

**UNIVERSIDADE LUTERANA DO BRASIL
CURSO DE SISTEMAS DE INFORMAÇÃO
CAMPUS GUAÍBA**



**Projeto de uma rede sem fio (wireless),
implementando sistemas
de segurança (firewall e proxy).**

Geandré Meller Zacher

Relatório de atividades desenvolvidas durante o Estágio Supervisionado e apresentada ao Curso de Sistemas de Informação da Universidade Luterana do Brasil, campus Guaíba, como pré-requisito para a obtenção do título de Bacharel em Sistemas de Informação.

Supervisor: Prof. Luiz Gustavo Galves Mahlmann

Guaíba, Dezembro de 2006.

Epígrafe

"Nunca se afaste dos seus sonhos, pois se eles se foram você continuara vivendo, mas terá deixado de existir". (charles chapli)

Dedicatória

Dedico este trabalho a todos aqueles que me ajudaram, de uma forma ou de outra, a chegar até aqui.

Agradecimentos

Agradeço a Deus pela oportunidade de finalizar este trabalho.

Agradeço aos meus pais, por sempre acreditarem em mim e no meu potencial, sempre me apoiando e me fornecendo tudo o que eu precisava para concluir este trabalho.

Agradeço ao meu irmão pelo apoio me concedido e as dúvidas de metodologia em que ele me ajudou.

Agradeço ao meu orientador, Prof^o Luiz Gustavo Galves Mahlmann, pelas críticas, pois me ajudaram a melhorar, pelos elogios, que me motivaram a continuar trabalhando nesta pesquisa, por ter sido tão prestativo e atencioso, sempre estando pronto para me atender e me ajudar com qualquer que fosse minha dúvida e dificuldade.

Um forte abraço a todos.

Sumário

Epígrafe.....	2
Dedicatória	3
Agradecimentos	4
Lista de Figuras.....	7
Lista de Abreviações	7
Resumo.....	9
1. Introdução	11
1.1 Motivação	12
1.2 Objetivo	12
1.3 Metodologia Utilizada	13
2. Apresentação da Empresa	13
2.1 New Holland no Brasil e no Mundo	13
2.2 New Holland em Camaquã.....	15
2.2.1 Localização.....	15
2.2.2 Histórico.....	15
2.3 ORGANOGRAMA DA ESTRUTURA ADMINISTRATIVA.....	17
3. Referencial Teórico	18
3.1 Tipos de rede Sem Fio	20
3.2 Segurança de Redes Wireless	22
3.2.1 Posicionamento Físico.....	23
3.2.2 Configurações.....	24
3.2.2.1 Configuração Aberta	24
3.2.2.2 Configuração Fechada.....	24
3.2.5 Endereçamento Físico	25
3.2.6 Criptografia	26
3.2.6.1 WEP	26
3.2.6.2 WPA.....	27
3.2.6.2.1 Mecanismos de Criptografia WPA.....	28
3.2.7 VPN	29
3.3 Softwares Complementares	31
3.3.1 Firewall	31
3.3.2 Proxy	32

3.3.3 Wireless Switch Manager	33
4. Analise de Requisitos.....	33
4.1 Levantamento dos Dados	33
4.1.1 Entrevista	33
5. Requisitos de Hardware	35
6. Requisitos de Software	35
7. Projeto	35
7.1 Implantação Dos Access Points	36
7.2 Implantação Do Proxy	37
7.3 Implantação Do Firewall	40
8. Investimentos	42
9. Conclusão	43
10. Referencial Bibliográfico.....	44
11. Glossário	47

Lista de Figuras

FIGURA 1: BRASÃO DA NEW HOLLAND	14
FIGURA 2: CLASSIFICAÇÃO PELA ABRANGÊNCIA DAS REDES SEM FIO.....	19
FIGURA 3: REDE SEM FIO NO MODO DE INFRA-ESTRUTURA.	22
FIGURA 4: REDE SEM FIO NO MODO <i>AD HOC</i>	22
FIGURA 5: DISPOSIÇÃO DOS ACCESS POINT'S.....	36

Lista de Abreviações

AP	<i>Access Point</i>
ARP	<i>Address Resolution Protocol</i>
AES	<i>Advanced Encryption Standard</i>
BSS	<i>Basic Service Set</i>
CRC-32	<i>Cyclic Redundancy Check</i>
D.o.S	<i>Denial Of Service</i>
DHCP	<i>Dynamic Host Configuration Protocol</i>
EFS	<i>Encrypted File System</i>
ESS	<i>Extended Service Set</i>
EAP	<i>Extensible Authentication Protocol</i>
EAP-LEAP	<i>Extensible Authentication Protocol - Lightweight Extensible Authentication Protocol</i>
EAP-TLS	<i>Extensible Authentication Protocol - Transport Layer Security</i>
EAP-TTLS	<i>Extensible Authentication Protocol - Tunneled Transport Layer Security</i>
FTP	<i>File Transfer Protocol</i>
GHz	<i>Gigahertz</i>
IAS	<i>Internal Authentication Server</i>
ICP	<i>Infra-estrutura de chaves públicas</i>
IEEE	<i>Institute of Electrical and Electronic Engineers</i>
ICV	<i>Integrity Check Value</i>
IPSec	<i>Internet Protocol Security</i>
ISM	<i>Industrial, Scientific and Medical</i>
LAN	<i>Local Area Network</i>
MAC	<i>Media Access Control</i>
Mbps	<i>Megabits per second</i>
MIC	<i>Message Integrity Code</i>
MSCHAPv2	<i>Microsoft Challenge-Handshake Authentication Protocol v. 2</i>
NetBEUI	<i>NetBIOS Extended User Interface</i>
NetBIOS	<i>Network Basic Input/Output System</i>
OSI	<i>Open Systems Interconnection</i>
PCI	<i>Peripheral Component Interconnect</i>
PCMCIA	<i>Personal Computer Memory Card International Association</i>
PEAP	<i>Protected Extensible Authentication Protocol</i>

RADIUS	<i>Remote Authentication Dial-In User Server</i>
RC4	<i>Route Coloniale 4</i>
SSID	<i>Service Set Identifier</i>
STA	<i>Stations</i>
TKIP	<i>Temporal Key Integrity Protocol</i>
USB	<i>Universal Serial Bus</i>
VPN	<i>Virtual Private Network</i>
WPA	<i>Wi-Fi Protected Access</i>
WPA-PSK	<i>Wi-Fi Protected Access - Pre-Shared Key</i>
WPA-PSK.TKIP	<i>Wi-Fi Protected Access - Pre-Shared Key. Temporal Key Integrity Protocol</i>
WEP	<i>Wired Encryption Protocol</i>
WLAN	<i>Wireless Local Area Network</i>
WLL	<i>Wireless Local Loop</i>
WMAN	<i>Wireless Metropolitan Area Network</i>
WPAN	<i>Wireless Personal Area Network).</i>
WWAN	<i>Wireless Wide Area Network</i>
Wi-Fi	<i>Wireless-Fidelity</i>
WiMAX	<i>Worldwide Interoperability for Microwave Access</i>

Resumo

Tendo em vista a oportunidade de desenvolvimento deste projeto para empresa FORTRAL, visando obter diversos benefícios a curto e longo prazo no que diz respeito a uma nova tecnologia na área de redes, com a preocupação de implementar medidas de segurança.

Este projeto vem para somar benefícios a esta empresa, dado enfoque ao desenvolvimento de uma proposta, que altera o estado atual da rede interna de computadores (cabos) para rede sem fio (wireless), acrescentando um firewall e um proxy para segurança da rede e dos dados que trafegam na mesma.

Devido ao constante crescimento da empresa, sendo que há bastante alteração do quadro físico dos computadores, este projeto se dispõe em resolver este problema e projetar uma estrutura de rede sem fio, que comportará novas conexões.

Palavras-chaves: Wireless, Firewall, Proxy, VPN.

1. Introdução

Atualmente a FORTRAL, empresa de porte médio no que se refere a sistemas computacionais, porém em crescimento constante, sendo uma empresa consolidada a mais de 10 anos no ramo agrícola, que carrega a marca New Holland seguindo todas as suas exigências.

Devido ao constante crescimento da empresa, as suas exigências tecnológicas passaram a ser maiores, principalmente no que se refere à área de redes de computadores. A partir disso este projeto pretende propor uma solução viável e de custo acessível.

A proposta deste projeto visa efetuar a migração da rede atual (cabos) para uma rede sem fio (wireless) com possibilidades de expansão. Por ser uma nova tecnologia, também será incluído um módulo para garantir a segurança dos dados trafegados nesta rede, já que a comunicação dá-se da através de ondas de rádio.

O projeto preocupar-se-á em obter uma solução considerada segura que corresponda a um sistema que funcione conforme o esperado, portanto, o sistema deve possuir:

Confidencialidade – quem não possui autorização para acessar determinada informação não deve ser capaz de fazê-lo;

Integridade de dados – para alterar ou apagar uma determinada informação é necessário autorização e, quem não possui esta autorização não deve ter a possibilidade de fazê-lo;

Disponibilidade – o serviço deve estar operacional e correto quando requisitado;

Consistência – o sistema deve comportar-se conforme o projetado;

Controle – nenhum usuário deve ser capaz de realizar ações não autorizadas sem ser detectado;

Auditoria – ações intencionais contra o sistema, ou usuários autorizados que cometem erros não intencionais devem ser identificados.

1.1 Motivação

O principal eixo motivador para o desenvolvimento deste projeto foi sem dúvida perceber as dificuldades e apontar os ganhos:

Dificuldades:

- Expansão constante X Estrutura;
- Estar preso ao número de pontos existentes;
- Tecnologia limitada;
- Falta de mobilidade;
- Manutenção da estrutura física da rede;

Ganhos com o projeto:

- Mobilidade;
- Estrutura flexível para expansão da empresa;
- Utilização de uma tecnologia atualizada;
- Manutenção facilitada;

1.2 Objetivo

Dentre os muitos objetivos existentes para realização deste projeto posso ressaltar os seguintes:

- Definir políticas de segurança através da utilização de Proxy e Firewall;
- Definir a localização dos Access Point possibilitando a expansão para novos equipamentos;
- Projeto visando facilitar a manutenção da rede;

1.3 Metodologia Utilizada

O método de pesquisa utilizado para este trabalho foi à pesquisa documental, fazendo-se através de referências bibliográficas disponíveis em livros, revistas, *sites* e artigos *online*.

Este projeto é qualitativo, buscando propor soluções para os problemas observados na empresa FORTRAL no que se refere a reestruturação e segurança da rede com e implementação de um firewall e um proxy.

2. Apresentação da Empresa

2.1 New Holland no Brasil e no Mundo

Uma pequena oficina de consertos, localizada na cidade de New Holland, na Pensilvânia, criada no final do século XIX pelo mecânico Abert Zimmerman, representou o nascimento de uma companhia que um dia se tornaria uma grande marca, com forte presença em todos os continentes.

Na década de 50, o belga chamado John Clayer, fabricante de colheitadeiras, criou uma empresa em sociedade com seus filhos, a Clayson. Esta empresa foi comprada pela norte-americana New Holland.

Em 1917, também nos Estados Unidos era fabricado o primeiro trator Ford.

Em outubro de 1986 a divisão da Ford Motor Company adquire a fábrica de colheitadeiras New Holland, formando a Ford New Holland. Os tratores continuariam a ser fabricado sob o nome Ford, enquanto que as colheitadeiras assumiriam o nome Ford New Holland.

Dois anos mais tarde, em 1988, o Grupo Fiat adquire a Ford New Holland, passando então a adotar a marca New Holland para todos os produtos. Além das colheitadeiras, os tratores agrícolas passariam a chamar-se New Holland.

Em 1919, o Brasil começa a importar seus primeiros tratores, sendo estes da marca que mais tarde vem a ser New Holland (vide figura 1). O Brasil continuou a importar seus tratores até 1960, quando foi produzido o primeiro trator inteiramente fabricado no Brasil, também com esta mesma marca.



Figura 1: Brasão da New Holland

No Brasil, as primeiras colheitadeiras New Holland chegaram no início da década de 70, marcando uma forte relação entre as máquinas amarelas e o homem do campo. O sucesso foi tão grande que a empresa se instalou no Brasil, inaugurando a fábrica da New Holland Latino-Americana em Curitiba, em 1975.

A New Holland trouxe modernidade e inovação ao setor no País e foi conquistando mais espaço à medida em que a nossa agricultura crescia e se profissionalizava. A diversidade da agricultura brasileira impulsionou a New Holland a se desenvolver e a atender, cada vez melhor, às suas especificidades.

Somando hoje mais de trinta anos de Brasil, a New Holland pode dizer que participou e viu bem de perto o desenvolvimento do agronegócio brasileiro, cobrindo os campos de azul e amarelo.

Líder mundial em equipamentos agrícolas, a New Holland é um dos maiores e mais respeitados fabricantes de equipamentos agrícolas. Para atender especificamente a cada tipo de necessidade dos produtores de todos os portes, a New Holland produz uma ampla e completa linha de tratores de pequena, média e grande potência, além de colheitadeiras de grãos e implementos.

Em qualquer ponto do planeta, a New Holland garante desempenho e alta qualidade em todos os produtos que levam a sua marca. A cada 5 tratores vendidos no mundo, um é New Holland. E suas colheitadeiras, referência em tecnologia, eficiência e produtividade, são as mais vendidas na América Latina. Esta grande conquista de mercado se deve ao constante investimento da New Holland em novos produtos destinados a todos os segmentos de atividades agrícolas.

Presente em todos os continentes, com uma rede de mais de 5 mil concessionários, a New Holland apresenta uma forte e eficiente estrutura de pós-vendas que garante a alta qualidade, a tecnologia e a segurança dessa marca mundial.

2.2 New Holland em Camaquã

2.2.1 Localização

A filial da New Holland em Camaquã é a FORTRAL Comércio de Maquinas e Equipamentos Agrícolas Ltda, que está localizada na Av. José Loureiro da Silva, N° 1393, bairro Carvalho Bastos no município de Camaquã / RS. O município de Camaquã possui um total de 1.680 Km².

A população estimada é de 63.128 habitantes, sendo que possui 47.069 residentes na sede do município e outras áreas urbanizadas e 16.059 na área rural. Sua densidade demográfica é de 37 habitantes/Km².

O município faz divisa ao norte com os municípios de São Jerônimo, Barão do Triunfo, Cerro Grande do Sul. Ao sul com os municípios de Cristal e São Lourenço, ao leste com os municípios de Tapes, Arambaré e Laguna dos Patos e a oeste com os municípios de Chuvisca e Dom Feliciano.

Sua economia é gerada através da agricultura, provenientes das seguintes culturas: arroz, tabaco, soja e milho.

2.2.2 Histórico

O casal Solismar Paulo Freitas Fonseca, pecuarista e agricultor, e Gisela Longaray Fonseca, engenheira civil, resolveram diversificar suas atividades profissionais e adquiriram a empresa Fortral – Fornecedoras de Tratores. Em 16 de Maio de 1994 iniciou-se as atividades da então Fortral Comércio de Máquinas e Equipamentos Agrícolas Ltda, localizada na Av. José Loureiro da Silva, nº 1393,

nesta cidade, sendo esta, uma concessionária da marca New Holland Latin Americana Ltda.

Decorridos 10 anos de efetiva participação num mercado competitivo cujas políticas governamentais no setor agrícola sempre foram de altos e baixos e muitas incertezas, exigindo um constante aprimoramento de atendimento à sua clientela, a empresa, hoje, tem um excelente posicionamento no mercado local. Este espaço constituí-se no abastecimento de 18 municípios da região centro sul, com a distribuição de produtos da marca New Holland, com serviços da marca Fortral. Tudo com suporte de uma estrutura qualificada, de uma equipe de pessoas alinhadas com os objetivos traçados pela diretoria.

Visando sempre manter-se com alto conceito entre os clientes da região que atende, zelando pela marca a qual representa, a empresa tem a preocupação constante em investimentos com tecnologia, informação e treinamento de pessoal para melhor servir seu mercado, consolidando assim seu nome.

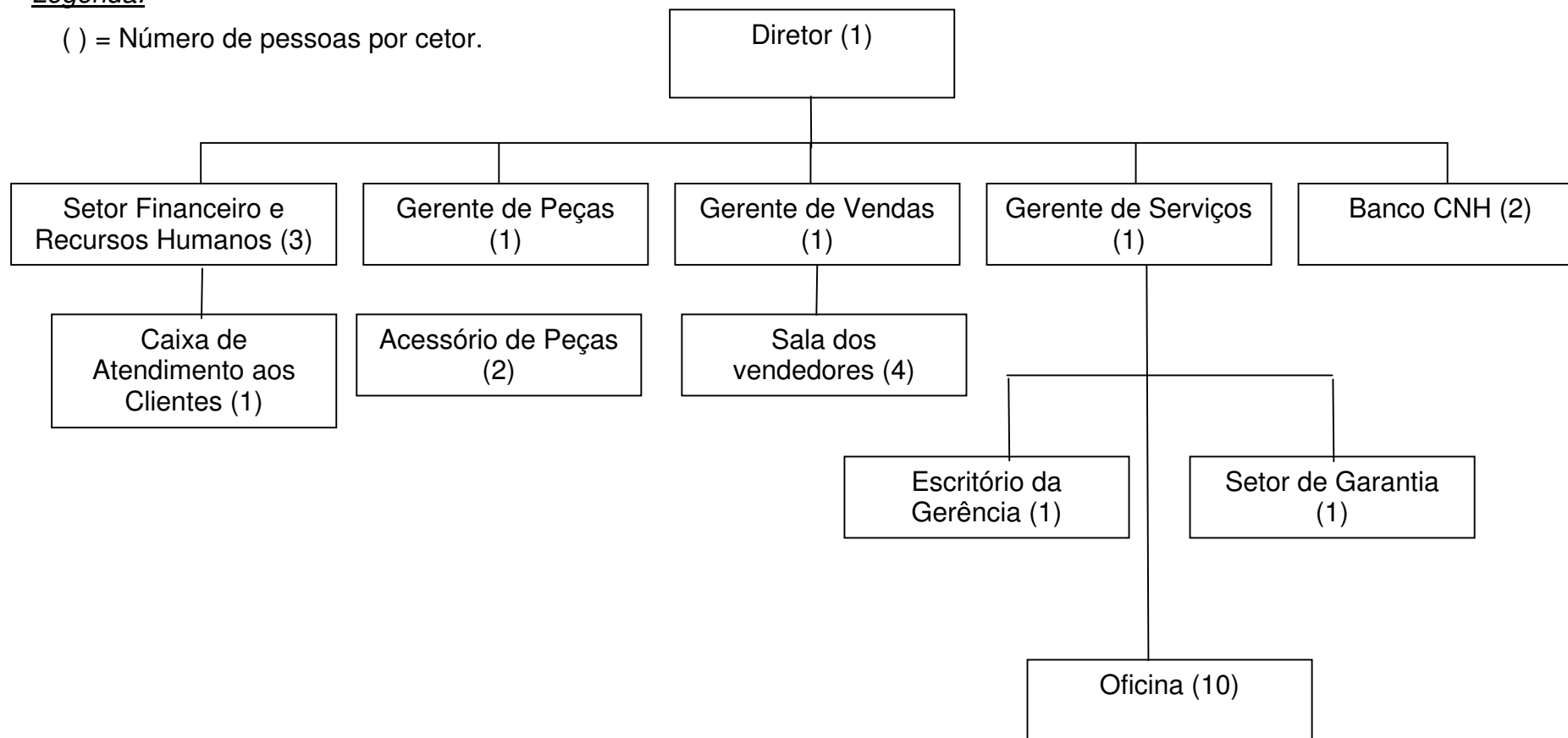
A empresa também conta com importantes fornecedores de implementos como a Marchesan S/A, que sustenta a renomada marca Tatu, Jacto S/A especialista em pulverizadores, Semeato S/A especialista em plantadeiras, entre outras. E também FL Brasil S/A, fornecedora de lubrificantes, Ferramentas Gerais, entre diversos parceiros que dão suporte ao departamento de peças.

Além de oferecer uma equipe de profissionais especializados para dar assistência técnica necessária, visando sempre a satisfação total do cliente tanto com a marca New Holland como com a marca Fortral.

2.3 ORGANOGRAMA DA ESTRUTURA ADMINISTRATIVA

Legenda:

() = Número de pessoas por setor.



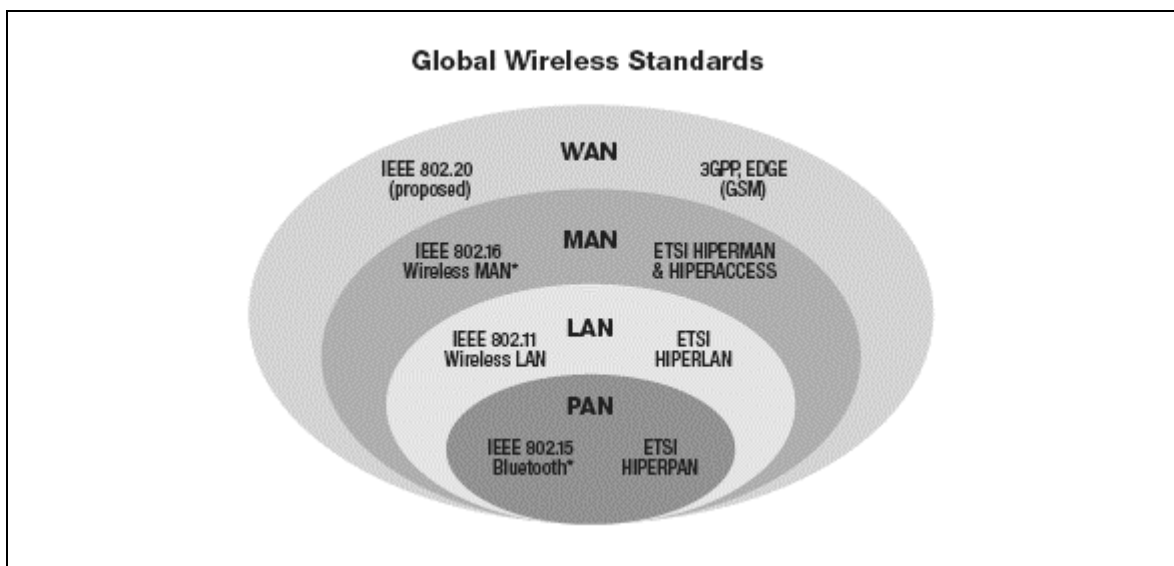
3. Referencial Teórico

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

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

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

Encaixam-se nessa categoria os seguintes tipos de rede: Locais Sem Fio ou WLAN (*Wireless Local Area Network*), Redes Metropolitanas sem Fio ou WMAN (*Wireless Metropolitan Area Network*), por exemplo o WiMAX (*Worldwide Interoperability for Microwave Access*), Redes de Longa Distância sem Fio ou WWAN (*Wireless Wide Area Network*), redes WLL (*Wireless Local Loop*) e o novo conceito de Redes Pessoais Sem Fio ou WPAN (*Wireless Personal Area Network*). (ARTHAS, 2004)



Fonte: TEIXEIRA (2005)

Figura 2: Classificação Pela Abrangência das Redes Sem Fio

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

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

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

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

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

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

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

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

Grupo 802.11f – Está a desenvolver *Inter-Access Point Protocol* (Protocolo de acesso entre pontos), por causa da corrente limitação de proibir *roaming* entre pontos de acesso de diferentes fabricantes. Este protocolo permitiria dispositivos sem fios passar por vários pontos de acesso feitos por diferentes fabricantes.

Grupo 802.11g – Estão a trabalhar em conseguir maiores taxas de transmissão na banda de rádio 2,4GHz.

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

3.1 Tipos de rede Sem Fio

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

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

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

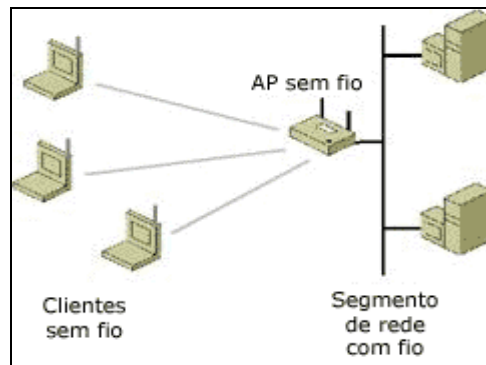
AP - *Access Point* - funciona como uma *bridge* entre a rede *wireless* e a rede tradicional. Coordena a comunicação entre as STA dentro da BSS. Existem APs que também atuam como roteador, possibilitando o compartilhamento de *Internet* pelos outros micros da rede. Eles vêm de fábrica como servidores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

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

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

Dois modos de operação são previstos:

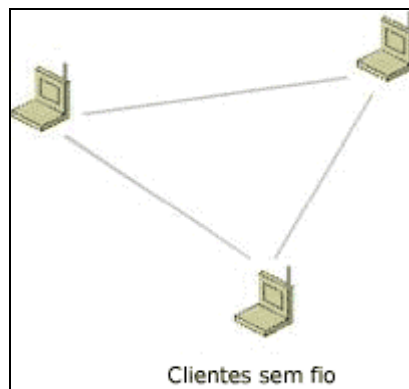
Infrastructure mode - quando existe a presença de um AP coordenando a comunicação entre as estações de uma célula (BSS). (ARTHAS, 2004)



Fonte: Microsoft Brasil (2005)

Figura 3: Rede sem fio no modo de infra-estrutura

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



Fonte: Microsoft Brasil (2005)

Figura 4: Rede sem fio no modo Ad Hoc

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

3.2 Segurança de Redes Wireless

“A explosão das redes sem fio não é nenhuma surpresa para as empresas atuais. Isso se deve ao grande aumento de produtividade que as tecnologias sem fio proporcionam o que é difícil de ser ignorado. Em um recente estudo, a Gartner descobriu que funcionários com *notebooks* atingiram um aumento de produtividade de meia hora a três horas, comparado aos usuários de *desktops*. Quando a conexão sem fio é adicionada a esses notebooks, ocorre um aumento de até 11 horas de produtividade adicional por semana.

Porém, as redes sem fio vêm também acompanhadas de desvantagens significativas e talvez a segurança seja a principal delas. Conforme observou Laura Garcia-Manrique, gerente da *Group Product - Wireless* da Symantec, a segurança é um dos três maiores problemas enfrentados por gerentes de TI, com relação às redes sem fio e computação remota.

Ela afirma que os principais problemas de segurança com relação aos sistemas sem fio incluem:

- Intercessão de transmissão sem fio à medida que viaja via aérea.
- Perda de um dispositivo portátil, comprometendo os dados nele contidos.
- "Relacionamentos de confiança" quando os dispositivos sem fio são usados para comércio (por exemplo, para a o envio de pedidos ou compras).

Para lidar com esses problemas, Garcia-Manrique afirma que as empresas precisam determinar procedimentos muito específicos para o uso de dispositivos sem fio, incluindo as funções para as quais os mesmos podem ser usados, o que pode ou não ser armazenado e qual a tecnologia de segurança que deve estar instalada, para evitar que os dados sejam comprometidos, no caso de roubo do dispositivo.

A definição de políticas e padrões para os dispositivos sem fio é imprescindível, de acordo com Garcia-Manrique. Por exemplo, sempre que uma LAN sem fio for ativada, a tecnologia VPN deve ser implementada. Além disso, notebooks com recursos sem fio devem ter proteção antivírus e de *firewall* instaladas.

Mas a segurança não termina aí. Uma rede sem fio pode realizar transmissões em distâncias muito além de um prédio, permitindo a qualquer um que esteja por perto ou até mesmo passando perto de uma instalação, espreitar dados. Só é necessária uma antena potente e um software de hacker facilmente disponível no mercado.” (SYMANTEC, 2003)

Segundo DUARTE (2003), a rede deve estar operante e garantir:

- Confiabilidade – O sinal transmitido pela rede pode ser captado por qualquer receptor atuante na área em que o sinal estiver ativo.
- Integridade da Informação – Garantir que os dados trafegados na rede não sejam alterados entre o receptor e o transmissor.
- Disponibilidade da Rede – Manter a rede acessível.
- Autenticidade – Fazer com que a autenticação para o acesso à rede ocorra.

3.2.1 Posicionamento Físico

Segundo RUFINO (2005), a segurança física em uma rede cabeada era constituída em proteger o acesso físico a um computador que estivesse ligado à rede ou mesmo, proteger ou desativar um ponto de rede não utilizado.

Para este tipo de segurança, basta proteger o acesso das pessoas, mas, em uma rede sem fio, onde os dados trafegam pelo ar, o perímetro a ser coberto pela segurança seria de metros e metros, as vezes, além das paredes da empresa. (RUFINO, 2005)

Para acessar uma rede sem fio, basta estar munido de dispositivos de acesso a ela e se posicionar de forma a obter um sinal cuja potência permita uma conexão.

Para ajudar a minimizar o problema de acesso não permitido, algo a se levar em conta quando se for construir uma rede sem fio é a posição do *Access Point*, para que as ondas eletromagnéticas fiquem centralizadas, minimizando a área coberta pela rede fora do perímetro desejado. (RUFINO, 2005)

3.2.2 Configurações

Os concentradores, também conhecidos por *Access Point*, são, em geral, pré-configurados ainda na fábrica, para facilitar a instalação da rede. (RUFINO, 2005)

Conforme BALIEIRO (2004), publicado na revista INFO Exame (n° 218 ANO 19 Maio/2004 – Redes *Wi-Fi*), após a instalação da rede, por falta de conhecimento ou simplesmente por desatenção e despreocupação, as pessoas não alteram as configurações de fábricas dos concentradores.

As configurações de fábricas não habilitam os mecanismos de segurança, tornando o tráfego da rede mais vulnerável a um ataque. (RUFINO, 2005)

Praticamente todos os aparelhos possuem uma configuração padrão de fábrica, desde de o SSID (*service set identifier*), endereços IPs e senhas, por tanto, o acesso indevido a rede se torna fácil e simples. (RUFINO, 2005)

3.2.2.1 Configuração Aberta

De acordo com RUFINO (2005), este tipo de configuração é caracterizado pelo envio do SSID da rede pelo concentrador, ou seja, ele aceita conexões de qualquer pessoa cuja compatibilidade de hardware seja atendida.

Ao requisitar conexão, o concentrador possui um servidor DHCP (*Dynamic Host Configuration Protocol*), provendo um endereço IP válido para a rede, liberando o acesso à ela. (RUFINO, 2005)

3.2.2.2 Configuração Fechada

Neste modo de configuração, o concentrador não envia o seu SSID, portanto, só permitindo conexão aqueles que souberem o SSID da rede. (RUFINO, 2005)

Para um atacante (pessoa sem autorização que pretende entrar numa rede privada, com segundas intenções), basta “escutar” o tráfego desta rede para determinar seu SSID correto, podendo assim acessar a mesma. (RUFINO, 2005)

3.2.5 Endereçamento Físico

Outra forma de proteção de acesso a uma rede *wi-fi*, segundo RUFINO (2005), é definir os endereços físicos acessíveis a esta.

Endereçamento físico, também conhecido por endereçamento MAC, faz parte da camada de Enlace do modelo OSI (*Open Systems Interconnection*). (GUERRA, 2002)

Todo dispositivo de rede possui um endereçamento físico (*Media Access Control*). Antigamente, os endereços físicos não eram únicos, os fabricantes produziam placas cujos endereços físicos eram iguais, ocasionando alguns conflitos. Atualmente, todo dispositivo de rede possui um endereço físico único. (GUERRA, 2002)

Pode-se configurar um concentrador para receber conexões apenas dos endereços físicos definido pelo administrador. Este dispositivo autentica apenas o equipamento e não o usuário, tornando possível que uma pessoa não autorizada a utilizar a rede a utilize por meio de um equipamento que tem o acesso liberado à mesma. (RUFINO, 2005)

Existem algumas desvantagens em utilizar este tipo de autenticação, pois, é necessário obter manualmente os endereços físicos e cadastrá-los manualmente no concentrador. (RUFINO, 2005)

Além de trabalhoso, as alterações podem ser mais freqüentes dependendo da alternância entre os usuários.

Para se conectar a uma rede *w-fi* é necessário ter um dispositivo que atenda os padrões da rede, como placas PCI (internas), adaptadores USB, adaptadores *Ethernet* e cartões e placas PCMCIA.

Em geral, estes dispositivos são portáteis e removíveis, ou seja, uma pessoa mal intencionada pode obter um *hardware* que tem permissão para acessar a rede e plugá-lo em seu computador, obtendo assim, o acesso a rede.

Outra desvantagem é que por obtenção do tráfego, que contem o endereço MAC dos dispositivos, o atacante com um endereço físico válido de acesso à rede pode renomear o endereço físico de sua placa e obter o acesso. (RUFINO, 2005)

Para alterar o endereço físico no *Windows* (somente as versões 2000, XP e 2003), segundo RUFINO (2005), utiliza-se o caminho: conexões de rede, propriedades da rede local, configurar, avançado e *NetwrokAddress*.

Um outro modo de obter um endereço MAC válido é utilizar a força bruta, testando repetidamente endereços MAC aleatórios, podendo criar uma lista de acesso para determinada rede.

3.2.6 Criptografia

Uma forma de proteção aos dados trafegados na rede é a criptografia. Caso um atacante tente obter os dados trafegados na rede, a criptografia vai cuidar de deixar todos os dados fora de uma ordem lógica e entendível. (ENGST & FLEISHMAN, 2005)

3.2.6.1 WEP

O *Wired Equivalency Privacy* (WEP), segundo a Microsoft, é o método criptográfico usado nas redes *wireless* 802.11. O WEP opera na camada de enlace de dados e fornece criptografia entre o cliente e o *Access Point*. O WEP é baseado no método criptográfico RC4 (*Route Coloniale* 4) da RSA, que usa um vetor de inicialização (IV) de 24 bits e uma chave secreta compartilhada (*secret shared key*) de 40 ou 104 bits. O IV é concatenado com a *secret shared key* para formar uma chave de 64 ou 128 bits que é usada para criptografar os dados. Além disso, o WEP utiliza CRC-32 (*Cyclic Redundancy Check*) para calcular o *checksum* da mensagem, que é incluso no pacote, para garantir a integridade dos dados. O receptor então recalcula o *checksum* para garantir que a mensagem não foi alterada.

Surge então o WEP que traz como promessa um nível de segurança equivalente à das redes cabeadas. Na prática o WEP também tem suas falhas, mas não deixa de ser uma camada de proteção essencial, muito mais difícil de

penetrar que o SSID e a lista de endereços físicos permitidos, também conhecido por endereço MAC (*Media Access Control*).

O WEP se encarrega de encriptar os dados transmitidos através da rede. Existem dois padrões WEP, de 64 e de 128 bits. O padrão de 64 bits é suportado por qualquer ponto de acesso ou interface que siga o padrão *Wi-Fi*, o que engloba todos os produtos comercializados atualmente. O padrão de 128 bits por sua vez não é suportado por todos os produtos. Para habilitá-lo será preciso que todos os componentes usados na sua rede suportem o padrão, caso contrário os nós que suportarem apenas o padrão de 64 bits ficarão fora da rede. (MICROSOFT, 2004)

Segundo RUFINO (2005), alguns programas já largamente disponíveis são capazes de quebrar as chaves de encriptação caso seja possível monitorar o tráfego da rede durante algumas horas e a tendência é que estas ferramentas se tornem ainda mais sofisticadas com o tempo. Como disse o WEP não é perfeito, mas já garante um nível básico de proteção. Esta é uma chave que foi amplamente utilizada, e ainda é, mas que possui falhas conhecidas e facilmente exploradas por softwares como *AirSnort* ou *WEPCrack*. Em resumo o problema consiste na forma com que se trata a chave e como ela é "empacotada" ao ser agregada ao pacote de dados.

O WEP vem desativado na maioria dos pontos de acesso, mas pode ser facilmente ativado através do utilitário de configuração. O mais complicado é que será preciso definir manualmente uma chave de encriptação (um valor alfanumérico ou hexadecimal, dependendo do utilitário) que deverá ser a mesma em todos os pontos de acesso e estações da rede. Nas estações a chave, assim como o endereço SSID e outras configurações de rede podem ser definidas através de outro utilitário, fornecida pelo fabricante da placa. (RUFINO, 2005)

3.2.6.2 WPA

De acordo com Eduardo PRADO, Comunidade *Wireless* Brasil (2005), com os problemas de segurança no WEP, a *Wi-Fi Alliance* adiantou a parte de autenticação e certificação elaboradas para o 802.11i e liberou o protocolo WPA (*Wi-Fi Protected Access*).

Apesar de avanços terem ocorridos nesse protocolo, a maioria deles requer novos elementos na infra-estrutura da rede e ainda deve trabalhar em conjunto com outros protocolos, como o 802.1x.

Na versão 1 do WPA não há suporte à conexões *Ad-Hoc*, portanto, apenas as redes utilizando um concentrador podem fazer uso deste recurso.

O WPA atua em duas áreas. A primeira é a qual substitui o WEP, cifrando os dados e garantindo a privacidade do tráfego, e a segunda, autentica o usuário, utilizando para isso padrões 802.1x e EAP (*Extensible Authentication Protocol*).

3.2.6.2.1 Mecanismos de Criptografia WPA

O WPA (*Wi-Fi Protected Access*) possui diferentes modelos de segurança, adaptável ao tipo do uso em que ele será implementado, uma para aplicações pequenas, como redes domésticas e pequenos escritórios, utilizando uma chave previamente compartilhada (Pré-shared key ou WPA-PSK), sendo responsável pelo reconhecimento do aparelho. Outro método é conhecido como infra-estrutura, adicionando um servidor RADIUS (*Remote Authentication Dial-In User Server*) para autenticação, podendo ainda necessitar de uma infra - estrutura de chaves públicas (ICP), caso se utilize certificados digitais para autenticar usuários. (RUFINO, 2005)

O método de chave compartilhada é semelhante ao WEP, onde a troca de chaves é feita manualmente, fazendo com que seu uso se torne melhor adequado em redes pequenas onde os participantes estão acessíveis na maior parte do tempo. Não existem ainda problemas divulgados nos protocolos usados com WPA-PSK.TKIP, responsável pela troca dinâmica das chaves. (RUFINO, 2005)

O protocolo TKIP (*Temporal Key Integrity Protocol*) é o responsável pelo gerenciamento da troca de chaves, no WEP as chaves eram estáticas e seu vetor de inicialização era de apenas 24bits, passando agora para 48bits. (RUFINO, 2005)

O TKIP pode ser programado para alterar o vetor de inicialização a cada pacote, por sessão ou por período, tornando mais difícil a obtenção do mesmo via captura de tráfego.

“Com 802.11 e WEP, a integridade dos dados é fornecida por um valor de verificação de integridade, o ICV (*Integrity Check Value*) de 32-bit que aparece com a carga útil 802.11 e é criptografado com WEP. Embora o ICV esteja criptografado, pode-se alterar os bits na carga criptografada e atualizar o ICV criptografado sem ser detectado pelo receptor.

Com WPA, um método conhecido como *Michael*, especifica um novo algoritmo que calcula um código de integridade da mensagem, o MIC (*Message Integrity Code*) de 8 bytes usando os recursos de cálculo disponíveis nos dispositivos existentes. O MIC está localizado entre a parte de dados do quadro 802.11 do IEEE e o ICV de 4 bytes. O campo MIC é criptografado com os dados do quadro e o ICV.

Michael também ajuda a fornecer proteção à reexecução. Para ajudar a evitar ataques de repetição, é usado um novo contador de quadros no IEEE 802.11.” (SUPPORT MICROSOFT, 2005)

No WPA também foi inserido um modelo para autenticação de usuários, conhecido como EAP (*Extensible Authentication Protocol*), que utiliza o padrão 802.11x e permite vários métodos de autenticação, incluindo a possibilidade de certificação digital. Este padrão pode ser utilizado em conjunto com outras tecnologias existentes, como o servidor de autenticação RADIUS. (SUPPORT MICROSOFT, 2005)

Uma das vantagens em se utilizar equipamentos adicionais para a autenticação do usuário é de ter uma base centralizada, onde todos os métodos de acesso (não apenas wi-fi, mas cabeadas e/ou discadas também) utilizem a mesma forma, sem a necessidade de manter uma sincronização. (SUPPORT MICROSOFT, 2005)

3.2.7 VPN

Virtual Private Network ou Rede Privada Virtual é uma rede privada construída sobre a infra-estrutura de uma rede pública, normalmente a *Internet*. (SANTOS, 2001)

O sigilo do tráfego da rede, a autenticação inicial dos usuários, a integridade das mensagens da rede sem fio serão garantidos através da implementação de uma VPN segura, para tanto utiliza-se do protocolo IPSec a fim de garantir a privacidade virtual da rede e a segurança das eletrônicas que por ela passam. (CARRIÓN, 2003)

Nesta arquitetura todo o tráfego entre as estações e o AP é encriptado independente do destino dos pacotes enviados pelas estações. A VPN poderia ser configurada de forma que somente alguns pacotes com endereços de destino definidos fossem encriptados. (CARRIÓN, 2003)

“No estabelecimento de um túnel IPSec (*Internet Protocol Security*) todo o pacote IP é protegido e todas as mensagens provenientes das estações saem com o endereço do AP como endereço de destino. Garante-se com esta última característica uma privacidade maior para os usuários, dificultando a análise passiva do tráfego da rede.” (CARRIÓN, 2003)

O servidor VPN pode se tornar um gargalo. Todo o acesso do cliente WLAN será canalizado pelo servidor. Os dispositivos VPN tradicionalmente atendem muitos clientes remotos de baixa velocidade. Ser solicitado a controlar a taxa de transferência de um grande número de clientes que funcionam na velocidade total da LAN significará que muitos dispositivos VPN não conseguirão atender mais de poucas dezenas ou centenas de clientes. (MICROSOFT, 2004)

O foco deste trabalho se prende a estudar métodos e processos que tornam uma comunicação sem fio no padrão IEEE 802.11. Uma VPN pode ser usada para qualquer tipo de meio de transmissão de dados (redes cabeadas, *wi-fi*, infravermelho, etc), portanto, para proteger as informações de uma rede *wi-fi* recomenda-se que se utilize dos protocolos de criptografia específicos para este tipo de rede (WEP ou WPA), pois possuem um determinado nível de segurança e não causam tanto impacto a performance da rede quanto uma VPN causa.

3.3 Softwares Complementares

3.3.1 Firewall

Segundo Luiz Carlos dos Santos, *firewall* é o mecanismo de segurança interposto entre a rede interna e a rede externa com a finalidade de liberar ou bloquear o acesso de computadores remotos aos serviços que são oferecidos em um perímetro ou dentro da rede corporativa. Este mecanismo de segurança pode ser baseado em hardware, software ou uma mistura dos dois.

A função do *firewall* é bloquear tráfego malicioso, que poderia colocar em risco os computadores da rede. Eles examinam o tráfego a fim de procurar por certos padrões ou se tem por alvo recursos vulneráveis. O tráfego que possui os padrões definidos são descartados para que não cheguem ao seu destino final. (ENGST & FLEISHMAN, 2005)

“A maioria dos *Gateways (access point)* oferece recursos de *firewall* que permitem filtrar tipos específicos de tráfego, como aquele destinado a um dado serviço *Internet*. A maioria desses *firewalls* é simples, permitindo limitar todo o tráfego que entra que não seja uma resposta a uma solicitação feita ou a serviços *Internet* específicos, como FTP.

Como boa parte dos *gateways* também inclui múltiplas portas *Ethernet*, você pode criar um *firewall* não apenas entre sua conexão *Internet* de banda larga – conectada à porta de rede remota – e seus computadores e dispositivos sem fio, mas também entre a rede sem fio e quaisquer máquinas conectadas a portas *Ethernet* da rede local (LAN) no *gateway*”. (ENGST & FLEISHMAN, 2005)

Como opção para plataforma windows temos o software ISA Server que é um gateway integrado de segurança de borda que ajuda a proteger seu ambiente de TI das ameaças baseadas em Internet, ou seja é um firewall e um proxy integrados no mesmo produto. Uma de suas versões que possibilitam um melhor custo benefício é o ISA Server 2004 Standard Edition, que custa em torno de \$1.499 dólares por processador.

Como opção para plataforma Linux dispomos do iptables um firewall que vem junto com o sistema operacional linux, sendo assim tanto o sistema operacional quanto o firewall são distribuições sem custo nenhum e contam com uma vasta bibliografia.

3.3.2 Proxy

Um proxy é um software que armazena dados em forma de cache em redes de computadores. São máquinas com ligações tipicamente superiores às dos clientes e com poder de armazenamento elevado.

É de salientar que, utilizando um proxy, o endereço que fica registado nos servidores é o do próprio proxy e não o do cliente.

Por exemplo, no caso de um HTTP caching proxy, o cliente requisita um documento na World Wide Web e o proxy procura pelo documento em seu cache. Se encontrado, o documento é retornado imediatamente. Senão, o proxy busca o documento no servidor remoto, entrega-o ao cliente e salva uma cópia no seu cache.

O serviço de proxy consiste em manter, em uma área de acesso rápido, informações já acessadas. Geralmente, há um servidor dedicado para esse tipo de serviço.

Sempre que há uma requisição de serviços HTTP ou FTP, o servidor proxy captura os dados que o destinatário disponibiliza ao cliente (usuário) e os guarda em uma área em disco. Na próxima vez que este *site* for acessado, o *web browser* primeiro fará a procura no servidor proxy. Se os dados forem encontrados neste servidor, a transferência de dados se dará entre ele e o cliente (*web browser*). Se o servidor proxy não dispuser dos dados requisitados, o acesso será feito diretamente ao *site* de destino.

Como opção para plataforma windows temos o software ISA Server, que incorpora um firewall e um proxy integrados no mesmo produto, conforme já foi citado.

Como opção para plataforma Linux dispomos do Squid um proxy de fácil manuseio e configuração e que assim como o sistema operacional linux e o firewall Iptables são distribuições sem custo nenhum e contam com uma vasta bibliografia.

3.3.3 Wireless Switch Manager

O software Wireless Switch Manager trabalha com os controladores e switches para redes wireless centralizando o gerenciamento e o controle dos Access Points Gerenciados (MAPs) em redes com especificações de implantação complexas, como múltiplos escritórios ou severos requisitos de segurança para redes locais wireless.

4. Análise de Requisitos

4.1 Levantamento dos Dados

O levantamento de dados foi feito através da vivência com os funcionários da empresa FORTRAL e entrevista com os mesmos, como demonstrado logo abaixo. A entrevista foi sobre as necessidades e dificuldades que a empresa possuía na área de redes de computadores.

4.1.1 Entrevista

Foi realizada uma entrevista (em 7 de novembro de 2006, na empresa FORTRAL) com o funcionário, Fabio Laupes, para confirmar os dados levantados e identificar a sistemática atual, as suas necessidades e problemas.

1) Como funciona atualmente a rede física de computadores da FORTRAL?

R.: No processo atual a FORTRAL possui 13 computadores ligados em rede através de cabeamento comum(par trançado), contando com um servidor, switch e vários hub's.

2) Quais são os problemas que a empresa encontra neste tipo de rede?

R.: Os problemas que dão mais transtornos na nossa empresa são:

- Estar preso ao número de pontos existentes;
- Falta de mobilidade dos equipamentos;

- Grande dificuldade na manutenção da estrutura física da rede;

3) Quais as medidas de segurança que a empresa adota para proteção dos dados trafegados na rede?

R.: Atualmente não possuímos nenhum tipo de política de segurança para o gerenciamento dos dados que trafegam na rede.

4) Qual seria a sugestão para as necessidades encontradas?

R.: Acredito que com a implantação deste projeto todas as necessidades serão corrigidas, trazendo inúmeros benefícios a empresa.

Cenário Atual:

Podemos perceber no cenário atual da empresa FORTRAL, que houve diversas reestruturações na estrutura física da mesma, como novas salas e mudanças nos departamentos em todos os aspectos.

Problemas Encontrados:

Com estas mudanças sempre surgia o problema de migração dos computadores, pois se faz necessário refazer a rede de cabos para ligar os computadores novamente, além da rede antiga não possuir nenhum sistema de segurança vindo a sofrer com perda de dados e outros incômodos.

Necessidades:

Sendo este alguma das necessidades encontradas, a empresa procurava meio para contornar tal situação disponibilizando de recursos e incentivando novos investimentos, pois necessitava de mobilidade dos seus equipamentos computacionais, já que vinha tendo constantes reestruturações a nível físico, e perda de seus dados.

Sugestões:

Este projeto vem propor como sugestão a migração da rede atual (cabos) para uma rede sem fio (Wireless), com um modulo de segurança (porxy e

firewall), para que se possa sanar as necessidades e solucionar os problemas que foram levantados durante o projeto.

5. Requisitos de Hardware

Equipamento de desenvolvimento

- Computador AMD Athlon 2800+
- 1 GB de RAM
- HD de 80 GB
- Placa de rede 10/100
- Monitor, teclado, mouse
- Impressora

6. Requisitos de Software

- Sistema Operacional Windows XP
- Firewall IPTables
- Proxy Squid
- Office 2000
- Wireless Switch Manager

7. Projeto

Tendo em vista plataformas abordadas e mais utilizadas no mercado e tendo efetuado uma comparação de ambas podemos chegar nas seguintes escolhas:

Windows: As ferramentas para esta plataforma que devem efetuar o controle do tráfego e a segurança dos dados trafegados na mesma, tem como principal desvantagem o alto custo pela aquisição do software e uma difícil configuração tendo em vista que o produto engloba um firewall e um proxy na mesma ferramenta.

Linux: As ferramentas para esta plataforma que devem efetuar o controle do tráfego e a segurança dos dados trafegados na mesma, possuem como principal vantagem a questão custo benefício pois são ferramentas free (sem custo monetário) e de fácil configuração além de possuírem uma vasta bibliografia.

Pelos motivos citados acima foi optado pela plataforma linux e seus respectivos softwares para efetuação do controle de tráfego e segurança dos dados na rede.

Este projeto foi desenvolvido propondo uma solução pra o cenário atual da Fortral, visando suprir suas necessidades e sanar os problemas encontrados, porém fica a cargo do diretor da empresa decidir implantar o projeto.

Para instalação dos softwares de proxy (Squid) e de Firewall (Iptables), será necessário à instalação do sistema operacional Linux, as configurações abaixo para implementação do projeto estão otimizadas para o Ubuntu (uma versão do sistema operacional Linux).

7.1 IMPLANTAÇÃO DOS ACCESS POINTs

Utilizando o Software da 3com o Wireless Switch Manager Software foi possível constatar a necessidade de dois (2) Acess Point's para cobrir toda a área necessária da empresa FORTRAL, sem que ouve-se liberação de sinal para fora da empresa, impossibilitando ataques por excesso de sinal.

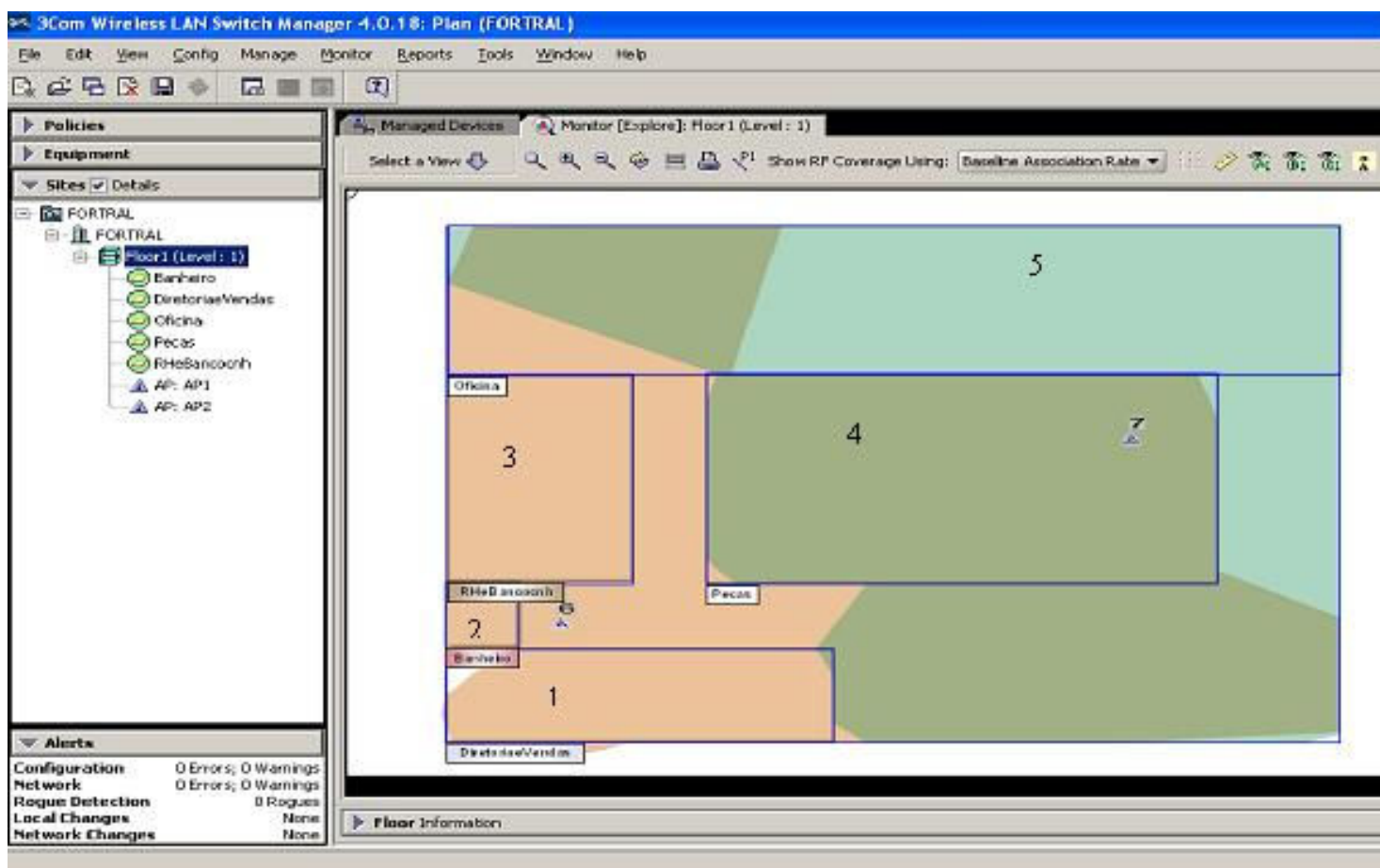


Figura 5: disposição dos Acess Point's

Essa figura representa o layout da empresa FORTRAL e seus respectivos setores a onde este projeto propôs a migração da rede física (cabos) para uma rede nova (wireless).

Para figura acima segue legenda descrevendo seus atributos:

Os quadrados e retângulos em azul representam as repartições da empresa com seus respectivos setores.

1. Sala da Diretoria e Sala dos vendedores;
2. Banheiro;
3. Sala do RH e Banco CNH;
4. Balcão de Vendas de Peças;
5. Dependências da Oficina;
6. Localização do 1° Acess Point;
7. Localização do 2° Acess Point;

A cor bege representa o alcance do 1° Acess Point e a cor verde claro representa o alcance do 2° Acess Point, já o verde escuro representa a área na qual ambos Acess Point's cobrem.

Sendo assim percebemos que toda a empresa possui a cobertura pelo sinal dos Acess Point's além de ter sido verificado para que não houve-se vazamento do sinal para o ambiente externo.

7.2 IMPLANTAÇÃO DO PROXY

Para implantação do proxy Squid o qual fará a filtragem de conteúdo da web, será necessário seguir os passos abaixo.

Arquivo a ser editado /etc/squid/squid.conf (conforme dist)

Parâmetros:

#porta que o servidor vai atender:

http_port 3128

#onde serão armazenados os logs

cache_access_log /var/log/squid/access.log

#acl all – acl que será utilizada como regra default

acl all 0.0.0.0/0.0.0.0

Criação de ACLs (listas de acesso)

#definição da rede (TAG acl)

acl rede_interna src 192.168.1.0/24

#regra de acesso (TAG http_access)

http_access allow rede_interna

Filtros:

#definição do arquivo com a lista de domínios bloqueados

acl sites_bloqueados url_regex -i "/etc/squid/bloq.txt"

acl sites_permitidos url_regex -i "/etc/squis/perm.txt"

#regra de acesso (TAG http_access)

http_access deny sites_bloqueados !sites_permitidos

Primeiro arquivo squid.conf

#squid.conf

http_port 3128

cache_access_log /var/log/squid/access.log

acl all 0.0.0.0/0.0.0.0

acl sites_bloq url_regex -i "/etc/squid/bloq.txt"

acl rede_interna src 192.168.1.0/24

```
http_access deny sites_bloq
http_access allow all rede_interna
http_access deny all
```

Arquivos:

```
#bloq.txt
#sites...
(ex..) www.tim.com.br
(ex..) www.playboy.com.br
```

```
# ou palavras
sexo
moda
```

```
#perm.txt
www.terra.com.br
www.bb.com.br
```

Para otimização do proxy segue os seguintes parâmetros, tendo em vista que a máquina que estará executando o Squid será a mesma que executara o Firewall:

Parâmetros de desempenho:

```
#definição de uso de RAM (normalmente 40% a 50%):
cache_mem 420 MB
```

#substituição de um objeto (quando o swap em disco estiver neste limite – em percentual):

```
cache_swap_low 90
cache_swap_high 95
```

```
#tamanho máximo de um objeto em cache:
maximum_object_size 5120 KB
```

Parâmetros de desempenho:

#tamanho máximo de um objeto em memória:
maximum_object_size_in_memory 20 KB

#diretório de cache, quantidade de espaço no HD em MB, quantidade de pastas a serem criadas e quantidade de subpastas
cache_dir ufs /var/spool/squid 10240 16 256

Arquivo completo com toda a configuração apresentado acima:

```
http_port 3128
cache_access_log /var/log/squid/access.log
cache_mem 400 MB
maximum_object_size_in_memory 64 KB
maximum_object_size 15 MB
cache_swap_low 90
cache_swap_high 95
cache_dir ufs /var/spool/squid 512 16 256
acl all src 0.0.0.0/0.0.0.0
acl rede_interna 192.168.1.0/24
acl sites_bloq url_regex -i "/etc/squid/bloq.txt
http_access deny sites_bloq
http_access allow all rede_interna
http_access deny all
```

7.3 IMPLANTAÇÃO DO FIREWALL

Para implantação do Firewall Iptables o qual fará a proteção da rede e dos dados trafegados nela, será necessário seguir os passos abaixo.

O Iptables já vem o sistema operacional então no prompt faça os seguintes passos:

```
iptables -F INPUT
iptables -F OUTPUT
```

```
iptables -F FORWARD
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
iptables -P FORWARD DROP
```

```
# regras para tornar o firewall stateless
```

```
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -m state --state INVALID -j DROP
iptables -A INPUT -m state --state UNTRACKED -j DROP
iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -m state --state INVALID -j DROP
iptables -A OUTPUT -m state --state UNTRACKED -j DROP
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j
ACCEPT
iptables -A FORWARD -m state --state INVALID -j DROP
iptables -A FORWARD -m state --state UNTRACKED -j DROP
```

```
# regras para acesso local (ao firewall)
```

```
iptables -A INPUT -s 192.168.0.0/24 -d 0.0.0.0 -p tcp --dport 3128 -j
ACCEPT
iptables -A INPUT -s 192.168.0.0/24 -d 0.0.0.0 -p tcp --dport 22 -j ACCEPT
```

```
# regras para acesso da rede interna para Internet
```

```
iptables -A FORWARD -s 192.168.1.0/24 -d 0.0.0.0/0 -p udp --dport 53 -j
ACCEPT
iptables -A FORWARD -s 192.168.1.0/24 -d 0.0.0.0/0 -p tcp --dport 110 -j
ACCEPT
iptables -A FORWARD -s 192.168.1.0/24 -d 0.0.0.0/0 -p tcp --dport 993 -j
ACCEPT
iptables -A FORWARD -s 192.168.1.0/24 -d 0.0.0.0/0 -p tcp --dport 25 -j
ACCEPT
```

```
# SNAT (para que os comps. internos naveguem)
```

```
iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -j MASQUERADE
```

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

8. Investimentos

Para a implantação deste projeto implicaria na aquisição de novos equipamentos. Entretanto, devido à empresa possuir parcerias, justamente com intuito de padronizar seus equipamentos, este investimento apresentará somente modelos dos parceiros.

Os equipamentos são os seguintes:

- 2 Access Point D-LINK Dwl-G700ap
 - Investimento: R\$ 260,00
- 13 Placas D-Link DWL-G510 Wireless PCI
 - Investimento: R\$ 1.209,00

9. Conclusão

O desafio deste trabalho e, talvez o principal eixo motivador, seja a oportunidade de utilizar todo o conhecimento obtido durante o curso de Sistemas de Informação para a elaboração de um projeto que propunha-se a alcançar os benefícios, sanar as dificuldades e solucionar os problemas encontrados na empresa FORTRAL utilizando-se de novas tecnologias.

Conforme foi apresentado este projeto se dispôs a alterar o estado atual da rede interna de computadores (cabos) deste empresa para rede sem fio (wireless), acrescentando um firewall (Iptables) e um proxy (Squid) para segurança da rede e dos dados que trafegam na mesma, efetuando também uma filtragem do tráfego da Web.

10. Referencial Bibliográfico

ALBUQUERQUE, Luciano Renovato de. **Uma Visão Geral do Funcionamento do Protocolo RADIUS**. 2003. Disponível em:

http://www.lockabit.coppe.ufrj.br/rlab/rlab_textos.php?id=81 .

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

<http://www.babooforum.com.br/idealbb/view.asp?topicID=269602> .

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

<http://www.babooforum.com.br/idealbb/view.asp?topicID=335352> .

BALIEIRO, Silva. **Na Rua Com As Redes Sem Fio**. São Paulo. INFO Exame, ano 19, n° 218, pp.: 46-48. Maio/2004.

CARDOSO, Rogério. **WLANS São Inseguras?**. Disponível em:

<http://www.ciscoredacaovirtual.com/redacao/perfistecnologicos/conectividad.asp?id=24> .

CARRIÓN, Demetrio de Souza Diaz. **Implementação De Um Ponto De Acesso Seguro Para Redes 802.11b Baseado No Sistema Operacional OPENBSD**.

Trabalho de Conclusão do Curso de Engenharia Elétrica, Universidade Federal do Rio de Janeiro. 2003. Disponível em:

http://www.ravel.ufrj.br/arquivosPublicacoes/demetrio_projfinal.pdf .

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

4.13.6. Monitoração da Rede *Wireless*. 2003. Disponível em:

<http://www.cert.br/docs/seg-adm-redes/seg-adm-redes.html#sec2> .

DUARTE, Luiz Otávio. **Análise de Vulnerabilidades e Ataques Inerentes a Redes Sem Fio 802.11x**. Trabalho de Conclusão do Curso de Bacharel em

Ciência da Computação. UNESP São José do Rio Preto. 2003. Disponível em:

<http://www.apostilando.com/download.php?cod=230&categoria=Redes> .

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

FORTES, Débora. **A Explosão Das Redes Sem Fio**. São Paulo. INFO Exame Coleção *Wi-Fi*, pp.: 7-13. Ed.: Abril. 2005

GUERRA, André Roberto. **Entendendo os Protocolos**. 2002. Disponível em: <http://www.clubedasredes.eti.br/rede0013.htm> .

INCORPORATED, Communication Services. **Warchalking**; 2005. Disponível em: <http://www.1csi.com/warchalking.html>.

MACIEL, Paulo Ditarso *et al.* **Influência dos Mecanismos de Segurança no Tráfego das Redes sem Fio 802.11b**. Natal. Workshop de Segurança realizado durante o XXI Simpósio Brasileiro de Redes de Computadores (SBRC2003) em Natal, RN. 2003. Disponível em: http://www.lockabit.coppe.ufrj.br/rlab/rlab_textos.php?id=79 .

MARTINS, Marcelo. **Protegendo Redes Wireless 802.11b**. 2003. Rio de Janeiro. Disponível em: http://www.modulo.com.br/pdf/wireless_mmartins.pdf .

MICROSOFT. **Configurando Redes Sem Fio IEEE 802.11 Com Windows XP Para Residências e Pequenas Empresas**. 2005. Disponível em <http://www.microsoft.com/brasil/security/guidance/prodtech/winxp/wifisoho.msp> .

MICROSOFT. **Decisão sobre uma Estratégia de Rede sem Fio Protegida**. 2004. Disponível em: <http://www.microsoft.com/brasil/security/guidance/topics/wireless/secmod168.msp> [x](#) .

MICROSOFT. **Usando o 802.1X e a Criptografia Para Proteger WLANs**. Disponível em:

<http://www.microsoft.com/brasil/security/guidance/topics/wireless/secmod172.msp>
[X](#) .

MICROSOFT. **Visão Geral da Atualização de Segurança WPA Sem Fio no Windows XP**. 2005. Disponível em: <http://support.microsoft.com/kb/815485/pt-br> .

PRADO, Eduardo. **Segurança em WLAN**. 2004. Disponível em:
http://www.wirelessbrasil.org/eduardo_prado/wifi_bible/seguranca.html .

RUFINO, Nelson Murilo de Oliveira. **Segurança de Redes Sem Fio**. 1ª ed. São Paulo: Ed.: Novatec, 2005.

SANTOS, Luiz Carlos. **Como funciona a VPN?**. 2001. Disponível em:
<http://www.clubedasredes.eti.br/rede0004.htm>.

SANTOS, Luiz Carlos. **Uma Combinação Ideal, DSL/Cable Modem e WLAN**. 2003. Disponível em: <http://www.clubedasredes.eti.br/hard0007.htm> .

SYMANTEC. **Implementando Uma LAN Sem Fio Segura**. 2003. Disponível em:
http://www.symantec.com/region/br/enterprisesecurity/content/framework/BR_3074.html .

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

VERÍSSIMO, Fernando. **O Problema de Segurança em Redes Baseadas no Padrão 802.11**. 2003. Disponível em:
http://www.lockabit.coppe.ufrj.br/rlab/rlab_textos.php?id=82 .

11. Glossário

Autenticador	Equipamento que transmite a identidade do usuário para o servidor de autenticação.
<i>Bluetooth</i>	Conexão de rede sem fio de curto alcance.
<i>Backdoor</i>	Programa que permite a ação remota de um hacker sobre um computador infectado.
<i>Checksum</i>	Forma de detectar a consistência dos dados.
<i>Desktops</i>	Microcomputadores de mesa.
<i>Defacers</i>	Pessoas que alteram páginas de Internet alheias sem a devida autorização.
<i>Ethernet</i>	Tecnologia de interconexão para redes locais (LAN) baseada em envio de pacotes.
<i>Firmware</i>	<i>Software</i> embarcado, software que controla o <i>hardware</i> diretamente.
FTP	<i>File Transfer Protocol</i> . Protocolo de transferência de arquivo utilizado na <i>Internet</i> .
<i>Gateways</i>	Porta de ligação entre redes, interligando redes internas com outras internas ou com externas.
<i>Hardware</i>	Parte física do computador.
<i>Hosts</i>	Máquinas pertencentes à uma rede (computadores, <i>notebooks</i> , palms).

ISM	Faixas de frequência destinada a equipamentos que não necessitam de licenciamento da Agência Nacional de Telecomunicações – ANATEL.
<i>Laptop</i>	Computador portátil.
<i>Notebook</i>	Computador portátil.
NetBEUI	Versão melhorada do NetBIOS
NetBIOS	É uma interface que fornece às aplicações de rede um serviço de transmissão orientado à conexão
Pacotes	Estrutura de dados unitária que circula numa rede de computadores.
Rede	Dois ou mais <i>hosts</i> ligados entre si.
Servidor, <i>Server</i>	Máquina que atua servindo uma rede (<i>dados, Internet</i>)
<i>Software</i>	Seqüência de instruções a serem executadas no tratamento, direcionamento e manipulação de dados ou informações.
Suplicante	Usuário que deseja obter acesso à rede.
<i>Wireless</i>	Comunicação sem fio.