torno de 60 Mbps".

2.5.11 Padrão 802.11r

Sguarezi (2007 apud Grunewald, 2005, p. 39), padroniza o hand-off (troca de sinais) rápido permitindo um cliente com rede sem fio se re-associar quando houver a locomoção de um PA para outro na rede.

2.5.12 Padrão 802.11s

De acordo com Sguarezi (2007), o padrão 802.1s foi criada pela empresa Intel, permitindo que os pontos de acesso comuniquem entre si, num sistema de auto-configuração, onde a principal funcionalidade é fazer a cobertura em grandes áreas com grandes usuários utilizando a tecnologia de forma simultânea.

2.5.13 Padrão 802.11x

> Mesmo não sendo projetado para redes sem fio (até por ter sido definido anteriormente a esses padrões), o 802.1x possui características que são complementares a essas redes, pois permite autenticação baseada em métodos já consolidados, como o RADIUS (Remote Authentication Dial-in User Service), de forma escalável e expansível. Desta maneira é possível promover um único padrão de autenticação, independentemente da tecnologia (vários padrões de redes sem fio, usuários de redes cabeadas e discadas etc.), e manter a base de usuários em um repositório único, quer seja em banco de dados convencional, LDAP ou qualquer outro reconhecido pelo servidor de autenticação. (RUFINO, 2005, p. 28)

2.5.14 Padrão 802.11 Multimídia

Segundo Sguarezi (2007), esse padrão tem como objetivo aplicações residenciais e de entretenimentos, pois fornece a transmissão rica, de vídeos, áudios e etc. Este padrão também tem por destaque antecipar alguns recursos e avanços de outro protocolo.

2.5.15 Padrão 802.16

Para Tanenbaum (2003), o padrão 802.16 foi publicado em abril de 2002, depois que o comitê do IEEE definiu um padrão de LMDS. O IEEE chama o padrão 802.16 de MAN sem fio.

Segundo Silva et al. (2005 apud Alves, 2009, p.33) dizem que, primeira especificação aprovada em 2002 trabalha na faixa de freqüência que varia entre 10 Ghz a 66 Ghz e atingir um alcance de 50 km. A taxa de transmissão pode chegar até 134,4 Mbps em bandas licenciadas e até 75 Mbps em bandas não licenciadas. A transmissão entre as torres de transmissão é unidireccional, ou seja, tem de existir uma linha de vista entre os torres para que se venha ter a transmissão. Porém, mais tarde surgiu a nova especificação do padrão, a 802.16a que foi ratificado em 2003, que opera na freqüência que varia de 2 Ghz a 10 Ghz, podendo atingir a mesma distância atingida pela primeira especificação, alcançado uma velocidade de 10 Mbps a 70 Mbps. Ao contrário da primeira especificação, a 802.16a não necessita de uma linha de vista entre as torres de transmissão.

2.5.16 Padrão 802.20

Segundo Sguarezi (2007), o padrão 802.20 foi estabelecido em fevereiro de 2003 antes do lançamento do padrão 802.16 foi apelidado de Mobile-Fi. As taxas de transmissão são de 1mbps podendo chegar a 4mbps em espectros licenciados abaixo de 3,5 GHZ em distancias de 15 km aproximadamente.

2.6 Comparação entre os principais padrões sem fio

A tabela 4 faz uma comparação entre os principais padrões das redes sem fio, descrevendo a velocidade nominal de conexão, taxa real de conexão e a freqüência dos principais padrões wireless.

Tabela 4 – Comparação entre padrões de redes sem fio

Padrão wireless da IEEE	Velocidade nominal de conexão	Taxa real de conexão	Freqüência
802.11a	11Mbps	5Mbps	5GHZ
802.11b	54Mbps	25Mbps	2.4GHZ
802.11g	54Mbps	25Mbps	2.4GHZ
802.11n	300+Mbps	58Mbps[8]	2.4GHZ ou 5GHZ

Fonte: MOREIRA E MALHEIROS, 2006, p. 6.

2.7 Segurança em redes sem fio

Segundo Tanenbaum (2003), a maior parte dos problemas de segurança e causada intencionalmente por pessoas maliciosas que tentam obter algum beneficio, chamar a atenção ou prejudicar alguém. Como mostra a Tabela 5.

Tabela 5 – Algumas pessoas que podem causar problemas de segurança

Adversário	**Objetivo**
Estudante	Divertir-se bisbilhotando as mensagens de correio eletrônico de outras pessoas
Cracker	Testar o sistema de segurança de alguém; roubar dados
Representante de vendas	Tentar representar toda a Europa e não apenas Andorra
Executivo	Descobrir a estratégia de marketing do concorrente
Ex-funcionário	Vingar-se por ter sido demitido
Contador	Desviar dinheiro de uma empresa
Corretor de valores	Negar uma promessa feita a um cliente através de uma mensagem de correio eletrônico
Vigarista	Roubar números de cartão de crédito e vendê-los
Espião	Descobrir segredos militares ou industriais de um inimigo
Terrorista	Roubar segredos de armas bacteriológicas

Fonte: TANENBAUM, 2003, p.543

Para o mesmo autor, os problemas de segurança das redes podem ser divididos nas seguintes áreas interligadas: sigilo, autenticação, não repudia e controle de integridade.

Segundo BRASIL (2000 apud Bezerra, 2004, p. 15), esses protocolos visam atender os seguintes requisitos de segurança:

- Sigilo: os dados são mantidos secretos e somente as partes autorizadas podem visualizar seu conteúdo;

- Integridade: a informação deve permanecer inalterada durante a sua transferência;
- Autenticação: a identidade das entidades deve ser legítima e confirmada;
- Não-repúdio: o emissor da mensagem não poderá negar posteriormente a autoria da mesma.

2.7.1 Mecanismo de Segurança

Para Silva e Souza (2002), como as redes locais sem fio estão se tornando cada vez mais utilizadas nos ambientes corporativos, os requisitos de segurança são importantes, em vista que acessos indevidos a redes, leitura e alteração de dados podem ser invadidos se tornando uma ameaça.

Segundo Alves (2009, p. 35), "para se obter um nível de segurança desejado, é necessário implementar medidas como, criptografia, configuração apropriada, autenticação forte e monitorização das redes sem fio".

2.7.2 Endereçamento MAC

Segundo Rufino (2005), O IEEE controla e identifica o número único de identificação de cada dispositivo de rede utilizado tanto para redes ethernet como para redes sem fio, permitindo assim, identificar de forma inequívoca um equipamento em relação a outro fabricado, mesmo que seja ele de fabricantes diferentes. Porém em certo modelos de placas antigas, esse número pode ter o mesmo número, precisando assim de programa fornecido pelo fabricante da placa para trocar o endereço MAC único.

> Pensando em que cada placa tem um único endereço, uma das maneiras disponíveis para aumentar a segurança de uma rede é o cadastramento desse endereço MAC no concentrador, restringindo assim o acesso a somente quem estiver cadastrado ali, essa técnica visa somente autorizar o equipamento e não o usuário. (MARTINS, 2005, p.23).

O mesmo autor complementa que, um método para melhor a segurança utilizando o endereço MAC é substituir a entrega de endereços IP via DHPC por IP, assim trabalhando em conjunto dificultaria um possível ataque.

Segundo Rufino (2005 apud Alves, 2009, p.36), este mecanismo de autenticação possui as seguintes desvantagens:

- Esse mecanismo exigirá manutenção, que será maior ou menor de acordo com os utilizadores que entra e sai do cadastro. Essa manutenção é feita manualmente, onde endereços físicos são obtido e cadastrados manualmente no ponto de acesso;
- Como esse mecanismo pode utilizar a técnica em que o utilizador é quem configura o endereço MAC do ponto de acesso, o atacante com um endereço físico válido pode renomear o endereço físico da sua placa e obter o acesso à rede.

2.7.3 Criptografia

Segundo Alves (2009), com o crescimento da comunicação sem fio abriu um buraco na segurança da transmissão dos dados, pois é feito pelo ar e os dados podem ser facilmente conseguidos. Foi necessário o desenvolvimento das técnicas de criptografia.

Para Alecrim (2005), o termo criptografia surgiu da fusão das palavras gregas "kryptós" e "gráphein", que significam "oculto" e "escrever", respectivamente.

> Criptografia é a ciência de proteger dados para que ninguém que não seja autorizado os leia. Além de criptografar os dados, as técnicas de criptografia também são usadas para garantir que os dados transmitidos não sejam modificados até chegar ao seu destino e verificar se os dados recebidos foram realmente enviados pelo emissor. Existem dois tipos de criptografia utilizados: criptografia de chave pública (criptografia assimétrica) e de chave privada (criptografia simétrica). Basicamente, esses dois processos seguem o modelo da figura abaixo, onde uma mensagem é criptografada usando uma chave e decriptografada usando outra chave (a mesma chave no caso da criptografia simétrica, e uma chave diferente no caso da criptografia assimétrica), de modo a se obter a mensagem original. (EIRAS, 2010)

A figura 7 abaixo, mostra a criptografia.

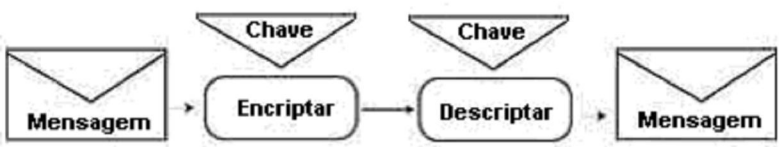

Figura 7 – Criptografia

Fonte: EIRAS, 2010.

2.7.4 WEP

Para Ozório (2007), O IEEE foi o responsável pelo desenvolvimento do padrão WEP, cujo objetivo é proporcionar a proteção para redes sem fio que cumpram o padrão 802.11.

De acordo com Rufino (2005 apud Alves, 2009, p.36), “WEP é um protocolo que utiliza algoritmos simétricos, portanto existe uma chave secreta que deve ser compartilhada entre as estações de trabalho e o concentrador, para cifrar e decifrar as mensagens tracejadas.”

O WEP tem como base um processo criptográfico chamado RC4. Ele emprega uma chave secreta de 40 ou 104 bits que pode ser compartilhada entre os clientes e o Access point da rede. Para transmitir o pacote IV (vetor de iniciação) de 24 bits é escolhido randomicamente e anexado a chave WEP para assim formar a chave de 64 ou 128 bits. (COZER, 2006).

A figura 8, apresenta a arquitetura do protocolo WEP.

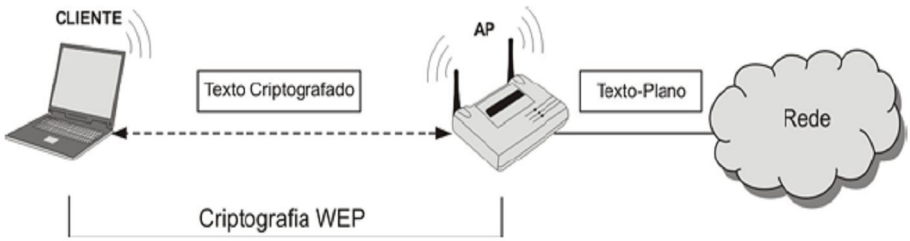

Figura 8 – WEP
Fonte: LINHARES E GONÇALVES, 2006, p.3.

Segundo Ozório (2007), o WEP se propôs a atender as seguintes necessidades: autenticação, confiabilidade e integridade.

2.7.4.1 Autenticação

Para Farias (2006), o padrão IEEE 802.11 é responsável dois métodos de autenticação: autenticação de chave compartilhada e autenticação de sistema. O mais simples e mais seguro dos dois é a autenticação de sistema aberto. O cliente que quiser se tornar autenticado deve caminhar por uma série de passos durante esse processo, esses passos variam de um método para o outro.

Segundo o mesmo autor, o método padrão usado para equipamento *wireless* é a autenticação de sistema aberto. Usando este método uma estação pode se associar com qualquer AP que também use o método. Este método de autenticação é baseado no SSID, ou seja, basta que a estação e o AP tenham o mesmo SSID para que a autenticação ocorra. Esse processo de autenticação de sistema aberto é usado de forma eficaz tanto em ambientes seguros quanto não seguros.

Na figura 9, mostra o processo: o cliente faz um pedido para se associar ao AP e O AP toma conhecimento desse pedido, envia uma resposta positiva e autentica o cliente.

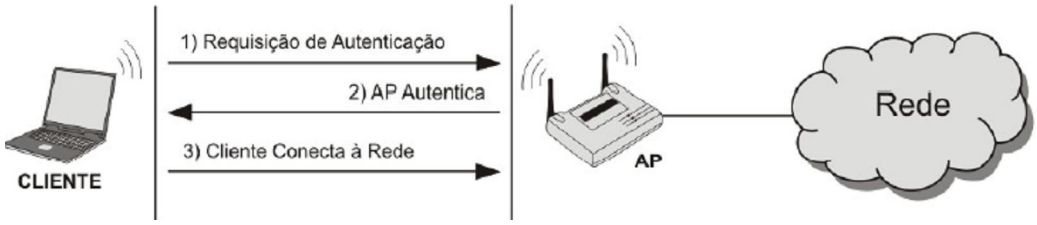

Figura 9 – Processo de autenticação de sistema aberto

Fonte: LINHARES E GONÇALVES, 2006, p.4.

> Existe ainda a opção de se usar WEP (não é obrigatório) para criptografar o processo. Porém a criptografia não é feita durante o processo de autenticação em si, ou seja, a chave WEP não é verificada por ambos os lados durante a autenticação, mas para criptografar os dados depois que o cliente já estiver autenticado e associado. (FARIAS, 2006)

Para Farias (2006), há duas razões principais para o uso de autenticação em diversos cenários:

- É considerado o mais seguro dos dois métodos disponíveis.
- Já é usado por padrão nos dispositivo *wireless*, o que não requer configuração adicional.

Segundo o mesmo autor, o cliente faz uma requisição de autenticação para o AP. O AP envia uma pergunta ao cliente. Essa pergunta é um texto gerado aleatoriamente e enviado ao cliente na forma de texto puro. O cliente responde a essa pergunta. A chave WEP do cliente é usada para criptografar a pergunta e por fim a mesma é enviada já codificada de volta ao AP. O AP responde a resposta do cliente. A resposta codificada enviada pelo cliente é então decodificada usando a chave WEP do AP, verificando assim

se o cliente tem a mesma chave. Se a chave do cliente é a correta, o AP responderá positivamente e autenticará o cliente. Se a chave do cliente não for a correta, o AP responderá negativamente e não autenticará o cliente. Como mostra a Figura 10:

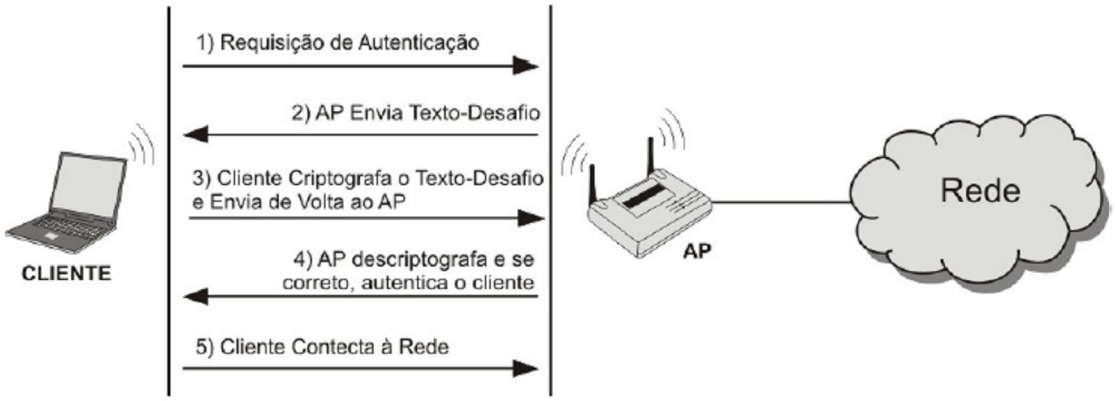

Figura 10 – Processo de autenticação de sistema aberto 2

Fonte: LINHARES E GONÇALVES, 2006, p.4.

Diferentemente do que possa parecer, o processo de autenticação de chave compartilhada não é mais seguro que o processo de autenticação de sistema aberto. O processo de chave compartilhada abre uma porta para crackers.

2.7.4.2 Confidencialidade

Segundo Alves (2009 apud Rufino, 2005), a confidencialidade é a proteção de informação contra acesso de pessoas não autorizada. Ela e opcional, mas quando está ativada, cada estação tem uma chave secreta que é compartilhada com o ponto de acesso. O protocolo não define uma forma padrão de como essas chaves devem ser distribuída, sendo assim ela é feita manualmente em cada estação.

O protocolo WEP utiliza o algoritmo de criptografia RC4 (Route Coloniale 4) para garantir a confidencialidade. O RC4 foi projetado por Ronald Rivest em 1987 e foi publicado em 1994, e é um algoritmo amplamente utilizado em aplicações comerciais, especialmente em transações na Internet que utilizam SSL. (Tanenbaum, 2003).

Segundo Tanenbaum (2003), o RC4 usa um vetor de inicialização (IV), 24 bits e uma chave secreta compartilhada de 40 ou 104 bits. Devido ao fato da chave secreta

compartilhada ser susceptível a ataque de dicionário por força bruta, o IV e concatenado com a chave secreta para forma chave de 64 bits ou 128 bits. Esta serve de entrada para um gerador de números pseudo-aleatórios PRNG, que através de uma operação XOR produz um texto cifrado.

O mesmo autor complementa que, entretanto o IV, ou seja, os 24 bits e enviado em claro, pelo fato de que a mesma chave é usada para codificar e descodificar os dados. Como mostra a Figura 11:

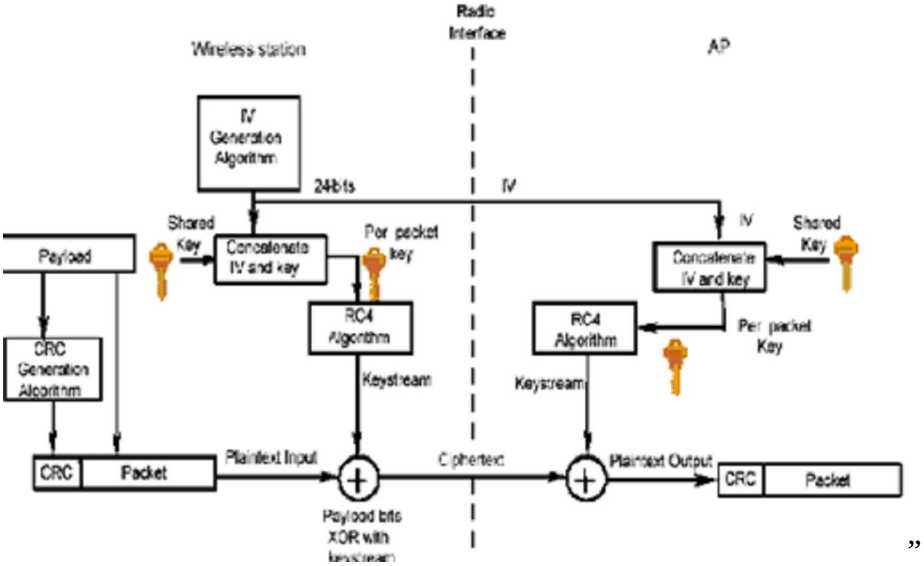

Figura 11 – Confidencialidade do protocolo WEP

Fonte: ALVES, 2009.

2.7.4.3 Integridade

Segundo Alves (2009, apud Santos, 2003), para garantir a integridade o protocolo WEP utiliza CRC-32 para detecção de erros e calcular o checksum5 da mensagem a serem transmitidos, e gera um resultado ICV para cada frame enviado. Ao receber a mensagem o utilizador executa a mesma função CRC-32 e compara o ICV obtido com o ICV enviado, com o objetivo de verificar se a mensagem foi corrompida ou alterada no meio do caminho. Como mostra a Figura 12:

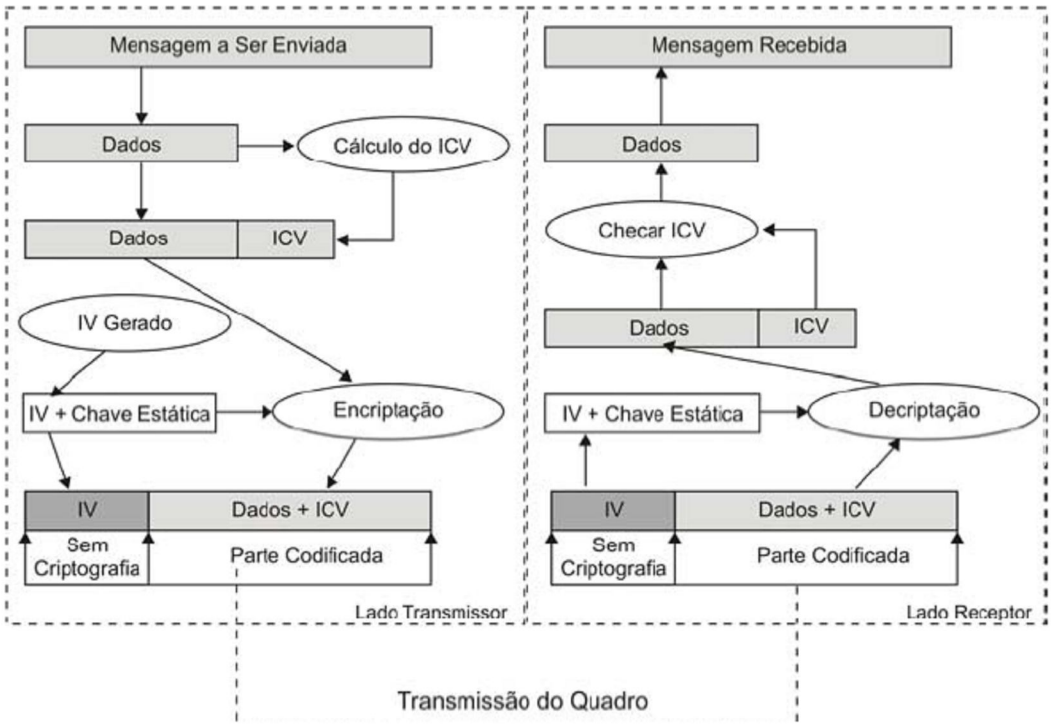

Figura 12 – Integridade do protocolo WEP

Fonte: LINHARES E GONÇALVES, 2006, p.5.

2.7.5 WPA

De acordo com Ozorio (2007), o WPA apresenta um melhor tratamento de segurança WEP, pois é compatível com o hardware que roda o WEP. Chamado de TKIP foi desenvolvido com esforço junto aos membros do IEEE e membros da Wi-Fi, a fim de aumentar o nível de segurança das redes sem fio e para corrigir alguns erros do WEP. A atualização do WEP para WPA é feita através de atualizações do firmware dos mesmos dispositivos Wi-Fi.

Para Rufino (2005, apud Alves, 2009), este protocolo ”atua em duas áreas distintas: o primeiro, que visa substituir completamente o WEP, e a segunda, foca a autenticação do usuário utiliza, por isso, padrões 802.1x e EAP (Extensible Authentication Protocol).”

2.7.5.1 Autenticação

Segundo Rufino (2005, apud Alves, 2009, p.42), o protocolo WPA define dois métodos de autenticação. Um denominado de Pre Shared Key, que é direcionado para redes pequenas ou redes de uso domésticos, e o outro denominado de Interprise, que é

direcionado para redes corporativas, e utiliza um servidor de autenticação, portanto uma infra-estrutura complementar, podendo ainda necessitar de uma infra-estrutura de chaves públicas (ICP), caso se utilize certificados digitais para autenticar os utilizadores.

De acordo com Brian (2003 apud Junior, Brabo e Amoras, 2004, p.57), no WPA, é necessária a autenticação 802.1x. No padrão 802.11, essa autenticação era opcional. Para ambientes sem uma infra-estrutura RADIUS (Remote Authentication Dial-In User Service), WPA suporta o uso de uma chave pré-compartilhada. Para ambientes com uma infra-estrutura, EAP (Extensible Authentication Protocol) e RADIUS são suportados.

Segundo Alves (2009), o padrão de autenticação 802.1x é usado entre ponto de acesso e servidor de autenticação. Um cliente envia credenciais ao ponto de acesso solicitando a autenticação, que por sua vez os encaminha ao servidor de autenticação (que na maioria das vezes é um servidor RADIUS). O servidor de autenticação verifica as credenciais, em caso de validos envia um MSK (Master Segurança em Redes Sem Fio Session Key), ao ponto de acesso que o encaminha ao cliente. Como é ilustrado na figura 13 abaixo.

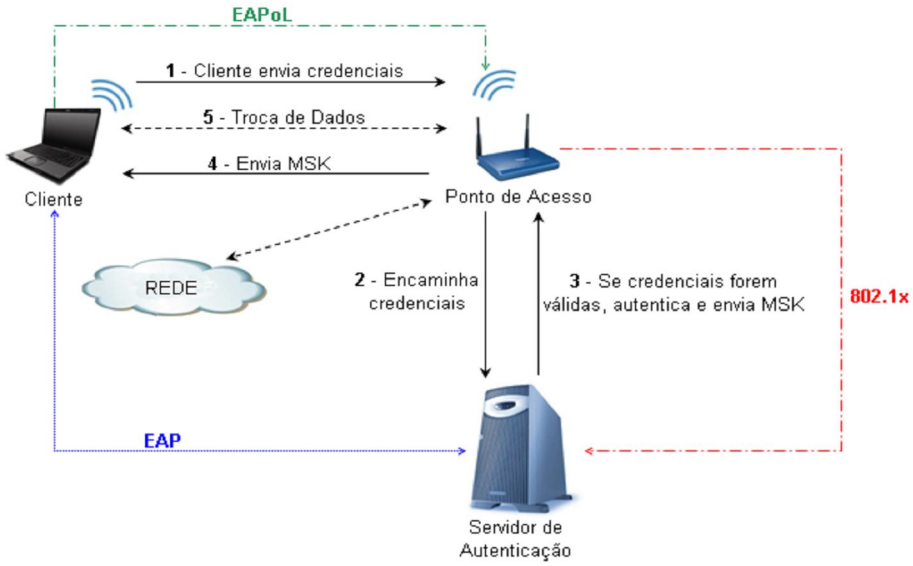

Figura 13 – Autenticação WPA Interprise (802.11x/EAP)
Fonte – Alves (2009)

De acordo com Sartorato et al. (2009), os certificados digitais, biometria, binômio usuário e senha são credenciais de autenticação e trafegam de modo seguro através de um canal lógico criado pelo EAP entre o cliente e o servidor de autenticação.

O mesmo autor complementa que o EAP muitas vezes não é um mecanismo especifico de autenticação, mas é usado em algumas funções que negociam com o mecanismo de autenticação definida pela RFC 3748, que pode ser usado para redes *wireless* quanto para conexões ponto-a-ponto. Atualmente existem quarenta tipos de EAP os mais usados sao: EAP-TLS (EAP-Transport Layer Security), EAP-TTLS (EAP-Tunneled Transport Layer Security) e PEAP (Protected Extensible Authentication Protocol).

2.7.5.2 Confidencialidade

Segundo Rufino (2005), o protocolo TKIP é uma das novidades do protocolo WPA, e resolve muitas vulnerabilidades apresentadas pelo protocolo WEP. O TKIP é responsável pela gerência das chaves temporais, ou seja, a chave é usada durante certo tempo e depois é substituída dinamicamente, visto que essa era uma das vulnerabilidades do protocolo WEP.

De acordo com Veríssimo, Rufino (2003; 2005 apud Alves, 2009, p.45), no TKIP, é utilizada uma chave base de 128 bits chamada de TK (Temporal Key). Esta chave é combinada ao endereço MAC do transmissor, denominado de TA (Transmitter Address), criando assim uma outra chave denominada de TTAK (Temporal and Transmitter Address Key). A TTAK é combinada com o IV do RC4 para criar chaves diferentes a cada pacote, por sessão ou por período, tornando assim difícil a captura das chaves.

2.7.5.3 Integridade

Para Bulhman e Cabianca (2006 apud Alves, 2009 p. 45 e 46), a integridade do protocolo WPA é fornecida pelo MIC que é implementado pelo algoritmo Michael. Michael é uma função diferente do RC4 utilizado pelo WEP, pois ele criptografa a chave para produzir a MIC de 8 bits, que juntamente com o ICV produz a integridade do protocolo WPA. Sendo assim a integridade do WPA é suporta pelo total de 12 bits, 8 bits gerado pelo Michael e 4 bits pelo CRC-32.

A figura 14 descreve a integridade do protocolo WAP:

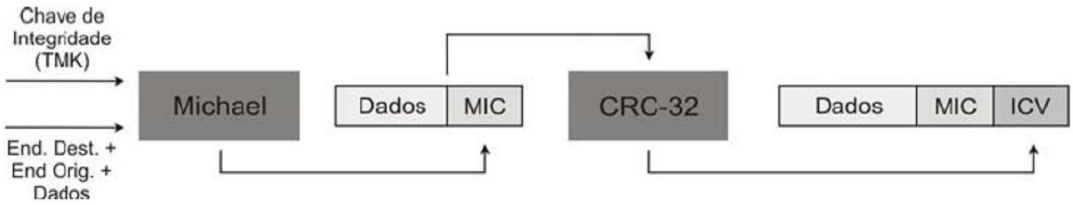

Figura 14 – Integridade do protocolo WAP
Fonte: LINHARES E GONÇALVES, 2006, p.11.

Uma das principais diferenças entre Michael e o CRC-32 é que o primeiro calcula o valor de integridade sobre o cabeçalho do frame também enquanto que o segundo só calcula o valor de integridade sobre a carga de dados e o Michael utiliza chaves para calcular o MIC. (Ozorio, 2007).

2.7.6 WPA2

Segundo Linhares e Gonçalves (2006), homologado em junho de 2004, o padrão 802.11i foi desenvolvido com o objetivo de prover mais segurança na comunicação, pois os protocolos de segurança então utilizado (WEP) apresentavam diversas vulnerabilidades. O WPA é baseado em rascunhos do WPA2 e parte dos mecanismos apresentados no WPA é utilizada no WPA2. Os principais avanços do WPA2 em relação ao WPA são os novos algoritmos de integridade e criptografia.

O WPA utiliza o RC4 e o WPA2 utiliza o AES em conjunto com o TKIP com chave de 256 bits, que é um método muito mais poderoso. (Ozório, 2007).

Segundo o mesmo autor, a AES é uma ferramenta poderosa de criptografia, pois permite a utilização de chaves de 128, 192 e 256 bits. A utilização de chave de 256 bits no WPA2 é padrão. Com a utilização do AES, introduziu-se também a necessidade de novo hardware, capaz de realizar o processamento criptográfico.

Segundo Berent (2005 apud Ozório, 2007, p.25) o AES é:

- Um cifrador: em blocos que criptografa blocos de 16 bits de cada vez, e repetindo várias vezes um conjunto definido de passos que trabalha com chave secreta que opera com um número fixo de bytes.
- Reversível: o procedimento utilizado para criptografar os dados, é utilizado para descriptografá-los.

- Trabalha: com operações de XOR entre os blocos e a chave, organiza o bloco em uma matriz e realiza trocas circulares em cada linha e promove uma mistura entre as colunas da matriz. Para controle de integridade e autenticação, o WPA2 trabalha como o WPA.

2.7.6.1 Autenticação

Segundo Linhares e Gonçalves (2006), o mecanismo de autenticação no WPA2 é, basicamente, o mesmo do WPA. O maior avanço na autenticação é uma preocupação com o roaming.

> Quando um usuário se autentica, há uma série de mensagens trocadas entre o AP e o cliente. Essa troca de mensagens introduz um atraso no processo de conexão. Quando um cliente desloca-se de um AP para outro, o atraso para estabelecer a associação pode causar uma interrupção notória da conexão, principalmente em tráfego de voz e vídeo. Para minimizar este atraso de associação, o equipamento pode dar suporte a PMK Caching e Preauthentication. O PMK Caching consiste no AP guardar os resultados das autenticações dos clientes. Se o cliente voltar a se associar com o AP, estas informações guardadas são utilizadas para diminuir o número de mensagens trocadas na re-autenticação. Já no Preauthentication, enquanto o cliente está conectado a um AP principal, ele faz associações com outros APs cujo o sinal chega até ele. Desta forma, quando há uma mudança de AP não há perda de tempo com a autenticação. (Linhares e Gonçalves, 2006).

2.7.6.2 Integridade

De acordo com Linhares e Gonçalves (2006), o responsável pela integridade e confidencia do WPA2 é o protocolo CCMP é o responsável pela integridade e a confidência do WPA. O CCMP é baseado no AES que é um Block Cipher. O modo de operação do AES implementado pelo WPA2 e o CCM cujas chaves e blocos são de 128 bits.

O CBC-MAC é responsável pela integridade dos quadros, seu funcionamento é mostrado na Figura 15.

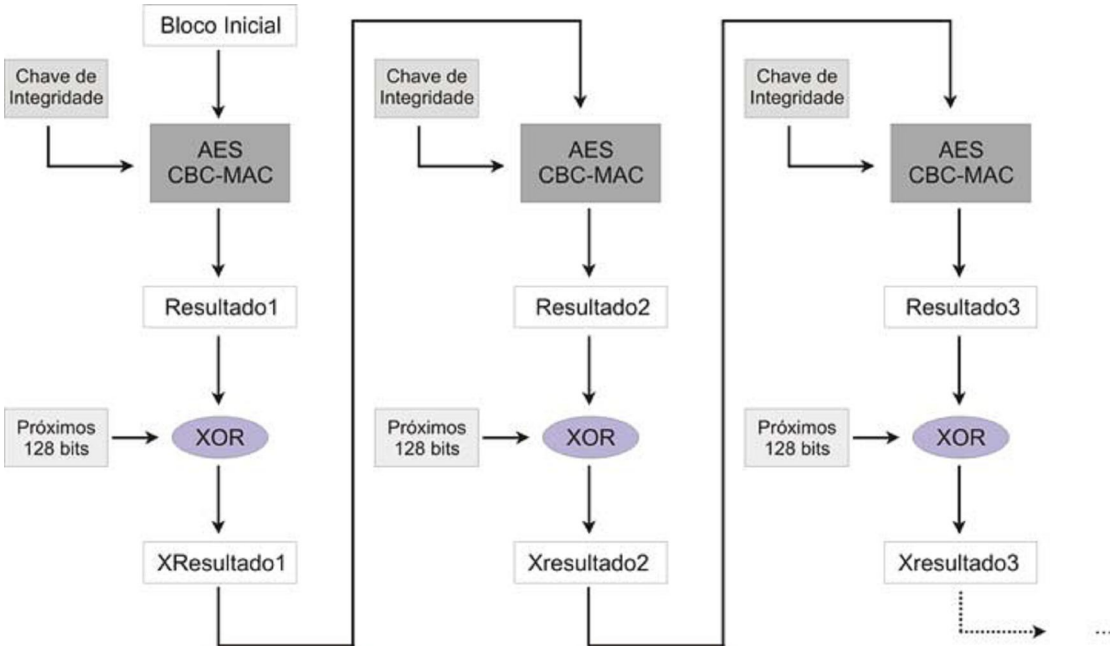

Figura 15 - Integridade WPA2

Fonte: LINHARES E GONÇALVES, 2006, p.14.

A caixa “Bloco Inicial” representa os primeiros 128 bits do campo de dados. São passados para o CBC-MAC o bloco e a chave de integridade, e como saída são gerados outros 128 bits, chamado de “Resultado1”. É feito um XOR entre o “Resultado1” e o próximo bloco. Ao resultado do XOR é dado o nome “XResultado1”. O “XResultado1” é passado para o CBC-MAC e, assim, gerado um “Resultado2”. Este procedimento se repete até o último bloco do campo de dados do pacote. No final do processo, dos 128 bits de saída apenas o 64 bits mais significativos vão para o MIC. (LINHARES E GONÇALVES, 2006).

2.7.7 WEP e WPA

A tabela 6 abaixo descreve a comparação entre os protocolos WEP e WPA.

Tabela 6- Comparação entre WEP e WPA

	WEP	**WPA**
"CIPHER"	RC4	RC4
TAMANHO DA CHAVE	40 BITS	128 BITS ENCRIPTAÇÃO 64 BITS AUTENTICAÇÃO
"KEY LIFE"	24 – BITS IV	48/128 BITS IV
PACOTE DE CHAVE	CONCATENADA	CONCATENADA MISTURANDO FUNÇÕES
INTEGRIDADE DOS DADOS	CRC – 32	MIC
INTEGRIDADE DO ENCABEÇAMENTO	NÃO POSSUI	MIC
GERÊNCIAMENTO DE CHAVE	NÃO POSSUI	EAP – BASEADO

Fonte: JUNIOR, BRABO E AMORAS, 2004, p. 60.

2.7.8 Certificado digital

A certificação digital é uma tecnologia de identificação que permite que transações eletrônicas dos mais diversos tipos sejam feitas considerando sua autenticidade sua integridade e sua confidencialidade, de forma a evitar que adulterações, interceptações ou outros tipos de fraude ocorram. (ALECRIM, 2010).

De acordo com Medeiros (2001, apud Alves, 2009 p. 48), o certificado digital é uma versão digital, de algo parecido a um Bilhete de Identidade de um determinado utilizador, que serve para comprovar a identidade do utilizador diante de qualquer situação, onde seja necessária a comprovação de identidade.

> Um documento eletrônico com assinatura digital que contém dados como nome do utilizador (que pode ser uma pessoa, uma empresa, uma instituição, etc), entidade emissora (você saberá mais sobre isso adiante), prazo de validade e chave pública. Com o certificado digital, a parte interessada obtém a certeza de estar se relacionando com a pessoa ou com a entidade desejada. (ALECRIM, 2010).

Para Medeiros (2001, apud Alves, 2009 p. 49), o certificado digital é constituído por um conjunto de elementos onde se destaca os três principais:

- Informação de atributo – É a informação sobre o objeto que é certificado.
- Chave de informação pública – É a chave pública da entidade certificada. O Certificado atua para associar a chave pública à informação de atributo, descrita acima

- Assinatura da Autoridade em Certificação (CA) – A CA assina os dois primeiros elementos e, então, adiciona credibilidade ao certificado.

2.7.9 Firewall

Conforme Junior, Brabo e Amoras (2004), o firewall atua como uma barreira de proteção, controlando o trafico de dados entre o computador e a internet ou entre uma rede e a internet. Seu principal objetivo é permitir somente a transmissão e recepção de dados autorizados. Atua como defesa, controlando os acessos de ambos os lados por meio de regras anteriormente definidas em sua configuração.

Para Alves (2009), o firewall é uma das ferramentas imprescindíveis para garantir a segurança de uma rede, pode ser por cabo ou sem fio, é uma barreira que fica entre a rede interna e a rede externa, e implementa um conjunto de regras que permite o controle de todo o trafego que entra e sai da rede.

Segundo Junior, Brabo e Amoras (2004), capaz de analisar informações sobre a conexão e notar as alterações suspeitas, os *firewalls* tem a capacidade de analisar o conteúdo dos pacotes e permitem um controle maior do que pode ou não ser acessível.

> "O firewall também pode assumir o papel de gateway entre duas redes, podendo estas redes ser uma WI-FI e a outra LAN (Local Área Network), desta forma é possível isolar as duas redes, evitando que pessoas não autorizadas que possuem acesso a uma rede, não tenham o mesmo privilégio em acessar a outra, bloqueando como desejado o tráfego que ocorre do lado WI-FI para a LAN e da LAN para WI-FI." (Júnior et Al, 2004, p. 41).

A figura 16 ilustra um exemplo para a implementação do firewall, que protege tanto rede com cabo com a rede sem fio.

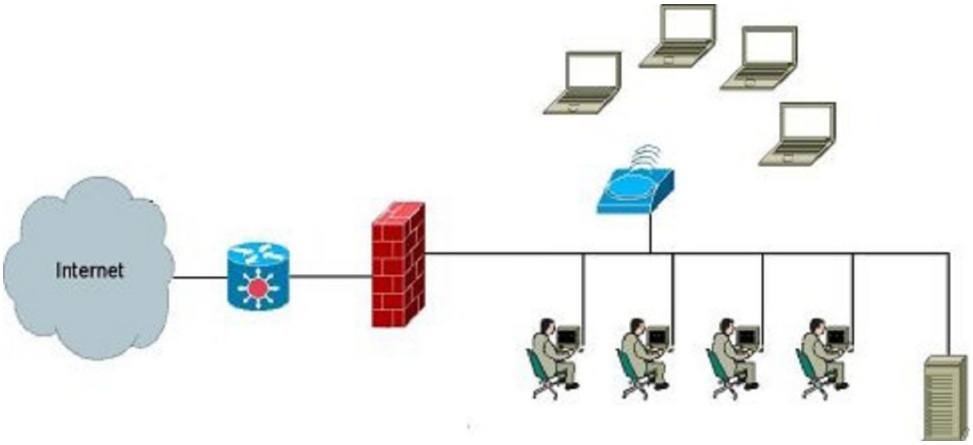

Figura 16 – Implementação do firewall
Fonte: ALVES, 2009, p.50.

Segundo Alecrim (2004) a seguir é citado às três principais razões para se usar um firewall:

1. O firewall pode ser usado para ajudar a impedir que sua rede ou seu computador seja acessado sem autorização. Assim, é possível evitar que informações sejam capturadas ou que sistemas tenham seu funcionamento prejudicado pela ação de hackers;
2. O firewall é um grande aliado no combate a vírus e cavalos-de-tróia, uma vez que é capaz de bloquear portas que eventualmente sejam usadas pelas "pragas digitais" ou então bloquear acesso a programas não autorizados;
3. Em redes corporativas, é possível evitar que os usuários acessem serviços ou sistemas indevidos, além de ter o controle sobre as ações realizadas na rede, sendo possível até mesmo descobrir quais usuários as efetuaram.

Conforme Junior, Brabo e Amoras (2004), os firewalls podem ser classificados em duas categorias: baseado em filtro e baseado em aplicação.

2.7.9.1 Baseado em filtro

Para Junior, Brabo e Amoras (2004), para a filtragem de pacotes é necessário se restringir a trabalhar nas camadas TCP/IP, decidindo quais dados podem ou não passar. As escolhas se tornam em regras baseadas nas informações do IP (Internet Protocol) remoto, endereço do IP dos destinatários, alem da porta TCP usada.

De acordo com Monteiro e Boavida (2000 apud Alves, 2009, p. 50), dizem,

> "A vantagem dos *firewalls* desse tipo referem-se o baixo custo e a facilidade de configuração. Como desvantagens há a destacar as implementações em termo de degradação de desempenho do router, a relativa facilidade com que se cometem erros de configuração das listas de acessos e o fato de só atuarem nos níveis protocolares inferiores o que impede filtragens com base nas aplicações e no comportamento dos utilizadores".

Segundo Barbosa (2006), as regras de filtragem de pacotes são as principais desvantagens na filtragem de pacotes, pois tendem a ser difíceis de configurar. Após serem configuradas, as regras de filtragem de pacotes tendem a ser difíceis de serem testadas. Dependendo do método utilizado, pode ser difícil ou impossível a implementação de certos tipos de filtros altamente desejáveis. Por exemplo, os pacotes informam o endereço IP de origem dos pacotes, mas não informam de qual usuário, impossibilitando então, impor restrições sobre usuários específicos.

2.7.9.2 Baseado em aplicação

Segundo Junior, Brabo e Amoras (2004), o *firewall* baseado em aplicação tende a ser mais complexo, porém mais seguro, pois todas as aplicações precisam de um *proxy* (exemplos de aplicação: SMTP, FTP, HTTP, etc.). Para esse tipo de aplicação não é permitido a comunicação direta entre a rede e a internet tudo deve passar pelo *firewall*, e atua como um orientador. O *proxy* proporciona a comunicação entre ambos os lados por meio de uma avaliação do número da sessão TCP dos pacotes.

De acordo Monteiro e Boavida (2000, apud Alves, 2009 p. 51) dizem que, a desvantagem desse tipo de *firewall* tem a ver com a complexidade de configuração e manutenção do *proxy* para cada aplicação, sendo que muitos não trabalham muito bem com *proxy* constituindo assim pontos únicos de falhas.

2.8 Riscos e Vulnerabilidades

As redes sem fio possuem limitações, e para que se garanta a tão sonhada e desejada segurança é necessário ter o conhecimento dos riscos e vulnerabilidades que podem ser explorados pelos possíveis invasores e atacantes. (ALVES, 2009).

2.8.1 Segurança Física

De acordo com Rufino (2005 apud Alves, 2009, p. 52), antes de montar uma rede sem fio, se faz necessário efetuar um estudo cuidadoso, que engloba desde o equipamento utilizado, as suas potências e a área de abrangência, bem como o mecanismo de segurança usados de modo a não comprometer o bom funcionamento de uma rede, de a não permitir o acesso de utilizadores não autorizados.

Segundo Rufino (2005 apud Shikota, 2006, p. 21), não se deve esquecer que antenas ou interfaces mais potentes ampliam a distância de recepção, portanto, para garantir que o sinal não vai ser capturado a uma determinada distância, não é suficiente percorrer os limites da instalação para verificar até onde o sinal chega, uma vez que um atacante munido de uma interface de maior potência poderá receber sinal a uma distância não prevista pelos testes.

Para Rufino (2005 apud Shikota, 2006, p. 21), um concentrador colocado em uma parede enviará sinal tanto para dentro, quanto para fora do ambiente. Quanto mais ao centro estiver o concentrador, melhor será o aproveitamento, pelas estações, do sinal irradiado por ele. Caso o concentrador tiver o sinal sendo extravasado para fora do ambiente, o atacante terá esse acesso, sendo suficiente para os propósitos do atacante. Como é mostrado na figura 17.

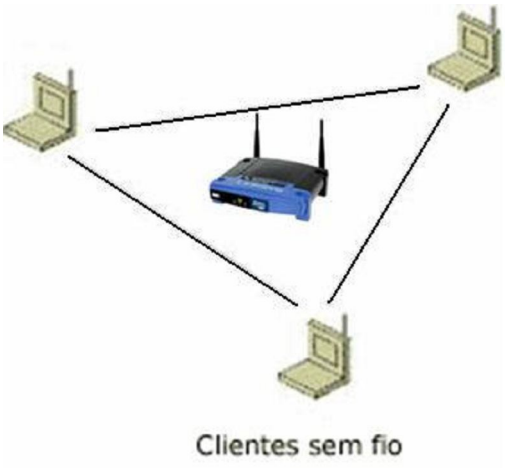

Figura 17 – Concentrador ao centro do ambiente

Fonte: SHIKOTA, 2006, p.21.

2.8.2 Configuração de fabrica

Segundo Rufino (2005 apud Pereira, 2009, p.8), a configuração de fabrica é sem dúvidas uma das principais vulnerabilidades detectadas em um grande número de redes Wifi. A grande maioria dos Pontos de Acesso saem de fábrica com ESSID, senha de administração e endereçamento IP padrões, sendo que essas informações encontram-se disponíveis nos manuais dos equipamentos e nas páginas WEB dos respectivos fabricantes. Sendo assim, caso não sejam trocadas, permitem fácil acesso de estranhos à rede, inclusive com a possibilidade de modificá-las posteriormente.

> O AP, em sua configuração de fábrica, ou vem sem nenhuma senha habilitada ou possui uma senha comum, de conhecimento geral. Uma das primeiras atitudes que devem ser tomadas seria a troca ou habilitação destas senhas. Devem-se escolher senhas apropriadas e de maneira que estas sejam conhecidas por um número bem restrito de pessoas (ou somente pelo administrador da rede). Estas senhas não devem ser divulgadas e ainda, deve ser alterada periodicamente. Esta medida, embora simples, não é tomada em muitos ambientes de rede. (FRANCISCATTI, 2005, p.62)

2.8.3 Mapeamento do ambiente

Para conseguir o máximo de informação possível sobre o potencial do alvo a invadir, as primeiras ações dos atacantes é realizar o mapeamento do ambiente. (ALVES, 2009).

De acordo Rufino (2005 apud Alves, 2009, p.54), atualmente uma das possibilidades disponíveis para identificar e localizar rede sem fio é através de mapeamento feito por dispositivo de localização por satélite, mais conhecido por GPS. Os mapas gerados pelo GPS são de grande precisão, podendo indicar a área onde a rede atua com grande interesse, bem como as redes que não utilizam o protocolo WEP e até mesmo um órgão ou empresa específica.

2.8.4 Posicionamento do ponto de acesso

De acordo Rufino (2005 apud Alves, 2009, p.54), a qualidade e a segurança da rede sem fio, está intimamente ligada ao posicionamento do ponto de acesso. Essas duas características são de simples percepção, pois o sinal do ponto de acesso é enviada para todas as direções, neste caso se faz necessário localizar o ponto de acesso num lugar onde

o sinal abrange somente a área pretendida, evitando assim que o sinal saia da sua área de segurança.

Segundo Alves (2009), se o ponto de acesso não estiver bem posicionado, o atacante pode ter acesso ao sinal, tornando assim a rede vulnerável. Se o ponto de acesso estiver bem posicionado o sinal fica internamente, aumentando assim a captura do sinal pelos equipamentos autorizados. Como mostra a figura 18 a seguir:

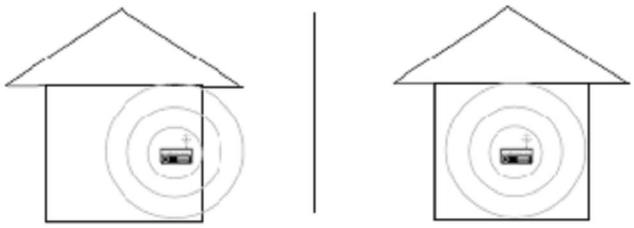

Figura 18 – Posicionamento do ponto de acesso

Fonte: ALVES, 2009, p.54.

2.8.5 WEP

Segundo Rufino (2005, apud Cozer, 2006, p.19), existe problemas administrativos e técnicos em relação ao protocolo WEP. O WEP caiu em descrédito quando foram publicadas maneiras de quebrar seu algoritmo. Muita pessoa mesmo sem entender que essa quebra poderia ocorrer condenaram-no para qualquer caso.

Para Veríssimo (2005 apud Martins, 2005, p.21), uma das vulnerabilidades do protocolo WEP utiliza chave única e estática compartilhada entre todos os dispositivos de uma rede. Portanto em caso de troca da chave isso se torna impraticável em redes com muitos clientes, pois é um processo muito trabalhoso, lembrando que essa troca deverá ser feita em todos os clientes. Sendo assim, se realmente necessitar utilizar WEP em uma rede com muitos usuários, a rede ficará de alguma forma com menor segurança pois quanto maior o número de pessoas que conhecer a chave maior a probabilidade de outras pessoas descobrirem visto que os equipamentos podem ser perdidos, compartilhados ou atacados.

De acordo com Rufino (2005 apud Shikota, 2006, p. 20), o algoritmo RC4, possibilidade de saber quantos bytes tem a mensagem original, pois ele recebe um byte que realiza um processamento e gera um byte também na saída, só que diferente do original, mas, a mensagem criptografada continua com o mesmo número de bytes que a original.

Veríssimo (2002 apud Junior, Brabo e Amoras, 2004, p. 53) complementa que , uma das vulnerabilidades desse protocolo está associada à reutilização do vetor de inicialização (IV). Como dito, o IV possui 24 bits, podendo assumir valores entre 0 e 16M. Como são utilizadas as mesmas chaves por um longo período, o padrão WEP recomenda que o IV seja alterado para cada pacote enviado, evitando assim a reutilização do fluxo de chaves. Normalmente, o IV começa do 0 e é incrementado de 1 a cada envio de pacote. Esse mecanismo tem dois problemas: o primeiro é que chegará um momento que o IV assumirá novamente o mesmo valor; e o segundo, reside no fato de que as pessoas, freqüentemente, removem e reinserem os adaptadores de redes sem fio em seus computadores, fazendo com que o IV receba novamente o valor 0, tornando comuns os pacotes com IV com baixos valores.

2.8.6 WPA

Segundo Rufino (2005 apud Cozer, 2006, p.20), o WPA tem características de segurança superiores do WEP, mesmo assim apresenta algumas vulnerabilidades. O uso de senhas compostas com um número de caracteres pequeno de fácil adivinhação, esta sujeito a ataques de força bruta ou dicionário onde o atacante utiliza senha em seqüência e/ou em palavras comum. No caso do WPA senhas com menos de 20 caracteres são mais susceptíveis a esse tipo de ataque. È comum os fabricantes de equipamentos de rede sem fio usarem senhas pequenas, supondo que o administrador do sistema ira alterar a senha no ato da configuração, porem isto muitas vezes não ocorre tornado o WPA tão vulnerável quanto o WEP.

Para Earle (2006 apud Alves, 2009, p.57), uma das vulnerabilidades do protocolo WPA é de ser susceptível a ataques DoS. Esse tipo de ataque pode se realizar devido a uma particularidade do MIC. Quando acorrer duas falhas MIC em menos de um minuto, o ponto de acesso cancela a comunicação por mais sessenta segundos. Assim quando voltar a restabelecer a comunicação, este requisita a todos os dispositivos clientes a alteração das chaves. Portanto, é possível efetuar um ataque DoS a uma rede que utiliza o protocolo WPA. Assim sendo, é só capturar os pacotes que circulam na rede alterá-los e reenviá-los a rede duas vezes por minuto fazendo com que a comunicação no ponto de acesso seja cancelada, por alguns segundos.

2.8.7 WPA2

Segundo Linhares e Gonçalves (2006), o protocolo WPA2 atualmente apresenta poucas vulnerabilidades. Pode ser que mais vulnerabilidades ainda não foram descobertas, pois os dispositivos que suportam o WPA2 não são muito utilizados.

De acordo com o mesmo autor, as principais vulnerabilidades conhecidas são: de negação de serviço e de PSK pequeno. Na negação de serviço todos os mecanismos de segurança existentes até agora não protegem os quadros de gerenciamento do tipo de autenticação. O PSK pequeno na verdade não é uma falha no protocolo e sim do usuário. Com menos de 20 caracteres são vulneráveis a ataques de dicionário.

Na Tabela 7, mostra um comparativo entre WEP e WPA2, demonstrando o quanto o WEP é falho em relação WPA2.

Tabela 7 - Comparação entre WEP e WPA

Ponto fraco do WEP	Como o ponto fraco é abordado pelo WPA2
O IV (vetor de inicialização) é muito pequeno	No CCMP do AES, o IV foi substituído por um campo de Número do pacote e duplicou em tamanho, para 48 bits.
Integridade dos dados fraca	O cálculo da soma de verificação criptografada pelo WEP foi substituído pelo algoritmo CBC-MAC do AES, que foi criado para fornecer uma integridade dos dados forte. O algoritmo CBC-MAC calcula um valor de 128 bits, e o WPA2 usa os 64 bits de ordem superior como um MIC (código de integridade da mensagem). O WPA2 criptografa o MIC com a criptografia do modo de contador do AES.
Usa a chave mestra em vez de uma chave derivada	Como o WPA e o protocolo TKIP (Temporal Key Integrity Protocol), o CCPM do AES usa um conjunto de chaves temporais derivadas de uma chave mestra e de outros valores. A chave mestra é derivada do processo de autenticação do 802.1X do EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) ou do PEAP (Protected EAP).
Sem rechaveamento	O CCMP do AES faz o rechaveamento automaticamente para derivar novos conjuntos de chaves temporais.
Sem proteção contra reexecução	O CCMP do AES usa um campo de Número do pacote como contador para fornecer proteção contra reexecução.

Fonte: OZORIO, 2007, p.26.

2.9 Tipos de ataque

Os ataques as redes sem fio não são novos. São baseados em ataques anteriores descobertos em redes guiadas. Muitos destes ataques não sofreram nenhuma modificação, já outros sofreram algumas modificações, para que possam ser disparados para obter melhores resultados. O objetivo dos ataques não é comprometer a rede sem fio e sim conseguir acesso ou comprometer a rede guiada. (DUARTE, 2003).

2.9.1 Associação maliciosa

Segundo Duarte (2003), a associação maliciosa ocorre quando o invasor passa por um Access point e ilude outro sistema, de maneira a fazer com que este acredite estar se conectando em uma WLAN real.

> A associação maliciosa é um tipo de ataque onde o invasor, utilizando-se de um ponto de acesso não monitorado ou não detectado pela rede sem fio, conhecido como Rogue AP, primeiramente associa-se a ele e depois se faz passar por um AP, e a partir daí passa a se associar a estações clientes da rede podendo realizar inclusive outros tipos de ataque a partir deste, como por exemplo o ataque de man-in-the-middle. (SGUAREZI, 2007, p.43).

A figura 19 abaixo, ilustra a associação maliciosa.

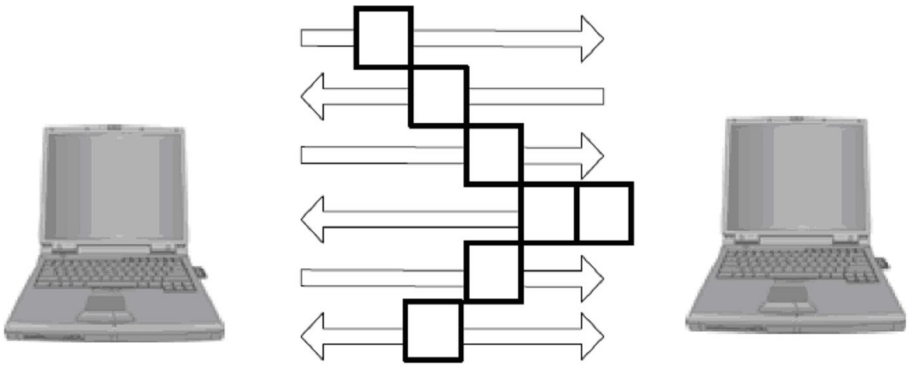

Figura 19 – Associação maliciosa
Fonte: DUARTE, 2003, p.38.

Para Duarte (2003), se a associação maliciosa for comprovada em nosso ambiente experimental, que constam de duas maquinas com dispositivos para redes sem fio e segue o seguinte conjunto de passos:

1. A vítima envia pacotes de Probe Request à procura de access points para conexão;
2. O atacante com o auxílio de um software responde a conexão;
3. A vítima requisita a associação e se associa ao atacante;

4. O atacante responde com as informações de rede necessárias como endereço IP;
5. O atacante envia uma requisição de NET USE;
6. A vítima responde com LOGIN;
7. Qualquer vulnerabilidade de qualquer serviço do cliente pode ser agora explorada.

Segundo o mesmo autor, neste exemplo, o invasor tenta se valer da vulnerabilidade do NETBEUI que permite o compartilhamento de impressora e arquivos em sistema Windows. Mas a partir do quarto passo, qualquer vulnerabilidade existente no cliente pode ser explorada pelo atacante.

2.9.2 ARP Poisoning

Segundo Duarte (2003), O ARP é o ataque de envenenamento do protocolo de resolução de endereços, é um ataque de camada de enlace de dados são disparados quando um invasor está conectado na mesma rede local que a vítima esta. As redes que estejam conectados por Hubs, Switches e Bridges são limitados a este ataque. Deixando de fora as redes conectadas por roteadores e Gateways.

> Muitos dos Access point's disponíveis hoje no mercado, atuam com um Bridge entre a rede guiada e a rede sem fio. Desta forma, um ataque que se utilize de ARP Poisoning como é o caso do ataque do "Homem do Meio", pode ser disparado de uma estação da WLAN a uma estação guiada, ou seja, este ataque não fica restrito apenas às estações sem fio. (DUARTE, 2003, p. 39).

Duarte (2003) complementa que, este ataque ARP Poisoning não é um ataque novo, mas é vulnerável na forma de concepção dos Access point e a ampliação da arquitetura gerada por Access point.

2.9.3 MAC Spoofing

Segundo Rufino (2005 apud Alves, 2009, p.59), uma das medidas de segurança na rede sem fio é o registro do endereço MAC, dos equipamentos que terão a permissão a

conexão à rede. Como os endereços são únicos para cada equipamento desta forma poderão distinguir um equipamento registrado.

A permissão de troca do endereço físico é uma particularidade dos dispositivos para redes sem fio. Com isso os invasores mal intencionados podem capturar através de Eavesdrooping & Espionage um endereço MAC válido de um cliente, trocar seu endereço pelo do cliente e utilizar a rede. (Duarte, 2003).

Segundo Duarte (2003, p. 40), “existe o MAC Spoffing da placa de rede guiada dos access points. Ou seja, os access points são capazes de trocar seus endereços MAC das placas de redes tradicionais burlando assim os firewall internos á LAN”.

Para comprovar esta facilidade, seguem os resultados de comandos entrados para a modificação do MAC, executados no ambiente de análises. Como mostra a figura abaixo:

```
#ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:02:2D:3D:4F:3C
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:13 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:1623 (1.5 Kb)  TX bytes:0 (0.0 b)
          Interrupt:3 Base address:0x100

#ifconfig eth0 down
#ifconfig eth0 hw ether 1B:11:CE:DC:CE:00
#ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 1B:11:CE:DC:CE:00
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:14 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:1659 (1.6 Kb)  TX bytes:0 (0.0 b)
          Interrupt:3 Base address:0x100
```

Figura 20 – MAC Spoffing – Sanitizado

Fonte: DUARTE, 2003, p.41.

2.9.4 Ataques de Denail of Service

Os Ataques de Denail of Service (D.o.S – Negativa de Serviço), procura tornar algum recurso ou serviço indisponível. Estes ataques podem ser tão perturbadores quanto maior sua sofisticação. (Duarte, 2003).

De acordo com Rufino (2005 apud Shikota, 2006 p. 20) É um tipo de ataque que não necessita de acesso ou invasão a rede-alvo, mas conseguem infligir o retardo nas redes Wi-Fi. Com isso, pode facilitar um ataque de negação de serviço, uma vez que é causada

uma grande interferência. Entretanto, podem ser gerados ataques mais sofisticados. Por exemplo, um atacante pode se passar por um Access Point com o mesmo SSID e endereço MAC de um outro Access Point válido para inundar a rede com pedidos de dissociação. Estes pedidos fazem com que os clientes sejam obrigados a se desassociarem e se reassociarem. Enviando as requisições de dissociação em períodos de tempo o DoS é concretizado, pois os clientes não conseguiram permanecer conectados por muito tempo.

Os ataques podem ser disparados de qualquer lugar, mas dentro da área de cobertura da WLAN. A radiofreqüência é de 2.4 GHZ e são utilizada em fornos microondas, aparelhos de monitoramentos de crianças, em telefones sem fio. (Duarte, 2003).

2.9.5 Ataques de Vigilância

Para Duarte (2003), o ataque de vigilante é considerado um ataque para os não estudiosos, mas pode se tornar um ataque de comprometimento muito grande dependendo da sua finalidade.

Segundo Klaus (2004, apud Franciscatti, 2005, p.29), este ataque consiste em se percorrer a cidade ou a instituição, a qual se deseja “vigiar”, apenas observando a existência ou não de WLANs. Para tanto, não existe a necessidade de nem um equipamento especial.

A idéia central deste ataque é rastrear e encontrar os dispositivos de redes sem fio para que possam, posteriormente, serem invadidos. Muitas vezes as configurações pode ser ressetada ou ainda roubada. (Duarte, 2003).

Segundo o mesmo autor, se o access point ser ressetado, um invasor pode gerar ataques dentro da porção guiada da rede. Conseqüentemente os equipamentos de rede sofreram uma grande exposição.

2.9.6 Wardriving

> O termo wardriving foi escolhido por Peter Shipley (http://www.dis.org/shipley/) para batizar a atividade de dirigir um automóvel à procura de redes sem fio abertas, passíveis de invasão. Para efetuar a prática do wardriving, são necessários um automóvel, um computador, uma placa Ethernet configurada no modo "promíscuo" (o dispositivo efetua a interceptação e leitura dos pacotes de comunicação de maneira completa), e um tipo de antena, que pode ser

> posicionada dentro ou fora do veículo (uma lata de famosa marca de batatas fritas norte-americana costuma ser utilizada para a construção de antenas) . Tal atividade não é danosa em si, pois alguns se contentam em encontrar a rede wireless desprotegida, enquanto outros efetuam login e uso destas redes, o que já ultrapassa o escopo da atividade. Tivemos notícia, no ano passado, da verificação de desproteção de uma rede wireless pertencente a um banco internacional na zona Sul de São Paulo mediante wardriving, entre outros casos semelhantes. Os aficionados em wardriving consideram a atividade totalmente legítima. (PEIXOTO, 2001).

De acordo com Rufino (2005 apud Shikota, 2006, p.22), o objetivo dessa técnica é percorrer de carro com um notebook a procura de redes abertas (sem segurança) e podendo utilizar um GPS para mapear as redes encontradas. Como mostra a figura 21 abaixo.

Figura 21 – Wardriving

Fonte: SHIKOTA, 2006, p.22

2.9.7 Warchalking

Para Peixoto (2001),

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

> posição de redes sem fio, facilitando a localização para uso de conexões alheias pelos simpatizantes da idéia.

A figura 22 abaixo mostra os exemplos de símbolos warchalking.

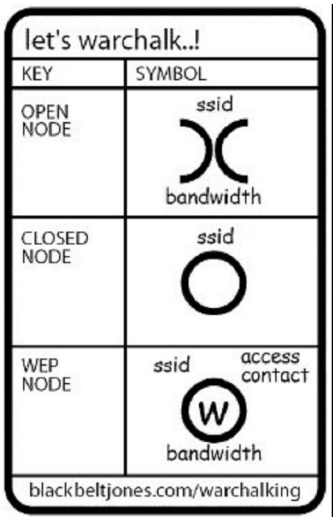

Figura 22 – Exemplo de símbolos warchalking

Fonte: Peixoto, 2001.

Os símbolos apresentados na Figura anterior possuem os seguintes significados:

- O primeiro símbolo indica que a rede é esta aberta, ou seja, ela é vulnerável, descrevendo o SSID e a largura da banda da rede.
- O segundo símbolo indica que a rede esta fechada, descrevendo somente o SSID da rede.
- O terceiro símbolo indica que a rede e protegida pelo protocolo WEP, descrevendo o SSID da rede, a sua largura de banda, bem como a chave utilizada pelo protocolo WEP. (PEIXOTO, 2001).

2.9.8 Ataque de Inserção

De acordo com Klaus (2001 apud Fransciscatti, 2005, p.25), os ataques de inserção estão baseados em colocar dispositivos sem autorização na rede sem fio, tipicamente um laptop ou PDA, para tentar acesso a um servidor ou a LAN interna, iludindo as rotinas de segurança para que pensem que ele realmente faz parte da rede e já recebeu autenticação. Podem ser configuradas estações de base para requerer uma contra senha antes que os

clientes possam ter acesso. Se não houver nenhuma contra-senha, um intruso pode conectar a LAN interna conectando um cliente à estação básica sem nenhuma dificuldade.

2.9.9 Ataque de Monitoração

De acordo com Klaus (2001 apud Fransciscatti, 2005, p.25), este ataque consiste em monitorar o tráfico da rede, através de ferramentas que permitam capturar pacotes para que eles possam ser analisados. Esse ataque é muito utilizado em redes Ethernet através de *sniffers* de rede. Já existe o chamado *Wireless Sniffers* que fazem o mesmo serviço, mas com adaptações para funcionarem melhor em redes sem fio.

Segundo Duarte (2003), um invasor pode capturar informações que trafegam pela rede em qualquer tipo de pacote. As ferramentas *sniffer* para redes *Ethernet* capturam a primeira parte da sessão de conexão onde estão os dados de username e senha, IP de origem, IP de destino, e etc. O invasor pode mascarara como aquele usuário esta usando essas informações capturadas. O invasor que monitora uma rede sem fio, pode aplicar este mesmo principio em ataques na rede sem fio.

Para o mesmo autor, a grande diferença entre ataques de monitoração de redes sem fio e ataques de monitoração em redes Ethernet é o tipo de rede que o atacante pode utilizar, nas redes sem fio é necessário que o invasor esteja dentro do alcance do sinal transmitido pelas antes que compõe a rede, geralmente em torno de 150 metros, depende da transmissão de sinal de cada equipamento. Enquanto nas redes *ethernet* o invasor pode utilizar a internet para furar a segurança e invadir a rede para monitorar o trafego de informações

2.10 Ferramentas de ataque

Segundo Rufino (2005 apud Alves, 2009, p.62), ao contrário das redes com cabos, em que os modelos das interfaces de rede nada influenciam o comportamento das ferramentas, em redes sem fio a maior parte das ferramentas dependem de equipamentos específicos e/ou modelos de placas de rede, ou de um padrão.

2.10.1 Netstumbler

De acordo com Duarte (2003), a Netstumbler é um software conhecida como scanner para redes sem fio. Oferece suporte a GPS, potencia no sinal, ESSID da rede em questão. Esta ferramenta revolucionou o mundo da rede sem fio, pois além de ser usado para ações maliciosas, pode ser usado pelo gerente da rede para monitorar a qualidade do sinal e quantos dispositivos estão instalados na sua instituição.

Segundo Rufino (2005 apud Alves, 2009, p.63), além disso, uma das grandes vantagens dessa ferramenta e que permite identificar as redes sem fio em todos os padrões comerciais e aceita uma grande variedade de interfaces de rede.

Esta ferramenta possui uma versão para Pocket PC intitulada MiniStumbler, a qual pode ser utilizada sem que desperte muita atenção e tenha a mesma eficácia do NetStumbler tradicional. (Duarte, 2003)

A seguir segue algumas figuras 23, 24, 25 e 26 do Netstumbler em ação:

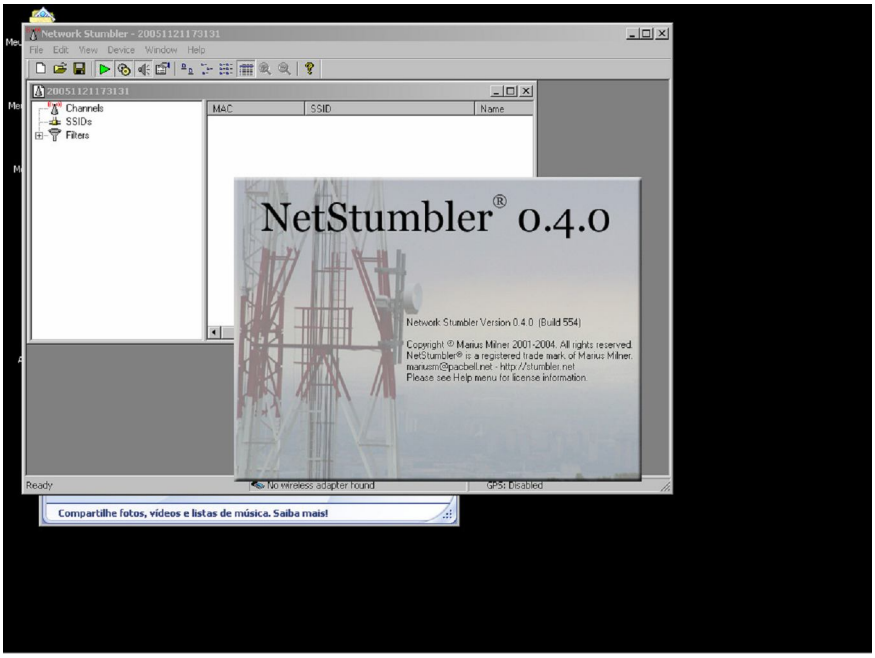

Figura 23 – Tela de abertura do NetStumbler

Fonte: MARTINS, 2005, p.30.

Procurando um concentrador e o canal que está utilizando

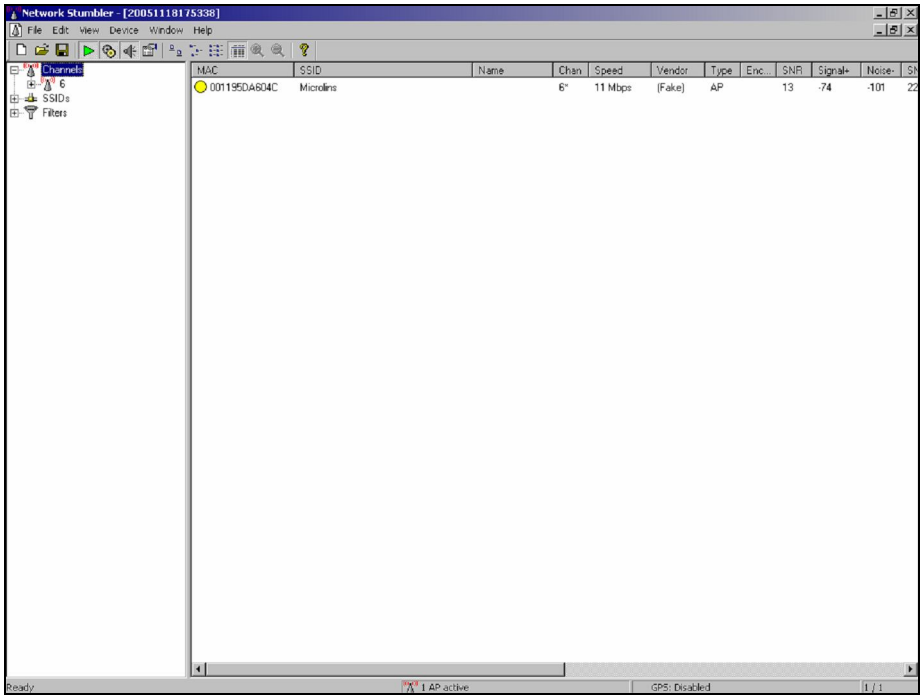

Figura 24 – NetStumbler procurando um concentrador e seu canal

Fonte: MARTINS, 2005, p.31.

Mostrando a qualidade do sinal e o endereço MAC

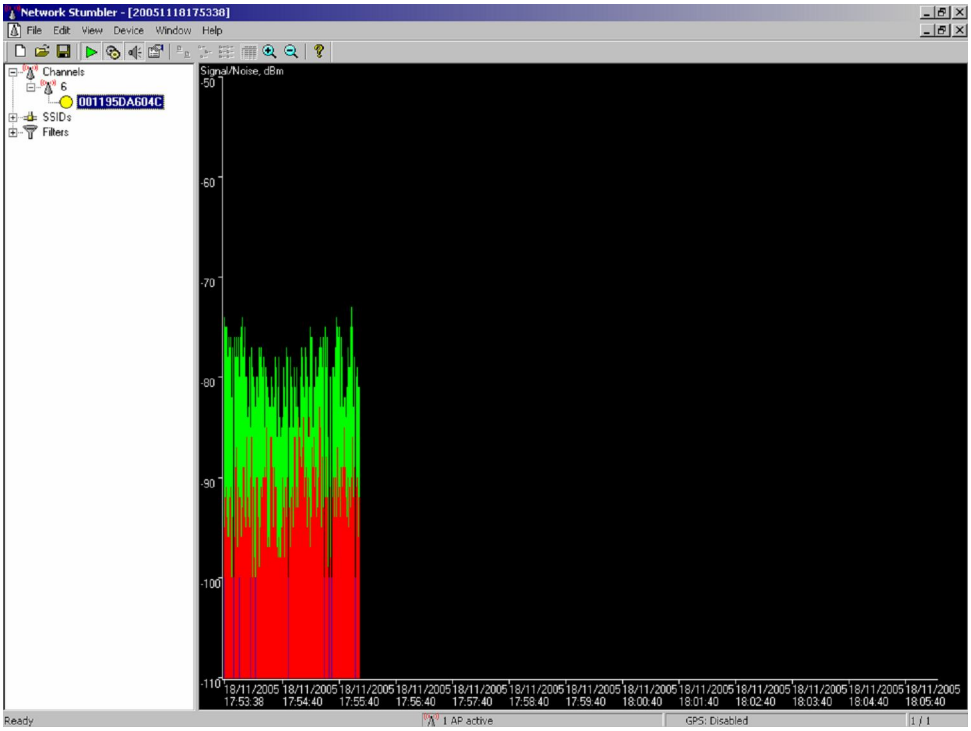

Figura 25 – NetStumbler mostrando a qualidade do sinal e se endereço MAC

Fonte: MARTINS, 2005, p.31.

Encontrando uma rede sem criptografia e com SSID disponível

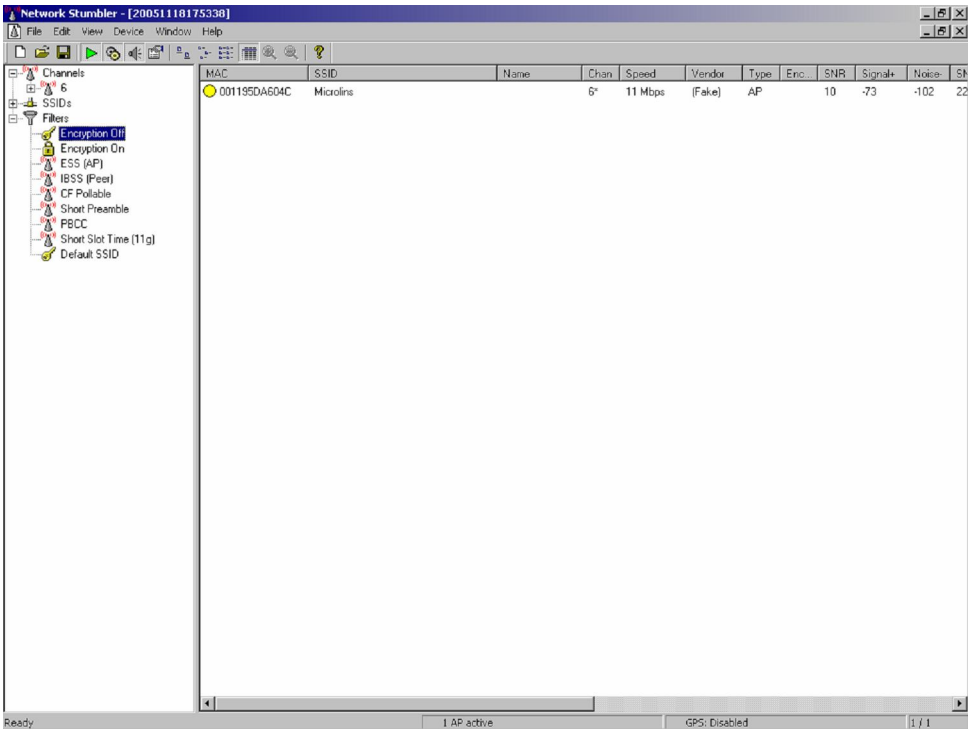

Figura 26 – NetStumbler encontrando uma rede aberta e seu SSID

Fonte: MARTINS, 2005, p.32.

A base de sua concepção é à base de seu maior problema, apesar de todas as inovações presentes nestes programas. Duarte (2003).

2.10.2 Airtraf

Para Souza (2005), este programa proporciona coletar uma enorme quantidade de informações sobre as redes identificadas, como: serviços utilizados, destino das conexões em tempo real e os clientes conectados.

> O programa é suportado somente por algumas placas como: Orinoco/Proximj, Prism2/Hostap ou Aeronet/Cisco. Em relação a quantidade de linhas e colunas que compõem a tela, a menos que identifique que existem 120 colunas e 45 linhas, o Airtraf simplesmente se recusa a rodar. (OLIVEIRA, 2006, p. 48).

Segundo Rufino (2005 apud Oliveira, 2006, p.48), por todas essas características, o Airtraf é uma ferramenta bastante prática tanto para possíveis invasores quanto para o administrador da rede que pode monitorar e visualizar as atividades da rede.

2.10.3 Fakeap

Segundo Rufino (2005 apud Souza, 2005, p.51), *fakeap* é um programa capaz de transformar um dispositivo de rede sem fio em um Access Point. Máquinas convencionais podem, portanto, agirem como um *Acess Point*, forjando algumas características que levem o cliente a pensar que está conectado ao concentrador correto Dentre elas, destacam:

- Receber conexões em um canal específico.
- Usar ESSID específico.
- Utilizar um endereço MAC específico ou o padrão de um determinado fabricante.
- Usar uma determinada chave WEP.
- Permitir configuração de potencia de saída.
-

Segundo o mesmo autor, dentre das limitações dessa ferramenta pode-se destacar:

- Não direciona o tráfego para o ponto de acesso legítimo depois de capturar as informações necessárias.

2.10.4 AirJack

AirJak é uma ferramenta que proporciona passar por um concentrador, e com isso, obter informações dos clientes que venham conectar a ele. Uma das funcionalidades são os cartões que suporta (Prism2 e Orinoco), como a capacidade de operar em modo de infra-estrutura, tal qual um concentrador. (Oliveira, 2006).

Segundo Rufino (2005 apud Alves, 2009, p.65), uma característica em particular que apresenta é a facilidade de fazer um ataque do tipo “homem no meio” com HTTPS, apresentando um certificado falso e torcendo por que o usuário o aceite sem questionamento.

2.10.5 AirSnort

De acordo com Rufino (2005 apud Souza, 2005, p.60), lançado após a divulgação de algumas falhas do protocolo WEP, essa ferramenta possui como característica das demais, a possibilidade de quebra da chave WEP poder ser feita em meio à captura do

trafego. Desta maneira, a quantidade de pacotes não precisa ser previamente definida. Além disso, possui algumas funcionalidades como:

- Identificação do SSID e endereço MAC.
- Uso ou não do WEP.
- Possibilidade de varrer em todos os canais.

A figura 27 abaixo mostra o programa Airsnort em ação tentando descobrir a chave criptográfica utilizada pela rede.

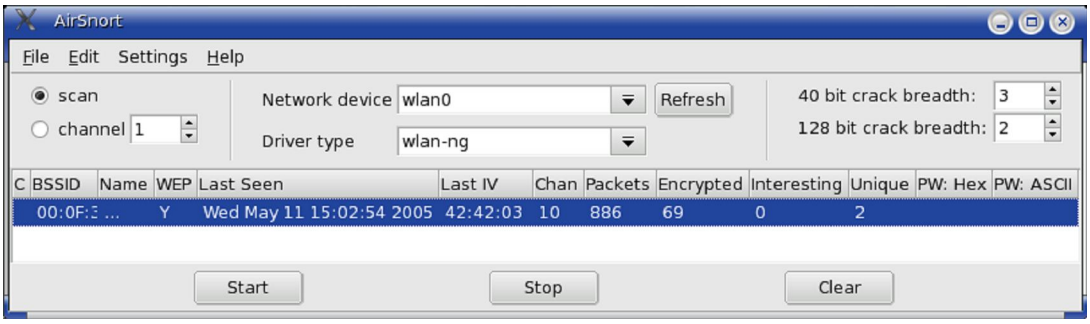

Figura 27 – Ferramenta Airsnort

Fonte: SOUZA, 2005, p.51.

2.10.6 Kismet

Segundo Duarte (2004), esta ferramenta foi desenvolvida pela filosofia opensource este sniffer possui um grande número de ferramentas e opções.

“Projetado como cliente e servidor, pode ter vários servidores rodando à distância de um único cliente. Além de monitorar uma gama muito grande de origens diferentes, pode armazenar os pacotes capturados em vários formatos diferentes”. (Duarte, 2003, p.34).

De acordo com Rufino (2005 apud Souza, 2005, p. 49), o Kismet consegue obter algumas informações sobre o estado geral da área abrangida pela WLAN como:

- Número de WLANs detectadas.
- Número total de pacotes capturados por WLAN.
- Ausência ou não de criptografia WEP.
- Número de pacotes com o vetor de inicialização(I.V).
- Nome da rede (SSID).

- Nível de sina.
- BSSID (relaciona-se ao endereço MAC do Access Point).
- Taxa máxima suportada pela rede.
- Se o dispositivo monitorado é um Access Point, ou não.
- Qual o canal que aWLAN esta configurada.
- Padrão utilizado (802.11 a/b/g).

A figura 28 abaixo apresenta a tela da ferramenta Kismet:

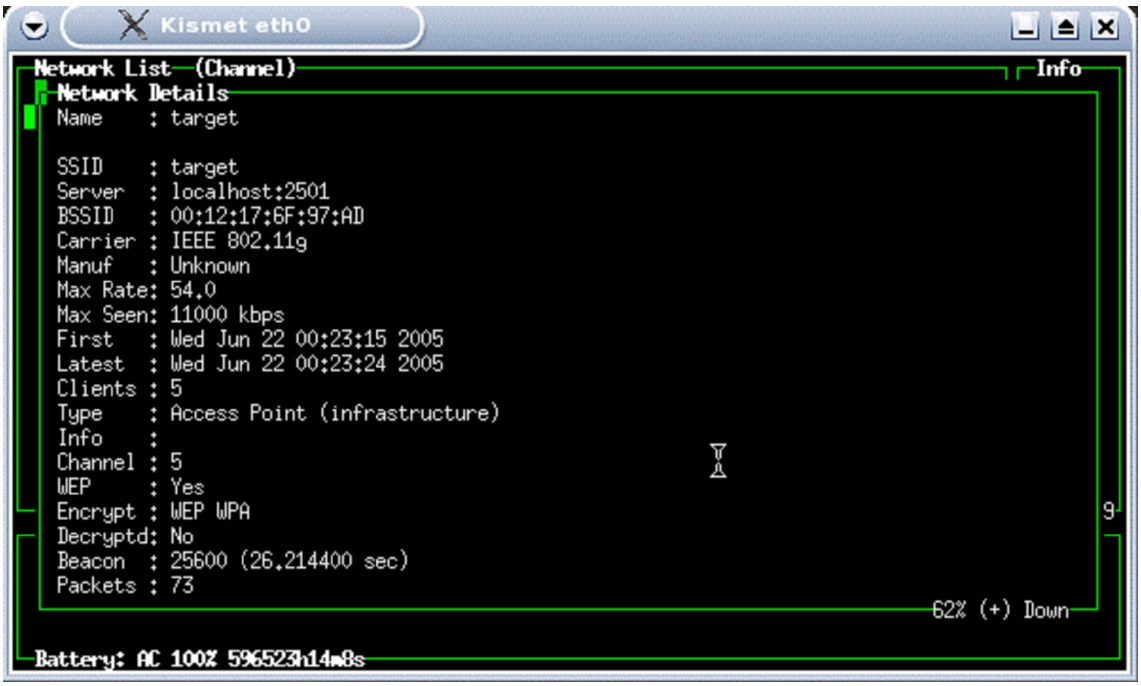

Figura 28 – Tela do Kismet.

Fonte: SOUZA, 2005, p.50.

4 METODOLOGIA

A metodologia utilizada no levantamento bibliográfico é de pesquisa exploratória. Este tipo de pesquisa tem por finalidade, analise bibliográficas através de pesquisa realizadas na internet, livros e artigos científicos. Para o questionário a metodologia usada no capítulo do estudo de caso foi a quantitativa com base, essencialmente no questionário.

Para analisar segurança de redes sem fio em algumas das empresas de Bauru foi elaborado um questionário (ver o anexo) contendo 10 perguntas sobre segurança de redes sem fio com o objetivo de conhecer o nível de segurança das redes sem fio em algumas empresas localizadas na cidade de Bauru.

O questionário foi enviado para 52 empresas de médio e grande porte, dos vários setores de atividades situados na cidade de Bauru. Dos 52 enviados, 38 responderam o questionário.

Enquanto do processo de resposta do questionário foi completado pelos responsáveis pela área de rede das empresas requeridas.

O questionário foi estruturado em um único grupo de questões referentes à segurança de redes sem fio em algumas empresas de Bauru, e as informações recolhidas foram sempre tratadas de forma agregada e nunca individual.

O questionário foi feito através da ferramenta Google docs e o envio e recebimento do questionário foram feitos por via e-mail.

4. RESULTADOS

A tecnologia de redes sem fio está crescendo nos últimos anos, devido a sua mobilidade e flexibilidade, conquistando assim mercados corporativos e domésticos.

Por ser uma tecnologia nova, apresenta vários ataques e vulnerabilidades.

Assim sendo, a segurança se tornou uma das principais necessidades das empresas.

Este capítulo tem por objetivo efetuar um estudo de modo a conhecer o nível de segurança das redes sem fio em algumas empresas da cidade de Bauru.

4.2 Apresentação e análise dos resultados

Atualmente as redes sem fio, são usadas em várias empresas da cidade de Bauru, devido a vários benefícios, como: mobilidade, produtividade, instalação rápida, flexibilidade e escalabilidade.

Segundo o questionário respondido por algumas empresas de Bauru, cerca de 81,58% delas possuem redes sem fio, porém 18, 42% não possuem redes sem fio, como é demonstrado na figura 29 abaixo:

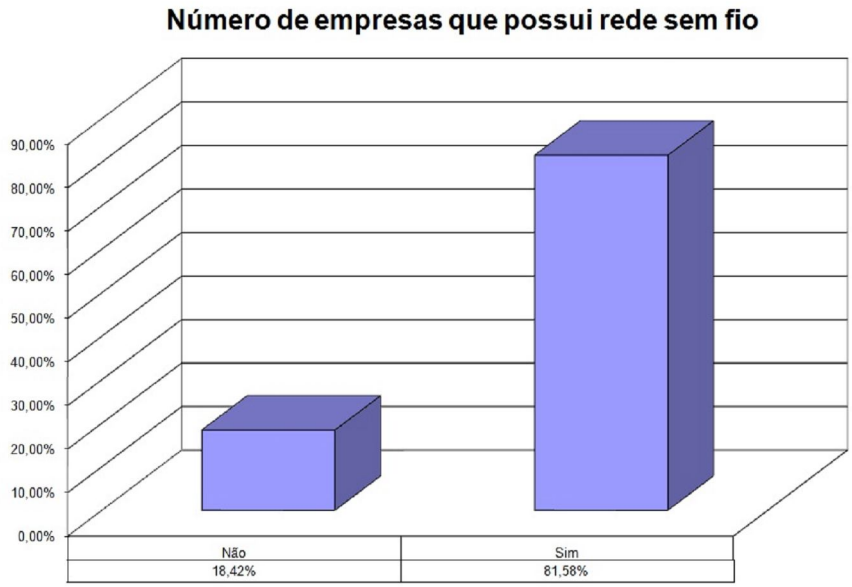

Figura 29: Empresas com rede sem fio na cidade de Bauru

As empresas que não possuem redes sem fio, devem-se ao fato da tecnologia ser nova, possuindo ainda diversas limitações, como é apresentado na figura 30:

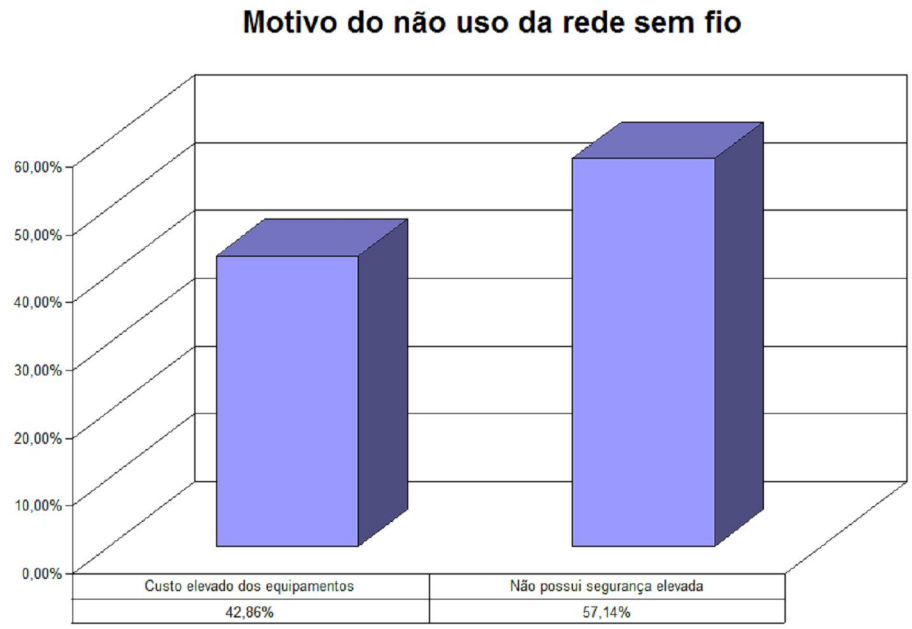

Figura 30: Motivo do não uso da rede sem fio nas empresas de Bauru

O custo dos equipamentos usados para a implementação de uma rede sem fio ainda é muito elevado em comparação com as redes com cabos, tornando assim um dos principais motivos apontado pelas empresas, cerca de 42,86%.

Porém 57,14% das empresas apontam como motivo principal a rede sem fio não possuir uma segurança elevada.

A segurança é muito importante na implementação da rede sem fio. A figura 31 mostra que no estudo foi verificado que o protocolo mais usado para proteger a rede sem fio pelas empresas é o protocolo WPA2.

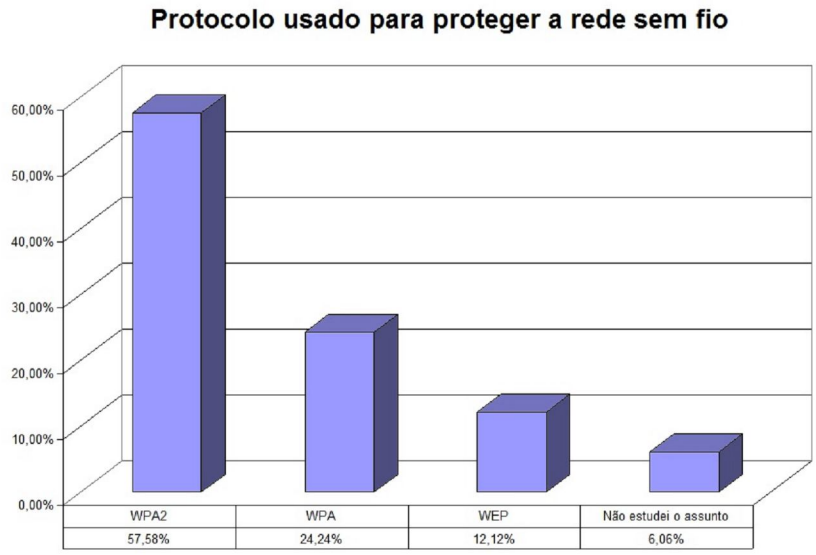

Figura 31: Protocolo usado para proteger a rede sem fio

Sendo assim, 57,58% das empresas usam o protocolo WPA2, por apresentar um nível de segurança mais elevado; Já 24,24% usam o protocolo WPA, pelas vantagens que o protocolo proporciona; 12,12% usam o protocolo WEP, apesar este apresentar maior fragilidade que os outros protocolos; cerca de 6,06% das empresas não estudou a questão de qual protocolo seria usado para proteger a rede sem fio.

Segundo o estudo efetuado nas empresas, verificou que algumas das empresas da cidade de Bauru usam rede sem fio devido a vários motivos. Como demonstra a figura 32:

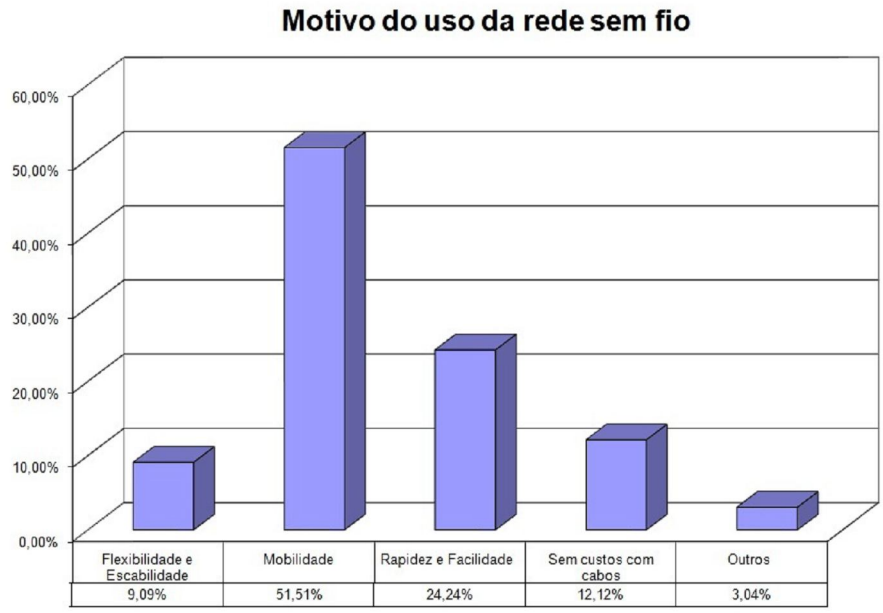

Figura 32: Motivo do uso de redes sem fio nas empresas de Bauru

Conclui-se que o principal motivo para o uso de redes sem fio em algumas empresas de Bauru, é a mobilidade, com 51,51% por não necessitar do uso de cabos; Já 24,24% das empresas usam a rede sem fio devido à rapidez e facilidade de instalação; 12,12% das empresas usam a rede sem fio, por não ter custos com cabos; 9,09% das empresas usam a rede sem fio devido à flexibilidade e escalabilidade da tecnologia; e o restante de 3,04% das empresas usa a rede sem fio por outros motivos.

O estudo feito em algumas das empresas de Bauru constatou que as mesmas possuem redes sem fio defrontam-se com alguns constrangimentos, tais como custos elevados dos equipamentos, não possuir segurança elevada, baixa velocidade de transmissão e entre outros. Como apresenta a figura 33:

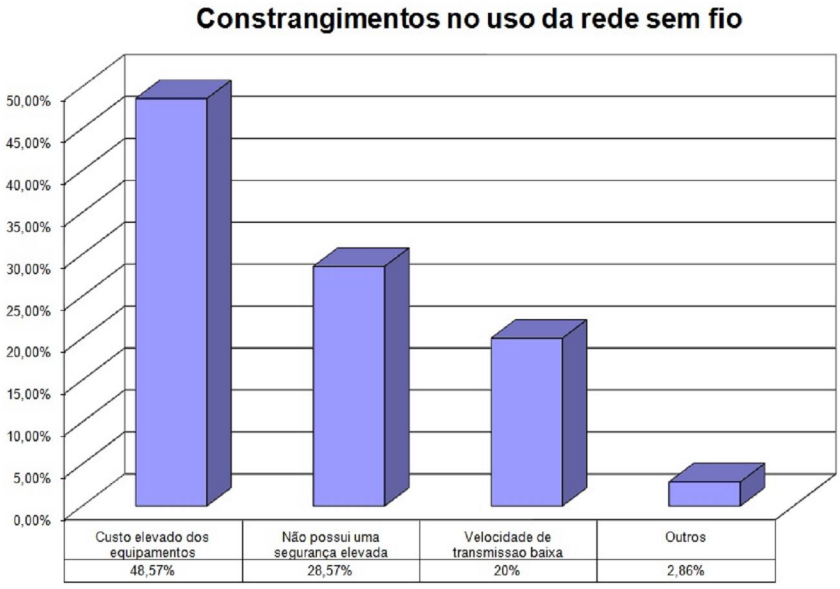

Figura 33: Constrangimentos no uso de rede sem fio nas empresas de Bauru.

Para 48,57% das empresas que usam redes sem fio apontam que o custo elevado dos equipamentos é o principal constrangimento no uso de rede sem fio. Já 28,57% das empresas acham que o principal constrangimento é a baixa segurança. 20% acham que a velocidade de transmissão baixa é o principal constrangimento no uso de redes sem fio e os restantes 2,86% consideram outros motivos como principal constrangimento no uso de redes sem fio.

O que leva a concluir que o custo elevado dos equipamentos seja o principal constrangimento quanto ao uso da rede sem fio em algumas das empresas de Bauru.

A figura 34 apresenta que no estudo feito em algumas das empresas de Bauru, usam as seguintes ferramentas para a monitoração da rede sem fio.

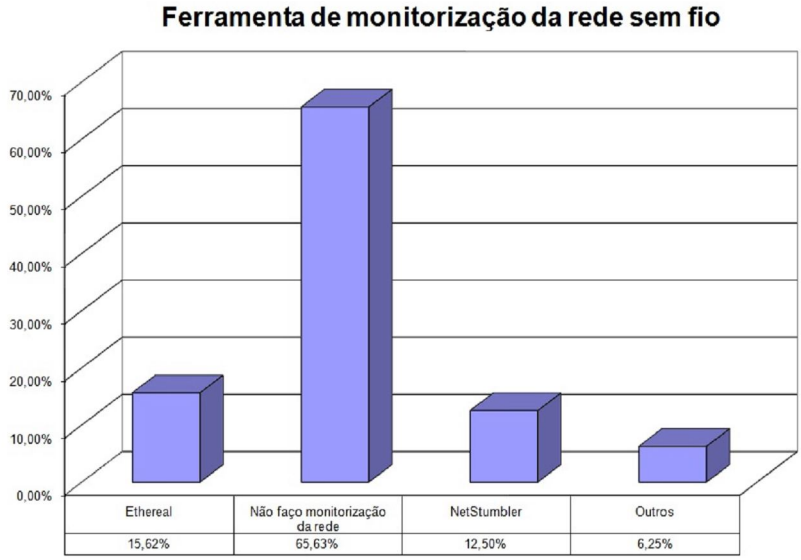

Figura 34: Ferramenta de monitorização da rede sem fio

15,62% das empresas utilizam a ferramenta Ethereal como ferramenta para a monitoração da rede sem fio, pelas vantagens que este proporciona; Cerca de 12,50% das empresas utiliza a ferramenta NetStumbler pelas suas vantagens; 6,25% das empresas utilizam outros tipos de ferramentas para monitorar a rede sem fio; Cerca de 65,63% das empresas não faz a monitoração da rede sem fio, o que torna a rede vulnerável.

Segundo Sguarezi (2007), o ponto de acesso é o principal componente para efetuar a conexão de redes sem fio, assim os usuários enviar e receber dados entre si. Essa transmissão é feita a partir de um sinal de uma ou duas antenas em um ponto de acesso.

O estudo feito em algumas das empresas de Bauru demonstra o seguinte posicionamento do ponto de acesso. Como mostra a figura 35:

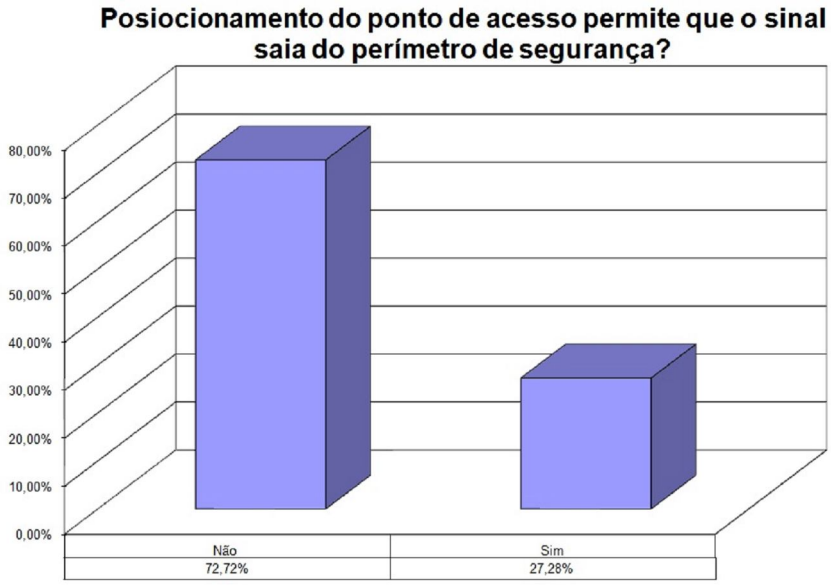

Figura 35: Posicionamento do ponto de acesso

Cerca de 27,28% da empresas o posicionamento do ponto de acesso permite que o sinal sai do perímetro de segurança; e 72,72% das empresas o posicionamento do ponto de acesso não permite que o sinal saia do perímetro de segurança.

Conclui-se a cerca de 27,28% das empresas, se encontra vulnerável, tendo em conta que o sinal ultrapassa o perímetro de segurança o que pode levar a concentração de uma invasão por um possível atacante.

Segundo o estudo feito em algumas das empresas de Bauru, chegou se a conclusão que cerca de 79,41% das empresas, modifica o SSID padrão na configuração do ponto de acesso, o que torna a rede mais segura, pois para que um atacante invada a rede é necessário conhecer algumas características das mesmas, podendo assim retardar um possível ataque; porem cerca de 20,59% das empresas não modificam o SSID padrão. Como apresenta a figura 36:

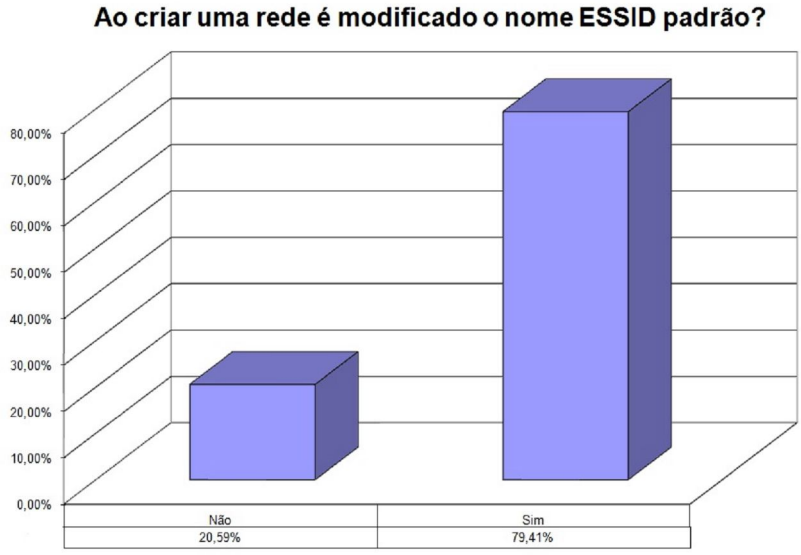

Figura 36: Configuração do ponto de acesso.

Para Alves (2009), o *firewall* é uma das ferramentas imprescindíveis para garantir a segurança de uma rede, pode ser por cabo ou sem fio, é uma barreira que fica entre a rede interna e a rede externa, e implementa um conjunto de regras que permite o controle de todo o trafego que entra e sai da rede.

De acordo com o estudo feito em algumas das empresas de Bauru, 97,05% das empresas usam o *firewall*, para aumentar a proteção da rede sem fio contra ataques externos; 2,95% das empresas não usam o *firewall*, deixando assim sua rede mais vulnerável a ataques externos. Conforme representado na figura 37 abaixo:

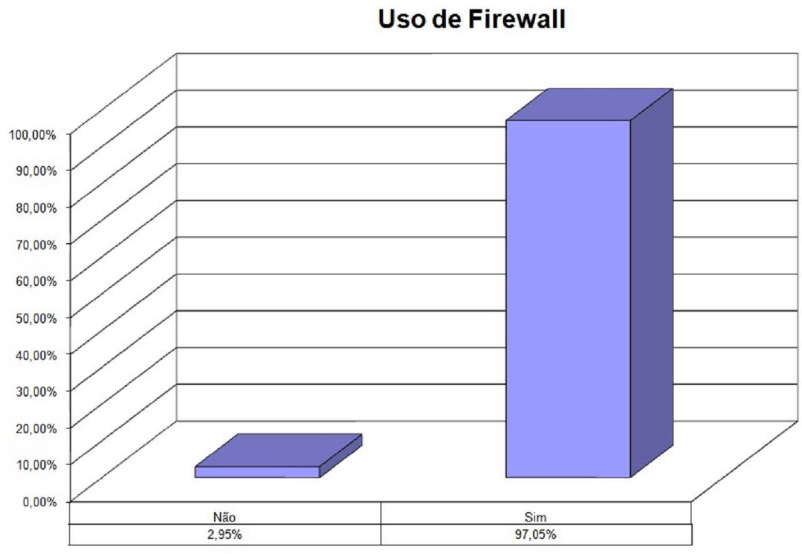

Figura 37: Uso do firewall

Por fim, segundo o estudo feito em algumas empresas de Bauru, verificou o uso de senhas descartáveis. Como demonstra a figura 38 abaixo:

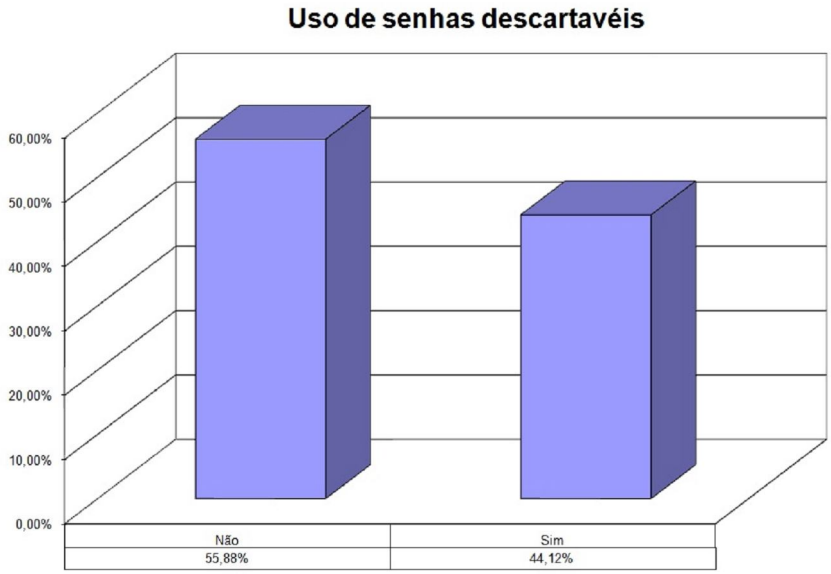

Figura 38: Uso de senhas descartáveis

Cerca de 44,12% das empresas usam senhas descartáveis, como política de segurança de rede sem fio; porém cerca de 55,88% das empresas não usam as senhas descartáveis, como política de segurança da rede sem fio, deixando sua rede mais vulnerável a ataques externos.

5 CONCLUSÃO

A rede sem fio veio ao encontro das necessidades de algumas empresas da cidade de Bauru, pois esta tecnologia aumentou a mobilidade das redes das mesmas, proporcionando assim maior produtividade. Porém as empresas defrontam com alguns constrangimentos no uso da rede sem fio como o custo elevado nos equipamentos usados para a implementação da rede sem fio serem elevados.

Em caso de implementação de uma rede, o protocolo usado seria o WPA2, pois o mesmo protocolo proporcionaria maior segurança.

De acordo com o estudo feito em algumas empresas de Bauru pode-se considerar que elas se encontram num nível de segurança médio, isso, tendo em conta o fato das empresas usar algum tipo de protocolo de criptografia, autenticação para proteger a rede de acesso não autorizado, da mesma forma no uso de *firewall*, senhas descartáveis, alteram o *SSID* padrão e o posicionamento do ponto de acesso, não permitindo a saída do sinal para fora do perímetro de segurança.

6 REFERÊNCIAS

ALECRIM, Emerson. Criptografia. **Infowester,** 2005. Disponível em: <http://www.infowester.com/criptografia.php>. Acesso em: 12 mai. 2010.

ALECRIM, Emerson. Entendendo a certificação digital. **Infowester,** 2009. Disponível em: <http://www.infowester.com/assincertdigital.php>. Acesso em: 05 mai. 2010.

ALECRIM, Emerson. Firewall: conceitos e tipos. **Infowester,** 2004. Disponível em: <http://www.infowester.com/assincertdigital.php>. Acesso em: 15 mar. 2010.

ALECRIM, Emerson. Tecnologia Bluetooth. **Infowester,** 2008. Disponível em: <http://www.infowester.com/bluetooth.php>. Acesso em: 10 abr. 2010.

ALVES, Walter Francisco Andrade. **Segurança de redes sem fio: o caso da assembléia nacional de cabo verde**. Cabo verde, 2009. Disponível em: <bdigita.unipiaget.cv:8080/dspace/handle/123456789/243>. Acesso em: 14 mai. 2010.

ANGELO, Ludmila aparecida; BARBOSA, Victor Antonio Mendonça. **Redes wireless – conceitos, projetos e especificações.** Goiânia, 2003. Disponível em: <http://www.eee.ufg.br/cepf/pff/2002/pf2002_07.pdf>. Acesso em: 08 mar. 2010.

BARBOSA, Akio Nogueira. **Um sistema para análise ativa de comportamento de firewall.** São Paulo, 2006. Disponível em: <http://www.teses.usp.br/teses/disponiveis/3/3142/tde-13122006-145140/>. Acesso em: 21 mar. 2010.

BEZERRA, Fabio Fernandes. **Ferramenta de análise modal de protocolos de segurança para redes sem fio.** Blumenau, 2004. Disponível em: <www.inf.furb.br/~pericas/orientacoes/VOIPCriptografado2005.pdf>. Acesso em: 07 mai. 2010.

COLUNGA, Marcio. Vantagens e desvantagens das redes sem fio. **Redes Wireless**, 2008. Disponível em: <http://redeswirelessdf.blogspot.com/2008/05/vantagens-e-desvantagens-das-redes-sem.html>. Acesso em: 19 abr. 2010.

COZER, Fabio Luiz. **Segurança redes sem fio.** Jaguariúna, 2006. Disponível em: <bibdig.poliseducacional.com.br/document/?down=100>. Acesso em: 15 mai. 2010

DUARTE, Luiz Otávio. **Análise de vulnerabilidades e ataques inerentes a redes sem fio 802.11x.** São José do Rio Preto, 2003. Disponível em: <bibdig.poliseducacional.com.br/document/?down=25**>**. Acesso em: 28 mar. 2010.

EIRAS, Marcelo. Criptografia. **Marcelo Eiras**, 2006. Disponível em: <http://www.marceloeiras.com.br>. Acesso em: 05 mar. 2010.

FAGUNDES, Eduardo Mayer. **Fundamentos de wireless LAN.** 2004. Disponível em: <http://www.efagundes.com/artigos/Arquivos_pdf/Wireless_LAN.PDF>. Acesso em: 12 abr. 2010.

FARIAS, Paulo Cesar Bento. Métodos de autenticação. **Julio Battisti,** 2006. Disponível em: < http://www.juliobattisti.com.br/tutoriais/paulocfarias/redeswireless021.asp>. Acesso em: 21 mai. 2010.

FLICKENGER, Rob et al. **Redes sem fio no mundo em desenvolvimento**. Londres, 2005. Disponível em: <http://www.scribd.com/doc/8304888/Redes-sem-fio-no-Mundo-em-Desenvolvimento>. Acesso em: 08 abr. 2010

FRANCISCATTI, Vagner. **Segurança em Redes sem Fio.** Londrina, 2005. Disponível em: <www2.dc.uel.br/nourau/document/?view=171>. Acesso em: 27 mar. 2010.

JUNIOR, Aurélio Amodei; DUARTE, Otto Carlos M.B. **Segurança no roteamento em redes móveis ad hoc.** Rio de janeiro, 2003. Disponível em: < http://www.gta.ufrj.br/seminarios/CPE825/tutoriais/aurelio/AmDu03.pdf>. Acesso em: 20 mai. 2010

JUNIOR, Carlos Alberto de Carvalho Vaz Pereira; BRABO, Gustavo da Silva; AMORAS, Romulo Augusto de Sales. **Segurança em redes wireless padrão ieee802.11b: protocolos wep, wpa e análise de desempenho.** Belém**,** 2004. Disponível em: <http://www.cci.unama.br/margalho/portaltcc/tcc2004/carlosgustavo&romulo.pdf> Acesso em: 19 mar. 2010.

KUROSE, James F; ROSS, Keith W. **Redes de computadores e a Internet:** Uma abordagem top-down. 3. ed. São Paulo: Pearson Addison Wesley, 2006.

LINHARES, André Guedes; GONÇALVES, Paulo André da S. **Uma Análise dos Mecanismos de Segurança de Redes IEEE 802.11: WEP, WPA, WPA2 e IEEE 802.11w**. Recife, 2006. Disponível em: <www.unibratec.com.br/jornadacientifica/diretorio UFPEAGL.pdf>. Acesso em: 05 abr. 2010.

MAIA, Roberto. Segurança em redes Wireless 802.11i. **GTA / UFRJ**, 2003. Disponível em: <http://www.gta.ufrj.br/seminarios/semin2003_1/rmaia/802_11i.html>. Acesso em: 13 mai. 2010.

MARTINS, Jorge Martins. **Análise de vulnerabilidades e ataques a redes sem fio 802.11.** Jaguariúna, 2005. Disponível em: <bibdig.poliseducacional com.br/document/?down=25>. Acesso em: 10 abr. 2010.

MELLO, Dirk de. **Wireless.** São Paulo, 2006. Disponível em: < http://www.profdirkmello.pro.br/cursos/RC/mat_rc/Aula_04_Wireless.pdf>. Acesso em: 23 abr. 2010.

MOREIRA, Alexandre Monassa; MALHEIROS, Eduardo Eber B. **Rede Wi-fi de comput adores.** Belém, 2006. Disponível em: <www.scribd.com/doc/8658/wifi>. Acesso em: 02 abr. 2010.

OLIVEIRA, Mauricio Panini. **Segurança de rede banda larga wi-fi ou IEEE 802.11 (wireless fidelity).** Jaguariúna, 2006. Disponível em: <bibdig.poliseducacional.com.br/document/?down=95>. Acesso em: 30 mar. 2010.

OZORIO, Wellington Cesar. **Análise comparativa entre os protocolos de segurança wep, wpa e wpa2.** Jaguariúna, 2007. Disponível em: <bibdig.poliseducacional.com.br/document/?view=47>. Acesso em: 07 mai. 2010.

PEREIRA, Helio Brilhante. **Segurança em redes wireless 802.11 infra-estruturadas.** Lavras, 2009. Disponível em: <www.ginux.ufla.br/files/artigo-HelioPereira.pdf>. Acesso em: 25 mar. 2010.

PEIXOTO, Rodney de Castro. Tecnologias wireless demandam cuidados extras - a prática do wardriving e warchalking. **Wireless Brasil**, 2001. Disponível em: <http://www.wirelessbrasil.org/wirelessbr/colaboradores/rodney_peixoto/seguranca_wireless.html>.Acesso em: 08 mar. 2010.

RUFINO, Nelson Murilo de Oliveira. Conceitos. In:_____. **Segurança em redes sem fio**: aprenda a proteger as suas informações em ambientes Wi-fi e Bluetooth. 1.ed. São Paulo: Novatec, 2005.

SARTORATO, Flavio Malfatti et al. Análise de Protocolo de Enlace IEEE 802.11. **Info Segura,** 2008. Disponível em: <http://www.infosegura.eti.br/artigos/80211.php> Acesso em: 10 mai. 2010.

SGUAREZI, João Vitorio dos Reis. **Ferramentas de segurança em redes sem fio.** Cuiabá, 2007. Disponível em: <www.ic.ufmt.br/siteIC/downloads/monografia/74131272928721.pdf> Acesso em: 21 abr. 2010.

SHAMMAS, Gabriel. Tecnologias. **Gabriel Shammas**, 2010. Disponível em: <http://www.shammas.eng.br/acad/sitesalunos0606/wireless/tecnologias.html>. Acesso em: 09 mai. 2010.

SHIKOTA, Ricardo Augusto. **Sistema especialista para verificar a vulnerabilidade de redes de computador sem fio.** Jaguariúna**,** 2006. Disponível em: < bibdig.poliseducacional.com.br/document/?view=99/>. Acesso em: 23 abr. 2010.

SILVA, Gilson Marques; SOUZA, João Nunes. **Uma analise dos mecanismos de segurança de redes sem fio e uma proposta de melhoria.** Uberlândia, 2006. Disponível em: < http://svn.assembla.com/svn/odinIDS/Egio/artigos/ SegurancaMovel/seguranca.pdf>. Acesso em: 05 abr. 2010.

SOUZA, Ricardo de Moura. **Análise das vulnerabilidades e ataques existentes em redes sem fio.** Uberlândia, 2005. Disponível em: <www.si.uniminas.br/TFC/monografias/Monografia-Ricardo-Moura.pdf>. Acesso em: 03 mar. 2010.

TANENBAUM. Andrew S. **Computer Networks.** 4.ed. Amsterdam: Editora Patti Guerrieri, 2003.

VISÃO geral sobre redes sem fio. **Microsoft TechNet**, 2010. Disponível em: < http://technet.microsoft.com/pt-br/library/cc784756%28WS.10%29.aspx>. Acesso em: 02 mai. 2010.

A. ANEXO

A.1 Questionário

Segurança de redes sem fio nas empresas de Bauru

1. Na empresa possui redes sem fio? *

- [ ] Sim
- [ ] Não

2. Se não porque a empresa não possui uma rede sem fio?

- [ ] Custo elevado dos equipamentos
- [ ] Velocidade de transmissão baixa
- [ ] Não possui segurança confiável
- [ ] Outro:

3. Qual tecnologia a empresa usa para proteger a rede sem fio?

- [ ] Não estudei sobre o assunto
- [ ] WEP
- [ ] WPA
- [ ] WPA2
- [ ] Outro:

4. Qual o motivo do uso da rede sem fio?

- [ ] Mobilidade
- [ ] Rapidez e facilidade de instalação
- [ ] Flexibilidade e escalabilidade
- [ ] Sem custos com cabos
- [ ] Produtividade
- [ ] Outro:

5. Na sua opinião qual é o maior constrangimento do uso da rede sem fio?

- [ ] Custo elevado dos equipamentos
- [ ] Velocidade de transmissão baixa
- [ ] Não possui uma segurança elevada
- [ ] Outro:

6. Qual ferramenta é utilizada para monitorar a rede?

- [ ] Não faço monitorização da rede
- [ ] Kisnet
- [ ] NetStumbler
- [ ] Ethereal
- [ ] HostAP
- [ ] Outro:

7. Faço uso de firewall para aumentar a proteção da rede sem fio?

- [ ] Sim
- [ ] Não

8. Ao criar uma rede modifico o nome ESSID padrão?

- [ ] Sim
- [ ] Não

9. Uma política de segurança na empresa é o uso de senhas descartáveis?

- [ ] Sim
- [ ] Não

10. Na empresa o posicionamento do ponto de acesso permite que o sinal saia do perímetro de segurança?

- [ ] Sim
- [ ] Não

Enviar

Tecnologia Google Docs

A.2 Coleta de dados

Coleta de dados enviados por algumas empresas de Bauru

1	Indicação de data e hora	1.Na empresa possui redes sem fio?	2.Se não porque a empresa não possui uma rede sem fio?	3.Qual tecnologia a empresa usa para proteger a rede sem fio?	4.Qual o motivo do uso da rede sem fio?	5.Na sua opinião qual é o maior constrangimento do uso da rede sem fio?	6.Qual ferramenta é utilizada para monitorar a rede?	7.Faço uso de firewall para aumentar a proteção da rede sem fio?	8.Ao criar uma rede modifico o nome ESSID padrão?	9.Uma politica de segurança na empresa é o uso de senhas descartáveis?	10.Na empresa o posicionamento do ponto de acesso permite que o sinal saia do perimetro de segurança?
2	25/08/2010 20:25	Sim		WPA2	Sem custos com	Não possui uma	Ethereal	Sim	Sim	Sim	Sim
3	26/08/2010 14:32	Sim		WEP	Flexibilidade e	problema na	Não faço	Não	Sim	Não	Sim
4	26/08/2010 14:38	Não	Custo elevado dos			Velocidade de					
5	26/08/2010 15:57	Sim		WPA	Mobilidade	Velocidade de	pfsense	Sim	Sim	Não	Sim
6	31/08/2010 14:46	Não	Custo elevado dos	sem rede sem fio	Disponibilizar para	Custo elevados nos	whats up	Sim	Sim	Não	Não
7	02/09/2010 07:38	Sim		WPA	Mobilidade	Não possui uma	Ethereal	Sim	Sim	Não	Sim
8	14/09/2010 08:41	Sim		Não estudei sobre	Mobilidade	Custo elevados nos	Não faço	Sim	Sim	Sim	Não
9	14/09/2010 14:59	Sim		WPA2	Rapidez e	Não possui uma	Não faço	Sim	Sim	Sim	Sim
10	14/09/2010 16:12	Sim		WPA2	Mobilidade	Custo elevados nos		Sim	Sim	Não	Não
11	15/09/2010 15:06	Não	Não possui	WPA	Mobilidade	Não possui uma	Não faço	Sim	Sim	Não	Não
12	16/09/2010 08:16	Sim		WPA2	Mobilidade	Velocidade de	Ethereal	Sim	Sim	Não	Não
13	16/09/2010 09:51	Sim		WEP	Mobilidade	Custo elevados nos	Não faço	Sim	Sim	Não	Não
14	17/09/2010 15:25	Sim		WPA2	Mobilidade	Velocidade de	Ethereal	Sim	Sim	Não	Não
15	17/09/2010 15:50	Sim		WPA2	Rapidez e	Custo elevados nos	Não faço	Sim	Sim	Sim	Não
16	20/09/2010 17:08	Sim		WEP	Mobilidade		Não faço	Sim	Não	Sim	Sim
17	21/09/2010 14:59	Sim		WPA2	Flexibilidade e	Não possui uma	NetStumbler	Sim	Sim	Não	Sim
18	21/09/2010 16:43	Sim		WPA2	Sem custos com	Custo elevados nos	Não faço	Sim	Sim	Sim	Sim
19	23/09/2010 14:36	Não	Não possui			Não possui uma		Sim	Sim	Sim	Não
20	23/09/2010 16:01	Sim		WPA2	Mobilidade	Custo elevados nos	Não faço	Sim	Sim	Não	Sim
21	24/09/2010 16:07	Sim		WPA	Mobilidade	Custo elevados nos	Não faço	Sim	Sim	Não	Não
22	27/09/2010 13:39	Sim		WPA2	Mobilidade	Custo elevados nos	NetStumbler	Sim	Sim	Não	Não
23	27/09/2010 15:35	Sim		WPA	Rapidez e	Não possui uma	Não faço	Sim	Sim	Sim	Não
24	28/09/2010 14:13	Sim		WPA2	Rapidez e	Custo elevados nos	Não faço	Sim	Sim	Não	Não
25	28/09/2010 14:37	Não	Não possui			Não possui uma		Sim			
26	28/09/2010 15:34	Sim		WPA2	Mobilidade	Custo elevados nos	Não faço	Sim	Sim	Não	Não
27	28/09/2010 15:49	Sim		WPA2	Rapidez e	Velocidade de	NetStumbler	Sim	Sim	Não	Não
28	28/09/2010 16:51	Sim		WPA2	Rapidez e	Custo elevados nos	Ethereal		Sim	Sim	Não
29	28/09/2010 17:14	Sim		WPA	Mobilidade	Não possui uma	NetStumbler	Sim	Não	Sim	Não
30	29/09/2010 12:38	Sim		WPA	Sem custos com	Não possui uma	Não faço	Sim	Sim	Sim	Não
31	29/09/2010 13:11	Não	Custo elevado dos								
32	29/09/2010 15:08	Sim		WPA2	Mobilidade	Custo elevados nos	Não faço	Sim	Não	Sim	Não
33	29/09/2010 16:54	Sim		WPA	Rapidez e	Custo elevados nos	Não faço	Sim	Sim	Não	Não
34	30/09/2010 14:02	Sim		WPA2	Rapidez e	Custo elevados nos	Não faço	Sim	Sim	Não	
35	30/09/2010 14:28	Sim		WEP	Flexibilidade e	Custo elevados nos	Não faço	Sim	Não	Não	Não
36	30/09/2010 15:11	Não	Não possui								
37	30/09/2010 16:05	Sim		WPA2	Mobilidade	Custo elevados nos	Não faço	Sim	Não	Sim	Não
38	30/09/2010 17:01	Sim		WPA2	Mobilidade	Velocidade de	Não faço	Sim	Não	Sim	Não
39	01/10/2010 16:00	Sim		WPA2	Sem custos com	Velocidade de	Não faço	Sim	Não	Sim	Não