Bento Pereira da Silva Filho
Flavio Rogério Duarte dos Santos
Flavio Viana Bueno

WIRELESS LAN

Funcionalidades e Instalação

São Paulo, SP

2008

BENTO PEREIRA DA SILVA FILHO
FLAVIO ROGERIO DUARTE DOS SANTOS
FLAVIO VIANA BUENO

WIRELESS LAN

Funcionalidades e Instalação

Trabalho de graduação apresentado como parte dos requisitos para conclusão do curso de Sistemas de Informação da Faculdade Mário de Andrade.

Orientador: Professor Mestre Alexandre Freitas

São Paulo, SP
2008

BENTO PEREIRA DA SILVA FILHO
FLAVIO ROGERIO DUARTE DOS SANTOS
FLAVIO VIANA BUENO

WIRELESS LAN

Funcionalidades e Instalação

Trabalho de graduação apresentado como parte dos requisitos para conclusão do curso de Sistemas de Informação da Faculdade Mario de Andrade.

Aprovado em .....

BANCA EXAMINADORA

DEDICATÓRIA

Dedicamos este trabalho a todos que contribuíram diretamente ou não, com nosso aprendizado e ideais na área de Redes, em especial, aos Professores, que além de nos respeitarem, nos contagiaram com o amor e a dedicação para EDUCAR.

Dedicamos também aos nossos pais, familiares e amigos, que compreenderam nossas ausências, devido dedicação à elaboração deste trabalho.

Não podemos esquecer-nos de nossos companheiros de trabalho, Marcelo Antonio Martins (MBA USP em Redes) e Cícero Irlandio (Certified 3com Wireless Expert) que nos auxiliaram e muito em sanar nossas dúvidas.

AGRADECIMENTOS

Primeiramente a Deus, pela dádiva da vida.

Aos educadores desta Faculdade, que nos acompanharam durante o curso, contribuindo com seus conhecimentos e seus ideais, sempre motivados a nos guiar pelo melhor caminho.

Em especial agradecemos ao nosso Professor Mestre Alexandre Freitas e o Professor Mestre Antonio Roberto da Silva, que nos orientaram e auxiliaram na elaboração deste trabalho.

E não podíamos deixar de agradecer aos nossos colegas de classe, que além das diversidades de características individuais, compartilharam suas vivências, inseguranças e acertos, contribuindo com nosso desenvolvimento reflexivo e social.

“A mente que se abre a uma nova idéia jamais voltará ao seu tamanho original”

(Albert Einstein)

RESUMO

O trabalho tem como objetivo esclarecer, conscientizar e popularizar a utilização de equipamentos, métodos, recursos tecnológicos em redes de computadores e dispositivos Wireless Lan para uma parcela da sociedade que desconhece essa tecnologia.

Devido nossa constante evolução e atualização tecnológica, temos que orientar as pessoas que não conhecem ou que nem sabem que existe, e muitas dessas, tem a necessidade de utilizar esse recurso para sanar um problema criado por essa evolução desordenada.

Obstáculos ou distância às vezes impossibilitam a comunicação entre empresas, matrizes e filiais e por esses motivos que o Wireless LAN propagou-se no mercado.

ABSTRACT

The work aims to clarify, awareness and popularize the use of equipment, methods, technological resources of the network of computers and wireless devices for a share of the company that ignores this technology.

Because our constantly changing and updating technology, we must guide the people who do not know or do not know they exist, and many of those, is the need to use this feature to remedy a problem created by these developments disorderly.

Obstacles or sometimes impossible distance communication between businesses, parent and subsidiaries and for these reasons that the wireless LAN spread in the market.

LISTA DE FIGURAS

SUMÁRIO

GLOSSÁRIO

Access List- Lista de Acesso;
ADSL- Tecnologia de banda larga para utilizar a rede de telefonia de voz para trafegar dados simultaneamente;
AES (Advance Encryption Standard)- Padrão de Criptografia Avançada;
AP(Access Point)- Ponto de acesso a Wlan;
AppleShare- Compartilhamento de arquivos na rede Macintosh;
APPC (Advance Program to Program Communication)- Comunicação Avançada do programa;
ATM- Rede de comutação de pacotes;
Backup- Cópia de segurança;
BSA (Basic Service Set)- Área de Serviço Básico;
BSS (Basic Service Set)- Grupo de Serviço Básico;
BSS - ID (Basic Service Identification)- Identificação do Grupo de Serviço básico;
Cable modem- Tecnologia de banda larga para utilizar os cabos da TV por assinatura para trafegar dados;
Closed Network Access Control- Controle de Acesso de Rede Fechada;
CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)- Sensor de Portadora de Múltiplo Acesso com detecção de colisão;
DCF (Distributed Coordination Function)- Função de Coordenação Distribuída;
DHCP (Dynamic Host Configuration Protocol)- Protocolo de configuração dinâmica de máquinas;
DS (Distribution System)- Sistema de Distribuição;
DV (Distance Vector)- Vetor distância;
ESA (Extend Service Area)- Área estendido de Serviço;
ESS (Extend Service SET)- Grupo estendido de Serviço;

FIPS (Federal Information Processing Standard) - Padrão de Processamento de informações Federais;

Frame-Relay- Oferece um desempenho maior que o L25;

FTP (File Transfer Protocol, FTAM File Transfer, Access and Management) – Protocolos de transferência de dados;

GPS (Global Positioning System)- é um sistema de posicionamento por satélite americano, por vezes incorrectamente designado de sistema de navegação, utilizado para determinação da posição de um receptor na superfície da Terra ou em órbita;

Handhelds- Dispositivos portáteis sem fio;

IBSS (Independent Basic Service SET)- Grupo de Serviço básico independente;

IEEE (Institute of Electrical and Eletronics Engineers)- Instituto criado para regulamentação da comunicação de dispositivos sem fio;

IP (Internet Protocol) – Protocolo de Internet

ISDN- Rede de telefonia digital, permitindo o tráfego de voz;

LAN (Local Area Network)- Rede local de computadores;

LS (Link State)- Estado do Link;

MAC (Media Access Control)- Controle de Acesso ao meio;

MAN (Metropolitan Area Network)- Rede Metropolitana de Computadores;

MIMO (Multiple-Input, Multiple Output)- Múltiplas entradas e múltiplas saídas;

MRD (Markenting Requirements Document)- Documento de Requisitos de Marketing;

Nwlink- Protocolo que realiza a comunicação entre os ambientes Windows e Netware;

OSA (Open System Authentication)- Sistema de autenticação aberta;

OSI/ISO (*Open Systems Interconnection*) - Esta arquitetura é um modelo que divide as redes de computadores em sete camadas, de forma a se obter camadas de abstração;

PC (Pessoal computer) – Um computador pessoal é um computador de pequeno porte e baixo custo, que se destina ao uso pessoal ou para uso de um pequeno grupo de indivíduos;

PCF (Pont Coordination Function)- Função de Coordenação Pontual;

PHY/MAC (Physical Layer and Médium Access Control Layer) – Camada Física e Camada de controle de Acesso ao meio;

QOS (Quality of Service)- Qualidade de Serviço;

RSN (Robust Security Network) – Redes de Segurança Robusta;

ROI – Retorno de Investimento;

SAP (Service Access Point)- Ponto de Acesso do Serviço;

Shared Key Authentication- Autenticação de chave compartilhada;

SPX (Seqüencial Packet Exchange)– Protocolo que faz parte do grupo dos protocolos IPX/SPX;

Smartphones– Smartphone é um telefone celular com funcionalidades estendidas por meio de programas executados no seu Sistema Operacional;

SMTP (Simple Mail Transfer Protocol) – Protocolo de acesso ao correio eletrônico;

SNMP (Simple Network Management Protocol)- Protocolo para uso de monitoração e gerenciamento de redes;

SNMP (Simple Network Management Protocol)- Protocolo de Gerenciamento Simples de Rede;

SSID (Service Set Identifier)- Identificação de Grupo de Serviço;

StandyBy- Em modo de espera;

TCP (Transmission Control Protocolo) – Protocolo integrante do TCP/IP que realiza a entrega garantida dos pacotes;

Telnet (Protocol Virtual Terminal)- Para conectar um computador remoto a outro local sendo que o remoto pode executar os mesmos serviços que o local;

TKIP (Temporal Key Integraty Protocol)- Protocolo de integridade de Chave Temporal;

TGn (Task Group N)- Grupo de tarefa N;

UDP (User Datagram Protocol)- Protocolo integrante do TCP/IP que realiza (sem ser garantida) dos dados;

X400- Protocolo de transmissão de correio eletrônico;

X 500- Protocolo padrão OSI de serviço de diretório global;

X 25- Rede de comutação de pacotes;

Zigbee- Comunicação sem fio em até 10 metros.

Wan (Wide Area Network)- é uma rede fisicamente distante;

WEP (Wired Equivalent Privacy)- Privacidade equivalente às redes com fios;

Wi-fi (Wireless Fidelity)- marca licenciada originalmente pela Wi-Fi Alliance para descrever a tecnologia de redes sem fios embarcadas;

Wlan (Wireless lan – wireless local área network)– Rede local sem fio;

WiMax- Conexão de redes sem fio para longas distâncias;

WPA (Wi-fi Protected acess)- Proteção de aceso para wifi;

WWW (Internet) – Rede de alcance mundial de computadores;

APRESENTAÇÃO

Este trabalho acadêmico tem como tema central, esclarecer sobre o uso da tecnologia da comunicação sem fio, por ser um tema crescente em nosso cotidiano.

Para iniciarmos é importante e fundamental entendemos rapidamente o elo da evolução humana com a comunicação durante os séculos. A comunicação é definida como:

A palavra comunicar vem do latim comunicare e significa “pôr em comum”, tornar comum. Em sentido prático, comunicar é transmitir idéias e informações com o principal objetivo de promover o entendimento entre os indivíduos. Para que ela se realize, é necessária à utilização de um código comum previamente estabelecido. Para existir a comunicação é necessário haver um emissor e receptor e não haver meios de interferência.

Destacam-se duas formas de comunicação: Verbais (quando são pronunciadas palavras para haver a comunicação) e as não verbais (não são utilizadas palavras para a comunicação. Ex: linguagem gestual, linguagem escrita, linguagem simbólica, etc.). [Marcos Tuler, 2005]

A comunicação passou por um grande avanço tecnológico durante os tempos. Um desses avanços foi a invenção de um dispositivo de telecomunicações que transmite e recebe som por meios de sinais elétricos, permitindo assim a troca de informações entre dois ou mais usuários. Essa invenção, o telefone, foi criado por Alexander Graham Bell por volta de 1860, com o único intuito de reduzir as distâncias e o tempo que se demorava a se comunicar de um ponto a outro.

Outro passo importante do avanço tecnológico que a humanidade realizou foi a invenção do rádio. A radiocomunicação é um meio de comunicação por transcepção de informação, podendo ser transmitida por Radiação eletromagnética que se propaga através do espaço.

No caso de emissão comercial, sem transcepção de sinais, somente transmissão, esta modalidade é definida como radiodifusão, utilizado para fazer a comunicação com vários usuários na mesma região. Isso pode ser bem exemplificado quando falamos da forma de comunicação utilizada na primeira guerra mundial. [wikipedia, 2008]

INTRODUÇÃO

Com o crescimento e o avanço tecnológico diário em nosso mundo corporativo, nós como meros mortais, precisamos acompanhar essa tendência ou ficamos para trás.

Este trabalho é voltado para a área de tecnologia, mais o que vem a ser tecnologia? Tecnologia é o termo utilizado que envolve o conhecimento técnico e científico, suas ferramentas, processos e materiais criados e ou utilizados a partir de tal conhecimento. Com essa base criamos um trabalho acadêmico com foco na área da comunicação sem fio, pois é um tema que está sofrendo uma constante evolução e cada vez mais utilizado. Mais o que é comunicação sem fio? É o ato de transmitir dados de um ponto para outro sem utilizar nenhum meio físico para esse tráfego.

Devido a alguns locais serem fisicamente limitados, impedindo a utilização de tecnologias de transmissão de dados físicas (cabo), com a utilização da comunicação sem fio isso não existe mais, pois essa tecnologia utiliza ondas de rádio para se comunicar. São utilizadas em:

- Grandes Indústrias - não é possível utilizar cabos, devido a grande interferência elétrica;
- Prédios e apartamentos - espaço físico disponível limitado;
- Escritórios - mobilidade de conexão a internet a qualquer lugar e instante;
- Celulares e outros dispositivos móveis.

No Brasil essa tecnologia está em desenvolvimento e possui suas limitações. Nos demais países desenvolvidos ela não é novidade. Atualmente, no Brasil, a utilizamos em diversos ramos, sendo os que mais se destacam são:

- CET (com a utilização de smartphones),
- Bombeiros (utilizando comunicadores e GPS),

- Polícia (utilização de rádio-comunicador),
- Bancos (comunicação via-satélite) e outros. A maior área de cobertura nacional existente é Campinas, possuindo um raio de conexão de 40 km quadrados, utilizando a tecnologia WiMax que será mais detalhada no decorrer do trabalho.

A comunicação sem fio traz diversos benefícios. Mas seu maior vilão é o seu melhor benefício ”a mobilidade”. Com a possibilidade de trafegar dados por meios não físicos, ainda não é possível rastrear ataques no sistema, fato que não ocorre com a utilização do transporte de dados por meios físicos (cabo). Existem muitas barreiras na tecnologia sem fio e o preconceito ainda é grande. Boa parte dos mitos existentes estão sendo desfeitos e logo essa tecnologia passará a fazer parte do dia-a-dia da sociedade.

1 Rede de computadores

No início dos anos 70, somente existiam os grandes computadores que ficavam em salas isoladas. A rede consistia apenas de terminais (teclado e vídeo) que eram compartilhados por vários usuários que podiam apenas consultar os dados de forma restrita por programas executados no computador. Além do acesso restrito, somente as grandes empresas tinham esse tipo de rede.

Por volta de 1974, disseminaram-se os computadores menores denominados de minicomputadores, possibilitando a descentralização do processo de alimentação de dados e impressão das informações.

Com o tempo perceberam que este processo não era mais eficaz para atender as necessidades da empresa. Resultava em duplicação de informações, recursos e não favorecia a padronização no gerenciamento da rede.

Nos anos 80, surgiram os microcomputadores PC (Personal Computer) com a especificação aberta, permitindo a quem quisesse a fabricação de microcomputadores compatíveis de tal forma que o preço tornou-se acessível até as pessoas físicas.

O PC era um equipamento de uso individual, porém utilizavam diferentes especificações de hardware e software. Essas diferenças causaram diversas incompatibilidades, redundância de informações e tornou difícil a comunicação entre redes. Surgiram então as redes locais (LANS- Local Area Network), conectando os PC's uns aos outros e compartilhando os periféricos utilizando uma tecnologia comum.
Para conectar as LANS surgiram as redes metropolitanas (MAN- Metropolitan Área Network). Atualmente temos a Internet (www - World Wide Web) que é a rede que mais se aproxima da visão de uma rede global, crescendo dia-a-dia tanto em termos de usuários como de serviços.
[Tenenbaum, 2003]

1.1 Definição

A Rede é a ligação de computadores para compartilhar recursos e interligar os usuários. Para padronizar a utilização da rede e para haver um consenso geral foi criado o modelo ISO/OSI. O Modelo ISO/OSI é um modelo de referência para a interoperabilidade de sistemas. Definem sete camadas independentes, cada camada comunica-se somente com as camadas inferior e superior e age como se estivesse comunicando com a camada equivalente no outro sistema.

1.2 OSI/ISO

A sigla ISO refere-se a Organismo Internacional para Padronização ou em inglês International Organization for Standardization que divide as redes de computadores em sete camadas, para ter um entendimento menos complexo.

O modelo OSI define 7 camadas e cada uma é responsável por um grupo de serviços. Cada camada se comunica apenas com a próxima camada inferior e superior de forma padronizada, possibilitando a implementação independente dos serviços em cada camada. As camadas agem como se estivessem comunicando-se com a sua camada associada no outro computador. Um fornecedor pode se especializar em um serviço de uma camada e facilmente integrar com os serviços das outras camadas formando a solução necessária.

CAMADA	FUNÇÃO
APLICAÇÃO	Funções especializadas
APRESENTAÇÃO	Formatação de dados e conversão de caracteres e códigos
SESSÃO	Negociação e estabelecimento de conexão com outro nó
TRANSPORTE	Meios e métodos para a entrega de dados ponta-a-ponta
REDE	Roteamento de pacotes através de uma ou várias redes
ENLACE	Detecção e correção de erros introduzidos pelo meio de transmissão
FÍSICA	Transmissão dos bits através do meio de transmissão

Descrição das camadas de rede.

1.3 Camadas

1.3.1 Camada 1 – Física:

É a camada de mais baixo nível. Definem as especificações elétricas, mecânicas, e funcionais para ativar, manter e desativar a ligação física entre dois computadores em rede. Especificam as características físicas como o tipo de cabo, a codificação dos sinais, conectores e limitações de distância e velocidade.
É responsável pela transmissão de bits de um computador para outro através de um meio físico. Transformando os bits em impulsos elétricos ou ópticos para que possam trafegar no cabo de rede.

1.3.2 Camada 2 – Enlace:

Providencia maneiras funcionais, interfaces, e procedimentos para interligar e realizar a comunicação entre as camadas Um protocolo da camada de enlace é usado para transportar um datagrama da camada de rede sobre um enlace individual. Entre suas características podemos citar:

- Conexão dos enlaces, ativação e desativação. Estas funções incluem o uso de facilidades multiponto físico para suportar conexões entre funções da camada de rede;
- Mapeamento de unidades de dados para a camada de rede dentro das unidades do protocolo de enlace para transmissão;
- Multiplexação de um enlace de comunicação para várias conexões físicas;
- Delimitação de unidades de transmissão para protocolos de comunicação;
- Detecção, notificação e recuperação de erros identificação e troca de parâmetros entre duas partes do enlace;

1.3.3 Camada 3 – Rede:

Executa o roteamento, determinando qual o melhor caminho do computador de origem ao computador de destino. Baseado nas condições da rede, prioridade do serviço e outros fatores. Gerencia o trafego da rede, controlando os congestionamentos, transferência de pacotes e problemas de roteamento.

1.3.4 Camada 4 – Transporte:

A função básica da camada de transporte é aceitar dados da camada de sessão, dividi-los em unidades menores em caso de necessidade, passá-los para a camada de rede e garantir que todas essas unidades cheguem corretamente à outra extremidade.

1.3.5 Camada 6 – Apresentação:

Fornece as funções de formato dos dados como o tipo de codificação e conversão de dados, incluindo compressão /descompressão e criptografia/descriptografia.

1.3.6 Camada 7 – Aplicação:

É a camada mais alta e atua como uma janela para processos do aplicativo que acessam os serviços da rede. Representa os serviços de suporte direto ao aplicativo do usuário, como os serviços de transferência de arquivo (FTP File Transfer Protocol, FTAM File Transfer, Access and Management), acesso ao correio eletrônico (SMTP Simple Mail Transfer Protocol), e demais serviços de rede. [Tenenbaum, 2003]

1.4 Protocolos

Protocolo é a definição de procedimentos e normas para a comunicação entre dois computadores. Quando um computador vai enviar dados, eles são passados para o protocolo ou pilha de protocolos que o converterá no formato mais adequado para a transmissão dependendo das características da rede. No formato mais adequado para a transmissão dependendo das características da rede. Existem protocolos em cada

camada do Modelo OSI realizando as funções de comunicação da rede. São classificados em três níveis. [Tenenbaum, 2003]

- Aplicativo: Camadas 7- Aplicação, 6 - Apresentação, 5 – Sessão;
- Transporte: Camada 4 -Transporte;
- Rede: Camadas 3 - Rede, 2 - Enlace

1.4.1 Protocolos de Aplicativos

Os protocolos de Aplicativo são os que trabalham nas 3 camadas mais altas do modelo OSI (Aplicação, Apresentação e Sessão). Eles proporcionam interação de aplicativo para aplicativo e a troca de dados. Os protocolos mais populares são:

- APPC (Advanced Program to Program Communication): para a comunicação par a par no IBM AS/400;
- FTP (File Transfer Protocol): para a transferência de arquivos, muito utilizado na Internet e Unix;
- SNMP (Simple Network Management Protocol): para monitoração e gerenciamento de redes;
- Telnet (Protocol Virtual Terminal): para conectar um computador remoto a outro local sendo que o remoto pode executar os mesmos serviços que o local;
- SMTP (Simple Mail Transfer Protocol): para a transferência de correio eletrônico;
- X.400: protocolo padrão OSI de transmissão de correio eletrônico;
- X.500: protocolo padrão OSI de serviço de diretório global;
- AppleShare: para compartilhamento de arquivo nas redes Macintosh.

1.4.2 Protocolos de Transporte

Os protocolos de Transporte asseguram o empacotamento e a entrega segura dos dados. Os protocolos mais populares
são:

- SPX (Sequential Packet Exchange): constitui uma parte do grupo de protocolos para dados seqüências IPX/SPX desenvolvido pela Novell para o seu sistema operacional Netware;
- TCP (Transmission Control Protocol): da pilha TCP/IP que realiza a entrega garantida de dados;
- UDP (User Datagram Protocol): da pilha TCP/IP que realiza a entrega de dados, mas sem a garantia de entrega dos dados por não executar a correção de erros e controle de fluxo;
- Nwlink: para a comunicação de dados entre os ambientes Windows e o Netware;
- NetBEUI NetBIOS (NET-Network Basic/EUI-Extended User Interface/IOS-Input/Output System): para proporcionar serviço de transporte de dados em computadores utilizando a interface NetBIOS (interface para estabelecer nomes lógicos na rede, estabelecer sessões entre dois nomes lógicos, entre dois computadores na rede e suportar a transferência de dados entre os computadores).

1.4.3 Protocolos de Rede

Os protocolos de Rede transportam os pacotes de uma origem para um destino. Estes protocolos realizam as funções de determinação de melhor caminho e comutação nas interfaces. O protocolo mais popular é o IP. Atualmente utilizamos o IP versão 4 (IPv4). Futuramente teremos IPv6 que, por exemplo, terá 128 bits de endereço.

A LAN é uma rede com alta velocidade de transmissão e baixa taxa de erros que cobre uma pequena área geográfica.

O padrão IEEE 802 (Institute of Electrical and Electronics Engineers) foi criado para regulamentar a comunicação entre os computadores, mas era apenas um modelo de referência para definir a arquitetura e as interfaces. [IEEE, 2008]

A principio foram criados 12 comitês para definir os padrões e regulamentar as evoluções necessárias para incorporar as novas tecnologias.

- IEEE 802.1 - Interconexão de redes;
- IEEE 802.2 - Controle de vínculo lógico;
- IEEE 802.3 - LAN CSMA/CD (Ethernet);
- IEEE 802.4 - LAN barramento token;
- IEEE 802.5 - LAN token ring;
- IEEE 802.6 - Redes Metropolitanas;
- IEEE 802.7 - Grupo consultivo técnico de Banda Larga;
- IEEE 802.8 - Grupo consultivo técnico de fibra ótica;
- IEEE 802.9 - Redes integradas de voz e dados;
- IEEE 802.10 - Segurança da rede;
- IEEE 802.11- Redes sem fio;
- IEEE 802.12 - Rede de acesso de prioridade de demanda.

Wan (Wide Área Network) é uma rede fisicamente distante, conectadas através de ligações fornecidas por empresas de comunicação. Podemos utilizar linhas comutadas, linhas privadas, T1, rede de pacotes ou rede de comutação de circuitos.

Os serviços disponibilizados pelas empresas são baseados nas principais tecnologias:

- X.25 - rede de comutação de pacotes, trabalhando ao nível de camada 3 - Rede.
- Frame-relay - oferece um desempenho melhor que o L25. Trabalha na camada 2 do Modelo OSI.
- ISDN - é uma rede de telefonia digital permitindo o tráfego de voz, dados e vídeo.
- ATM - é uma rede de comutação de pacotes, mas que trabalha com pacotes de tamanho fixo de 53 bytes denominado de célula. Permite o tráfego de voz, dados, vídeo com priorização de tráfego.

- ADSL - é uma tecnologia de banda larga para utilizar a rede de telefonia de voz para trafegar dados simultaneamente, sem a necessidade de discagem. O download é à velocidade de até 8 Mbps e upload até 640Kbps. Mas os serviços são oferecidos em velocidades menores devido a qualidade do cabo e da distância.
- Cable modem - é uma tecnologia de banda larga para utilizar os cabos da TV por assinatura para trafegar dados. O download é em velocidade de até 36 Mbps e o upload até 2 Mbps. Mas os serviços são oferecidos em velocidades menores porque trabalha com a tecnologia de compartilhamento entre vários assinantes.

1.5 Modelo utilizado antes do OSI

O protocolo TCP/IP é a pilha de protocolos padrão para a comunicação entre computadores inclusive na Internet.
Possui apenas 4 camadas:

- Camada de Interface de Rede;
- Internet;
- Transporte;
- Aplicação.

Define um sistema de endereçamento de 4 bytes que são divididos em endereço de rede (Net ID) e endereço de host (Host ID). Comercialmente temos 3 classes:

- Classe A com o bit mais a esquerda igual a 0 com 7 bits para Net ID e 24 bits para Host ID. (10.0.0.0 a 10.255.255.255)
- Classe B com os dois bits mais a esquerda igual a 10 com 14 bits para Net ID e 16 bits para Host ID. (172.16.0.0 a 172.31.255.255)
- Classe C com os três bits mais a esquerda igual a 110 com 21 bits para Net ID e 8 bits para Host ID. (192.168.0.0 a 192.168.255.255)

A sub-rede foi definida para melhorar a alocação dos endereços IP. Divide o Host ID em dois campos: Sub-rede e Host. De tal forma que uma empresa com apenas um endereço IP consegue definir várias sub-redes internas cuja estrutura não é visível fora da empresa.

1.6 Equipamentos e Softwares

Estação de rede: Atualmente, quase todos os computadores podem ser conectados a uma rede. A maioria das estações de rede são PCs, desktop ou notebooks na sua configuração mais comum.

Figura 1: Estações de rede
Fonte: http://www.hp.com.br (2008)

Servidor de rede: Os servidores de redes são computadores dedicados a fornecer recursos para as estações. Para ambientes de grande concentração de servidores como Data Center e de servidores WEB onde o espaço e a escalabilidade são muito importantes, podemos utilizar a tecnologia de servidores em 1U (aproximadamente 4 cm) para montagem em rack padrão.

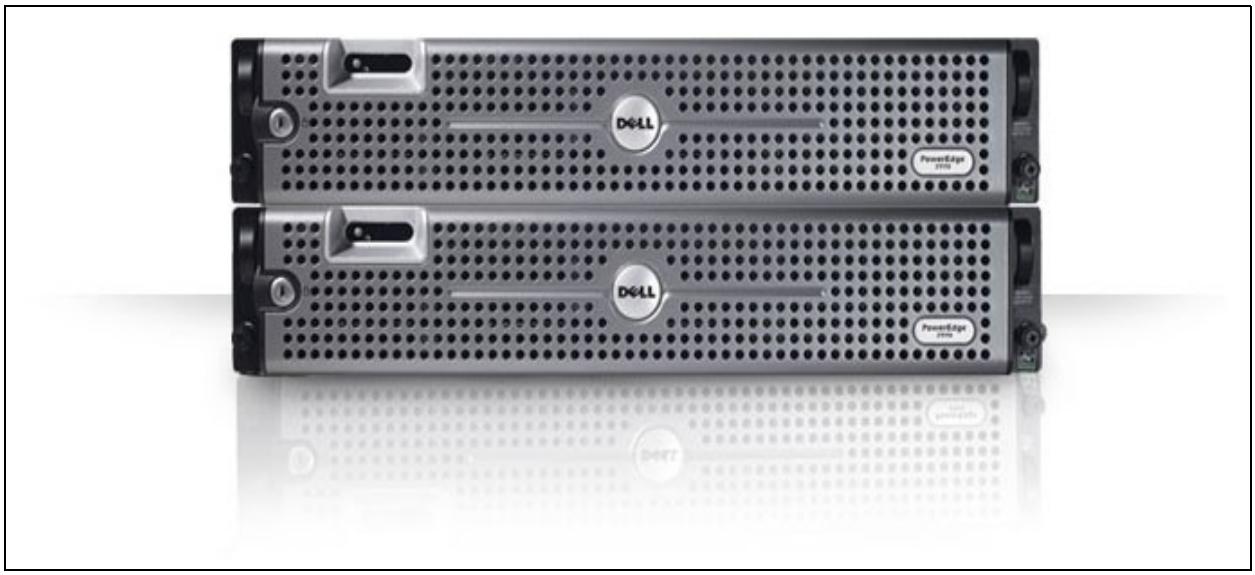

Figura 2: Servidor de rede, modelo para rack.
Fonte: http://www.dell.com (2008)

1.6.1 Sistema Operacional

O sistema operacional foi desenvolvido para facilitar a comunicação entre o ser humano e o computador e para padronizar a interface entre os softwares, aplicativos e os dispositivos. Permitindo assim que a troca de uma impressora não afetasse os softwares, ou seja, o software aplicativo emite o comando de impressão e passa os dados para o sistema operacional. Ele possui o driver (software que interpreta os comandos e converte os dados para o dispositivo) que manda o comando e os dados que são reconhecidos pela impressora.

1.6.2 Hub

Nas redes que utilizam o cabo UTP é necessário adotar um equipamento central denominado Hub, que concentra todos os cabos UTP's. O hub tem diversas portas onde são conectados os cabos vindos das estações e ao verificar que há algum problema na conexão de uma porta, esta é isolada de tal forma que não afeta as demais. A estação envia o sinal para o hub que o amplifica e propaga por todas as outras portas. A largura de banda é compartilhada por todas as portas.

1.6.3 Repetidor

O repetidor que amplifica e retransmite os sinais para estender o alcance dos cabos. Existe também em formato wireless, que será melhor explicado no decorrer desde trabalho.

1.6.4 Bridge (Ponte)

As Bridges que além de estender o alcance dos cabos, isola os tráfegos internos do segmento, trabalhando ao nível da camada 2 - enlace.

1.6.5 Roteador

Para evitar a difusão dos pacotes de controle, utilizamos os roteadores, que interligam duas ou mais redes lógicas, que podem ser de diferentes tipos e tecnologias.

1.6.6 Switch

É um equipamento similar ao hub mas possui a característica de dedicar a largura de banda para cada porta, ou seja, numa rede com largura de banda de 10 Mbps, o hub compartilha estes 10 Mbps para todas as estações.

1.6.7 Gateway

São servidores dedicados que realizam a comunicação entre dois sistemas de computação distintos, com diferentes protocolos de comunicação, diferentes arquiteturas de rede, diferentes estruturas para pacotes de dados etc.

1.7 Meios Físicos

Existem vários meios físicos que podem ser utilizados para ligar os computadores em rede. Conforme as características do material e do tipo de cabo, o sinal pode ser

transportado por uma distância maior ou menor e determina o comprimento máximo do cabo.

O meio físico por si só não determina a velocidade de transmissão, que é determinado pelo método de acesso especificado na camada 2 do modelo ISO/OSI.
O meio físico pode não suportar a velocidade exigida e deve ser trocado por outro que suporte a velocidade.

1.7.1 Principais meios físicos

- Cabo Coaxial - É um cabo com núcleo de cobre coberto por um isolante de PVC ou teflon e uma camada de blindagem de malha de cobre ou alumínio e por último um plástico protetor externo. Os sinais trafegam pelo núcleo do cabo. O PVC ou teflon protege o cabo evitando que se quebre. A blindagem de malha protege os sinais absorvendo os ruídos, para que não cheguem ao núcleo e distorçam os sinais que estão sendo propagados. O cabo coaxial também é utilizado na TV por assinatura e em várias conexões de antena de TV e também para conectar a TV ao videocassete.
- Cabo coaxial fino - É flexível com cerca de 0,63 cm de espessura, e pode transportar um sinal por 185 metros. A conexão é através de um conector BNC tipo T, um conector BNC fêmea em cada extremidade do T ligado ao cabo coaxial e um conector BNC macho na placa de rede local.
- Cabo Par Trançado - É formado por dois filamentos isolados de cobre torcidos e podem ser blindados (STP) ou não blindados (UTP). Sendo este último mais utilizado. Um cabo é formado por 2 ou 4 pares de fios agrupados e fechados em um revestimento protetor. Transporta o sinal até 100 metros. A conexão é através de um conector RJ45 macho no cabo e um conector RJ45 fêmea na placa de rede. São divididos em categorias dependendo de sua aplicação:

Categorias:

Categoria 1 - refere-se ao cabo UTP para telefonia. Transporta apenas voz.
Categoria 2 - certificado para transmitir até 4 Mbps. Contém 2 pares.
Categoria 3 - certificado para transmitir até 10 Mbps. Contém 2 pares.
Categoria 4 - certificado para transmitir até 16 Mbps. Contém 4 pares.
Categoria 5 - certificado para transmitir até 100 Mbps. Contém 4 pares.
Categoria 5e - certificado para transmitir até 100 Mbps. Contém 4 pares.
Categoria 6e - certificado para transmitir até 10 Gbps. Contém 4 pares.

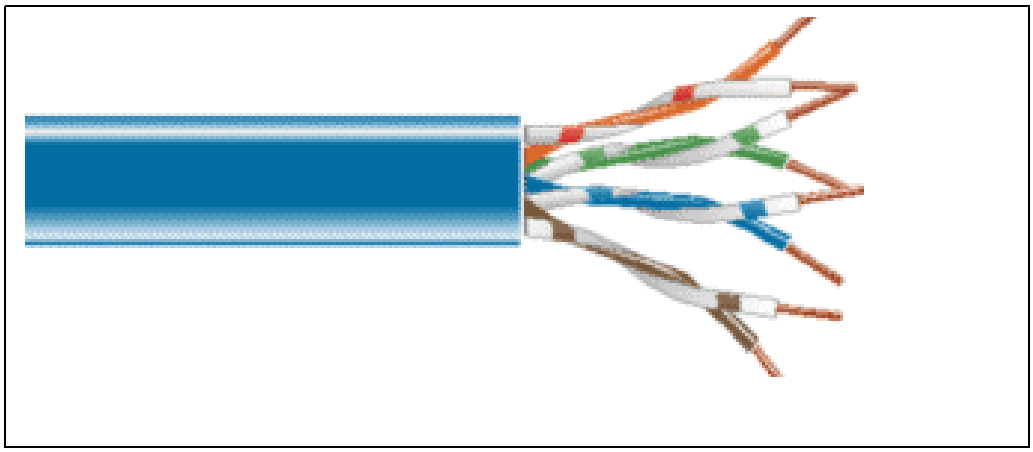

Figura 3: Modelo de cabo par trançado.
Fonte: www.store-suprinform.locasite.com.br/loja/images(2008)

- Fibra Óptica - É um filamento de vidro recoberto com uma substância com índice menor de refração, que fazem com que os raios sejam refletidos internamente, minimizando as perdas de transmissão. Sendo recoberto por uma camada de plástico de reforço. Cada filamento de vidro pode transportar o sinal somente em um sentido, portanto um cabo é formado por duas fibras óticas que são revestidas com plástico e com fibras de Kevlar entre elas para dar firmeza ao cabo.

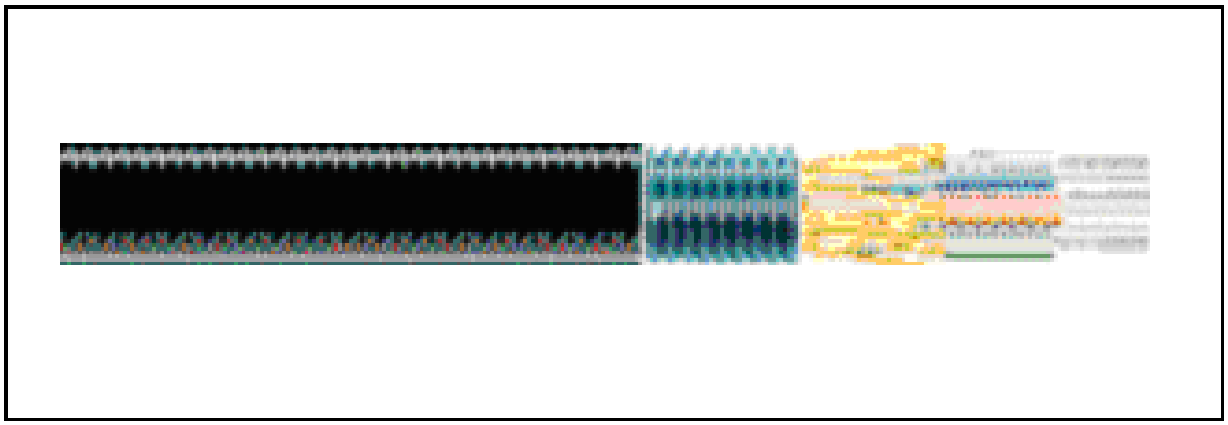

Figura 4: Modelo de cabo de fibra óptica.
Fonte: www.connectlan.com.br (2008)

A transmissão de dados em uma fibra ótica é possível por causa da característica do vidro em conduzir a luz. Esta característica também é utilizada para produzir um efeito de luz e cores em abajures e árvores de natal. Em um abajur coloca-se uma lâmpada de luz branca na base, na qual se prende um feixe com centenas de bastões de vidro com aproximadamente meio milímetro de diâmetro e flexíveis. A outra ponta fica livre formando uma esfera. Ao se acender a lâmpada, cada bastão conduzirá a luz da base para a outra ponta. Devido à refração cada ponta emite a luz de uma cor. Na árvore de natal, coloca-se a lâmpada na base e estende-se um feixe de alguns bastões de vidro similar ao do abajur até a ponta de cada galho. A luz será conduzida da base até as pontas dos galhos, visualizando-se vários pontos de luz com cores diferentes.

Existem dois tipos de fibra ótica:

- Multímodo - utiliza um LED como fonte de luz que é de menor custo. O filamento tem 62,5 mícron ou 50 mícron de diâmetro. Transporta o sinal por 2 km à velocidade de 100Mbps e por 550metros à velocidade de 1Gbps.
- Monomodo - utiliza o laser como fonte de luz. O filamento é mais fino com cerca de 10 microns de diâmetro.

Transporta o sinal por 5 km até na velocidade de 1Gbps. Atualmente a fibra ótica mais utilizada tem a espessura de 62,5 ou 50 microns. O mícron é igual a um milésimo de

milímetro, ou seja, em um tubo com 1 milímetro de diâmetro conseguimos colocar 20 fibras óticas de 50 microns. Comparando com um fio de cabelo isso representa de 3 a 4 vezes a espessura de um fio de cabelo.

2 Históricos das redes Wireless

A primeira rede a utilizar a comunicação sem fio foi desenvolvida no Havaí, no início da década de 70, mais precisamente em 1971. O objetivo era interligar os campos que se situavam em quatro ilhas com o computador central que ficava na ilha de Oahu. Apesar daquele projeto não ter sido utilizado em massa, devido a fatores como a baixa taxa de transmissão e de seu elevado preço, o mesmo despertou o interesse em se aperfeiçoar tal tecnologia para então torná-la viável. As redes Wireless utilizavam transmissão spread spectrum ou infravermelha difusa uma vez que a falta de padronização atrasava o desenvolvimento e, sobretudo, sua popularização. [ROSHAN, 2004]

Em maio de 1991 foi submetido ao IEEE (Institute of Electrical and Electronics Engineers - Instituto dos Engenheiros Elétricos e Eletrônicos) a elaboração de um grupo de pesquisa para criar um padrão único para as redes Wireless. Esse padrão denominado de Padrão 802.11, à medida que era elaborado, foi sendo adotado pelos fabricantes de redes Wireless, que então passaram a elaborar seus produtos baseando-se nas normas do 802.11, pois a padronização oferece interoperabilidade, confiabilidade e diminuição nos custos, provendo assim uma boa aceitação do mercado [LEITE, 2008].

2.1 O que é WLAN

Uma WLAN (Wireless Local Area Network – Rede Local Sem Fio) é uma rede que atende a uma área menor LAN (Local Area Network – Rede Local), com o objetivo de manter conectados todos os equipamentos de informática que se encontram no local.

Uma rede Wireless é um sistema de transmissão de dados que pode ser utilizado para substituir ou complementar as redes cabeadas, pois a mesma não utiliza fios. Os dados são transmitidos através da propagação de ondas eletromagnéticas. [ROSHAN, 2004]

O IEEE criou um padrão com o nome de 802.11, aonde tal padrão oferecia taxa de transmissão de dados de até 2 Mbps (Megabit Per Seconds - Megabits Por Segundos).

Apesar da significante elevação da taxa de transmissão de poucos Kbps para 2 Mbps, esse valor já não atendia satisfatoriamente a necessidade das empresas. Era preciso melhorar o padrão. Foi então que surgiu o 802.11b, que possuía a mesma tecnologia e arquitetura, mas com taxa de transmissão aumentada para até 11 Mbps, o que permitia alcançar valores aproximados aos da rede cabeada (Ethernet 10 Mbps). Esse padrão impulsionou de vez a indústria a investir em tecnologia e produtos para as redes Wireless [LEITE, 2008].

Ao mesmo tempo em que estava sendo criado o padrão IEEE 802.11b, também se trabalhava em cima do padrão 802.11a, que permitia uma taxa de dados de até 54 Mbps, no entanto, utilizando a freqüência de 5 Ghz (Gigahertz). Esse padrão que oferecia uma boa taxa de dados, não conquistou o seu espaço no mercado devido à sua incompatibilidade com o padrão 802.11b, seu alcance reduzido e também por ter sido lançado no mercado seis meses após o lançamento de seu concorrente, o 802.11b, que então já estava se consagrando nas grandes empresas. [ROSHAN, 2004]

Apesar de já existir no mercado um padrão com uma boa taxa de transmissão havia a necessidade de se criar um padrão para aumentar a taxa de dados do padrão 802.11b, no entanto, mantendo a compatibilidade com o mesmo. Em 2003 foi aprovado o padrão IEEE 802.11g, que possibilita uma taxa de dados de até 54 Mbps na freqüência de 2.4 Ghz, a mesma utilizada no padrão 802.11b, mantendo assim, a compatibilidade.

2.2 Vantagens e desvantagens da tecnologia

Destacam-se as vantagens [MATHIAS, 2008]:

- A estação de trabalho estando dentro da área de cobertura, pode ser alterada de lugar sem se preocupar com cabos;
- O custo da implementação de uma rede Wireless é baixo comparando-se com a rede cabeada;
- Flexibilidade para configurar e alterar dentro de qualquer tipo de topologia.

Destacam-se as desvantagens [MATHIAS, 2008]:

- Qualidade de serviço baixa;
- Os equipamentos têm um custo alto;

- As empresas não têm total confiança na segurança da rede Wireless, prejudicando assim sua expansão;
- Dependendo do sistema a ser utilizado em uma rede Wireless a taxa de transferência de dados é baixa.

2.3 Números de usuários suportados

Uma vez que a largura de banda de uma rede Wireless é limitada, o limite máximo de usuários simultâneos suportados por um AP (Access Point – Ponto de Acesso) varia dependendo da quantidade de tráfego utilizada. Tecnicamente não existe um valor exato do número máximo de usuários que um Access Point suporta.

Vale lembrar, portanto, que quanto maior o volume de dados em uma rede Wireless, menor será a quantidade de usuários suportada pelo Access Point.

2.4 Interferência em redes Wireless

Ao optar por uma rede Wireless devemos ter os seguintes cuidados em questão de interferência, por exemplo:

- Um telefone sem fio que utiliza a freqüência de 2.4Ghz, pode derrubar uma rede Wireless;
- Bluetooth gera interferência em uma rede Wireless, pois o meio de transferência em curta distância, aproximadamente 10 metros utilizados por celulares para transmissão de dados usa a freqüência de 2.4Ghz;
- Outros aparelhos como, forno de microondas e controle remoto de portões eletrônico também podem gerar interferência. [ZANNETI, 2008]

3 Situações práticas de utilização de redes wireless

A seguir várias situações na qual esta tecnologia pode ser utilizada:

- Hospitais, onde relatórios e exames podem ser transferidos em tempo real e obter assim um atendimento em tempo hábil, diminuir riscos de erros na operação do paciente, pois a informação é tratada no momento em que é transmitida através dos handhelds;
- Em auditorias e consultorias a produtividade é aumentada significativamente, pois as informações são acessadas constantemente e em diversos ambientes dentro da companhia;
- Em ambientes onde não existem meios de implantações de rede com fios, pois são antigos e não possuem calhas e pisos falsos;
- Sites remotos onde são realizados backup's de dados on-line, de forma que se houver um problema no ambiente em produção, poder ser contingenciado por este site remoto;
- Não podemos esquecer os restaurantes, na qual a prática vem sendo bastante utilizada, pois o cliente solicita ao garçom seu pedido e a cozinha imediatamente já o faz e ainda a despesa do cliente já se encontra processada no caixa;
- Em vídeo conferências podemos contar bastante com esta tecnologia, já que reuniões hoje em dia podem significar muito ganho para as empresas.

Conclui-se, então, que as redes Wireless podem ser utilizadas em todo tipo de lugar e atenderá de uma forma mais abrangente a visualização da informação.
[ZANNETI, 2008]

4 Padrões de arquitetura IEEE 802.11

4.1 Camada MAC (Media Access Control)

O padrão IEEE 802.11 cobre a camada física e MAC (Media Access Control – Controle de Acesso ao Meio), sendo que a camada MAC interage com a física. Ela é responsável por uma série de tarefas, como controlar o acesso ao meio de transmissão, prover a interação com a rede cabeada, prover a compatibilidade entre os diversos meios de transmissão que possuem taxas de transmissão diferentes. A camada oferece ainda o suporte ao gerenciamento de energia e suporte a roaming (estações que se deslocam de uma célula para outra) [LEITE, 2008].

A camada MAC suporta dois métodos para o acesso, chamados de DCF (Distributed Coordination Function - Função de Coordenação Distribuída) e PCF (Point Coordination Function - Função de Coordenação Pontual) [LEITE, 2008]:

- DCF: Nesse caso, a decisão de quando uma estação pode acessar o meio é realizada individualmente pelas estações de rede, ou seja, existe a possibilidade de ocorrerem colisões. O DCF é a base do mecanismo de acesso do CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance – Sensor de Portadora de Múltiplo Acesso com Impedimento de Colisão). Tal mecanismo é semelhante ao CSMA/CD (Carrier Sense Multiple Access with Collision Detect – Sensor de Portadora de Múltiplo Acesso com Detecção de Colisão) usado nas redes Ethernet cabeadas, ou seja, escuta o canal antes de enviar. A diferença entre o CSMA/CA e o CSMA/CD é que o segundo controla as colisões quando elas ocorrem, e o primeiro apenas tenta evitá-las;
- PCF: Essa função é construída sobre o DCF e tem a finalidade de transmitir quadros assíncronos, sendo que para integrar o PCF e o DCF é utilizado o conceito de super-quadro, fazendo com que o protocolo possa trabalhar de uma forma em que a função pontual situado no Access Point assuma o controle da transmissão para evitar a ocorrência de colisões.

4.2 BSA (Basic Service Area)

Uma rede Wireless IEEE 802.11 tem sua área coberta dividida em células. Essas células, chamadas de BSA (Basic Service Área - Área de Serviço Básica), têm tamanho variado, dependendo de fatores como a potência dos transmissores e receptores, sem falar nas características do ambiente, como por exemplo, a disposição física dos móveis [SOARES, 1997].

4.3 BSS (Basic Service Set)

O BSS (Basic Service Set - Grupo de Serviço Básico) é um grupo de estações que se comunicam via rádio difusão ou infravermelho em uma célula [SOARES, 1997].

4.4 DS (Distribution System)

Apesar de ser possível a existência de uma rede Wireless com apenas 1 célula conhecida como Ad-Hoc, normalmente as redes Wireless são formadas por várias células. Nesse caso, múltiplas BSAs são interligadas através de um DS (Distribution System – Sistema de Distribuição). Tal sistema pode ser uma rede que possui um meio de transmissão Wireless ou mesmo outro meio como UTP/STP (Unshield Twisted Pair / Shield Twisted Pair – Par Trançado Não Blindado e Par Trançado Blindado), BNC (Bayonet Neill-Concelman - Nome do Criador do Cabo Coaxial), mais conhecido como cabo Coaxial e Fibra Ótica, utilizando um Access Point para fazer a interligação entre o DS e o BSA [SOARES, 1997].

4.5 AP (Access Point)

O Access Point é um equipamento especial que captura as transmissões realizadas pelas estações de sua BSA e retransmite ao destino, localizado em outra BSA, utilizando o DS. Um Access Point é comparado a um HUB das redes cabeadas que tem várias funções [SOARES, 1997].

4.6 ESA (Extend Service Area)

Um ESA (Extend Service Area – Área Estendido de Serviço) são os diversos BSAs interligados pelo DS, via Access Point, sendo considerado o maior nível de abstração para redes 802.11 [SOARES, 1997].

4.7 ESS (Extend Service Set)

O ESS (Extend Service Set – Grupo Estendido de Serviço) é definido pela união de vários BSSs, conectados pelo DS. A identificação da rede é feita da seguinte forma: como cada ESS recebe uma identificação (ESS-ID - Extend Service Set Identification - Identificação do Grupo de Serviço Estendido), e cada BSS dentro dessa ESS também recebe uma identificação (BSS-ID - Basic Service Set Identification - Identificação do Grupo de Serviço Básico), o Network-ID de uma rede sem fio é obtido pelo ESS-ID e o BSS-ID [SOARES, 1997].

4.8 Redes sem infra-estrutura (Ad-Hoc)

Uma rede Ad-Hoc, também conhecida como IBSS (Independent Basic Service Set - Grupo de Serviço Básico Independente) é uma rede sem infra-estrutura. Nesse modelo de rede, as estações não precisam de um Access Point para se comunicar, pois comunicam-se diretamente umas com as outras, ao contrário de uma rede estruturada, onde os equipamentos devem enviar a informação ao Access Point, para então esse transmitir até o destino. A rede Ad-Hoc é geralmente uma rede sem infra-estrutura composta de poucas estações e por um período temporário, como por exemplo, em uma conferência, troca de informações em batalhas, em congressos, etc. Quando uma estação quiser transmitir uma informação para uma estação que não está ao seu alcance, outras estações serão utilizadas como ponte, até a informação chegar ao destino [CÂMARA, 2008].

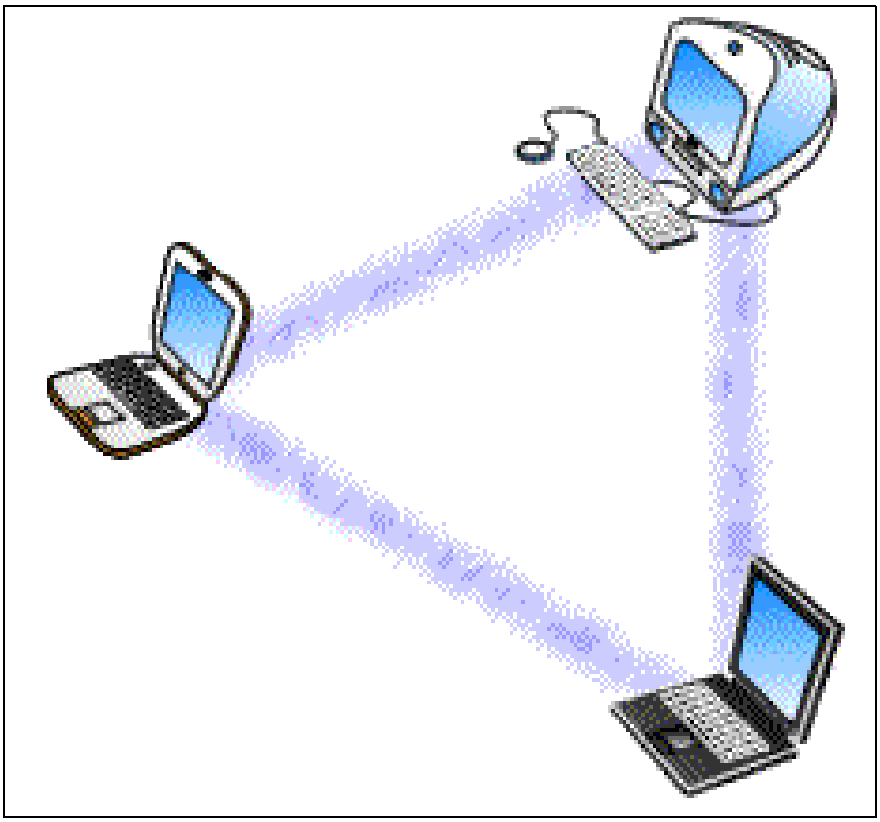

Figura 5: Redes sem Infra-Estrutura (Ad-Hoc)
Fonte: http://www.dc.ufscar.br (2006)

A não existência de um ponto central para distribuição de informações resulta da necessidade de existirem algoritmos de roteamento mais sofisticados, levando-se em conta a topologia das redes Ad-Hoc, que muda de forma freqüente e imprevisível, fazendo assim com que a conectividade entre equipamentos móveis mudem constantemente, obrigando ao sistema uma freqüente alteração nas rotas. Tudo isso devido ao fato de não existir nenhum equipamento fixo, no caso um Access Point.

Uma prova da complexidade dos algoritmos pode ser observada nas características necessárias para ser considerado um algoritmo de qualidade:

- Operar de forma distribuída;
- Ser livre de loops: O algoritmo deve ser robusto, com relação a pacotes que ficam trafegando na rede por períodos arbitrários de tempo. Isto degrada o desempenho da rede como um todo;

- Operações baseadas em demanda de trafego: O método deve ter a capacidade de se adaptar a diferentes condições de tráfego, o que proporcionará uma melhor utilização dos recursos de rede e energia da bateria;
- Segurança: Sem a ajuda de outros níveis do modelo TCP/IP, o protocolo de roteamento é vulnerável as mais variadas formas de ataque;
- Períodos de sonolência: O protocolo deve ter a capacidade de adaptar-se, sem muitas conseqüências, a períodos de inatividade dos hosts móveis;
- Suporte a links unidirecionais: Tipicamente algoritmos de roteamento para redes ad-hoc assumem links bidirecionais, sendo que muitas propostas não funcionam sobre links unidirecionais. [CÂMARA, 2008]

Existem três tipos de algoritmos mais utilizados, são eles:

- Flooding: Nesse método, todo pacote que chega ao nodo é enviado a todos os outros hosts, menos ao host de origem. Esse método é simples, e por isso oferece problemas como loop de roteamento e utilização demasiada de largura de banda;
- Link State (Estado do Link): Nessa abordagem, quando o nodo percebe uma mudança no estado de seus vizinhos, ele faz um flooding dessa mudança pela rede, fazendo assim com que no momento em que os outros nodos souberem da mudança, os mesmos atualizem sua topologia;
- Distance Vector (Vetor Distância): Esse método mantém uma tabela, cuja atualização ocorre periodicamente, com o menor caminho até todos os outros nodos.

4.9 Redes com infra-estrutura

Em uma rede com infra-estrutura é necessário obter Access Point como um centralizador formando então uma ESS com diversas BSSs. Sendo assim, o processo de comunicação relizará 2 Hops. Inicialmente a estação de origem envia as informações para o Access Point e conseqüentemente é transferido até o destino [SOARES, 1997].

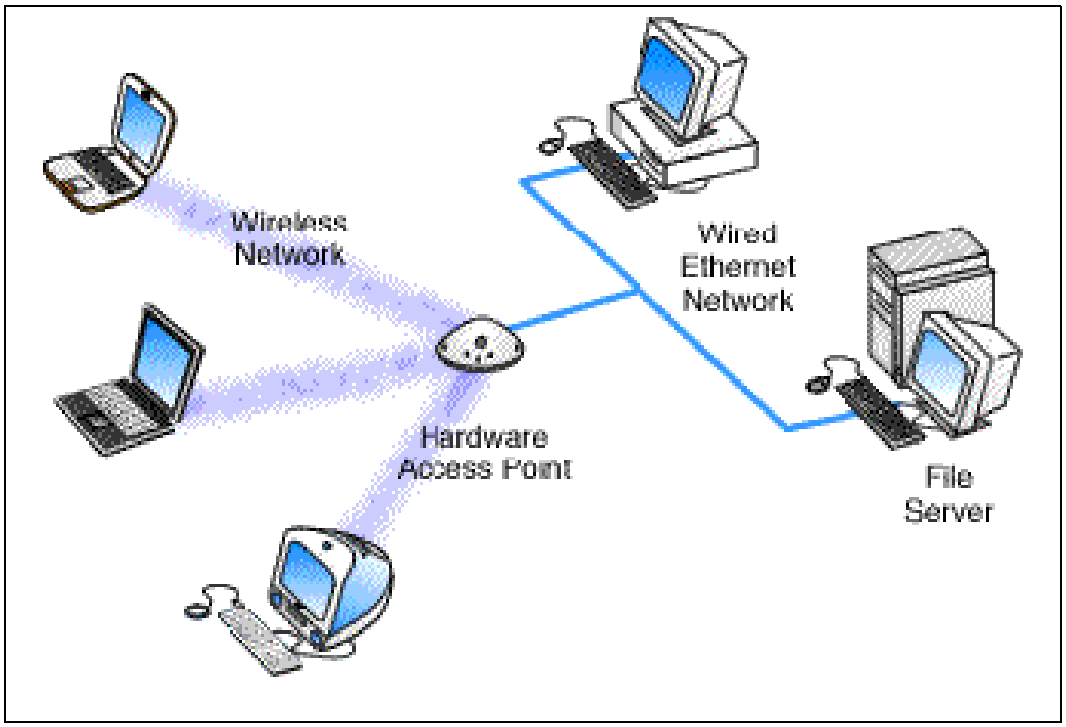

Figura 6: Redes com Infra-Estrutura
Fonte: http://www.dc.ufscar.br (2006)

Vantagens de utilização de uma rede com Infra-Estrutura em relação em uma rede Ad-Hoc:

- O custo não é tão elevado ao ser comparado a uma rede Ad-Hoc, pois não há necessidade de complexidade em sua camada física;
- Com a utilização de um Access Point obtém-se uma economia de energia, afinal quando não são transmitidos sinais as estações ficam em StandBy.

5 Roaming

O roaming é uma importante característica de comunicação Wireless. Permite que estações mudem de célula e continuem enviando e recebendo informações. Sistemas de roaming empregam arquiteturas de microcélulas que usam Access Point estrategicamente localizado. O handoff entre os Access Point é totalmente transparente para o usuário [MATHIAS, 2008].

Redes Wireless típicas dentro de prédios requerem mais que um Access Point para cobrir todos os ambientes. Dependendo do material de que é feito as paredes dos prédios, um Access Point tem um raio transmissão que varia de 10 a 20 metros, se a transmissão for de boa qualidade. Se um usuário passeia com uma estação conectada a uma rede Wireless, a estação tem que se mover de uma célula para outra. A função do roaming funciona da seguinte forma [MATHIAS, 2008]:

- A estação, ao perceber que a qualidade da conexão atual ao seu Access Point está muito pobre, começa a buscar por um outro Access Point;
- A estação escolhe então um novo ponto de acesso baseada, por exemplo, na potência do sinal, e envia um pedido de adesão à célula deste novo Access Point;
- Na célula visitada o Access Point desta, irá verificar se a estação móvel visitante não havia se registrado anteriormente. Caso esse procedimento não tenha sido efetuado, o referido Access Point irá informar ao Access Point da célula origem sobre a nova posição. O novo Access Point envia uma resposta de adesão, e a estação passa a pertencer a essa nova BSS;
- Com isso, o Access Point da célula origem fica sabendo da nova posição da estação móvel, e envia a informação a ela destinada, como se a referida estação estivesse em sua própria célula.

6 Estações (Hidden Node)

Um dos grandes problemas em redes Wireless ocorre quando uma estação fica incomunicável por um período de tempo com o Access Point. São vários os motivos porque isto ocorre. O desligamento da estação móvel, a saída da estação móvel da área de atuação do Access Point ou entrada da estação móvel em uma área onde as ondas de rádio proveniente de outro lugar não se propagam ou local com grande degradação de sinal, que pode ser por motivos geográficos ou ambientais (área de sombra) [MATHIAS, 2008].

O protocolo MAC trata o problema de estações perdidas da seguinte forma:
Ao tentar comunicar-se com a estação móvel, inúmeras vezes sem obter resposta, o Access Point envia um pedido de comunicação para todas as outras estações móveis sob sua área de cobertura. Cada uma destas envia um pedido de comunicação para a estação perdida, esta por sua vez, envia uma notificação de resposta para todos avisando que esta ativa;
As estações que ouvirem esta comunicação enviam um bridge request, diretamente para o Access Point, podendo assim encontrar a melhor opção de comunicação entre o Access Point e a estação perdida.

A comunicação do Access Point com a estação perdida será via ponte. O Access Point deve enviar dados para a ponte, como diretamente para a estação perdida. Assim se esta receber a comunicação, não há mais a necessidade da ponte.
Se o Access Point perder a comunicação com a ponte ou a ponte perder a comunicação com a estação perdida, o Access Point escolhe outra ponte entre as estações que respondera inicialmente.

Com este método o Access Point tem a chance de recuperar uma estação que por algum motivo tornou-se incomunicável com a rede.

7 Segurança em redes wireless

O fator principal que impede a popularização total do Wireless é a questão da segurança comparando-se com as redes cabeadas, mas com o crescimento foram desenvolvidas diversas formas para atender essas necessidades.

7.1 WEP (Wired Equivalent Privacy)

A WEP (Wired Equivalent Privacy - Privacidade Equivalente às Redes com Fios) foi um dos primeiros métodos utilizado para proteger o fluxo de dados e baseiam-se em criptografar os dados transferidos entre os equipamentos, utilizando chaves de criptografia, que pode ser de 64 ou 128 bits. Tais chaves são criadas utilizando o algoritmo de criptografia RC4. Vale lembrar que uma chave de 128 bits é muito mais eficiente do que uma chave de 64 bits [PERES, 2008].

7.2 Open System Authentication

No método, Open System Authentication (Sistema de Autenticação Aberta) sistema de autenticação padrão do IEEE 802.11. Qualquer estação será aceita na rede, sendo necessário somente requisitar a autenticação. Com esse método, caso o mecanismo de criptografia estiver desabilitado, qualquer estação terá acesso à rede, mas caso esteja habilitado, somente os equipamentos que tiverem uma chave secreta é que terão o acesso à rede [PERES, 2008].

7.3 Shared Key Authentication

No método, Shared Key Authentication (Autenticação de Chave Compartilhada), tanto as estações requisitantes como as autenticadoras devem compartilhar uma chave secreta. O processo é o seguinte [PERES, 2008]:

1. Inicialmente, a estação que quer se autenticar envia um frame de gerenciamento REQUEST, para a estação que prove a autenticação, indicando sua necessidade de autenticar-se via chave compartilhada;

2. Ela obtém então uma resposta através de um frame de gerenciamento AUTHENTICATION contendo 128 bytes, que é formado, utilizando-se o gerador de números aleatórios do WEP, com a chave secreta e um vetor de inicialização;
3. Tendo recebido, a estação requisitora extrai o texto do desafio em um novo quadro de gerenciamento, que é encriptado com o WEP, utilizando-se a chave secreta compartilhada junto com um novo vetor de inicialização selecionado por ele. Tal quadro é então enviado à estação autenticadora;
4. Quando tal estação recebe o quadro, ela o decripta e verifica se o texto corresponde aquele enviado anteriormente. Caso positivo, a autenticação foi realizada com sucesso e os envolvidos no processo trocam de função.

7.4 Closed Network Access Control

No método, Closed Network Access Control (Controle de Acesso de Rede Fechada), foi definido um mecanismo de controle de acesso proprietário, onde o Administrador de rede pode utilizar tanto uma rede aberta como fechada, sendo que na rede aberta, qualquer usuário pode se conectar, mas na rede fechada, somente o usuário que souber o nome da rede ou seu SSID, pode-se conectar à mesma [PERES, 2008].

7.5 Listas de Controle de Acesso

Esse método utiliza listas de controle de acesso baseadas no endereço MAC. Uma vez que cada equipamento possui seu endereço MAC (e o mesmo nunca poderá ser alterado), o Access Point pode, opcionalmente, conter uma lista com o MAC que terão permissão de acesso à rede. Assim, se uns equipamentos com um MAC diferente aos que constam na lista do Access Point tentar acessar a rede, o mesmo será impedido. Esse método não é padronizado pelo IEEE 802.11 [BARREIROS, 2008].

7.6 RSN (Robust Security Network)

O RSN (Robust Security Network - Redes de Segurança Robusta) elaborado pelo IEEE,substituiu o WEP em [PERES, 2008]:

- Maiores Vetores de Inicialização;
- Controle de acesso muito rígido através do 802.1x;
- EAP (Extensible Authentication Protocol - Protocolo de Autenticação Extensivo) permite o uso de diversos protocolos de autenticação à escolha do implementador;
- Distribuição de chaves per-session;
- Mais versatilidade, apesar de maior complexidade;
- Gerenciamento seguro de chaves.

7.7 WPA2 (Wi-Fi Protected Access 2)

Depois de ter sofrido várias acusações no mundo de não ter segurança, indiferenças de vários CIOs das Corporações e Bancos principalmente o IEEE ratificou o padrão IEEE 802.11i, que traz as primitivas de segurança intrínseca aos protocolos IEEE 802.11b, 802.11a e 802.11g de WLAN. Os três protocolos de WLAN existentes utilizam o esquema WEP para proteger o link de dados das conexões Wireless entre o Cliente e o Access Point. O WEP utiliza o conceito de Shared key (Chave Compartilhada) que utiliza o algoritmo RC4 de criptografia desenvolvido por Ron Rivest do MIT. É aqui que reside o problema. Com aproximadamente 10 horas de escuta maliciosa a chave pode ser quebrada. Tipicamente os Access Point atuais que utilizam WEP possuem poucas configurações de criptografia.

O novo padrão 802.11i ou WPA 2 (Wi-Fi Protected Access 2 - Proteção de Acesso 2 para Wi-Fi), utiliza o padrão de Criptografia Avançada (AES - Advanced Encryption Standard - Padrão de Criptografia Avançada) e suporta chaves de 128, 192 e 256 bits. O AES é um padrão aprovado para utilização do governo americano utilizando o programa de validação criptográfico FIPS 140-2 (FIPS = Federal Information Processing Standard - Padrão de Processamento de Informações Federais), ele pode fornecer para o Mercado Corporativo uma criptografia robusta e sofisticados codificadores que

poderão exigir novos cartões de acesso e, em muitos casos, novos Access Point. O NIST (a ABNT americana) tem designado o AES como um padrão de segurança para redes Wireless aonde trafeguem informações do Governo Americano.

O caminho para chegar-se ao padrão 802.11i foi longo. A indústria passou antes do WEP para o WPA (Wi-Fi Protected Access - Proteção de Acesso para Wi-Fi), um subconjunto do 802.11i, reparou muitos dos problemas do WEP mas não teve grande aceitação da indústria como proposta intermediária de segurança para redes Wireless, depois que as vulnerabilidades do WEP tornaram-se aparentes. O WEP era facilmente quebrado por hackers. [BARREIROS, 2008]

Atualmente o WPA2 é o nome escolhido pela Aliança de Wi-Fi para identificar o novo padrão IEEE 802.11i. No caso do WPA2 com a criptografia de 128 bits, infelizmente novos hardwares podem ser necessários.

Os processadores atuais nos cartões de Wi-Fi e em muitos Access Point não são poderosos o bastante para criptografar e decriptografar codificadores de 128 bits. Apesar de muitos anúncios afirmarem o contrário, a maioria dos chips de Wi-Fi é poderoso o bastante para manipular a nova especificação de segurança em ambientes Wi-Fi de WPA2, e precisarão simplesmente de atualização de firmware dos respectivos fabricantes, contudo uma quantidade significativa de hardware mais antigo deverá ser trocada. [BARREIROS, 2008]

O WPA inclui mecanismos de TKIP (Temporal Key Integrity Protocol - Protocolo de Integridade de Chave Temporal) e 802.1x. A combinação destes dois mecanismos proporciona criptografia dinâmica de chaves. O mecanismo 802.1x utiliza um servidor Radius para autenticação.

O padrão 802.11i é compatível com o padrão intermediário WPA, contudo o 802.11i pode necessitar incluir uma criptografia adicional AES, que pode necessitar de co-processadores não encontrados no hardware de 802.11i mais antigos.

[BARREIROS, 2008]

7.8 Importantes observações de segurança em redes Wireless

Há aspectos principais para a construção de uma rede Wireless de maneira segura. São eles [PLANETARIUM, 2008]:

- Planejar o local ideal da antena: Não é recomendável colocar a antena que oferece o sinal aos pontos de acesso próximo a janelas, e sim no centro da área a ser coberta;
- Mudar o SSID (Service Set Identifier - Identificação de Grupo de Serviço) e desabilitar o broadcast: O SSID é uma string de identificação utilizada pelos APs. Esse identificador é fixado pelos fabricantes, mas como muitos crackers conhecem esses identificadores, é recomendado alterar o seu código;
- Desabilitar o DHCP (Dynamic Host Configuration Protocol - Protocolo de Configuração Dinâmica de Máquinas): Desabilitando o DHCP, os crackers seriam forçados a decifrar o IP da máquina que querem invadir, além da máscara de rede e outros parâmetros exigidos pelo TCP/IP;
- Desabilitar ou modificar os parâmetros SNMP (Simple Network Management Protocol - Protocolo de Gerenciamento Simples de Rede): Deixando essa opção ativada só vai facilitar a vida dos crackers;
- Utilizar “Access List (Lista de Acesso)”: Deve-se utilizar listas de acesso para especificar quais máquinas poderão se conectar ao ponto de acesso da rede.

8 QoS – Quality of Service

O padrão chamado 802.11e vem sendo desenvolvida com o intuito de introduzir suporte a QoS (Quality of Service - Qualidade de Serviço), de forma que as WLANs possam atender as necessidades das aplicações multimídia em tempo real. Entretanto, as funcionalidades introduzidas não são suficientes para atender os requisitos de QoS das diferentes classes de tráfego em situações de alta carga na rede. Esta deficiência motiva o desenvolvimento de novos mecanismos para monitoramento e controle dos níveis de serviço.

Existem dois mecanismos de controle para complementar a funcionalidade de QoS:
Mecanismo de controle de admissão, adaptado de estudos realizados em redes fixas;
Mecanismo que ajusta dinamicamente os parâmetros de diferenciação de serviços usados no método de acesso com contenção da extensão 802.11e. Os mecanismos propostos contribuem na provisão do serviço requisitado pelas diferentes classes, bem como na utilização eficiente dos recursos da rede.

Na medida em que as aplicações vão sendo mais exigentes no que se refere a e g, surge a questão de como concretizar políticas globais de gestão de QoS em redes Wireless, sem introduzir paralelamente os necessários mecanismos de controle de QoS ao nível do MAC. Ao contrário das redes com fios atuais, a existência de um único domínio de colisão de capacidade reduzida não contribui para fornecer às camadas acima do MAC um serviço que suporte a implementação da gestão de QoS requerida.
A especificação 802.11 original utiliza um MAC baseado na contenção e como tal não fornece mecanismos que satisfaçam requisitos de QoS. A especificação 802.11e objetiva fornecer as extensões necessárias ao MAC 802.11 de forma a garantir QoS.

No entanto, as redes Wireless instaladas e em funcionamento são na sua maioria redes 802.11b que não suportam.

A caracterização de QoS pode ser feita de diversas formas. QoS pode ser considerada para definir o desempenho de uma rede em função das necessidades das aplicações, ou como o conjunto de tecnologias que possibilita às redes oferecer garantias de desempenho. De acordo com o nível de garantia oferecido podemos considerar QoS baseada em reserva de recursos (as garantias são oferecidas para cada fluxo individualmente) ou baseada em prioridades (as garantias são para grupos ou classes de serviço).

As propostas efetuadas para implementar QoS nas WLAN 802.11 incluem vários mecanismos que podem ser usados para atribuir prioridade às diversas classes de serviço. Estes mecanismos envolvem o que está designado na norma 802.11 designados por DCF e PCF, respectivamente, e correspondentes aos dois modos de operação do MAC.

As especificações de qualidade de serviço 802.11e foram desenvolvidas para garantir a qualidade do tráfego de voz e vídeo e, particularmente, será importante para empresas interessadas em usar telefones Wi-Fi.
Apresentou-se ainda o mecanismo de escalonamento ELF para redes onde se utiliza PCF e DCF onde o tráfego com limites temporais é considerado no período PCF, e o restante tráfego no período DCF, mas em que existe uma adaptação do peso dos fluxos em função de um fator de potência. Por último, apresentaram-se os conceitos base do EDCF e HCF mecanismos de acesso da norma 802.11e ainda em estudo.

Como forma de suavizar a transição para os cenários 802.11 de próxima geração e tendo em conta a grande base instalada de WLANs 802.11b, apresentaram-se novas soluções que permitem adicionar alguma qualidade de serviço a estas redes. Utilizam-se soluções que acarretam apenas a modificação dos gestores de dispositivos das interfaces 802.11 disponíveis no mercado.

Considerando os aspectos técnicos associados às soluções apresentadas e mecanismo de quotas/prioridades suportado no modo de gestão de energia, conclui-se que não tem as limitações do PCF, uma vez que é aplicado no período de contenção. É concretizável no hardware existente redes 802.11, 802.11b e prevê a compensação dos erros para além da diferenciação dos serviços. Neste caso, a divisão do período de contenção em diversos períodos, um para cada classe de prioridade, permite uma maior garantia de QoS uma vez que a disputa pelo acesso ao meio se faz apenas entre as estações com a mesma classe de prioridade.

Deve-se registrar que as soluções apresentadas não consideram a interoperabilidade entre as classes de serviço aqui definidas e as definidas na norma 802.11e. No entanto, verifica-se a interoperabilidade básica prevista na norma 802.11e.
O trabalho a realizar futuramente consiste na conclusão da implementação da funcionalidade de Host Access Point, na realização de testes de desempenho da solução implementada (avaliação do débito, utilização média, taxa de colisões, atraso médio no acesso e distribuição de atraso em função da carga) e, por último, na transposição da solução para uma rede Ad-hoc (IBSS).

O WME (Wireless Multimedia Extensions - Extensão Multimídia para Wi-Fi) também conhecido como WMM (Wi-Fi Multimedia - Multimídia para Wi-Fi), trata-se de um conjunto de recursos baseados no rascunho do padrão IEEE 802.11e que oferece recursos básicos de QoS nas redes IEEE 802.11. Priorizam o tráfego de certas aplicações como voz, áudio e vídeo dentro de certas condições e ambientes. A prioridade de tráfego é baseada em quatro categorias de acesso citadas aqui na sua ordem de importância:

- Voz;
- Vídeo;
- Melhor esforço (navegação web e e-mail, por exemplo);
- Background (aplicações que não dependem de latência, como impressão).

9 Materiais e equipamentos

Segue abaixo alguns modelos de equipamentos e materiais para implementar uma rede Wireless compatível com o padrão 802.11g e b, basicamente utiliza-se um Access Point ou um Broadband Router para servir de ponte entre a rede Wired e a rede Wireless.

Deve-se observar principalmente a questão da segurança, ou seja, quais tecnologias de segurança de rede o dispositivo oferece.

Outro cuidado a se tomar é a questão da compatibilidade. Apesar dos dispositivos terem informações de que seguem os padrões IEEE, podem ocorrer conflitos entre dispositivos de fabricantes diferentes. Do ponto de vista do usuário, será necessário um cartão Wireless PCMCIA, placa PCI ou USB para se conectar a rede Wireless.

Figura 7: Access Point Wireless Cisco Modelo: Airronet 1100 AP1121G
Fonte: www.dcsplc.co.uk/product/21186 (2008)

Figura 8: PCMCIA Wireless Cisco Modelo: AIR-CB21AG-W-KP
Fonte: http://www.5ti.com.br/?busca=air (2008)

Figura 9: Adaptador PCI Wireless Modelo: WMP54G-LA
Fonte: http://www.lojacisco.com.br (2008)

Figura 10: Adaptador USB Wireless Modelo: WUSB54GC-LA
Fonte: http://www.lojacisco.com.br (2008)

Para o caso de Hot Spots, a antena a ser utilizada deverá ser Omni-direcional. Estas antenas permitem que se cubra uma área muito maior do que quando se utiliza as antenas vindas de fábrica com os Access Point.

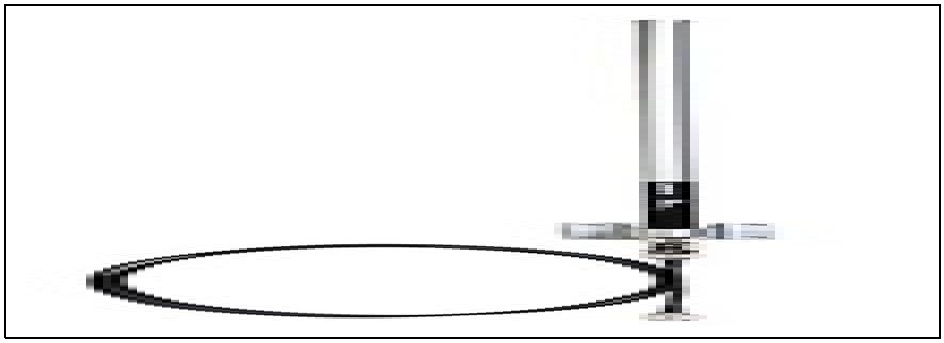

Figura 11: Antena Omni Direcional Linksys Modelo: HGA9N
Fonte: http://www.projetec.com.br/wireless.htm (2008)

Para o caso de se ter um acesso externo (outdoor), a antena utilizada seria direcional como mostrado abaixo. Uma boa antena direcional pode permitir que se conectem

pontos distantes em alguns km, mesmo utilizando tecnologia de redes locais como o IEEE 802.11g ou b.

Figura 12: Antena Direcional
Fonte: http://www.projetec.com.br/wireless.htm (2008)

Além do Access Point e das antenas, serão necessários também cabos, centelhadores e conectores:

Figura 13: Cabo para ambiente externo
Fonte: http://www.wavelan.com.br (2007)

Figura 14: Cabo Pigtail
Fonte: http://www.wavelan.com.br (2007)

Figura 15: Cabo RGC-213
Fonte: http://www.wavelan.com.br (2007)

Figura 16: Conectores
Fonte: http://www.wavelan.com.br (2007)

10 Estudo de Caso

10.1 Implantação de rede Wireless em uma Rádio via Internet

Este é um projeto de implantação de rede Wireless realizado no decorrer do ano de 2007 dentro de uma Rádio via internet, envolvendo um imóvel com três ambientes, sendo um o térreo e mais dois andares superiores, vários dispositivos móvies, estações de trabalho com placa interna wireless, notebooks e Smartphones.

O CPD fica no térreo, hospedando todos os equipamentos, sendo eles: um roteador wireless (TEW-432BRP da Trendnet), um roteador cabo com duas portas WAN (DI-LB 604 da Dlink) e um Switch com 8 portas Dlink e três formas de acesso a internet (dois links Virtua e 1 link Speedy) todos organizados dentro de um rack.

Ainda no térreo, o roteador DI-LB 604 recebe dois canais de (um link virtua e um link speedy) internet, realiza o balanceamento, administrando e alimentando cinco estações, inclusive a de transmissão da rádio. O roteador wireless TEW-432BRP recebe o sinal do segundo link Virtua e envia via cabo para o primeiro e segundo piso.

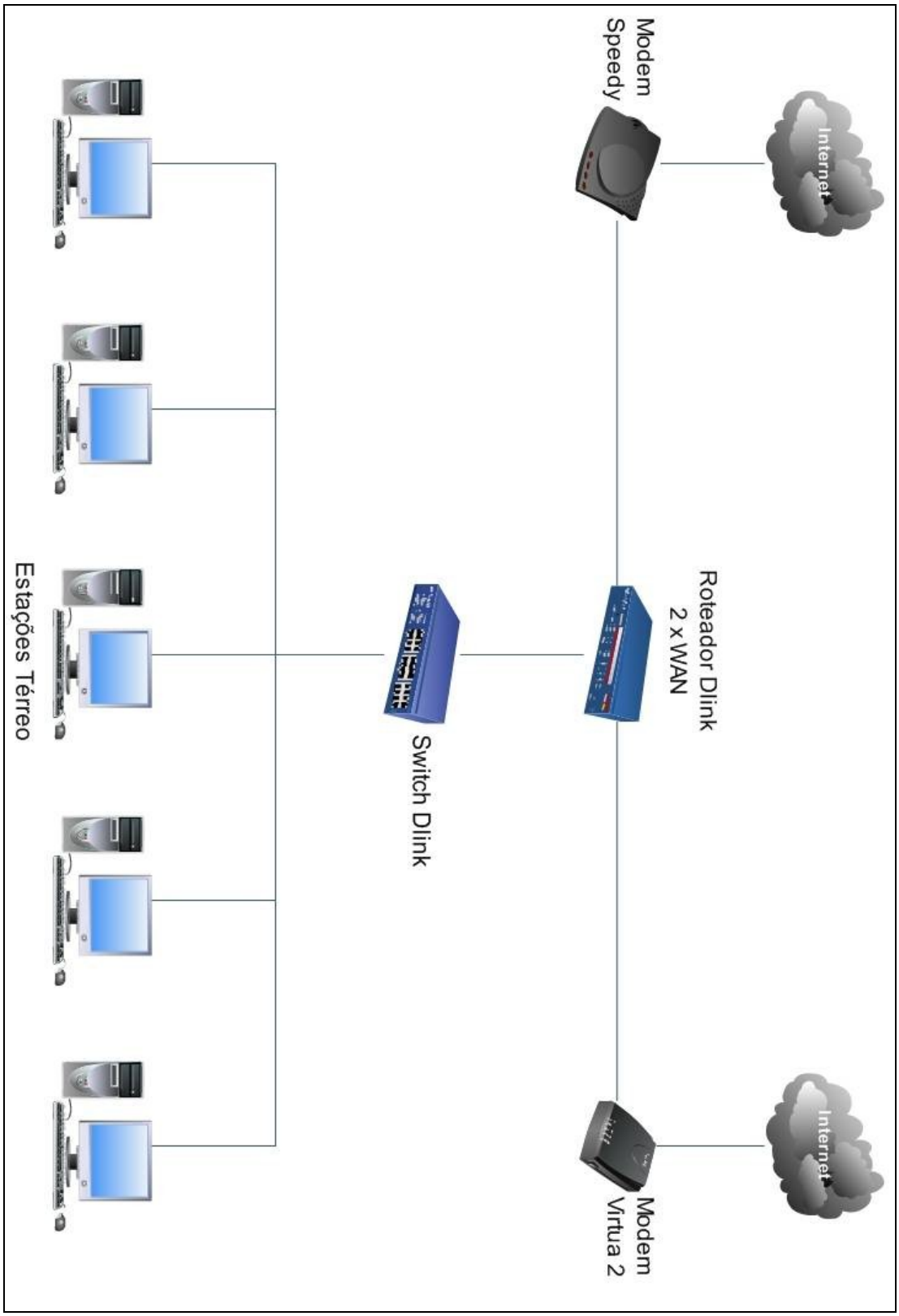

Figura 17: Ambiente Térreo

No primeiro piso existe um Access Point que recebe o sinal via cabo e distribui para todo o andar, alimentando e administrando mais cinco estações e uma impressora wireless HP C6180. Esse piso é independente (em termos de rede) dos demais, pois encontra-se a área administrativa da rádio.

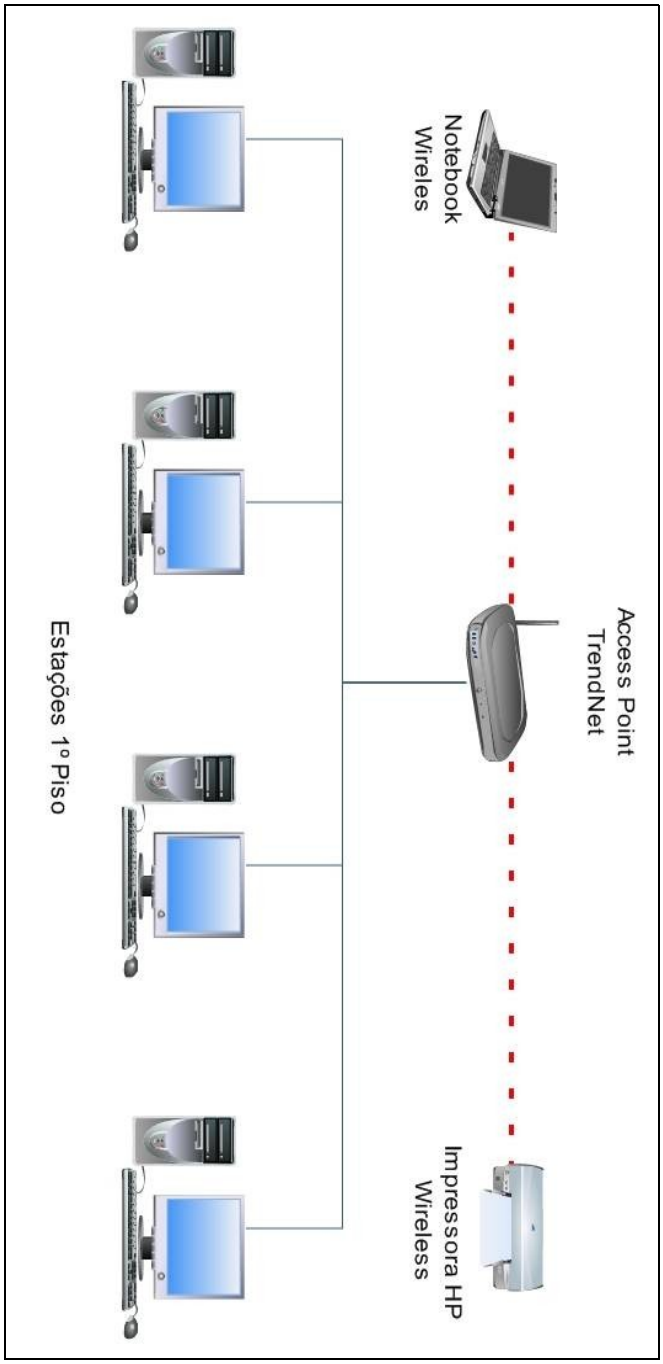

Figura 18: Ambiente 1º Piso

No segundo piso existe um segundo Access Point que recebe o sinal via cabo do roteador e distribui para quatro estações, um servidor e uma impressora, sendo todos wireless. Nesse piso encontra-se a área de desenvolvimento da rádio, possuindo a maior banda de navegação do link Virtua (8mbps).

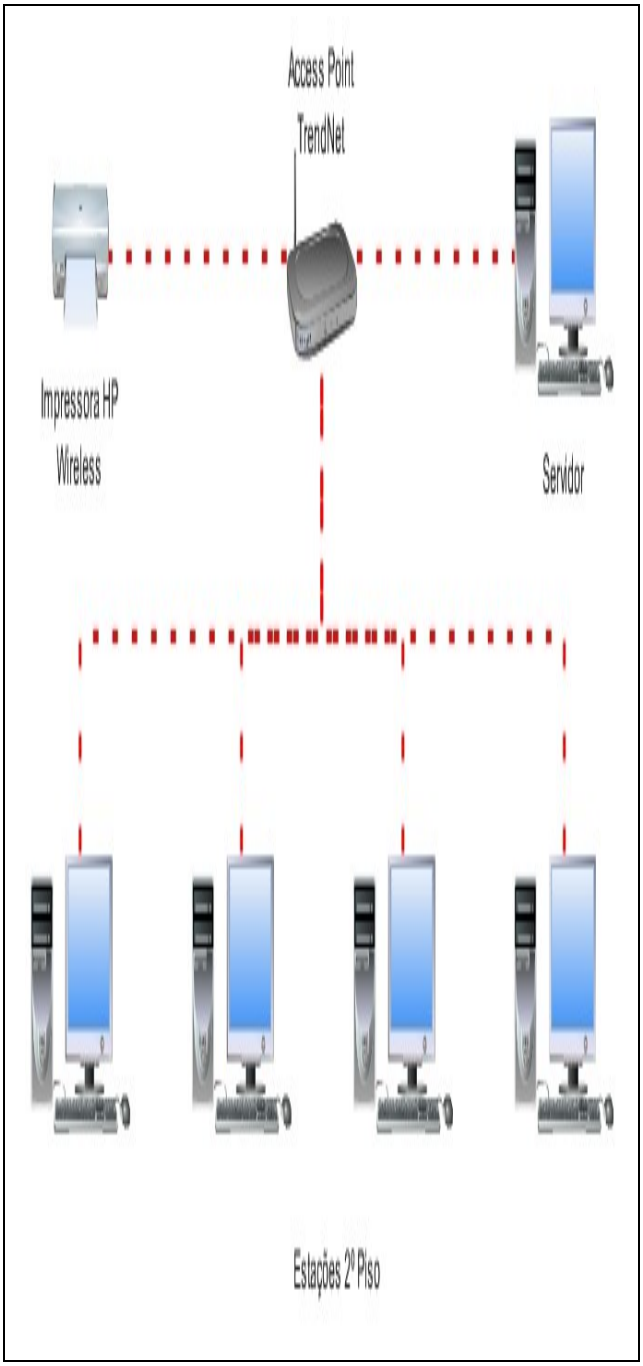

Figura 19: Ambiente 2º Piso

10.2 Opções de Segurança Wireless

Figura 20: Tipos de Segurança

Na figura 20 representa os tipos de segurança em redes Wireless:

- Sem Segurança – Utilizado para acesso público, sem WEP e Broadcast Mode, ou seja, fica totalmente vulnerável;
- Segurança Básica – Utilizado em pequenas empresas, escritórios e residências. É configurado Wi-Fi 40-bit ou 128-bit e WEP estática, ou seja, sem autenticação mutua;
- Segurança Estendida – Utilizado em empresas de médio e grande porte. Toda a parte de autenticação segura utiliza o protocolo EAP-TLS para os clientes e é montada toda uma estrutura de servidores para validar o processo de autenticação: Authority Certificate e Radius.

10.3 Wireless LAN – ROI (Return on Investment)

Numa recente pesquisa pela Wireless LAN Association, 92% das grandes empresas que implementaram WLANs obtiveram benefícios econômicos e comerciais após a instalação e planejam continuar com implementações WLAN no futuro.

11 As próximas gerações de wireless

11.1 O padrão 802.11n

Em resposta à demanda cada vez maior do mercado por redes Wireless com desempenho superior, o IEEE aprovou a criação do IEEE 802.11 TGn (Task Group N – Grupo de Tarefa N). O escopo do objetivo do TGn é definir modificações para a PHY/MAC (Physical Layer and Medium Access Control Layer — Camada Física e Camada de Controle de Acesso ao Meio) que ofereçam uma throughput mínima de 100 Mbps no SAP (Service Access Point — Ponto de Acesso do Serviço) da MAC.

Essa exigência de throughput mínima representa um salto de aproximadamente o quádruplo do desempenho da throughput da WLAN, quando comparado às redes atuais do padrão 802.11a/g. O objetivo nessa próxima etapa do desempenho da WLAN é aprimorar a experiência do usuário com os atuais aplicativos de WLAN e ainda habilitar novos aplicativos e segmentos do mercado. Ao mesmo tempo, o TGn prevê uma transição suave da adoção, exigindo a compatibilidade com versões anteriores nas soluções da tecnologia prévia existente da WLAN do IEEE (802.11a/b/g). A Wi-Fi Alliance também demonstrou interesse no trabalho do TGn relacionado ao 802.11n. Representantes do setor industrial se uniram sob o Grupo de Tarefa Marketing de Alto Throughput da Wi-Fi Alliance para definir e publicar um MRD (Marketing Requirements Document — Documento de Requisitos de Marketing). O MRD da Wi-Fi Alliance especifica as expectativas de desempenho que aperfeiçoarão a experiência do usuário final em relação ao aumento da throughput, aumento da faixa, mais robustez à interferência e uma experiência do usuário mais confiável, no BSS inteiro.
[ROSS, 2003]

Atualmente, a WLAN dos padrões 802.11a/b/g proporcionam um desempenho adequado aos aplicativos de operação em rede de hoje em dia, enquanto a praticidade de uma conexão sem fio pode propiciar.

Com o surgimento dos aplicativos sem fio da próxima geração, será necessária uma throughput de dados mais alta na WLAN. Para atender a essa necessidade, o IEEE TGn e a Wi-Fi Alliance definiram expectativas para o desempenho da próxima geração de WLANs.

A perspectiva do padrão IEEE 802.11n alcançará e excederá a expectativa do IEEE de 100 Mbps no MAC SAP (Topo da MAC). A tecnologia 802.11n deverá suportar todas as principais plataformas, inclusive equipamentos eletro-eletrônicos, tecnologia pessoal e plataformas portáteis nos principais ambientes de hotspots empresariais, residenciais e públicos. O âmbito abrangente dessa perspectiva defende implementações práticas que funcionem de modo robusto, com abordagens técnicas que possam ser desenvolvidas e implementadas dentro dos períodos especificados pelo TGn do IEEE. [ROSS, 2003]

Os principais aspectos ao arquitetar a próxima geração de WLAN são os custos e o desempenho robusto. A tecnologia MIMO (Multiple-Input Multiple-Output - Múltiplas Entradas e Múltiplas Saídas) e os canais com mais largura de banda serão necessários para atender de modo confiável às demandas por throughput mais alta dos aplicativos da próxima geração. Ao mesmo tempo, a throughput global no SAP da camada MAC será possível com os novos recursos MAC que maximizam a eficiência da throughput.

11.2 WI-MESH

O WI-Mesh é uma Rede baseada no padrão IEEE 802.11x, ou seja, é Wi-Fi em que cada nó e cada ponto de acesso possam se comunicar entre si, sem a necessidade de encaminhar o tráfego pelo ponto central.

Assim a rede possui múltiplos caminhos redundantes. Se um link que interliga dois nós falha por qualquer razão, a rede automaticamente encaminha as mensagens por outro caminho.

Por outro lado, a banda total do Wi-Fi é compartilhada entre todos os nós da rede, ou seja, a rede possui 11 Mbps (padrão “b”) ou 54 Mbps (padrões “a” e “g”) e esta taxa é

dividida por entre todos os pontos da rede. Desta forma, não podemos imaginar grandes redes Mesh, pois elas não seriam capazes de fornecer grandes taxas.
Podemos dizer que os principais drivers das redes Mesh são:

- Mobilidade
- Custo
- Tolerância a falhas

Desta forma, elas são um excelente complemento de solução WiMAX (World Wide Interoperability of Microwave - Interoperabilidade Mundial para Acesso Microondas) cujos principais drivers das redes são:

- Qualidade de Serviço
- Cobertura

A Tecnologia Mesh tem sido muito utilizada em projetos de Cidades Digitais. Apesar desta fama da Tecnologia Mesh no segmento de Cidades Digitais ela pode ser explorada em outros pontos como veremos a seguir:

1. Acesso a Internet com mobilidade: Principalmente em áreas abertas permitindo acesso a Internet a dispositivos padrões Wi-Fi em áreas de lazer/parques, eventos, (condomínios horizontais).
2. Aplicações Corporativas Privadas (campus networking): Principalmente, em áreas de grandes indústrias e universidades permitindo acesso a Internet a dispositivos padrão Wi-Fi.

Segurança Pública/Surveillance: Principalmente, em áreas abertas permitindo acessos de dispositivos como câmeras com Wi-Fi para segurança pública.

A Tecnologia Mesh ainda não é um padrão do IEEE como o Wi-Fi (802.11 “a”, “b” e “g”), como o WiMAX (802.16 “d” e “e”) e como o ZigBee (803.15.4), mas estão em vias de se tornar o padrão IEEE 802.11s. [HOCHMAN, 2008]

CONCLUSÃO

Através deste trabalho, concluímos que as redes Wireless podem ser uma alternativa interessante em várias aplicações, já que não são em todas as situações que uma ligação por fios é viável. Com o estudo de uma Rádio via internet, podemos ver claramente a eficiência desta tecnologia, pois se trata de uma tecnologia nova no mercado e que prova que a transferência de dados via wireless é tão eficiente quanto via cabo.

Com este nosso desafio podemos concluir que as redes Wireless além de muito segura e eficiente também tem uma das principais vantagens que é seu custo baixo comparado há uma rede baseada por fios.

Este projeto serviu para implantação da primeira rádio via internet monitorada via wireless, onde nenhuma outra instituição havia implantado antes. Foi utilizado o padrão IEEE 820.11g, segurança WEP com chave dinâmica de 128bits e acesso de administração segura aos Access Point (SSh) através de rede cabeada.

Podemos informar também que além da implementação em redes locais (LANs) e pontes (bridges) entre dois ou mais prédios, novas tecnologias Wireless nos dão a possibilidade de conectar todo o tipo de equipamento periférico de maneira quase instantânea e simples.

Com o aumento da utilização desta tecnologia no mercado, o IEEE desenvolveu um novo padrão chamado de IEEE 802.11n, onde oferece um throughput mínimo de 100 Mbps no Service Access Point da MAC. Também temos o WI-Mesh onde não é necessário enviar o tráfego de dados pelo ponto central, sendo assim podemos ter redundância de link automaticamente. O WI-Mesh ainda não é um padrão IEEE, mas já está prestes de se tornar o padrão IEEE 802.11s.

Como visto neste trabalho, as redes sem fio têm tudo para ser a tecnologia de transmissão de dados mais utilizada em praticamente todos os setores, assim como o cabo de par trançado é atualmente. A quem diga que num futuro próximo existirão somente duas tecnologias de transmissão de dados: fibra ótica e redes sem fio.

Um dos maiores fatores que impediam a popularização das redes sem fio era a questão da segurança, mas esta já foi resolvida com o WPA2, o método mais recente de segurança.

Além da praticidade oferecida pelas redes Wireless, outro fator que contribuirá para a popularização da mesma é o seu custo final, uma vez que os fabricantes irão fornecer mais produtos na área.

REFERÊNCIAS

BARREIROS, Caio Carrone. Segurança no 802.11.
Disponível em: http://www.gta.ufrj.br/~rezende/cursos/eel879/trabalhos/wep/.
Acessado em: 07/02/2008

CÂMARA, Daniel. *Roteamento em Redes Ad-Hoc*.
Disponível em: http://www.dcc.ufmg.br/~danielc/redes/roteamento.html.
Acessado em: 29/01/2008

DELL, Servidores e estações.
Disponível em:
http://www1.la.dell.com/content/products/category.aspx/enterprise?c=br&cs=brbsdt1&l=pt&s=bsd
Acessado em: 10/05/2008

HOCHMAN, Kátia. WIMESH: TELES ENCONTRAM OPÇÃO AO WIMAX.
Disponível em: http://www.malima.com.br/blog/blog_commento.asp?blog_id=53
Acessado em: 12/05/2008

HP, Notebooks e estações.
Disponível em: http://www.hp.com/latam/br/lar/produtos/notebooks.html
Acessado em: 10/05/2008

IEEE. O que é o IEEE.
Disponível em: http://www.ieee.org.br/conselho/organiza.htm.
Acessado em: 11/04/2008

LEITE, Danilo Rangel Arruda. Redes 802.11.
Disponível em: http://sites.uol.com.br/helyr/drangel1.html.
Acessado em: 05/02/2008

MATHIAS, André Pimenta. IEEE 802.11- Redes Sem Fio.
Disponível em: www.gta.ufrj.br/grad/002/ieee.
Acessado em: 30/04/2008

PERES, André, WEBER, Raul Fernando. Considerações sobre Segurança em Redes Sem Fio.
Disponível em: www.sbrc2003.ufrn.br/portugues/programawseg.php
Acessado em: 25/03/2008

PLANETARIUM. Segurança em Redes Wireless.
Disponível em:
http://www.planetarium.com.br/planetarium/noticias/2003/8/1059909106/index_html?pp.
Acessado em: 13/03/2008

PRADO, Eduardo. O mundo Wireless.
Disponível em:
http://www.revistadewimax.com.br/Revista/Mundo_Wireless/tabid/81/Default.aspx.
Acessado em: 14/02/2008

ROSS, John O *Livro de Wi - Fi - Instale, Configure e Use Redes Wireless (Sem - Fio)* Alta Books, 2003.

ROSHAN, Pejman, 802.11 *Wireless Lan Fundamentals* Editora: Cisco Press, 2004.

SOARES, Luiz Fernando Gomes, LEMOS, *Guido*, COALCHER, Sérgio. Redes de Computadores, 1997.

TENENBAUM, Adrew S. *Redes de Computadores*, Editora Campus, 2003.

TULER, Marcos, Comunicação – Ato de comunicar.
Disponível em: http://marcostuler.blogspot.com/
Acessado em 15/04/2008

ZANNETI, Alberto René. Redes Locais Sem Fio.
Disponível em: http://www.dc.ufscar.br/~carvalho/WLAN/index.html.
Acessado em: 12/05/2008

WIRELESS, Redes Enthernet.
Disponível em: www.wirelessbrasil.org/wirelessbr/secoes/sec_ethernet.html
Acessado em: 07/05/2008

WIKIPEDIA, Radiocomunicação.
Disponível em:
http://pt.wikipedia.org/wiki/R%C3%A1dio_(comunica%C3%A7%C3%A3o)
Acessado em: 07/05/2008