UNIMINAS

CURSO DE SISTEMAS DE INFORMAÇÃO

TRABALHO DE FINAL DE CURSO

UTILIZAÇÃO DA METODOLOGIA "SITE SURVEY" EM PROJETOS DE REDES WIRELESS LAN (WLAN)

Edson Machado de Araújo

Junho de 2005

EDSON MACHADO DE ARAÚJO

UTILIZAÇÃO DA METODOLOGIA "SITE SURVEY" EM PROJETOS DE REDES WIRELESS LAN (WLAN)

Projeto de final de curso apresentado à Uniminas como requisito parcial à obtenção do título de Bacharel em Sistemas de Informação.

Banca Examinadora:

Uberlândia, 11 de Junho de 2005

_____

Prof. M.Sc. Johan Max Magalhães

_____

Prof. Esp. Flamaryon Guerin Borges

_____

Prof. Luiz Leonardo Siqueira

À Deus, em primeiro lugar.
À minha mãe em memória, que muito me incentivou através de seu intenso carinho.

AGRADECIMENTOS

Agradeço aos meus amigos e a toda minha família, particularmente ao meu pai, minha irmã e os meus sobrinhos, que ao longo destes 4 anos, abriram mão de uma grande parcela de nosso convívio familiar para que na faculdade eu pudesse me preparar para enfrentar uma nova realidade profissional.

Aos funcionários e professores da Uniminas pelo apoio, especialmente agradeço ao meu orientador Prof. Johann Max, que com muita dedicação contribuiu em minha formação pessoal e profissional, e aos colegas de curso pela amizade e companheirismo de sempre.

Resumo

Nos últimos anos, a comunicação sem fio ganhou um espaço considerável nas tecnologias de transmissão de dados, deixando de existir apenas nas comunicações de longa distância, para fazer parte de ambientes locais. Assim, este trabalho tem como objetivo apresentar um estudo desta tecnologia de rede local sem fio, denominada de wireless Lan (WLAN). Esta tecnologia, apesar de ser possível operar totalmente sem fio, ela tem como característica principal a capacidade de ser tipicamente uma extensão da rede cabeada. Através do equipamento denominado ponto de acesso, que converte os dados em ondas de rádio para a transmissão através do ar. Esta forma de comunicação sem fio visa proporcionar mobilidade no acesso às informações, e flexibilidade na instalação de redes de computadores, sem a necessidade de instalar cabos para a transmissão dos dados. Atualmente, o emprego destas redes está concentrado em locais de difícil acesso, e onde a instalação de fios se torna totalmente inviável. O estudo demonstra que esta tecnologia inicialmente foi desenvolvida apenas para uso doméstico, mas devido a sua constante evolução realizada pelo grupo de pesquisa IEEE 802.11, buscando atingir maiores taxas de transmissões, e maior segurança na utilização destas redes locais sem fio, já esta sendo adotada tanto em domicílios, como em locais públicos e em empresas. Para isto, ao final deste trabalho, apresenta-se um projeto de implantação de uma rede local sem fio, em uma empresa que busca maior mobilidade em seus negócios. Destaca-se a utilização da técnica “Site Survey”, a qual permite maior eficiência e redução de custos de implantação da rede.

Abstract

In the last number of years, wireless communication has assumed considerable space in technologies of data transmission, existing not only in long distance communications, but becoming part of local environments. As such, the objective of this work is to present a study of the technology of local wireless networks, known as wireless LAN (WLAN). Although this technology can operate in a totally wireless environment, typically, its principal characteristic is its use as an extension of the cable network. This occurs through equipment known as point of access, which converts data in radio waves for transmission in air. Wireless communication seeks to provide mobility in access to information, and flexibility in the installation of computer networks, without the necessity of installing cables for data transmission. Currently, its applications are concentrated in areas of difficult access, and where the installation of cables is totally unviable. This study shows that this technology was initially developed only for domestic use. However, owing to constant evolution achieved by research group IEEE 802.11, seeking to achieve ever greater transmission rates and greater security in the utilization of local wireless networks, the technology is being adopted not only for domestic use, but also in public areas and companies. For this reason, we present a case study of an installation project for a local wireless network in a company which seeks greater mobility in its operations. For this, to the end of this work, a project of implantation of a local net without wire is presented, in a company who searchs greater mobility in its businesses. It is distinguished use of the technique “Site Survey”, which allows to greater efficiency and reduction of costs of implantation of the net.

Sumário

Lista de Figuras

Lista de Tabelas

P.

Lista de Siglas e Abreviaturas

AES	Advanced encryption standard
AP	*Access Point*
ATIM	*Ad Hoc TIM*
BPSK	*Binary Phase Shift Keying*
BSA	*Basic Service Area*
BSS	*Basic Service Set*
CBC	*Cipher Block Chaining*
CCK	*Complementary Code Keying*
CCMP	*CCM Protocol*
CRC	*Cyclic Redundancy Check*
CSMA/CA	*Carrier Sense Multiple Access / Collision Avoidance*
CSMA/CD	*Carrier Sense Multiple Access With Collision Detection*
CTS	*Clear TO Send*
DARPA	*Defense Advanced Research Projects Agency*
DCF	*Distributed Coordiantion Function*
DIFS	*Distributed Inter Frame Spacing*
DFWMAC	*Distributed Foundation Wireless MAC*
DS	Sistema de Distribuição
DSSS	*Direct Sequence Spread Spectrum*
EAP	*Extensible Authentication Protocol*
EAPOL	*EAP over LAN*
ESA	*Extended Service Area*
ESS	*Extended Service Set*
ETSI	*European Telecommunications Standards Institute*
FCC	*Federal Communications Comission*
FHSS	*Frequency Hopping Spread Spectrum*
FSK	*Frequency Shift Keying*
GFSK	*Gaussian Frequency Shift Keying*
HP	*Hewlett Packard*
IAPP	*Inter-Access Point Protocol*
IBSS	*Independent Basic Service Set*
ICV	*Integrity Check Value*
IEEE	*Institute of Electrial and Electronics Engineers*
IrDA	*Infrared Data Association*
ISM	*Industrial Scientific and Medical*
LAN	*Local Área Network*
LLC	*Logical Link Control*
MAC	*Media Acces Control*
MIC	*Message Integrity Code*
NAV	*Net Allocation Vector*
NIST	*National Institute of Standardsand Technology*
OFDM	*Orthogonal Frequency Division Multiplexing*
PCF	*Point Coordination Function*
PCMCIA	*Associação Internacional de Cartão de Memória do Computador Pessoal*
PDA	*Assistente Pessoal Digital*

PIFS	*Priority Inter Frame Space*
PPTP	*Point-to-Point Tunneling Protocol*
QPSK	*Quadrature Phase Shift Keying*
RADIUS	*Remote Authentication Dial-In User Service*
RC4	*Ron's Code #4*
RTS	*Request To Send*
SIFS	*Short Inter Frame Space*
SS	*Spread Spectrum*
SSID	*Server Set ID*
WEP	*Wired-Equivalent Privacy*
WI-FI	*Wireless Fidelity*
WLAN	*Wireless Lan*
WPA	*Wi-Fi Protected Access*
WPANS	*Wireless Personal Areas Networks*
WWANs	*Wireless Wide Area Networks*
TIM	*Traffic Indication Map*
TKIP	*Temporal Key Integrity Protocol*
TSF	*Timming Sycronization Function*
VPN	Rede Privada Virtual

1. INTRODUÇÃO

Quando se fala de rede *wireless*, em geral, está-se referindo a três categorias principais, que se diferenciam pelo alcance do sistema. São elas: as redes locais sem fio (ou as WLANs, sigla em inglês de *Wireless Local Networks*), também conhecidas como redes WI-FI (*Wireless Fidelity*); as redes pessoais (ou WPANs, *de Wireless Personal Areas Networks*); e as redes corporativas de longo alcance (ou WWANs, de *Wireless Wide Area Networks*), estas providas pelas operadoras de celular (Silva,2004).

Tecnologias de rede e comunicação de rádio foram empregadas na Universidade do Havaí, em 1971. Foi o primeiro sistema de computadores a empregar a técnica de radiodifusão ao invés de cabos ponto a ponto. Quando o projeto foi implantado, as linhas telefônicas disponíveis na ocasião eram caras e pouco confiáveis. Havia a necessidade de interligação de sub-redes da universidade, espalhadas pelas ilhas, ao Centro de Computação. A comunicação foi realizada através da instalação, em cada estação, de um pequeno transmissor/receptor de rádio FM, com um alcance suficiente para comunicar-se com o transmissor/receptor do Centro de Computação.

Este projeto permitiu que computadores de sete campi, espalhados por quatro ilhas, se comunicassem sem utilização de linha telefônica. O projeto ganhou fama e popularidade pelo emprego da comutação de pacote e difusão por rádio e principalmente pelo apoio e interesse do DARPA (*Defense Advanced Research Projects Agency*), órgão de pesquisa militar americano, que pretendia utilizar redes sem fio como elemento tático de apoio nas comunicações em campo de guerra. O referido projeto não obteve êxito em função da pequena taxa de transmissão de dados pela limitada largura de espectro.

Experiências conduzidas pela HP (*Hewlett Packard*), examinavam a comunicação sem fio entre terminais, o que levou ao pedido junto ao órgão de regulamentação de telecomunicações americano FCC (*Federal*

Communications Comission) de uma faixa de freqüência para redes sem fio. Em 1985, o FCC autorizou o uso público e desregulamentado das bandas Industrial, Científica e Medica (ISM - *Industrial, Scientific and Medical*), tornando o fato um catalisador positivo no desenvolvimento comercial das redes locais sem fio.

A partir de 1985, com a miniaturização dos componentes eletrônicos e a comunicação pessoal sem fio, surgiu em fins de 1990 a tecnologia de rede local sem fio. Desenvolvida pelo grupo IEEE (*Institute of Electrial and Electronics Engineers*), que também acreditando nessa nova tecnologia constituiu um grupo de pesquisa específico com a finalidade de criar padrões para redes sem fio. Sendo definido por este grupo, um nível físico para estas redes, estabelecendo a transmissão de dados através da freqüência de rádio ou infravermelho, e um protocolo de controle de acesso ao meio, o DFWMAC (*Distributed Foundation Wireless MAC*), (C.C. Ribas).

Este padrão é denominado de Projeto IEEE 802.11 e tem, entre outras, as seguintes premissas: suportar diversos canais; sobrepor diversas redes na mesma área de canal; apresentar robustez com relação à interferência; possuir mecanismos para evitar nós escondidos; oferecer privacidade e controle de acesso ao meio para criar padrões abertos que pudessem tornar a tecnologia sem fio cada vez mais realidade.

Este projeto ficou inerte para o mercado por aproximadamente sete anos devido principalmente à baixa taxa de transferência de dados que inicialmente a tecnologia oferecia, que era em torno de Kbps. Com a elevação dessa taxa de transferência de dados, que passou a atingir Mbps, a rede sem fio começou a ser vista como uma tecnologia promissora e a receber ainda mais investimentos para a construção de equipamentos que possibilitassem a comunicação sem fio entre computadores.

Assim, como existe o padrão Ethernet 802.3 para as redes LANs, a norma IEEE 802.11 está presente para definir a forma como as estações wireless se comunicam, mesmo entre elas e com os pontos de acesso da rede cabeada, as chamadas “*Bridges wireless*”. Como no

padrão *Ethernet*, o padrão 802.11 também possui um protocolo de Mac para suportar duas possíveis tecnologias de *receivers* e *tranceivers*: O Infravermelho e a tecnologia de Espalhamento Espectral (Spread Spectrum) em rádios que se divide em três modalidades: sequenciamento direto (*Direct Sequence*), freqüência "saltadora" (*Frequency Hopping*), e OFDM (*Orthogonal Frequency Division Multiplexing).*

As WLANs, ou redes WI-FI, são links de médio alcance (até 100metros para aplicações indoor: ambientes internos, como escritórios, e até 300metros para aplicações outdoor: ambientes externos, como a interligação de dois edifícios) que permitem acesso em banda larga a sistemas corporativos e à Internet, por meio de PDAs, notebooks, handhelds e desktops. Elas podem ser redes totalmente sem fio, ou seja, independentes, ou tipicamente uma extensão de uma rede local (*Local Área Network – LAN*) convencional com fio, criando-se o conceito de rede local sem fio. Elas podem ser instaladas tanto em prédios para uso restrito quanto em locais públicos, os chamados hotspots, onde há grande fluxo de pessoas (aeroportos, hotéis, cafés, universidade). Atualmente os seus principais protocolos possuem as seguintes definições: 802.11a, tem uma taxa de transferência de 54Mbps, e trabalha na freqüência 5GHz, o 802.11b, tem velocidade nominal de 11Mbps e opera na freqüência de 2,4 GHz, já o 802.11g, é considerado o sucessor do b, utilizando a mesma freqüência, mas com uma tecnologia de rádio diferente para atingir até 54Mbps nominais (SUCESU-ES,2004).

Estas redes têm como características, maior flexibilidade e economia se comparada às redes locais cabeadas, e têm como principais objetivos proporcionar a tão sonhada mobilidade no acesso às redes. WI-FI está se disseminando em todo o mundo, com uma tendência de adoção deste sistema sem fio de forma crescente. Muitas soluções WLANs estão ou já foram implantadas em empresas, universidades e outras instituições do mundo inteiro. Isso indica, sem dúvida, que as redes de computadores sem fio são uma realidade e, provavelmente, nos próximos anos, substituirão ou serão adicionais aos sistemas com fio já existentes, passando a ser uma solução bastante interessante para as organizações.

Desta forma os pontos que necessitam de mobilidade são conectados à rede pelo meio *"wireless*" e as estações fixas são ligadas à rede via cabo.

Desta maneira, este trabalho pretende apresentar um estudo dos principais conceitos da tecnologia WLAN, e abordar a importância de elaborar um projeto de implementação desta rede utilizando a técnica "Site -Survey".

Assim, este trabalho foi estruturado da seguinte forma: no segundo capítulo são apresentados alguns conceitos sobre a tecnologia Wireless Lan (WLAN), como: A evolução dos protocolos de transmissão, a arquitetura e os modos de operação da rede, as técnicas de transmissão, os equipamentos necessário nestas redes, as principais aplicações e a evolução dos protocolos de segurança. O terceiro capítulo apresenta as características do nível físico, apresentando as técnicas de transmissão e as faixas de freqüências utilizadas para a transmissão de dados através do ar. No quarto capítulo, são descritos os principais serviços da camada de enlace, e os protocolos de controle de acesso ao meio. O quinto capítulo descreve um projeto de implementação de uma rede local sem fio em uma empresa, utilizando a técnica "Site-Survey". E finalmente, as conclusões são apresentadas no sexto capítulo.

2 CONHECENDO A TECNOLOGIA WLAN

2.1 Introdução

Os avanços nas comunicações nos últimos anos possibilitaram o surgimento de várias tecnologias, que então procuram atender a necessidade de mobilidade dos usuários, com a melhor qualidade possível. Nos últimos anos a comunicação sem fio ganhou um espaço considerável nas tecnologias de transmissão de dados, deixando de existir apenas nas comunicações de longa distância (feitas através de satélite), para fazer parte de ambientes locais.

Essa tendência foi fortalecida pelo investimento de instituições e empresas no sentido de aplicar a transmissão sem fio em redes de computadores. Uma rede sem fio (*Wireless*), é implementada tipicamente como uma extensão ou alternativa para redes locais convencionais *(Local Área Network - LAN)*, criando-se o conceito de rede local sem fio *(Wireless Local Área Network - WLAN)*.

Uma WLAN converte pacotes de dados em ondas de rádio ou infravermelho e os envia, através do ar atmosférico, para outros dispositivos sem fio ou para um ponto de acesso que serve como uma conexão para uma LAN com fio. A FIGURA 1 ilustra uma rede sem fio conectada por um ponto de acesso *(Access Point - AP*) a uma rede convencional com fio.

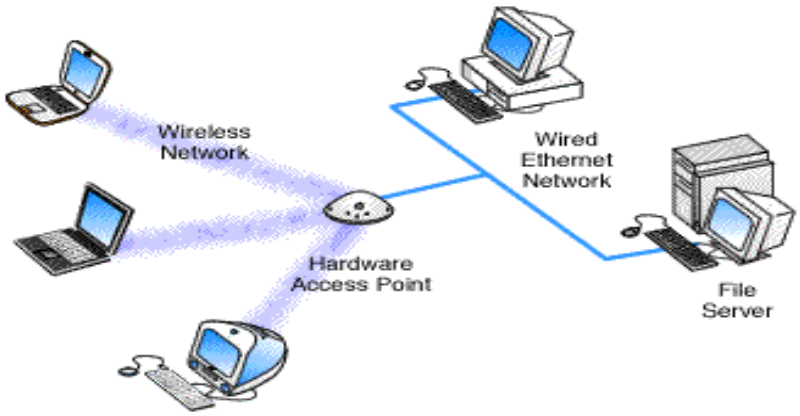

FIGURA 1 : CONEXÃO DE UMA REDE SEM FIO WLAN, COM UMA REDE CABEADA LAN.
FONTE : (Garcia,2004).

2.2 A transmissão em redes locais sem fio (WLANs)

Essas redes basicamente utilizam sinais de radiofreqüência para a transmissão de dados, através das técnicas: DSSS *(Direct Sequence Spread Spectrum),* FHSS *(Frequency Hopping Spread Spectrum)*, e recentemente a OFDM *(Orthogonal Frequency Division Multiplexing)*, codificando dados e modulando sinais de modos diferentes para equilibrar velocidade, distância e capacidade de transmissão.

Outra forma de transmissão também pode ser usada em redes locais sem fio, a transmissão em infravermelho. Mas transmissões com infravermelho não atravessam materiais sólidos, como por exemplo: paredes e portas. Apesar de enviar mais dados do que a transmissão com radiofreqüência. Com isso, a transmissão através de radiofreqüência acaba sendo o padrão adotado nas transmissões WLAN.

As WLANs baseadas em radiofreqüência usam as faixas de freqüência ISM *(Industrial - Scientific - Medical)*, que assumem freqüências de 900MHz, 2.4GHz e 5GHz (Garcia,2004).

2.3 Evolução dos padrões

2.3.1 IEEE 802.11 e IEEE 802.11b

A primeira especificação IEEE 802.11, que foi lançada no mercado em 1997, define basicamente todas as necessidades estruturais para a utilização de redes sem fio. Nesta especificação foram definidos os protocolos de controle de acesso ao meio CSMA/CA *(Carrier Sense Multiple Access / Collision Avoidance),* os tipos de técnica de transmissão utilizadas na rádio freqüência: DSSS *(Direct Sequence Spread Spectrum)* e FHSS *(Frequency Hopping Spread Spectrum)*, a criptografia WEP *(Wired-Equivalent Privacy*), e os principais componentes: placa de rede e ponto de acesso. Com a velocidade de transmissão desta especificação atingindo no máximo 2Mbps, a fabricação de seus produtos não foram muitos prósperos, pois não suportavam as aplicações.

Dois anos após o lançamento da primeira especificação, em 1999, surgiu uma nova especificação, a IEEE 802.11b, que atendia a uma necessidade crescente do mercado, uma maior velocidade de transmissão. As mudanças ocorreram somente na camada física para que fosse possível atingir maior velocidade, neste caso de até 11Mbps. Foi especificado para operar em 2,4GHz utilizando a banda ISM *(Industrial, Scientific and Medical band*), e a técnica de transmissão DSSS.

A especificação IEEE 802.11 foca nas duas camadas de mais baixo nível do modelo OSI, a camada física e a de enlace. A diferença entre a especificação 802.11 e 802.11b é somente na camada física, especificamente na técnica de transmissão DSSS. Alterando a técnica de codificação Barker sequence, para CCK(Complementary Code Keying), permitindo taxas de transferências mais altas (Abras e Sanches,2004).

2.3.2 IEEE 802.11a

Esta especificação em surgiu no mercado em 2001, principalmente devido a necessidade de uma maior taxa de transferência. Outro fator de grande influência foi a grande quantidade de dispositivos utilizando a faixa de 2,4GHz, como por exemplo: redes 802.11b, telefones sem fio, microondas, dispositivos *bluetooth*, etc. Atuando na faixa de 5GHz, os ruídos e tráfego gerados pelos dispositivos anteriormente citados não interferem na comunicação desta rede.

A taxa de transferência pode chegar a 54Mbps. Para isto, utiliza-se um esquema de modulação diferente da especificação 802.11b, este esquema é chamado OFDM (*Orthogonal Frequency Division Multiplexing)*. Esta modulação tem um *overhead* menor que a DSSS, comparando-se uma rede 802.11b a 11Mbps e uma rede 802.11b a 6Mbps, o *thoughput* é basicamente o mesmo devido à eficiência do protocolo.

Apesar dos padrões serem incompatíveis, a camada MAC (*Media Acces Control*) utilizada na especificação 802.11a é a mesma da 802.11b.

Uma analogia pode ser feita em relação às redes *Ethernet* (10Mbps) e *Fast Ethernet* (100Mbps), já que ambas utilizam camada MAC idênticas. Contudo, assim como os padrões *Ethernet* e *Fast Ethernet* utilizam camadas físicas diferentes, 802.11a e 802.11b utilizam técnicas de modulação diferentes, OFDM e DSSS, respectivamente.

Devido à alta freqüência utilizada, 5GHz, a propagação eletromagnética através do canal deve atenuar o sinal duas vezes mais que as redes que utilizam freqüência de 2,4GHz. Porém em condições reais de uso em ambientes fechados, como por exemplo, escritórios, essa diferença pode ser menor.

Um grande problema que os fabricantes vêm enfrentando para a implementação desta especificação é o alto consumo de energia que os dispositivos utilizam (Abras,2004). A sua pouca comercialização, refere-se ao fato da incompatibilidade com as redes 802.11b, que são a maioria já instalada, e o alto custo em relação aos outros padrões existentes. Em 2002 a Intel colocou no mercado um chip com os padrões 802.11b e 802.11a, após atrasos relacionados a testes e validação. Alguns fabricantes adotaram este chip em seus equipamentos devido ao insucesso do 802.11a, mas o seu custo permanecia alto.

2.3.3 IEEE 802.11g

Em 2003, foi lançado um quarto padrão no mercado: 802.11g, considerado como o sucessor do padrão 802.11b, devido a sua compatibilidade com este padrão. O IEEE 802.11g prevê a especificação do MAC e da camada física (PHY). A camada física utilizando a faixa de freqüência 2.4GHz, sendo uma extensão do IEEE 802.11b, com uma taxa de transmissão de 54Mbps, usando a modulação OFDM, a mesma utilizada na especificação 802.11a. Mas como o 802.11b, este novo padrão é também incompatível com o 802.11a.

Utilizando um protocolo estendido, o 802.11g permite o uso misto da rede. Esta característica de uso misto permite que equipamentos que usam o 802.11b operando em 11Mbps possam compartilhar a mesma

rede com os novos equipamentos operando em 54Mbps. Mas havendo um único equipamento 802.11b na rede 802.11g, a performance desta rede diminuirá para algo próximo da velocidade do padrão 802.11b. Mas, existem tecnologias que permitem o aumento da performance destas redes 802.11b e 802.11g. Fabricantes como a *Texas Instruments* e a *Atheros* desenvolveram chipsets para a elevação desta velocidade a novos patamares. A taxa de transmissão nominal da rede pode aumentar de 22Mbps para 108Mbps, e o alcance da rede pode ser aumentado com o uso de antenas mais potentes e de equipamentos como as *bridges*, que permitem alcançar distâncias maiores no caso de uma solução LAN a LAN (Débora,2004).

A compatibilidade com o padrão 802.11b é um ponto forte para a evolução deste padrão, sendo que a maioria das redes locais já existentes são 802.11b. Com a capacidade de proporcionar uma maior taxa de velocidade, a tendência consiste em muitas destas redes migrarem para o padrão 802.11g, diferentemente do padrão 802.11a que é incompatível com o 802.11b (Abras,2004).

2.4 Arquitetura

O padrão IEEE 802.11 define uma arquitetura para as redes sem fio, baseada na divisão da área coberta pela rede em células. Essas células são denominadas de BSA *(Basic Service Area)*. O tamanho da BSA (célula) depende das características do ambiente e da potência dos transmissores/receptores usados nas estações. Outros elementos fazem parte do conceito da arquitetura de rede sem fio, quais sejam:

- **BSS** ***(****Basic Service Set****)*** – ou Conjunto Básico de Serviço, representa um grupo de estações comunicando-se por radiodifusão ou infravermelho em uma BSA.
- **Ponto de acesso** ***(****Access Point – AP****)*** – são estações especiais responsáveis pela captura das transmissões realizadas pelas estações de sua BSA, destinadas às estações localizadas em outras BSAs, retransmitindo-as, usando um sistema de distribuição.

- **Sistema de distribuição** – representa uma infra-estrutura de comunicação que interliga múltiplas BSAs para permitir a construção de redes cobrindo áreas maiores que uma célula.
- **ESA *(Extended Service Area)*** – ou Área de Serviço Extendida, representa a interligação de vários BSAs pelo sistema de distribuição através dos APs.
- **ESS *(Extended Service Set)* –** ou Conjunto de Serviço Extendido, representa um conjunto de estações formado pela união de vários BSSs conectados por um sistema de distribuição *(*P.S.S. Land).

2.4.1. Modo de operação ponto a ponto (Ad Hoc)

No modo ponto a ponto as estações sem fio se comunicam diretamente, sem a necessidade de um ponto de acesso. Todas as estações devem estar dentro da faixa de alcance das placas de rede instaladas em cada estação, formando assim uma configuração de rede.

O modo ponto a ponto é também definido como Ad Hoc ou IBSS (*Independent Basic Service Set*) devido à rede ser independente (Sem comunicação com outras redes) e formada apenas pelas estações sem fio, em uma área denominada de célula. A FIGURA 2 ilustra uma célula da rede ponto a ponto.

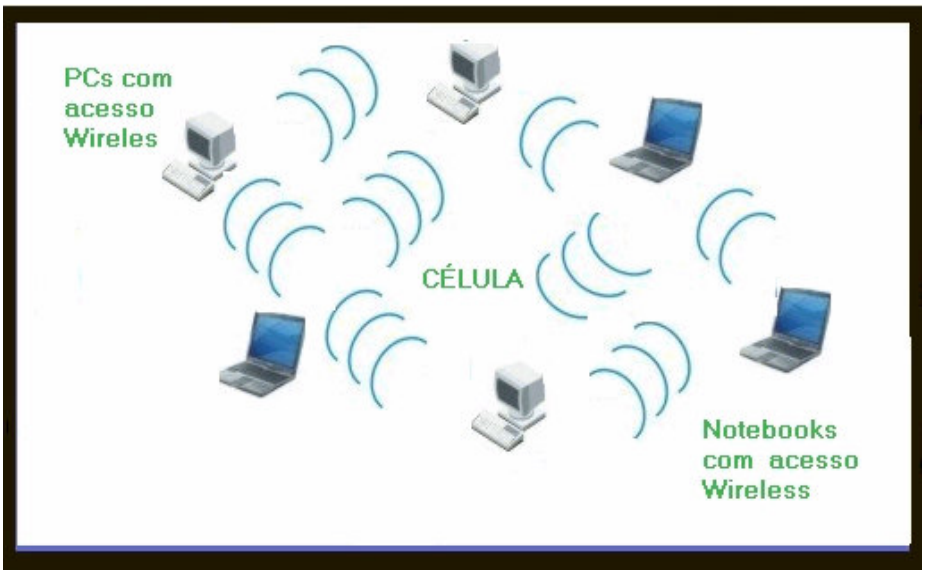

FIGURA 2 : MODO DE OPERAÇÃO PONTO A PONTO (AD HOC).

2.4.2 Modo de operação de Infra-estrutura Básica

O modo infra-estrutura básico, consiste de no mínimo uma base wireless (router, ou ponto de acesso), conectado a rede com fios e um conjunto de uma ou mais estações com acesso a rede sem fio. Nesta configuração todas as máquinas se comunicam com o AP, ao contrário do ponto a ponto, que cada máquina se comunica diretamente com o destino. Esta configuração proporciona economia de energia para as máquinas da rede, já que seu destino é sempre o AP, e uma maior abrangência da área de rede. A FIGURA 3, ilustra uma rede local sem fio com o modo de operação infra-estrutura básica.

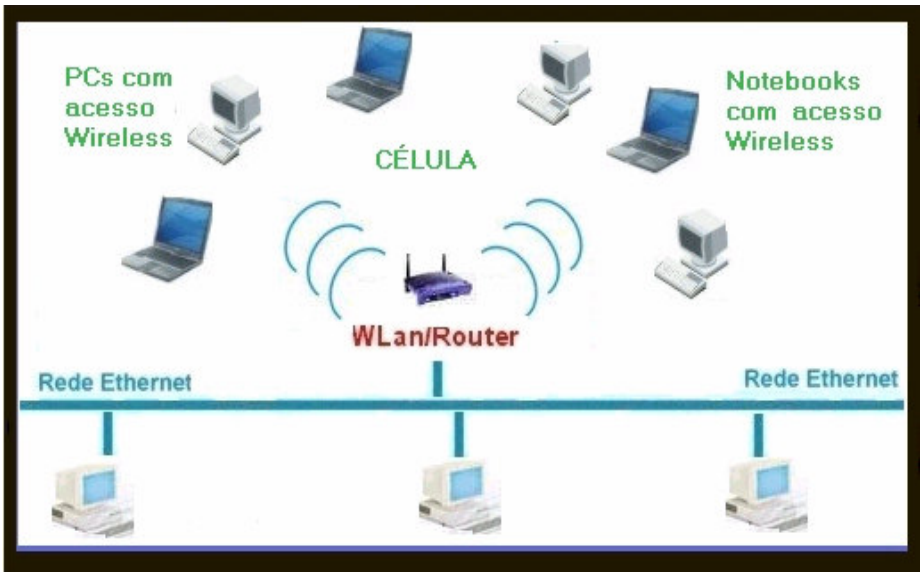

FIGURA 3 : MODO DE OPERAÇÃO COM INFRA-ESTRUTURA BÁSICA.

2.4.3 Modo de Operação de Infra-estrutura com Sistema de Distribuição

O modo de infra-estrutura com sistema de distribuição, consiste de no mínimo duas bases wireless (routers, ou pontos de acesso). Um sistema de distribuição é uma forma de interligar os serviços das redes sem fio além dos limites de uma BSS, formando assim uma grande rede. A especificação não determina a forma como ou em que camada (Dados ou rede) o sistema de distribuição deve atuar, ela apenas especifica quais os serviços devem ser realizados. Sendo assim, o sistema de distribuição

pode ser formado por redes cabeadas convencionais ou outras redes sem fio. A FIGURA 4, apresenta a união de duas células de rede sem fio, e uma rede cabeada, conectadas por um sistema de distribuição. Sendo o sistema de distribuição entre as células com cabo, e a interligação da rede cabeada com as células, com sistema de distribuição sem fio.

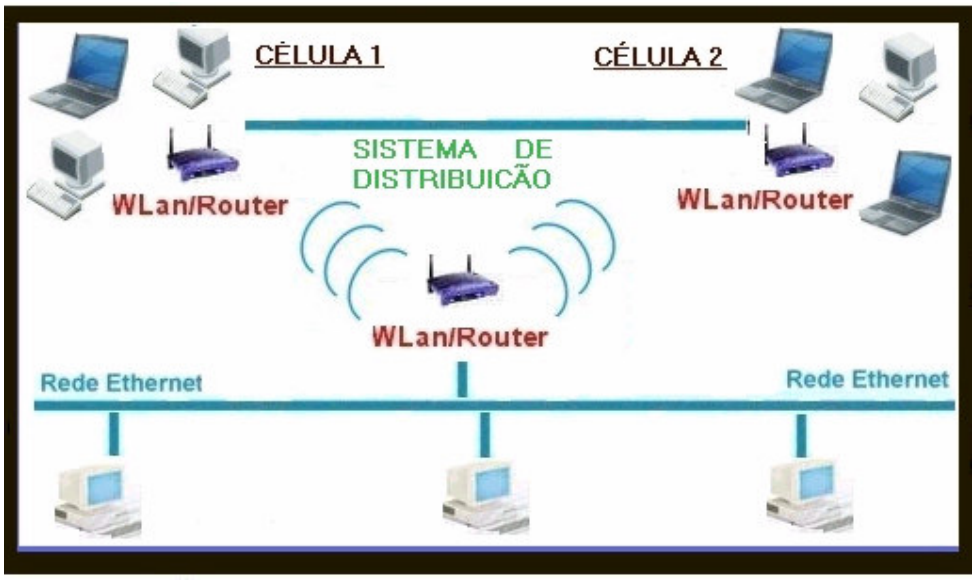

FIGURA 4 : MODO DE OPERAÇÃO INFRA-ESTRUTURA COM SISTEMA DE DISTRIBUIÇÃO.

2.5 Equipamentos de uma rede local sem fio

Os equipamentos de uma rede local sem fio são divididos em dois tipos : os dispositivos do cliente (desktops, notebooks, Pdas, etc...), equipados com adaptadores wireless. E as bases wireless (routers, e pontos de acesso), que realiza a comunicação dos dispositivos entre as redes wireless, e pode-se ainda realizar uma conexão com a rede cabeada. A FIGURA 5, mostra estes equipamentos em uma rede local sem fio.

FIGURA 5 : EQUIPAMENTOS DE UMA REDE LOCAL SEM FIO.

2.5.1 Dispositivos dos clientes

A comunicação sem fio dos dispositivos do cliente, é realizada através de adaptadores wireless. Nos dispositivos fabricados recentemente, estes adaptadores são embutidos de fábrica, já nos dispositivos antigos estes são instalados manualmente. Os adaptadores wireless são:

- **Cartões de PCMCIA (Associação Internacional de Cartão de Memória do Computador Pessoal):** Instalados nos notebooks e Pdas, para “transmitir” os dados através de uma faixa de rádio. Eles possuem uma antena internamente, e também possui um conector minúsculo na extremidade para que possa conectar a uma antena externa, para aumentar o sinal de radio. A FIGURA 6 ilustra os cartões PCMCIA.

FIGURA 6 : CARTÕES PCMCIA.

- **Adaptadores do USB ou uma placa de rede PCI e ISA:** A maioria dos desktops, ainda não possui o entalhe para comunicação via radio. Para resolver este problema, é necessário a instalação de um adaptador USB ou uma placa de rede PCI/ISA. A FIGURA 7 mostra os adaptadores USB e as placas PCI/ISA.

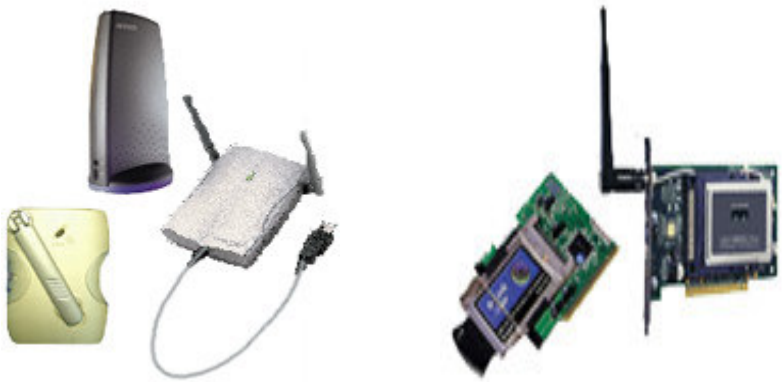

FIGURA 7 : ADAPTADORES USB, E PLACAS DE REDE PCI WIRELESS.

- ***Compact Flash* :** O cartão *compact flash wireless* se instala diretamente no PDA (Assistente Pessoal Digital), usando um slot.

FIGURA 8 : CARTÃO COMPACT FLASH NO PDA.

2.5.2 Bases *wireless*

As bases *wireless* são utilizadas para intermediar os serviços da rede, principalmente em aplicações complexas, e também na extensão de uma rede cabeada. A FIGURA 9 ilustra as bases *wireless* de uma rede local sem fio. Estas bases são denominadas como pontos de acesso, ou passagem de acesso (routers):

- Ponto de acesso simples: funciona com uma “*bridge*”, interligando a rede cabeada existente com a rede sem fios. Este equipamento dispõe somente de uma porta RJ45 para a ligação à rede da instituição.
- Passagens de acesso ("*Router wireless*"): são equipamentos mais complexos com a capacidade de funcionarem como servidores de VLAN's e de DHCP, endereçarem portas e filtrarem pacotes. Este equipamento integra um "switch" com várias portas RJ45.

FIGURA 9 : BASES WIRELESS.

2.6 Como Funcionam as WLANs

Através da utilização de portadoras de rádio ou infravermelho, as WLANs estabelecem a comunicação de dados entre os pontos da rede. Os dados são modulados na portadora de rádio e transmitidos através de ondas eletromagnéticas. Múltiplas portadoras de rádio podem coexistir num mesmo meio, sem que uma interfira na outra. Para extrair os dados, o receptor sintoniza numa freqüência específica e rejeita as outras portadoras de freqüências diferentes.

Num ambiente típico, como o mostrado na FIGURA 1, o dispositivo transceptor (transmissor/receptor) ou ponto de acesso (*Access Point*) é conectado a uma rede local Ethernet convencional (com fio).

Os pontos de acesso não apenas fornecem a comunicação com a rede convencional, como também intermediam o tráfego com os pontos de acesso vizinhos, num esquema de micro células com *roaming* semelhante a um sistema de telefonia celular.

Um grupo de empresas está coordenando o desenvolvimento do protocolo IAPP (*Inter-Access Point Protocol*), cujo objetivo é garantir a interoperabilidade entre fabricantes fornecendo suporte a *roaming* através das células. O protocolo IAPP define como os pontos de acesso se comunicarão através do *backbone* da rede, controlando os dados de várias estações móveis.

2.7 Principais obstáculos e interferência na transmissão

As principais barreiras que podem afetar a propagação do sinal da transmissão de uma rede local sem fio são:

- Antenas ou Pontos de acesso baixos: Uma das orientações repetida à exaustão pelos manuais de pontos de acesso refere-se à localização do equipamento. Quanto mais alto estiver posicionado, menos barreiras o sinal encontrará no caminho até o dispositivo receptor.
- Telefone sem fio: Nas casas e nos escritórios, a maioria dos telefones sem fio operam na freqüência de 900MHz. Mas há modelos que já trabalham na freqüência 2.4GHz, justamente a mesma usadas pelos equipamentos 802.11b e 802.11g. Em ambientes com esse tipo de telefone, ou próximos a ele, a qualidade do sinal pode ser afetada.
- Concreto: Muito prejudicial à propagação das ondas através do ambiente.
- Vidro e Árvore: O vidro é outro material que pode influenciar negativamente na qualidade do sinal. Na ligação de dois prédios por uma rede local sem fio, as arvores altas que estiverem entre os dispositivos podem comprometer a transmissão.

- Água: Grandes recipientes com água, como aquários e bebedouros, são inimigos da boa propagação do sinal.
- Micro no Chão: O princípio das antenas dos pontos de acesso – quanto mais altas, melhor – também vale para as placas e os adaptadores colocados nos computadores.
- Microondas: A lógica é a mesma dos aparelhos de telefone sem fio. Os microondas também usam a disputada freqüência de 2.4GHz. Por isso, o ideal é que fiquem isolados do ambiente onde está a rede.

2.8 Protocolos de Segurança

Talvez para uma empresa, a única coisa mais importante que as informações que trafegam na sua rede, é a capacidade de mantê-las segura. Baseado nesse pensamento, dúvidas sobre a segurança em redes wireless *(WLAN – Wireles Local Area Network*) levam muitos administradores a evitá-las, apesar das vantagens que possam trazer. Contudo, por que esse medo nas redes wireless maior do que em redes cabeadas? Isso se explica pelo fato que em redes cabeadas, se sabe o caminho que a informação percorre, sendo mais difícil alguém conseguir intervir no meio físico para pegar uma informação que não lhe pertença. Enquanto que em redes wireless, o meio sendo o ar, torna muito mais fácil se ter acesso a essas informações e muito mais difícil de ser percebido o ataque. As redes wireless utilizam ondas de rádio para transmitir informações e estas ondas podem viajar além das paredes do escritório ou do prédio, fazendo com que esta informação atinja áreas que podem ser perigosas. Com redes wireless, as bordas de uma rede crescem. Traçando um paralelo com a rede cabeada, quando se instala uma rede wireless, sem medir o alcance do sinal, seria equivalente a se colocar portas ethernet em todo lugar, incluindo locais públicos e estacionamentos.

Além do correto dimensionamento da rede, muito está se investindo nessa área para tentar acabar com essa insegurança no que diz respeito a redes wireless. Existem vários protocolos, chaves e regras para tentar minimizar esse problema.

2.8.1 Protocolo WEP (*Wired Equivalent Privacy*)

Trata-se de um protocolo de camada 2 (camada de enlace) que provê segurança aos dados na transmissão de informações entre o cliente e o ponto de acesso, oferecendo, basicamente, três serviços: confidencialidade, integridade e autenticação. Este mecanismo funciona com base na utilização de uma encriptação com chave simétrica RC4 (Ron´s Code #4). Um vetor de iniciação aleatório associado à chave permite renovar a encriptação em cada nova transmissão. É então a vez de uma segmentação linear do pacote verificar se um pacote recebido está encriptado convenientemente e rejeitar os pacotes forjados. Este protocolo já foi amplamente utilizado, ainda sendo aplicado em muitos casos, pelo menos como umas das opções de segurança disponíveis. Porém, já existem algumas maneiras de conseguir burlá-lo: (Maia,2004).

- **Confidencialidade**: O RC4 utiliza uma nova chave a cada frame enviado, sendo que a chave é formada por uma parte fixa de 104bits (chave secreta) e uma variável (IV). O problema está na parte variável da chave, que possui apenas 24 bits e pode repertir-se em pouco tempo, comprometendo a chave como um todo. Em uma rede com grande fluxo de mensagens, através do monitoramento do tráfego da rede é possível derivar chaves de 128 bits após o envio de cerca de quatro milhões de frames ou depois de quatro horas de monitoramento. Softwares especializados realizam tal ataque, por exemplo, o Airs nort.

- **Integridade** : A garantia que o frame não seja alterado entre o transmissor e o receptor é implementado a partir da técnica de CRC-32 (Cyclic Redundancy Check), que gera um ICV (Integrity Check Value) para cada frame enviado. Ao receber o frame, o destinatário executa a mesma função de CRC e compara o ICV obtido com ICV recebido. Caso o valor do ICV calculado for igual ao ICV recebido, a mensagem está integra, caso contrário, o frame sofreu alguma alteração. A utilização da técnica de CRC para gerar a integridade do frame, torna o WEP vulnerável à ataques do tipo replay.

2.8.2 Protocolo 802.11i

O protocolo 802.11i criado pelo grupo IEEE, com o objetivo e eliminar as vulnerabilidades existentes no WEP. O 802.11i se divide em duas arquiteturas: o TKIP (*Temporal Key Integrity Protocol*), e também o AES *(Advanced Encryption Standard).*

2.8.2.1 TKIP

Também chamado de WEP2, ou WPA (*WI-FI Protected Access*), é apenas um subconjunto do 802.11i. Ele continua utilizando o sistema de encripatação RC4, mas também disponibiliza um mecanismo de controle de confidencialidade e integridade eficaz. A integridade no TKIP é garantida através do MIC (*Message Integrity Code*). O MIC é um campo do frame 802.11i, calculado a partir de diversas informações contidas no próprio frame, como por exemplo, os endereços MAC de origem (SA) e destino (DA). O MIC é calculado a partir de uma função de hashing, conhecida como Michael.

Para confidencialidade, ele utiliza um vetor de inicialização de 48 bits, ao invés de 24 como no WEP e um mecanismo de distribuição de chaves (Maia, 2004).

2.8.2.2 AES - CCMP

Substituindo a criptografia simétrica RC4, o protocolo CCMP (*CCM Protocol*) utiliza o novo padrão para criptografia simétrica AES (*Advanced Encryption Standard*), aprovado pelo NIST (*National Institute of Standardsand Technology*) em 2002. O AES trabalha com blocos de 128 bits e, no caso do 802.11i, chaves de 128 bits.

O AES trabalha com diferentes modos de operação, que alteram a forma como o processo de criptografia é realizado. Os modos de operação têm o objetivo de prevenir que uma mesma mensagem quando criptografada gere o mesmo texto cifrado. O CCM utiliza o modo de operação conhecido como CBC (*Cipher Block Chaining*). Neste modo de operação, o texto cifrado no passo anterior é utilizado como entrada no processo de criptografia subseqüente. No primeiro passo, como ainda não existe um texto cifrado, é utilizado o vetor de inicialização. Sendo que o vetor de inicializacão é incrementado a cada bloco criptografado, gerando uma chave única para cada bloco. A integridade é implementada através do MIC, gerado a partir do vetor e informações contidas no header do frame (Maia,2004).

2.8.3 Protocolo IEEE 802.1X

O padrão IEEE 802.1X foi concebido para oferecer autenticação, controle de acesso e distribuição de chaves criptográficas em redes locais com e sem fio. É importante destacar que o 802.1X não está ligado apenas ao padrão IEEE 802.11, mas a todos os padrões de redes locais e metropolitanas, patrocinados pelo IEEE 802. Além disso, o padrão pode ser utilizado em conjunto com diversos protocolos de autenticação localizados nas camadas superiores. O grupo de trabalho 802.11i definiu que o mecanismo de autenticação a ser utilizado no IEEE 802.11 deverá seguir o modelo do IEEE 802.1X.

A autenticação no IEEE 802.1X é realizada nos dois sentidos (*mutual autentication*) e utiliza o esquema de *challenge-response*. Existem três componentes a serem considerados no padrão: autenticador, supplicant e servidor de autenticação. Em uma rede sem fio, o autenticador é geralmente o AP (*Access Point*) e o supplicant uma estação que deseja conectar-se ao AP. O servidor de autenticação é o verdadeiro responsável por autenticar o supplicant, com base nas informações oferecidas por ele. O padrão não especifica qual servidor de autenticação deve ser utilizado, podendo ser, por exemplo, um servidor RADIUS (*Remote Authentication Dial-In User Service*). Na verdade, o servidor de autenticação não precisa ser necessariamente um elemento externo, podendo fazer parte do próprio AP.

O IEEE 802.1X implementa o protocolo EAP (*Extensible Authentication Protocol*), em conjunto com o EAP over LAN (EAPOL). O EAP permite o encapsulamento de diversos protocolos de autenticação oferecidos nas camadas superiores e, conseqüentemente, não definidos pelo 802.1X. Estes protocolos oferecem diferentes métodos de autenticação, como Kerberos, senhas, certificados digitais e chaves públicas. Desta forma é possível que o usuário também seja autenticado e não apenas a estação (Maia,2004).

2.8.4 Tecnologia VPN (Rede Privada Virtual)

Muitas companhias grandes utilizam a tecnologia de VPN (Rede Privada Virtual) para a equipe de funcionários que necessitam acessar remotamente a base de dados incorporada da companhia. Os sistemas de VPN trabalham também para redes *Wireless LAN*.

Uma VPN cria um túnel virtual de seu computador até a sua matriz, através do ponto de acesso wireless local, utilizando a Internet. Mesmo que possa ser complicado e caro, utilizar a tecnologia VPN, cria uma parede quase impenetrável de segurança para suas comunicações sem fio.

2.9 Aplicações

As redes podem funcionar em ambientes indoor (escritórios, residências, lojas, etc..) ou outdoor (lugares abertos, como interligações de prédios), e apresentam aplicações tanto residenciais quanto corporativas, sendo encontradas principalmente na substituição ou complementação dos cabos em empresas, pequenos escritórios, ou na moradia de um consumidor.

As principais aplicações estão presentes em ambientes que a instalação de fios é mais complexa, e até mesmo inviável. Assim, como opção, a rede local sem fio está dominando estes serviços. Alguns destes serviços são:

- Ambientes de difícil cabeamento (museus, edifícios históricos, etc.)
- LAN's provisórias (conferências, seminários, etc.)
- Ambientes móveis dentro das instalações (posto de venda móvel, assistência médica, etc.)
- Locais públicos com grande fluxo de pessoas (aeroportos, cafés, estádios, etc.)
- Em hotéis, onde ficam hospedados executivos que acessam a tecnologia através de notebooks.

A FIGURA 10, ilustra as principais aplicações de uma rede local sem fio :

FIGURA 10 : APLICAÇÕES WIRELESS LAN.

3. CAMADA FÍSICA

3.1 Introdução

O IEEE 802.11 permite a conectividade das WLANs com as redes cabeadas tradicionais. Ou seja, o padrão especifica as camadas mais baixas (física e enlace – do modelo OSI), mas mantém a mesma interface com as camadas superiores. O grupo IEEE 802.11 definiu um nível físico para transmitir os dados pelo ar através da freqüência de rádio ou infravermelho, e um protocolo de controle de acesso ao meio, o DFWMAC (*Distributed Foundation Wireless MAC*). Da mesma forma como em qualquer outro padrão 802.x, a subcamada LLC (*Logic Link Control*) e os demais níveis superiores não percebem as particularidades da subcamada MAC e de seus possíveis níveis físicos. A FIGURA 11 ilustra o padrão IEEE 802.11, comparando-o com o modelo padrão de redes de computadores, o RM-OSI da ISO (*Reference Model – Open Systems Interconnection of the International Standardization Organization*).

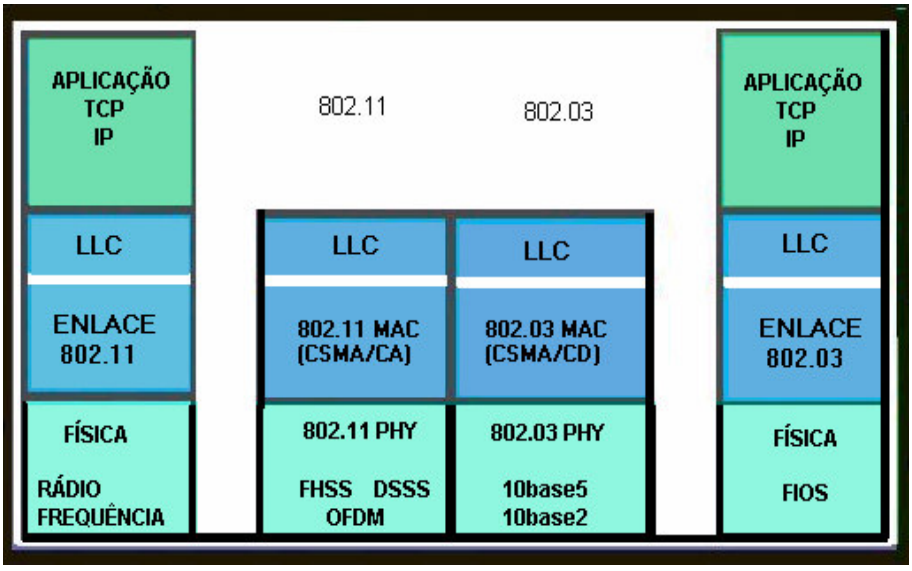

FIGURA 11 : COMPARAÇÃO DAS REDES WLAN X LAN.

A Camada Mac de uma WLAN é diferente de um rede convencional, a subcamada LLC (*Logical Link Control*) serve para acobertar essas diferenças. Em muitas redes atuais, nenhuma camada explícita LLC é visível. A FIGURA 12 mostra um cenário típico: uma WLAN IEEE 802.11 conectada com uma rede Ethernet por uma ponte. A camada de aplicação não deve perceber nenhuma diferença em relação às camadas inferiores das duas redes (uma possível diferença seria o tempo de acesso maior em relação à WLAN). Conseqüentemente, as camadas mais altas (Aplicação, Transporte, Rede) “vêem” as estações sem fio ou as estações cabeadas da mesma forma.

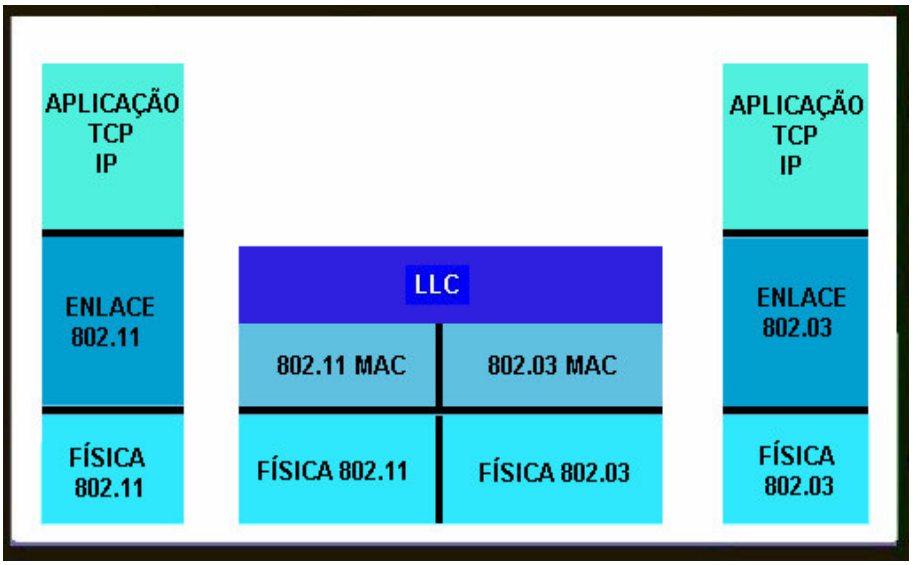

FIGURA 12 : WLAN IEEE 802.11 CONECTADA COM UMA REDE ETHERNET.

3.2 Freqüências de transmissão sem fio

As freqüências utilizadas nas redes locais WLAN, não precisam de autorização. As condições de uso destas no Brasil estão estabelecidas pelo Regulamento sobre Equipamentos de Radiocomunicação de Radiação Restrita. Atualmente o Brasil está atualizando a Resolução 305 da ANATEL, nas partes referentes a 2.4 e 5 GHz, disponibilizando a distribuição apresentada na FIGURA 13 (Teleco,2004).

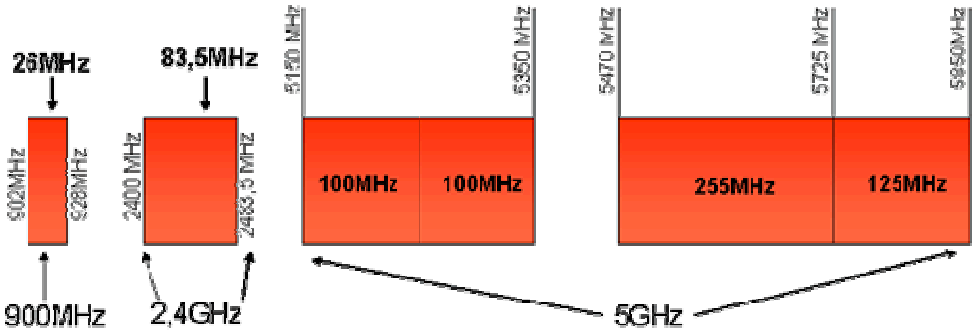

FIGURA 13: FAIXAS DE FREQUÊNCIAS PARA WLAN. FONTE (TELECO,2004)

A faixa de 900 MHz, utilizada no primeiro protocolo 802.11, apresentava dois pontos negativos para a expansão da tecnologia WLAN: O primeiro era em relação à largura de banda de somente 26MHz, que limitava o número de usuário e as taxas de transmissão. O Segundo estava relacionado às interferências causadas devido a grande quantidade de serviços que utilizam esta faixa, tornando a qualidade das operações de computadores sem fio impraticável. Entre as fontes de interferências, pode-se citar: telefone sem fio, rádio amador, sistemas móveis celulares, dentre outros.

Com os limitantes apresentados na faixa de 900MHz, para não implicar no fracasso destas redes, o grupo IEEE desenvolveu o protocolo 802.11b e posteriormente o 802.11g, utilizando a freqüência de 2.4GHz. Esta faixa minimiza as interferências em relação à 900MHz, mas não é aceita por alguns países, gerando limitações no uso mundial dos equipamentos.

A freqüência de 5GHz utilizada pelo protocolo 80211a, apresenta uma maior banda, com melhores condições para transmissões, e em conjunto com um maior número de usuários. Além de minimizar os problemas de interferências e qualidade de serviços em relação às outras faixas. O problema em 5GHz começa a ser a divisão do mercado criada pela adoção de diferentes padrões e faixas de operação em regiões como as Américas, a Europa e o Japão. No IEEE tem-se o desenvolvimento do padrão 802.11a com taxas até 54Mbit/s. Na Europa, o ETSI (*European Telecommunications Standards Institute*) participa do desenvolvimento dos

padrões Hiperlan1, com taxas até 20Mbit/s, e o Hiperlan2, com taxas até 54Mbit/s. No Japão tem-se o desenvolvimento do HisWAN (Teleco,2004).

3.3 As técnicas de transmissão sem fio

Na rede local sem fio os pacotes são transmitidos através do ar, utilizando as técnicas de espalhamento espectral em canais de freqüência de rádio (freqüências na faixa de KHz até GHz) ou infravermelho (freqüências da ordem de THz). São especificados três padrões de espalhamento espectral: o tipo de modulação OFDM (*Orthogonal Frequency Division Multiplexing*), o espalhamento espectral por seqüência direta (DSSS – *Direct Sequence Spread Spectrum*), e o espalhamento espectral por saltos em freqüência (FHSS- *Freqüência Hopping Spread Spectrum*).

O SS (*Spread Spectrum*), ou Espalhamento Espectral, é um meio de transmissão adequado para fornecer uma comunicação segura em um ambiente hostil. O SS espalha o sinal portador de informação fazendo-o ocupar uma faixa muito maior que o necessário para transmiti-la. A técnica faz com que o sinal ocupe toda a faixa e assuma uma "aparência" de ruído, dificultando a sua detecção e aumentando a sua imunidade a outras fontes localizadas de interferência.

3.3.1 FHSS (*Frequency Hopping Spread Spectrum*)

Conforme apresentado na FIGURA 14, a técnica de *Frequency Hopping* consiste na utilização de saltos pseudo-aleatórios, nas frequências utilizadas em uma modulação do tipo FSK (*Frequency Shift Keying*). Ou seja, ao invés de utilizar freqüências f1 e f2 pré-definidas, as freqüências utilizadas para se transmitir 0 ou 1 são alterados de acordo com uma seqüência pseudo-aleatória gerada (código PN), conhecido somente pelo transmissor e pelo receptor. Sincronizados adequadamente, eles mantêm um único canal lógico. Para um receptor não desejado, o FHSS aparece como ruído de pulso de curta-duração.

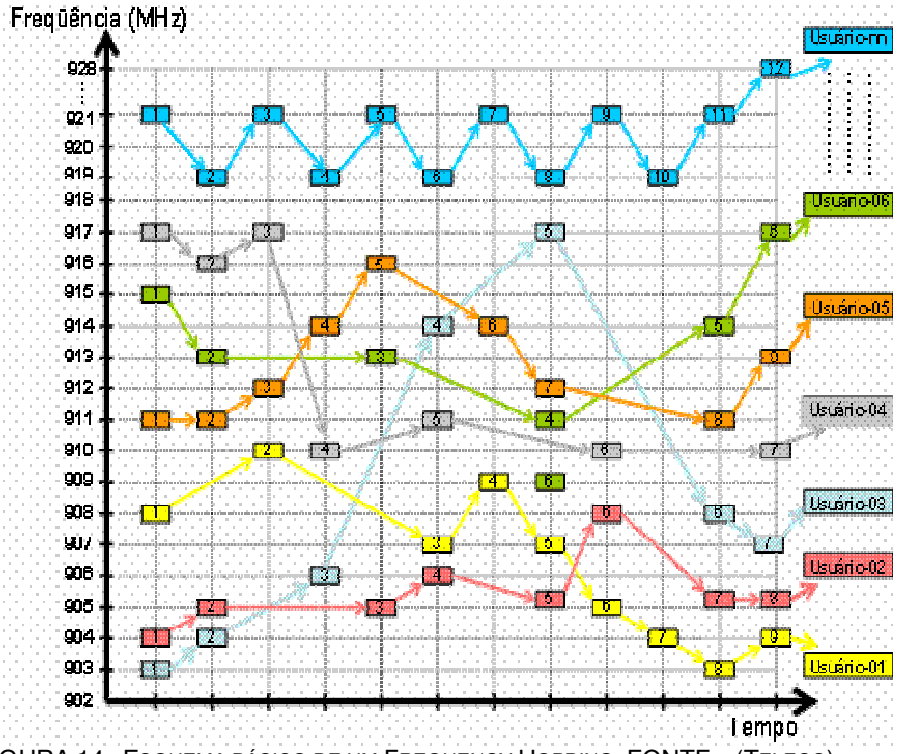

FIGURA 14 : ESQUEMA BÁSICO DE UM FREQUENCY HOPPING. FONTE : (TELECO)

Utilizada somente na especificação IEEE 802.11, a técnica FHSS envia segmentos curtos de dados que são transmitidos através de freqüências específicas. Controlando o fluxo com o receptor, que negocia velocidades menores comparadas às velocidades oferecidas pela técnica DSSS, mas menos suscetíveis a interferências devido a cada transmissão ocorrer seguindo um padrão diferente de saltos, minimizando a chance de dois transmissores utilizarem o mesmo canal simultaneamente.

Com esse espalhamento, consegue-se um melhor desempenho do sistema, melhorando sua imunidade a ruídos, e impedindo que uma pessoa que não conheça a seqüência de saltos consiga escutar a transmissão.

A modulação definida para a camada FHSS é o 2-GFSK para a taxa de 1 Mbps, e o 4-GFSK para 2 Mbps, utilizando um canal de 1 Mhz. O GFSK (*Gaussian Frequency Shift Keying*) é uma técnica de modulação similar ao FSK, que utiliza pulsos gaussianos, ao invés de pulsos senoidais, para obter uma melhor eficiência espectral.

O 2-GFSK utiliza 2 freqüências possíveis, transmitindo 1 bit por símbolo, enquanto o 4-GFSK utiliza 4 freqüências possíveis, transmitindo então 2 bits por símbolo.

Por ser menos eficiente que a outra técnica de espalhamento espectral, o uso da técnica *Frequency Hopping* foi praticamente descontinuado com a introdução do 802.11b, que se manteve compatível apenas com a técnica de *Direct Sequence* (UFRJ).

3.3.2 DSSS (*Direct sequence Spread Spectrum*)

Nesta técnica de espalhamento espectral, a banda de 2.4GHz é dividida em 14 canais de 22MHz. Canais adjacentes sobrepõe um ao outro parcialmente, com 3 dos 14 canais sendo totalmente não sobrepostos. Os dados são enviados por um destes canais de 22MHz sem saltos para outras freqüências. Para compensar o ruído que pode existir no canal, uma técnica chamada *chipping* é utilizada. Cada bit de dados do usuário é convertido em um padrão de série de bits redundantes chamados *chips*. Essa redundância agregada à dissipação do sinal através do canal de 22 MHz proporciona uma forma de checagem de erro e correção, até mesmo se o sinal for danificado, há possibilidade de recuperação do sinal em muitos casos, evitando assim a necessidade de retransmissão.

Na especificação 802.11, o DSSS utiliza 11-bit chipping, chamado de *Barker sequence*, para codificar os dados enviados pelo ar. Cada seqüência de 11-chip representa um simples bit de dado, o qual no formato de uma onda pode ser chamado de símbolo. A taxa de transferência destes símbolos é de 1MSps (1 milhão de símbolos por segundo), equivalente a 1Mbps, utilizando uma técnica de modulação chamada BPSK (*Binary Phase Shift Keying*). No caso da transmissão a 2Mbps, apesar de manter a mesma taxa de transferência de símbolos, é empregada uma técnica de modulação bem mais avançada chamada de QPSK (*Quadrature Phase Shift Keying*), onde dois bits de dados podiam ser codificados em 1 símbolo.

Para aumentar a taxa de transferência, na especificação 802.11b mudou-se a técnica de codificação de *Barker sequence* para uma denominada CCK (*Complementary Code Keying*). Esta nova codificação consiste de um conjunto de 64 palavras de 8 bits. Esse conjunto de palavras tem propriedades matemáticas únicas que permitem que haja uma distinção entre elas mesmas com a presença de ruído. Para uma velocidade de 5Mbps é utilizada a codificação CCK com 4 bits de dados do usuário por símbolo. Para transmissão à 11Mbps, 8 bits de dados são representados por símbolo. Ambas as velocidades utilizam a técnica de modulação QPSK com taxa de transmissão de 1.325 MSps. Para suportar ambientes onde o ruído pode ser elevado em determinados momentos, a especificação 802.11b determina a troca da taxa de transferência dinamicamente dependendo das condições do sinal, sendo essa troca transparente às camadas superiores do protocolo. As possíveis velocidades são de: 11Mbsp, 5.5 Mbps, 2 Mbps e 1Mbps (Tabela 1).

Tabela 1 – Velocidades de DSSS

Velocidade	Tamanho do Código	Modulação	Taxa de Símbolos	Bits por Símbolos
1 Mbps	11 (Barker Sequence)	BPSK	1 MSps	1
2 Mbps	11 (Barker Sequence)	QPSK	1 MSps	2
5.5 Mbps	8 (CCK)	QPSK	1.375 MSps	4
11 Mbps	8 (CCK)	QPSK	1.375 MSps	8

3.3.3 OFDM (Orthogonal Frequency Division Multiplexing)

Esta técnica de modulação utilizada no protocolo 802.11a é totalmente diferente das anteriores, é chamado como modulador *multicarrier,* utilizado por portadores múltiplos de sinais de diferentes freqüências para enviar bits sobre cada canal. Este é similar ao FDM. Entretanto, no caso de OFDM, todos os subcanais são dedicados para uma fonte de dados.

As taxas de dados possíveis para esta especificação são 6, 9, 12, 18, 24, 36, 48 e 54 Mbps. O sistema utiliza acima de 52 sub-portadores que são modulados utilizando BPSK, QPSK, 16 QAM, ou 64 QAM, dependendo das taxas requeridas, conforme apresentado na Tabela 2. Também utiliza um código convolucional corretor de erros, com taxas de 1/2, 2/3 ou 3/4, que provê correção de erros avançado.

Tabela 2 - Tabela de configurações possíveis para a Técnica OFDM.

Data rate (Mbits/s)	Modulation	Coding rate (R)	Coded bits per subcarrier (N_{BPSC})	Coded bits per OFDM symbol (N_{CBPS})	Data bits per OFDM symbol (N_{DBPS})
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	3/4	4	192	144
48	64-QAM	2/3	6	288	192
54	64-QAM	3/4	6	288	216

Em técnicas normais de FDM, o espaçamento entre canais deve ser maior que a taxa de símbolos para evitar a sobreposição dos espectros. No OFDM, as sub-portadoras se sobrepõem, mas são escolhidas sub-portadoras ortogonais, ou seja, que mantém certa relação matemática de modo que não haja interferência entre elas. Como elas possuem um espectro do formato [sen (x) / x], colocam-se as sub-portadoras, de modo que elas estejam centradas nos zeros das sub-portadoras adjacentes. A FIGURA 15, ilustra o espectro nesta sub-portadoras.

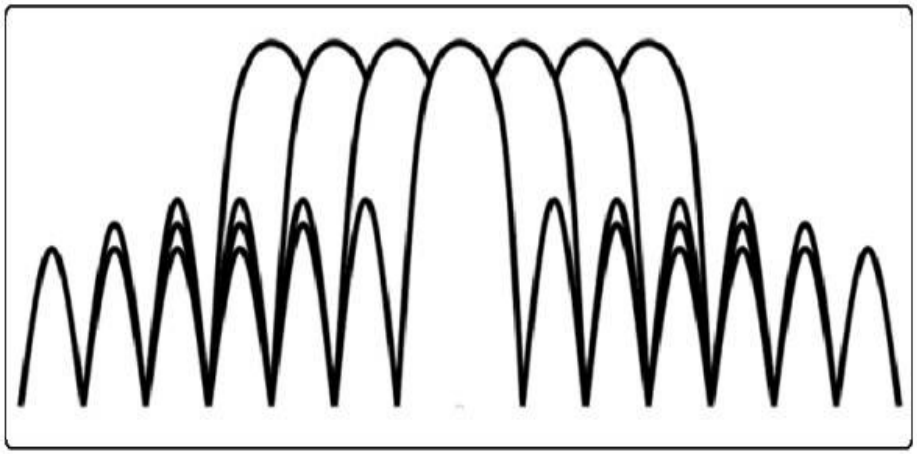

FIGURA 15 : ESPECTRO DAS SUB-PORTADORAS OFDM.

No 802.11a, as sub-portadoras são espaçadas de 312,5 kHz. Como um símbolo é representado por 48 sub-portadoras de dados, 4 sub-portadoras piloto, mais uma sub-portadora nula, resultando em 53 sub-portadoras, que multiplicadas pelo espaçamento de 312,5 kHz, resulta em uma banda ocupada de 16,6 MHz.

3.3.4 Transmissão por infravermelho

De forma geral, o acesso de dispositivos pessoais através de infravermelho se dá pelo simples fato de apontar, por exemplo, um *laptop* ou uma calculadora para uma impressora, com o fim de transferir arquivos. Esse tipo de aplicação está se disseminando rapidamente, pela redução substancial do tamanho (1 mm^2) e do custo (US $5) do transceptor, além do surgimento dos padrões da IrDA a partir de 1993. A IrDA (*Infrared Data Association*) é uma organização que cria e promove padrões de interconexão de dados através de equipamentos que utilizam infravermelho.

Existem, basicamente, duas modalidades de enlace curto por infravermelho: a conexão por linha de visada, na qual dois pontos são interconectados por um feixe diretivo que vai do transmissor ao receptor; e o chamado infravermelho difuso, no qual o transmissor "inunda" o recinto com luz infravermelha que é lançada em todas as direções, refratando pelas paredes e assim alcançando todos os receptores do recinto.

No infravermelho por linha visada, a ausência de múltiplos caminhos entre transmissor e receptor permite que se alcancem taxas maiores de transmissão, mas o sistema é totalmente vulnerável à presença de obstáculos que eventualmente se coloquem na linha de visada. Em redes Ethernet, as taxas podem alcançar até 10 Mbps, e em redes do tipo token ring até 16 Mbps, devendo os nós consecutivos se situar até 25 m um de outro, sem obstáculos. Para isso, pode ser usada a parte do recinto que se situa entre o teto e a mobília, especialmente em grandes espaços ocupados por pequenos escritórios separados por biombos.

Para aplicações ponto-multiponto ou broadcast, é necessário usar o infravermelho difuso, mas aí as taxas caem devido à propagação por múltiplos caminhos. Uma maneira interessante de amenizar este problema é a transmissão quase-difusa, na qual todos os transmissores apontam para um refletor (que pode ser passivo ou ativo) situado no teto do recinto numa posição central. A refração fica então limitada à superfície do refletor, reduzindo a variação de comprimento dos percursos.

O princípio do enlace por infravermelho está baseado na intensidade da modulação e a detecção direta da portadora ótica. A intensidade da modulação é realizada variando a corrente do diodo laser ou LED. A detecção direta é realizada por fotodiodos PIN que produzem uma corrente proporcional à força ótica incidente.

4. CAMADA DE ENLACE

4.1 Introdução

A camada de enlace de uma rede local sem fio, pode ser dividida em duas subcamadas: Controle Lógico do Link (*LLC - Logic Link Control)* e Controle de Acesso ao Meio (*MAC – Medium Access Control*). A subcamada de LLC é idêntica a qualquer outro padrão 802.x, porém a camada MAC é exclusiva da Wireless Lan (Abras, 2004).

A camada MAC realiza as seguintes tarefas: Controlar o acesso ao meio, mas ela também pode oferecer suporte para roaming (quando uma estação se desloca e muda de AP), e gerenciamento de energia. O protocolo para 802.11 usa o CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*). Este protocolo evita colisões (ao contrário de detectar uma colisão, como fazia o algoritmo CSMA/CD (*Carrier Sense Multiple Access With Collision Detection*), usado no 802.3, porque é difícil detectar colisões em uma rede de transmissão por rádio-freqüência.

4.2 Controle de Acesso ao Meio

Para o controle de acesso em um meio sem fio, o IEEE definiu um protocolo de acesso ao meio (subcamada MAC do nível de enlace de dados), denominado de DFWMAC (*Distributed Foundation Wireless Medium Access Control*). Os mecanismos utilizados neste protocolo são chamados de funções de coordenação (*coordination functions*). Estas funções são usadas para dar suporte à transmissão de tráfego assíncrono ou tráfego com retardo limitado. São elas que determinam quando uma estação específica tem permissão para transmitir.

O DFWMAC define dois métodos, ou “funções de coordenação” para o acesso: uma função de coordenação distribuída (DCF – *Distributed Coordination Function*), obrigatória, onde a decisão de quando transmitir é tomada individualmente pelas estações, o que pode resultar em transmissões simultâneas (colisões).

E uma a função de coordenação centralizada ou pontual (PCF – *Point Coordination Function*), opcional, onde a decisão é centralizada em um ponto, que determina qual estação deve transmitir em que momento, evitando a ocorrência de colisões. Os dois métodos de acesso podem coexistir. Na realidade, o método de acesso distribuído forma a base sobre a qual é construído o método centralizado (Soares).

Em todos os métodos de acesso, é importante controlar o tempo de espera antes do acesso ao meio. A FIGURA 16, mostra três diferentes parâmetros que definem a prioridade de acesso ao meio:

- ***DIFS* (*Distributed Inter Frame Spacing*) –** espaço entre quadros da DCF. Este parâmetro indica o maior tempo de espera, portanto a menor prioridade; ele monitora o meio, aguardando no mínimo um intervalo de silêncio para transmitir os dados.
- ***PIFS* (*Priority Inter Frame Space*) –** espaço entre quadros da PCF; um tempo de espera entre o DIFS e o SIFS (prioridade média) , é usado para o serviço de acesso com retardo, ou seja um ponto de acesso controlando outros nós, só precisa esperar um tempo PIFS para acessar o meio.
- ***SIFS* (*Short Inter Frame Space*) –** é usado para transmissão de quadros carregando respostas imediatas (curtas), como ACK, que possuem a mais alta prioridade.

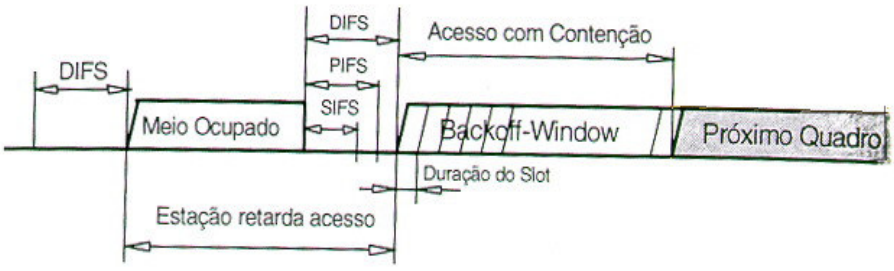

FIGURA 16 : TEMPOS DE ESPERA DO MÉTODO DE ACESSO CSMA / CA. FONTE: (MATHIAS,2004).

4.2.1 DFWMAC-DCF (CSMA/CA) – Básico

O método de acesso básico do DFWMAC é uma função de coordenação distribuída (DCF) conhecida como CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) com reconhecimento. A utilização desse método é obrigatória para todas as estações e pontos de acesso (APs), nas configurações Ad Hoc e com infra-estrutura. O serviço fornecido pela DCF é usado para transmissão de tráfego assíncrono (Soares).

Esse mecanismo de acesso projetado para reduzir a probabilidade de colisões na rede entre múltiplas estações possui um esquema de acesso com sensor que escuta o meio. Se o meio está inativo por pelo menos a duração de um tempo DIFS, uma estação pode acessar imediatamente. Este mecanismo é muito eficiente quando o meio não está muito carregado. Mas, tão logo mais e mais estações tentarem acessar o meio, outros mecanismos de controle são necessários. A FIGURA 17 mostra o método de acesso DFWMAC-DCF básico (CSMA/CA).

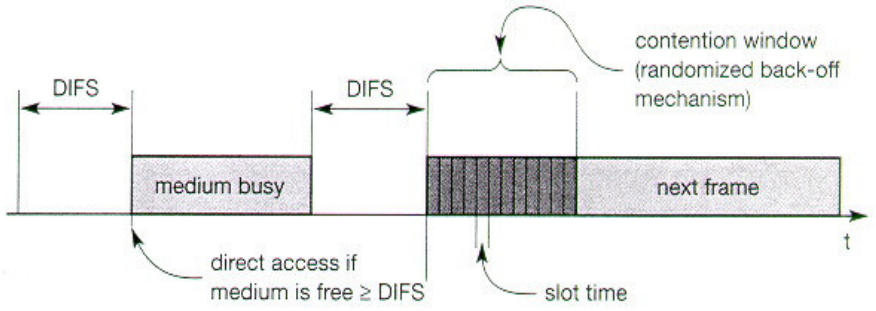

FIGURA 17 : MÉTODO ACESSO DFWMAC-DCF (CSMA/CA) - BÁSICO. FONTE: (MATHIAS,2004).

Conforme ilustra a FIGURA 17, se o meio estiver ocupado após um tempo DIFS, as estações têm que esperar novamente pela duração de um DIFS, e depois entrar em uma fase de contenção. Nesta fase, cada estação escolhe um tempo aleatório, dentro de uma janela de contenção (*contention window*).

Após este intervalo de tempo aleatório, as estações tentam acessar o meio. Permanecendo ocupado após este intervalo, é determinado que essa estação perdeu este ciclo, ou seja, é necessário repetir todo o ciclo, iniciando pela espera da duração de um tempo DIFS.

Para proporcionar que as estações que já estão no ciclo tenham vantagem em relação às novas que tentarem o acesso, é acrescentado um contador (*backoff*). Se uma determinada estação não consegue acessar no primeiro ciclo, ela pára o seu contador, espera o canal estar inativo novamente por um tempo DIFS e o seu contador começa a decair novamente. Provavelmente a estação antiga terá o seu contador com um tempo menor, assim, quando o contador expirar, essa estação acessa o meio. Após o recebimento dos dados, o receptor envia um pacote Ack ao emissor, confirmando o recebimento. Caso contrário, se o receptor não enviar esta confirmação, então a estação emissora reinicia todo o processo de acesso ao meio, para o envio da mensagem novamente. Desta maneira, considera-se que tenha ocorrido alguma colisão, provocando o não recebimento da mensagem pelo receptor.(Mathias,2004).

4.2.2 DFWMAC-DCF (CSMA/CA) - Com o mecanismo RTS/CTS

Para solucionar o problema de terminais escondidos/perdidos, ou seja, uma estação que não escuta o trafego de rede gerado pela outra, ficando incomunicável por um período de tempo. Problema que ocorre devido a vários motivos, seja quando as estações estão de lados opostos em relação ao AP, ou quando a estação móvel se encontra em locais com grande degradação de sinal, que pode ser por motivos geográficos ou ambientais (área de sombra). A FIGURA 18 ilustra uma perda de conexão do AP com a estação móvel por razões geográficas.

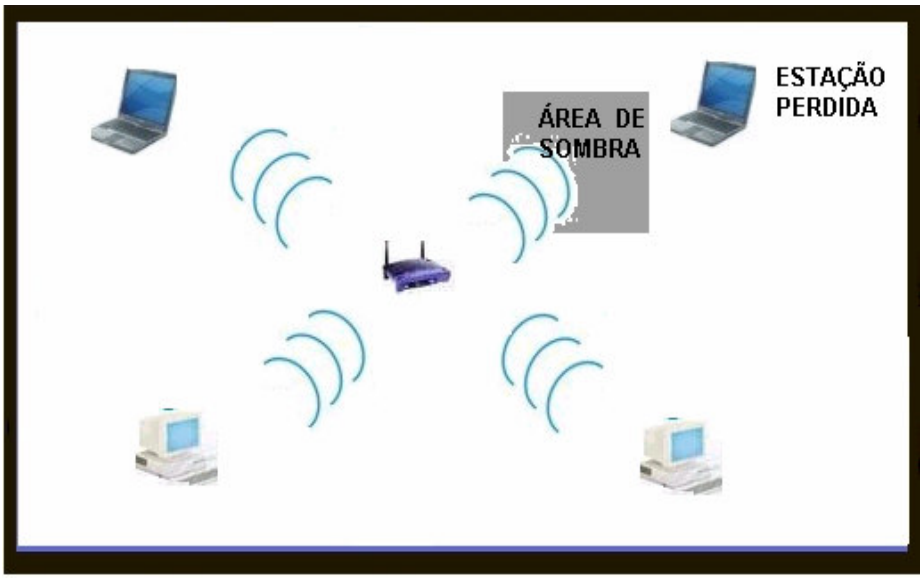

FIGURA 18 : PERDA DE CONEXÃO COM A ESTAÇÃO MÓVEL POR RAZÃO GEOGRÁFICA.

O padrão definiu um mecanismo adicional usando dois sinais de controle, RTS e CTS. A utilização desse mecanismo é opcional, entretanto todo nó 802.11 tem que implementar a função para poder reagir corretamente caso receba esses sinais. A FIGURA 19 ilustra o método de acesso com a utilização do mecanismo com sinais de controle RTS/CTS.

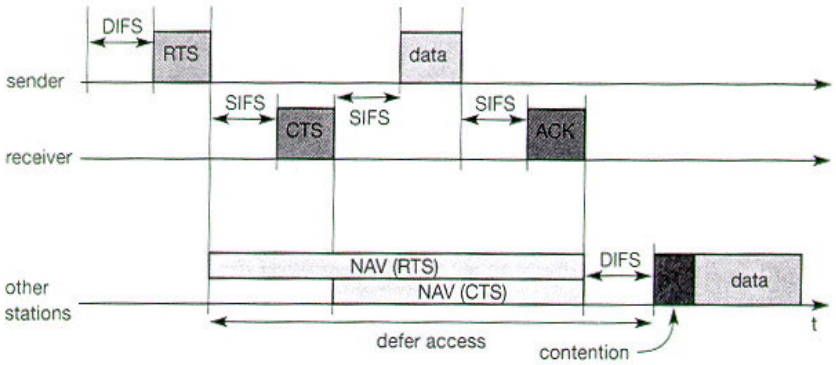

FIGURA 19 : MÉTODO ACESSO DFWMAC-DCF (CSMA/CA) COM MECANISMOS RTS/CTS.

Como apresentado na FIGURA 19, o emissor depois de esperar por DIFS (mais *um backoff time* aleatório, se o meio estiver ocupado), o emissor pode emitir um RTS (*request to send* – pedido para enviar), que não possui nenhuma prioridade em relação às outras mensagens. O pacote RTS inclui o destinatário e o tempo previsto para transmissão dos dados. Esse tempo previsto especifica o intervalo de tempo necessário para transmitir o quadro de dados integralmente mais o sinal ACK que será enviado pelo receptor. Toda a estação que receber o sinal RTS tem que fixar o seu NAV (*Net Allocation Vector*) de acordo com a duração do tempo previsto especificado no RTS. O NAV especifica o primeiro ponto no tempo onde a estação pode tentar acessar o meio novamente.

Se o receptor (da mensagem que o emissor quer enviar) recebe o RTS, ele responde com um CTS (*clear to send* – pode enviar), depois de esperar por SIFS. Esse sinal CTS contém novamente o tempo previsto para transmissão da mensagem propriamente dita. E todas as estações que receberem o CTS do receptor têm que ajustar seus NAV. O conjunto de estações que receberam o CTS não é, necessariamente, o mesmo conjunto de estações que receberam o RTS. Agora todas as estações dentro do raio de ação do emissor e do receptor foram informadas que vão ter que aguardar mais tempo para tentar acessar o meio. Isso contorna o problema do terminal escondido. Basicamente, o mecanismo reserva o meio para um único emissor.

Finalmente, o emissor pode enviar a mensagem propriamente dita depois de SIFS. O receptor recebe a mensagem, espera por SIFS, e envia o sinal ACK se a transmissão estiver correta. Agora a transmissão está completa a o NAV em cada estação indica que o meio está inativo e o ciclo padrão pode recomeçar.

Com esse mecanismo (uso do RTS e CTS), colisões só podem acontecer no início (quando o RTS está sendo enviado). Duas ou mais estações podem começar a transmissão ao mesmo tempo (RTS ou dados).

A utilização de RTS/CTS pode resultar num overhead significativo, ou seja, a eficiência da transmissão pode diminuir; causando perda de banda passante e um atraso elevado. Por isso, esse mecanismo, normalmente, só é utilizado para se enviar quadros grandes.

A taxa de erro de transmissão em redes sem fio é geralmente muito maior que em redes de fibra óptica, por exemplo. Uma maneira de diminuir a probabilidade de erro dos quadros é utilizar quadros pequenos. Nesse caso, a taxa de erros na transmissão é a mesma, mas somente quadros pequenos serão destruídos, e então, diminui a taxa de erro dos quadros. Entretanto, o mecanismo de fragmentação deve ser invisível para o usuário. Além disso, a camada MAC deve ter a possibilidade de ajustar o tamanho do quadro com a taxa de erro específica daquele meio. Para isso, o padrão IEEE 802.11 especifica um modo de fragmentação, mostrado na FIGURA 20.

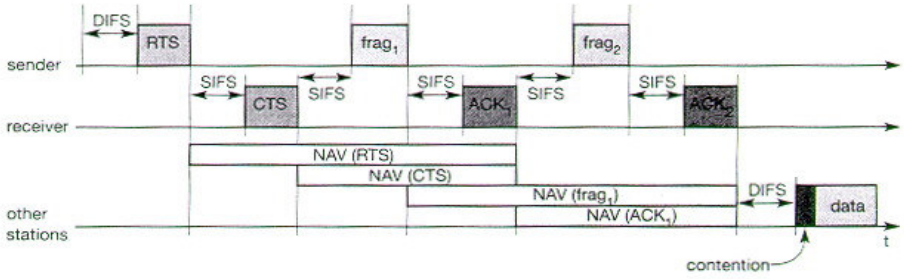

FIGURA 20 : FRAGMENTAÇÃO DE PACOTES.

Novamente o emissor envia o RTS e o receptor responde com o CTS. Depois disso, o emissor envia o primeiro quadro de dados (frag1). A novidade nesse caso, é que, dentro do frag1, tem um campo onde está armazenado o tempo previsto para o segundo quadro mais o sinal de ACK do receptor. Novamente, várias estações vão reajustar seus NAV. O conjunto de estações que farão esse reajuste pode ou não ser igual ao conjunto de estações que receberam o RTS, o que depende do movimento de cada estação do sistema. Depois de receber frag1, o receptor envia o sinal de ACK, que nesse caso também armazena o tempo previsto para o segundo quadro mais o segundo sinal de ACK.

Esse sinal será recebido pelo conjunto de que estão dentro do raio de ação do receptor da mensagem. Caso houvesse mais quadros para serem enviados, o procedimento se repetiria após o envio do frag2 (Mathias, 2004).

4.2.3 DFWMAC-PCF com Polling

Este padrão suporta opcionalmente uma função de coordenação pontual (PCF – *point co-ordination function*) centralizada, construída sobre a função de coordenação distribuída (DCF), proporcionando a transmissão de tráfego com retardo limitado ou trafego assíncrono. Usando PCF, um AP controla o acesso ao meio determinando, em cada momento, qual estação deve transmitir. Redes Ad Hoc não podem usar essa função, já que não possui nenhum nó central controlador.

Para promover a integração das duas funções de coordenação – pontual e distribuída, este método de acesso utiliza o conceito de superquadro, fazendo com que a função de coordenação pontual assuma o controle da transmissão, evitando a ocorrência de colisões. Para isso, o protocolo DFWMAC divide o tempo em períodos denominados superquadros. Um superquadro consiste em dois intervalos de tempo consecutivos: no primeiro, controlado pela PCF, o acesso é ordenado (não ocorrem colisões), após esperar PIFS, o ponto de coordenação dá acesso ã primeira estação, que pode responder após SIFS. Depois de aguardar mais SIFS, o coordenador dá a vez para a segunda estação e assim por diante.

Quando uma estação não responde após SIFS, o coordenador aguarda PIFS e passa a vez para a próxima. No segundo tempo, controlado pela DCF, o acesso baseia-se na disputa pela posse do meio, podendo ocorrer colisões. A FIGURA 21, mostra como são construídos os superquadros e mostra também muitas estações (todas na mesma linha) e os NAVs das estações (também na mesma linha).

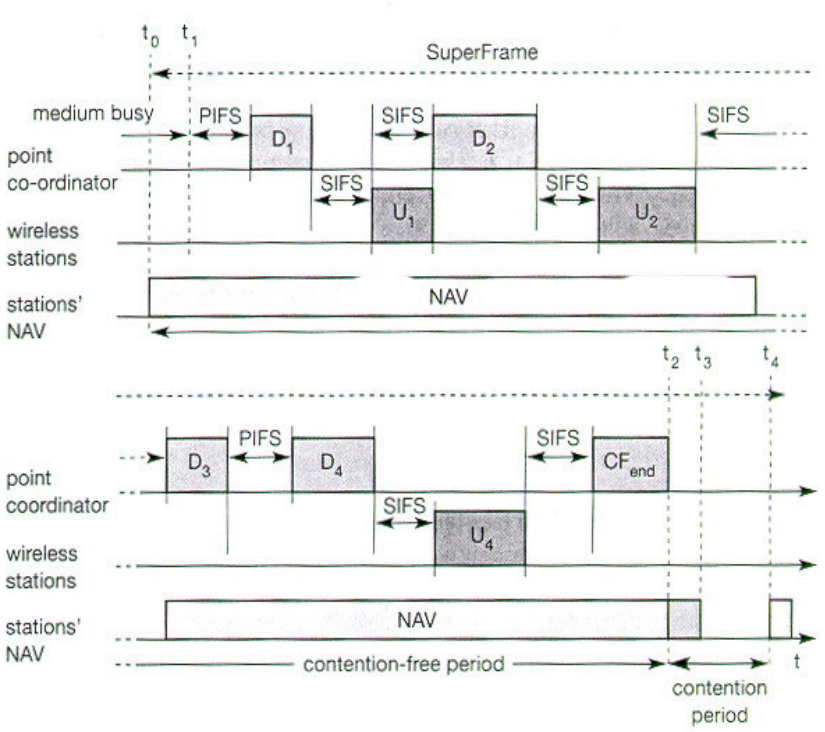

FIGURA 21: MÉTODO ACESSO DFWMAC-PCF (CSMA/CA) COM POLLING. FONTE: (MATHIAS,2004).

Conforme a FIGURA 21, no tempo t0, o período livre de contenção do superquadro deveria ser iniciado, entretanto uma outra estação está transmitindo (o meio está ocupado). Por causa disso o PCF espera o DCF, ou seja, o início do superquadro é adiado. A única possibilidade de evitar variações é simplesmente não existindo nenhum período de contenção. Depois que o meio se tornar inativo (no tempo t1), o coordenador pontual (AP) tem que esperar por PIFS antes de acessar o meio. Como SIFS é menor que DIFS, nenhuma outra estação consegue acessar o meio antes do AP.

O AP agora envia o dado D1 para uma primeira estação (a ordem das estações é tabelada). A estação então responde com o dado U1 depois de SIFS. Depois de esperar SIFS novamente, o AP pode requerer a transmissão da segunda estação (obs: a figura 21, ilustra o exemplo de como seria o procedimento incorreto, em que o AP não espera o SIFS novamente).

A estação responde enviando o dado U2. Novamente, o AP envia um requerimento para uma terceira estação, mas, desta vez, a estação não tem nada para enviar. Então, o AP não vai receber nada depois de SIFS.

Depois de esperar por PIFS, o AP pode requerer a transmissão da quarta estação através de D4. A estação responde com U4, e, depois de SIFS, o AP envia um sinal de finalização (CFend), ou seja, o período de contenção pode ser iniciado. Na utilização do PCF, são setados todos os NAVs, evitando a transmissão de outras estações. Neste exemplo, o período livre de contenção esperado era de t0 até t3. Entretanto, como a terceira estação não enviou dados, o período terminou em t2. Em t4, o ciclo se reinicia com um outro superquadro (Mathias, 2004).

4.3 Gerenciamento do MAC

O gerenciamento do MAC exerce um papel essencial nas estações já que controla quase todas as funções de integração do sistema, isto é, integração de uma estação com uma BSS, formação de uma ESS, sincronização das estações, etc. As funções abaixo serão detalhadas a diante (Mathias, 2004):

- Sincronização: funções para auxiliar o encontro de uma Wireless LAN, sincronização dos relógios internos, geração dos sinais beacon.
- Gerenciamento de energia: funções para controlar a economia de energia, por exemplo: inativação periódica, armazenamento sem perda do quadro.
- *Roaming*: funções que permitem o roaming alterando o AP para uma determinada estação.

4.3.1 Sincronização

Cada nó de uma rede 802.11 mantém um relógio interno. A sincronização destes relógios é fundamental para o tráfego de pacotes na rede, podendo prever o início e controlar o tempo de duração de um superquadro em uma função PCF. Como será visto mais adiante, também auxilia no gerenciamento de energia e no processo de migração de estações (Roaming). Para sincronizar, o IEEE 802.11 especifica uma função de sincronização de tempo TSF (*Timming Syncronization Function*).

Em redes com infra-estrutura, o AP é responsável pelo o envio dos sinais de sincronização para cada estação, a transmissão é realizada em intervalos de tempo quase periódicos, mas podendo ser adiado se o meio estiver ocupado. Estes sinais são denominados *beacon*. Um *beacon* contém um *timestamp* e outras informações usadas para o gerenciamento de energia e roaming (exemplo: identificação do BSS). O *timestamp* é usado por uma estação para ajustar seu relógio local. Uma estação não é requerida para estar constantemente ajustando seu relógio; entretanto, de tempo em tempo o relógio interno deve ser ajustado.

Já numa rede Ad Hoc, a situação é mais complicada, já que não existe um AP para transmitir o quadro de *beacon*. Nesse caso, cada estação mantém seu próprio relógio, e envia um sinal de sincronização após o tempo periódico ter passado. Entretanto, várias estações enviam este sinal ao mesmo tempo, então o relógio de todos os nós da rede é estabelecido por uma das estações (a que conseguir transmitir seu quadro depois de concorrer com as outras pelo acesso ao meio).

4.3.2 Gerenciamento de Energia

Aparelhos sem fio são alimentados à bateria. Portanto, mecanismos para economizar energia são importantes para o sucesso de cada aparelho.

A idéia básica do gerenciamento de energia do IEEE 802.11 é desligar o transceptor (dispositivo que tem a propriedade de receber e transmitir sinais de rádio) toda vez que ele for desnecessário. Como o gerenciador de energia não pode saber quando o transceptor tem que estar ativo, ele tem que ligar o transceptor periodicamente. O desligamento do transceptor deve ser transparente para os protocolos e deve ser flexível suficiente para suportar diferentes aplicações. Deve-se ter em mente que longos períodos com o transceptor desligado economizam bateria, porém reduzem a média de produção daquela estação, e vice-versa.

Se um emissor quiser enviar dados para uma estação capaz de economizar energia, e esta estiver inativa, os dados terão que ser armazenados. Por outro lado, a estação inativa tem que ser ativada periodicamente e permanecer ativa durante um tempo. Durante este tempo, os receptores devem ser avisados sobre seus quadros de dados. Se uma estação descobre que é o destino de um pacote armazenado, ela deve aguardar ativa até que a transmissão ocorra integralmente.

O gerenciamento de energia em rede infra-estruturada é muito mais simples que numa rede Ad Hoc. O AP armazena todos os quadros destinados a estações que estão operando no modo *power-save*. Junto com cada sinal de *beacon* enviado pelo AP, um mapa indicativo de tráfego TIM (*traffic indication map*) é transmitido. O TIM contém uma lista de estações para as quais quadros foram enviados e armazenados pelo AP.

Já numa rede Ad Hoc, o processo é bem mais complicado. Nesse caso, não há AP para armazenar quadros. Portanto cada estação precisa ter a capacidade de armazenar dados se ela quer se comunicar com uma estação capaz de funcionar economizando energia. Todas as estações devem anunciar uma lista de quadros armazenados durante um período em que todas elas estão ativas. As estações destinatárias devem ser avisadas através do ATIM (*Ad Hoc TIM*) - o período de aviso é chamado de ATIM *window* (Mathias, 2004).

4.3.3 *Roaming*

Se um usuário passeia com uma estação (aparelho sem fio), a estação tem que se mover de um AP para outro. A movimentação de um AP para outro é chamada de *roaming*. Sistemas de *roaming* empregam arquiteturas de microcélulas que usam pontos de acesso estrategicamente localizados. Os passos para um *roaming* entre APs seguem abaixo:

- Uma estação decide quando uma conexão com um determinado AP está muito ruim. Essa estação começa, então, a procurar por outro AP.
- A procura envolve uma busca ativa por outra BSS. O IEEE 802.11 especifica dois tipos de procura: *passiva* e *ativa*. Na procura passiva, a estação simplesmente observa o meio para encontrar sinais de sincronização provenientes de outros possíveis APs. Já a procura ativa compreende a emissão de uma *sonda* em cada canal e a espera por uma resposta. A resposta a uma sonda contém a informação necessária para a estação se juntar ao novo BSS.
- A estação então escolhe o melhor AP para *roaming* baseado, por exemplo, na clareza do sinal, e envia um requerimento de associação para o AP selecionado.
- O novo AP responde com uma resposta de associação. Se a resposta é positiva, a estação é transferida para o novo AP. Caso contrário ela continua procurando por outro AP.
- O AP aceitando o requerimento de associação indica a nova estação dentro de seu BSS para o sistema de distribuição (DS). O DS então realoca sua base de dados que contém a localização corrente das estações. Essa base de dados é necessária para transmissão de quadros entre diferentes BSSs.

4.4 Outras funcionalidades

Há mais duas funcionalidades na camada MAC que são: checagem de CRC e fragmentação de pacotes. Na checagem de CRC, a cada pacote transmitido é anexada a informação de checagem (CRC), para que quando o pacote chegue ao seu destino, a estação receptora possa checar se houve algum rompimento das informações. Esta funcionalidade em redes convencionais está presente na camada TCP da pilha de protocolo. Em relação à fragmentação de pacotes (mostrado na FIGURA 19), ela pode ser realizada em ambientes onde há muito tráfego ou ruído no sinal, para que em caso de perdas de pacotes, a menor quantidade possível de informações seja retransmitida. A junção dos pacotes fragmentados é responsabilidade da camada MAC, ficando transparente para as camadas superiores da pilha de protocolo (Abras, 2004).

5. UTILIZAÇÃO DA METODOLOGIA "SITE SURVEY" EM PROJETOS DE REDES WIRELESS LAN (WLAN)

5.1 Introdução

Este capítulo apresenta um projeto para implantação de uma rede local sem fio, em uma empresa que visa proporcionar mobilidade em seus negócios. Este projeto tem por objetivo aplicar os conceitos da tecnologia WLAN apresentados nos capítulos anteriores.

Para o funcionamento correto de uma de rede local sem fio, não basta apenas instalar e configurar os equipamentos, é necessário o desenvolvimento de um projeto que possua um planejamento para a sua implantação. O planejamento de uma rede desse tipo pode durar poucos dias ou mesmo semanas, dependendo da complexidade e funcionalidades exigidas pelo cliente.

5.2 O projeto

Os profissionais envolvidos em projetos de redes de comunicação podem utilizar a metodologia *site survey* para desenvolver um bom projeto. Por definição, o *site survey* é uma metodologia aplicada na inspeção técnica minuciosa do local que será objeto da instalação de uma nova infra-estrutura de rede. Esse procedimento é realizado normalmente durante a avaliação do projeto, para identificar a localização, e o número de estações base necessárias, e outros fatores importantes para a implantação da rede (cobertura, tráfego previsto, e obstáculos do sinal de comunicação), de forma a maximizar sua eficiência, bem como reduzir os custos de investimento. Os equipamentos utilizados são basicamente um notebook ou *handheld*, um *Access Point* e um cartão PCMCIA (no caso de se utilizar um notebook) ou *Compact Flash* (no caso de um *handheld*);

O projetista deve ter em mãos toda a documentação da análise realizada. Esse documento servirá como um mapa para a implementação da rede e também como futura referência aos técnicos e administradores.

Esse é um processo passo-a-passo, em que o projetista da rede deve descobrir/pesquisar características que podem ser divididas nos seguintes aspectos:

- **Finalidade do projeto:** A instalação de uma rede local sem fio deve atender às necessidades de negócio do cliente. Portanto, é de crucial importância saber a finalidade de sua implementação. Por exemplo, conhecendo a sua finalidade pode-se definir o protocolo de transmissão adequado para garantir um bom desempenho da rede.
- **Análise do ambiente:** É necessário analisar o ambiente onde a rede será implementada. Dentre os aspectos a serem analisados estão: a dimensão da área, os obstáculos provenientes do ambiente para a propagação do sinal. Além destes aspectos, é necessário levar em conta a quantidade de usuários existentes na rede, o nível mínimo de segurança exigido, a largura de banda desejada, o impacto que a rede terá sobre o ambiente etc.
- **Localização do ambiente:** Após a análise, já se sabe em que ambiente a rede será instalada: indoor, outdoor ou em ambos. No ambiente outdoor, como a ligação entre prédios, podemos ter inúmeras situações e obstáculos que dificultem a instalação e a manutenção de uma rede sem fio, tais como: árvores, montanhas, outros prédios e condições climáticas desfavoráveis (fortes chuvas, ventos e neve), que podem enfraquecer ou mesmo eliminar o sinal de transmissão.
- **Infra-estrutura da rede:** Com a análise do ambiente, é possível definir os equipamentos necessários, a quantidade de usuários, os protocolos de transmissão e segurança, a topologia da rede, etc.
- **Nível de segurança:** A segurança é um dos fatores que mais influenciam na decisão de se adotar uma nova tecnologia. E com as redes sem fio, essa preocupação não é diferente. Pelo contrário, deve-se utilizar todas as ferramentas disponíveis para se obter o nível mínimo de segurança.

- **Orçamento da aplicação:** No planejamento, é importante apresentar ao cliente o custo da aplicação. Portanto, possibilitando verificar a viabilidade do custo/benefício desta rede, em relação a uma rede cabeada.

5.3 Desenvolvendo o projeto

5.3.1 Finalidade do projeto

Este projeto visa à implantação de uma rede local sem fio, como extensão de uma rede cabeada. Esta extensão de rede sem fio, interligará dois departamentos da empresa: a recepção dos visitantes (fornecedores, executivos de negócios, etc.), e um pequeno escritório de marketing. Ela permitirá aos funcionários o acesso à rede interna e à internet. E uma outra rede local sem fio conectada diretamente ao modem DSL. Esta rede permitirá aos visitantes o acesso exclusivo à internet, visando a segurança da rede interna da empresa. Esta rede sem fio exclusiva para acesso a internet, abrangerá somente o departamento de recepção dos visitantes.

A finalidade destas redes locais sem fio, além de prover flexibilidade e facilidade na instalação, é proporcionar mobilidade nos negócios da empresa. Possibilitando aos visitantes o acesso à internet, sem a necessidade de um ponto de rede determinado. Aos funcionários proporcionar mobilidade e flexibilidade, para a realização e criação de novas idéias de negócios.

Os serviços destas redes serão: acesso à internet com envio de e-mails para os funcionários e os visitantes, e o acesso à rede interna da empresa somente pelos funcionários da empresa.

5.3.2 Análise do ambiente

5.3.2.1 Descrição do ambiente

O departamento para recepção de visitantes (fornecedores, executivos de negócios, etc.), inclui as salas dos compradores, uma sala de reunião, as salas da diretoria e um hall, proporcionando um ambiente descontraído para a realização de negócios com mobilidade. A FIGURA 22 ilustra este ambiente.

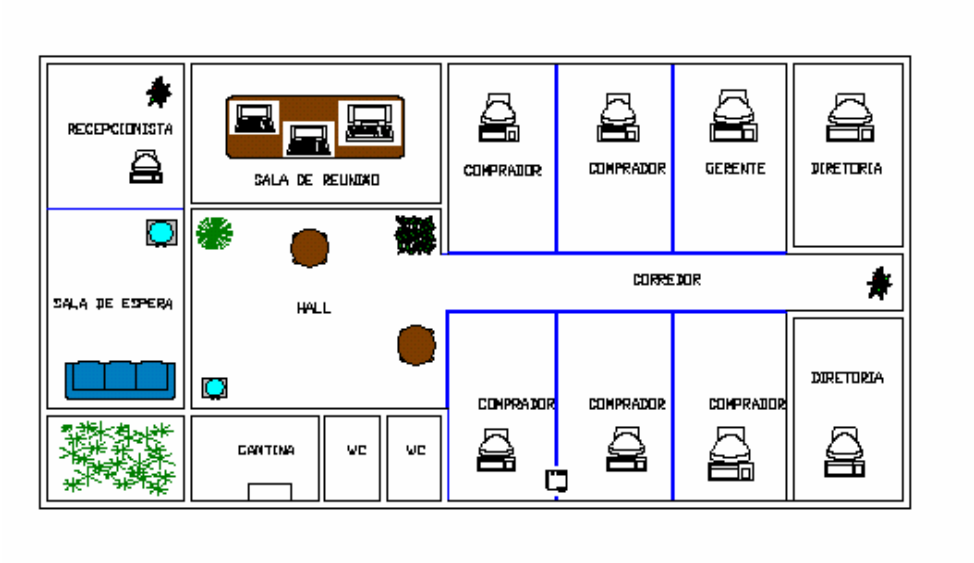

FIGURA 22 : RECEPÇÃO DE VISITANTES.

O outro departamento localiza-se em outro prédio. Este abrigará um pequeno escritório marketing da empresa, composto por uma sala de reunião, oito salas que abrigarão os usuários, e um hall que possibilitará também um ambiente descontraído para os funcionários de marketing. A FIGURA 23 ilustra o escritório de marketing.

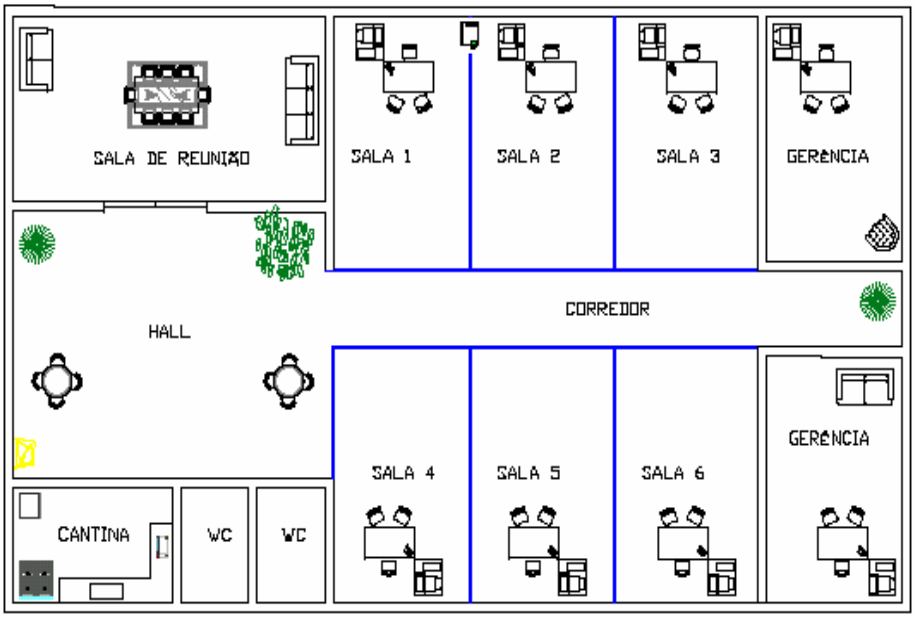

FIGURA 23 : ESCRITÓRIO DE MARKETING.

5.3.2.2 Localização do ambiente

Os departamentos da empresa estão localizados em prédios separados, localizados, em uma linha visada direta, com uma distância de 70 metros, sem obstáculos. Contendo assim neste projeto uma comunicação indoor, na área interna dos prédios, e uma comunicação outdoor na área externa, interligando estes prédios. A FIGURA 24, ilustra a localização destes departamentos.

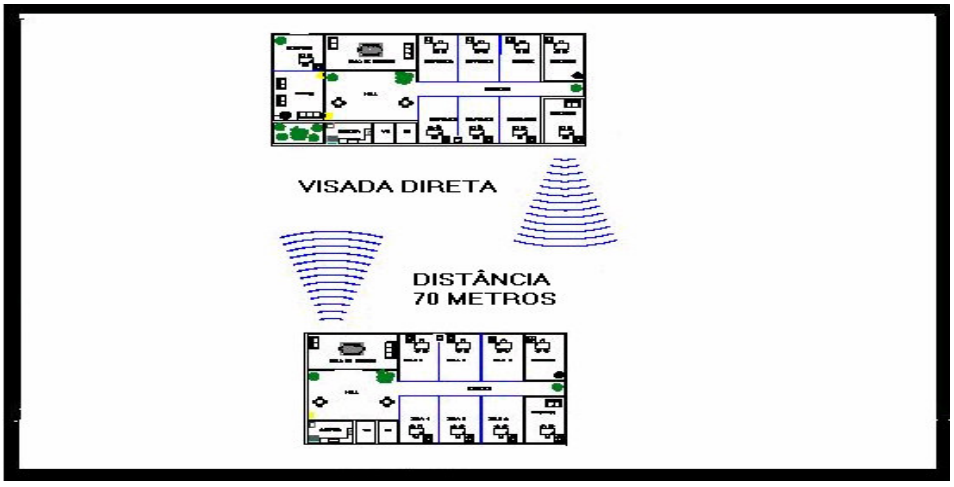

FIGURA 24 : LOCALIZAÇÃO DOS DEPARTAMENTOS DO AMBIENTE DA REDE.

5.3.2.3 O impacto da rede no ambiente

O desempenho das redes será bom, pois o tráfego e o fluxo de utilização são aceitáveis: A extensão da rede cabeada que atenderá aos funcionários da empresa será utilizada com maior freqüência somente pelos no escritório de marketing, já que na recepção continuará utilizando a rede cabeada, somente caso seja necessário mobilidade no atendimento aos visitantes, serão conectados os notebooks disponíveis para empresa. Por isso, torna-se bom o desempenho, pois um roteador Wireless suporta em média 20 usuários, e a quantidade de funcionários que acessará esta rede é inferior a este limite.

A rede exclusiva aos visitantes também conterá pouco tráfego, considerando que não haverá mais de 20 visitantes acessando a rede simultaneamente.

5.3.2.4 Obstáculos deste ambiente

Para a análise dos obstáculos do ambiente, o *site survey* é muito importante, pois facilita a identificação de interferências, e o local de baixo sinal de propagação. Além de definir a quantidade de equipamentos (roteadores, antenas, etc.), necessários para uma boa comunicação sem fio.

Os obstáculos nas comunicações deste ambiente são mínimos, possibilitando assim uma boa propagação do sinal. Na parte interna (indoor) dos prédios serão instaladas divisórias com meia altura, evitando as paredes. As bases wireless serão fixadas na parede (na parte mais alta), de forma que o sinal percorra todo o ambiente sem obstáculos, e os dispositivos do cliente serão posicionados de forma que a recepção do sinal seja facilitada, evitando colocá-los muito próximo do piso. Este ambiente é composto de algumas pequenas plantas, e não possui nenhum equipamento que utiliza a mesma freqüência de comunicação da rede (2.4 GHz). Os bebedouros estão localizados no canto, de forma que não influirá no sinal.

A instalação destas redes no mesmo departamento não causará interferências, pois serão configurados canais de comunicação diferentes para cada rede. Na parte externa (outdoor), tem-se uma linha visada direta, sem a convergência com obstáculos que possam interceptar o sinal.

5.3.3 Infra-estrutura da rede

5.3.3.1 Equipamentos

Para facilitar a instalação e configuração da rede, a aquisição de equipamentos será somente de um único fabricante. A tabela 3 ilustra os equipamentos necessários para comunicação sem fio para este projeto.

TABELA 3 : Equipamentos utilizados na aplicação.

EQUIPAMENTOS	RECEPÇÃO	ESCRITÓRIO
BASES WIRELESS	1 ROUTER	1 ROUTER
DISPOSITIVOS DO CLIENTE	2 NOTEBOOKS	3 NOTEBOOKS
ADAPTADORES WIRELESS		5 PLACAS PCI WIRELESS

As bases Wireless serão compostas por routers, devido a sua capacidade de partilha de acesso à internet, e à quantidade maior de recursos na configuração de uma rede mais segura, tanto no acesso interno da rede, e principalmente no acesso à internet. Será instalada uma base para cada rede local sem fio, ambas no departamento da recepção.

Nos dispositivos do cliente : os notebooks serão equipados com os adaptadores Wiereless embutidos de fábrica. Os adaptadores Wireless: as placas PCI Wireless serão instaladas manualmente nos PCs, já de posse da empresa.

5.3.3.2 Protocolo IEEE e o sistema operacional

O sistema operacional adotado nesta aplicação será o windows XP, pois a operação deste sistema é mais fácil, pois ele inclui vários utilitários específicos para redes locais sem fio. A Microsoft através de seu site (http://windowsupdate.microsoft.com/) disponibiliza várias atualizações do software, como por exemplo, uma atualização do windows XP para suportar o modo de cifra WPA, para proteção de dados.

O protocolo mais adequado para estas redes local sem fio é o IEEE 802.11g, pois ele proporciona uma compatibilidade com o protocolo IEEE802.11b, possibilitando aos visitantes utilizar a rede, mesmo que o protocolo de transmissão do dispositivo portátil (nootebook), de sua posse, seja 802.11b ou 802.11g. Outro fator importante é a velocidade de transmissão deste protocolo (54Mbps). Esta velocidade pode diminuir, caso utilize dispositivos 80211.b, mas a tendência é que os visitantes utilizem modelos novos, que já venham equipados com o protocolo 802.11g. A sua faixa de freqüência de 2,4GHz, pode causar bastante interferências com outros dispositivos sem fio (telefone sem fio, forno microondas, etc.), mas não será problema nesta aplicação, pois os ambientes não possuem estes dispositivos.

5.3.3.3 Modo de operação da rede

Estas redes formarão neste ambiente duas células de comunicação isoladas : a primeira, denominada célula1, será a rede local sem fio conectada à rede cabeada, que interligará os dois prédios da empresa. A outra, nomeada de célula2, será a rede exclusiva aos visitantes conectada diretamente ao modem DSL para acesso a internet, abrangendo somente o prédio da recepção. De acordo com os conceitos de arquitetura desta tecnologia, este ambiente com estas características definirá para cada rede o modo de operação infra-estrutura básica. A FIGURA 25 ilustra este modo de operação de infra-estrutura básica.

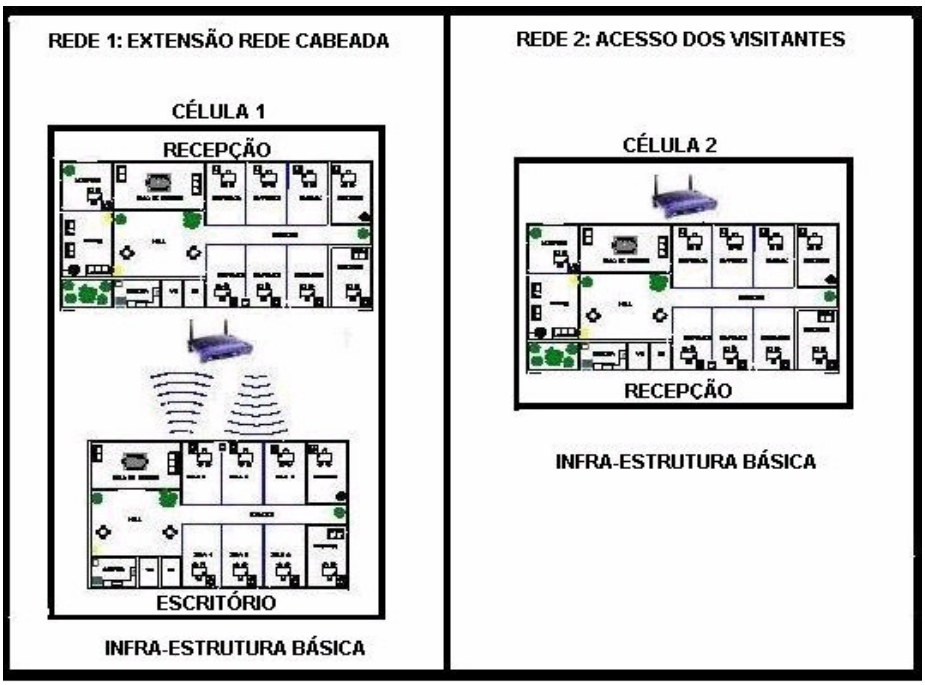

FIGURA 25 : MODO DE OPERAÇÃO DA APLICAÇÃO (INFRA-ESTRUTURA BÁSICA).

5.3.3.4 Nível de segurança

A segurança é considerada um aspecto muito relevante na implementação de redes em geral, seja ela convencional, ou Wireless. Mas nas redes Wireless as vulnerabilidades são maiores, considerando o meio físico que são transportados os dados.

Em projetos de rede local sem fio que permitirá o acesso à usuários externos, por exemplo os visitantes (fornecedores, executivos), é importante o levantamento dos utilitários adotados em seus dispositivos. Com isto pode-se definir o nível adequado de segurança adotado na rede. Neste projeto, com o intuito de garantir um nível maior de segurança, serão instaladas duas redes isoladas, evitando riscos de ataques à rede interna da empresa por causa do acesso de visitantes à rede.

Além destes aspectos serão implementados alguns procedimentos, considerados essênciais para um bom nível de segurança:

- Alterar as senhas de autenticação;
- Alterar o SSID (Server Set ID);

- Desabilitar o broadcast de SSID;
- Utilizar um protocolo de segurança, para criptografar o tráfego entre os clientes e o AP;
- Trocar as chaves criptográficas que acompanham a configuração padrão do equipamento. Procurar usar o maior tamanho de chave possível (128 bits);
- Desligar o router quando não estiver em uso na rede.

Nesta aplicação será adotado o protocolo de segurança WPA. O WPA, que deverá substituir o atual WEP (Wired Equivalent Privacy), conta com tecnologia aprimorada de criptografia e de autenticação de usuário. Cada usuário tem uma senha exclusiva, que deve ser digitada no momento da ativação do WPA. No decorrer da sessão, a chave de criptografia será trocada periodicamente e de forma automática. Assim, torna-se infinitamente mais difícil que um usuário não autorizado consiga se conectar à WLAN.

A chave de criptografia dinâmica é uma das principais diferenças do WPA em relação ao WEP, que utiliza a mesma chave repetidamente. Esta característica do WPA também é conveniente porque não exige que se digitem manualmente as chaves de criptografia - ao contrário do WEP.

5.3.3.5 Orçamento do projeto

Os preços dos equipamentos utilizados em redes locais sem fio, se comparado com a época em que surgiu esta tecnologia, pode-se considerar bastante acessíveis atualmente. Mas no orçamento de uma rede local sem fio, tem que avaliar o custo benefício desta rede, que na maioria dos casos torna-se lucrativo para a empresa.

TABELA 4 : Orçamento dos equipamentos utilizados na aplicação.

EQUIPAMENTOS	CUSTOS
2 ROUTERS	R$ 800,00
5 NOTEBOOKS	R$ 25.000,00
5 PLACAS PCI WIRELESS	R$ 1.100,00
CUSTO TOTAL =	R$ 26.900,00

5.4 Instalação e configuração dos equipamentos

As versões precedentes do Windows requerem assistentes de instalação e configuração dos equipamentos. Os fabricantes de equipamentos Wireless Lan fornecem estes assistentes para cada versão do Windows, com instruções detalhadas, para assegurar uma conexão bem sucedida. A instalação e configuração nestes assistentes podem ser realizadas através de CDs, que acompanham os equipamentos, ou em uma interface de administração Web, inserindo no browser o endereço fornecido com o equipamento.

5.4.1 Principais procedimentos de instalação e configuração

Para iniciar a instalação da rede local sem fio como extensão de uma rede cabeada, são necessários três componentes: 1) Os dispositivos do cliente (notebooks, PCs, etc.), com capacidade de Wlan. 2) Cabo ISP, modem DSL, ou outra tecnologia de banda larga. 3) Router sem fio.

5.4.1.1 A conexão do router

Agora que se têm os componentes necessários para a implementação da comunicação sem fio, pode-se então ligar os dispositivos da rede e configurá-los, de acordo com as instruções fornecidas no assistente do fabricante. A forma de conexão da base wireless (router), é ilustrada na FIGURA 26.

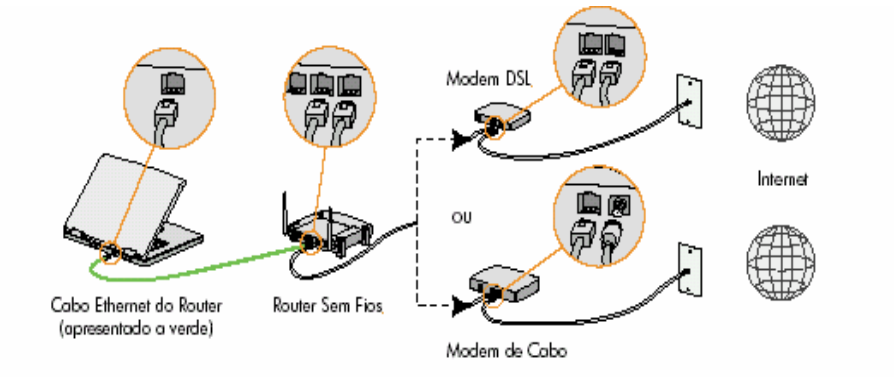

FIGURA 26 : CONEXÃO DO ROUTER WIRELESS.

Conforme ilustrado na FIGURA 26, o router é conectado ao equipamento de banda larga da rede cabeada (Modem DSL, ou Modem de cabo), e ao dispositivo do cliente utilizando os cabos Ethernet. A conexão entre o dispositivo do cliente e o router é feita através do cabo Ethernet temporariamente, somente até o término da configuração do equipamento.

5.4.1.2 Configuração do PC

Certifique que a rede está configurada para o protocolo TCP/IP, clique no item TCP/IP, e configure para obter o endereço IP automaticamente. Esta configuração é feita no painel de controle do PC, selecionando-se o ícone de conexão à rede ou internet, aparecendo uma tela com as propriedades da rede, onde é feita esta configuração. Terminando a configuração da rede no PC, é necessário reiniciar o computador, e iniciar a próxima etapa da instalação do router wireless.

5.4.1.3 Configuração do router

Para aceder o guia de configuração do router, Insira no browse, o endereço que virá no pacote de instalação do router, conforme mostrado na figura 27:

FIGURA 27 : BROWSE PARA ACESSAR GUIA DE INSTALACAO WEB.

Aparecerá uma tela pedindo uma senha. O router terá uma senha padrão, que para a segurança da rede deverá ser alterada após a configuração do router. Deve ser alterado também o nome da rede (SSID), que virá o nome padrão do fabricante. O nome da rede deverá ser o mesmo nos dispositvos do cliente e nos routers wireless. A FIGURA 28 ilustra a tela de autenticação da senha da rede.

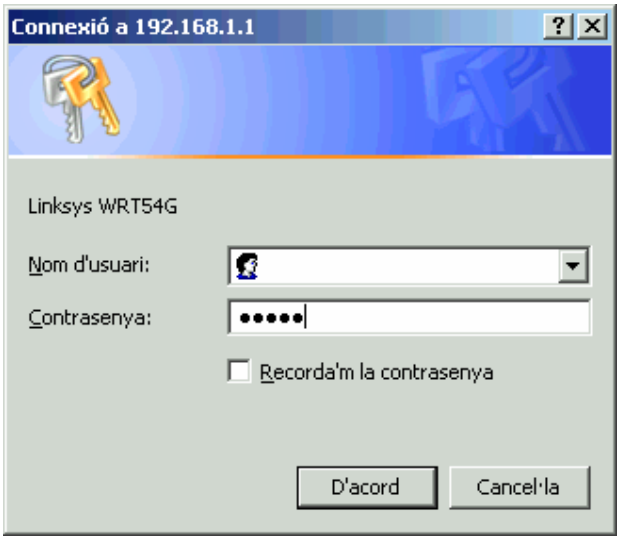

FIGURA 28 : TELA DE AUTENTICAÇÃO DA REDE WIRELESS.

Após a autenticação da senha, deve-se configurar o router através do assistente de configuração, que apresentará a tela inicial ilustrada na FIGURA 29.

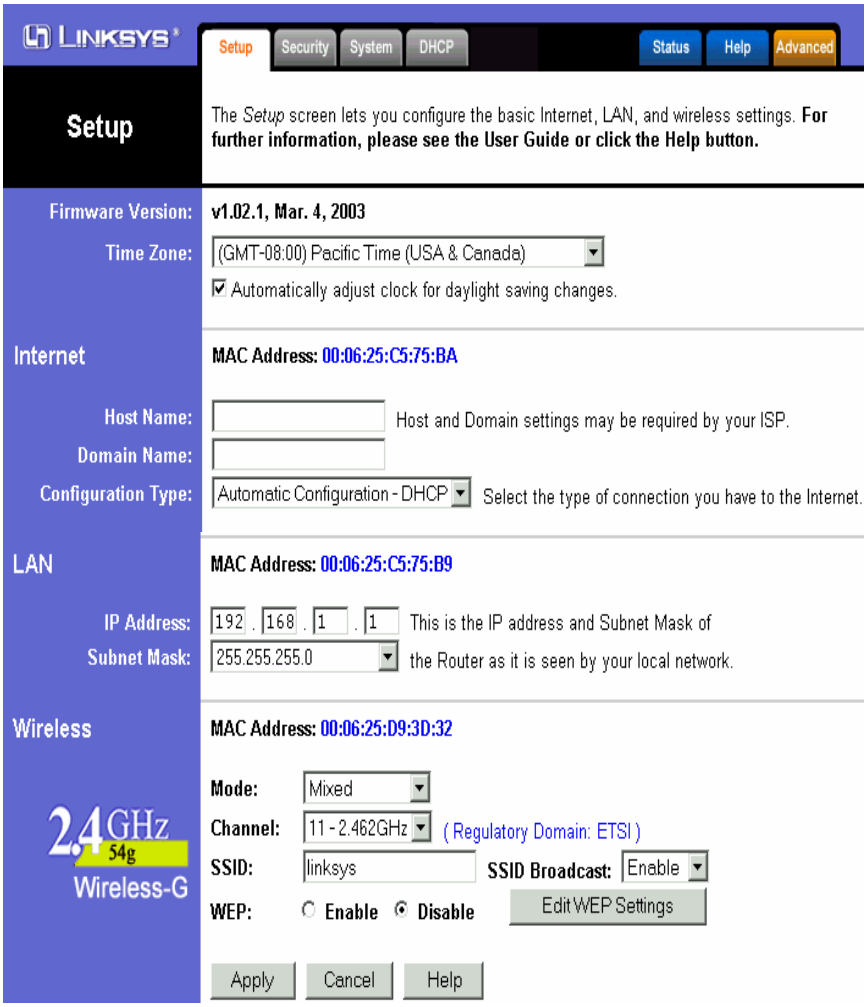

FIGURA 29 : TELA DO ASSISTENTE DE INSTALACAO DO FABRICANTE (LINKSYS).

Dentre todas as possíveis configurações do router, para a comunicação desta rede local sem fio, serão apresentadas nos itens posteriores, somente algumas básicas para o funcionamento da rede.

- A forma de conexão da internet, o IP, e máscara da rede local sem fio, conforme ilustra a FIGURA 30.

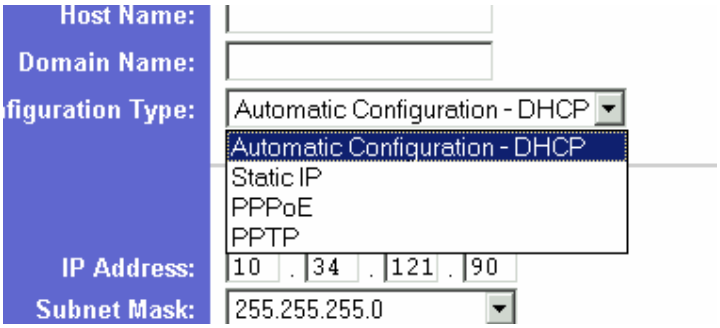

FIGURA 30 : CONFIGURAÇÃO DA CONEXÃO DA INTERNET.

- DHCP – Esta opção só deve ser utilizada se quiser que o router assuma um endereço IP atribuído automaticamente.

- Static IP – Esta opção funciona apenas em ambientes em que já exista uma rede instalada e serve para que o utilizador indique um endereço IP estático ao router.

- PPPoE – Esta opção é utilizada quando o router está ligado diretamente a um modem ADSL ou cabo que suporte este protocolo e permite que o router controle a ligação à Internet.

- PPTP – Esta opção permite a utilização do protocolo Point-to-Point Tunneling Protocol que é utilizado em redes VPN.

- O modo de serviço da rede wireless, conforme mostra a FIGURA 31.

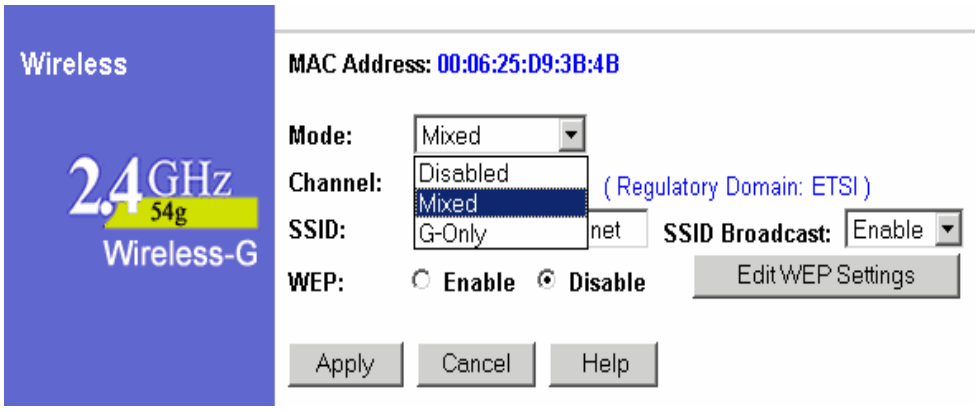

FIGURA 31 : CONFIGURAÇÃO DO MODO DA REDE WIRELESS.

- A configuração do canal que a rede funcionará, conforme ilustra a FIGURA 32.

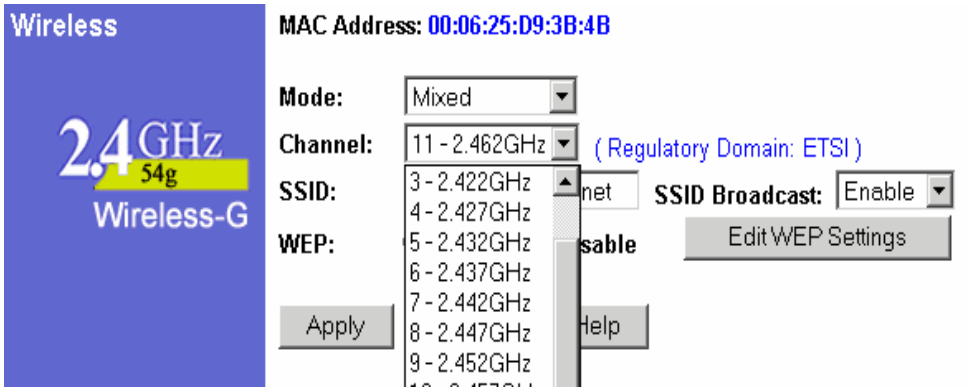

FIGURA 32 : CONFIGURAÇÃO DO CANAL QUE FUNCIONARÁ A REDE.

- A figura 32, ilustra também as seguintes configurações:

- Wireless Network Name(SSID) – SSID é o nome utilizado pela rede. Pode ser qualquer palavra e não pode utilizar espaços ou caracteres acentuados. Este nome é utilizado para identificar a rede quando um dispositivo se liga pela primeira vez.
- WEP – Neste menu, pode-se definir o protocolo de criptografia e a chave de autenticação da rede. Nesta aplicação será utilizado o protocolo WPA, mais seguro em relação ao protocolo WEP.

5.4.1.4 Configuração dos dispositivos do cliente

A configuração dos dispositivos do cliente é mais simples, pois são configurados apenas para a comunicação com o router, que controla todos os serviços. Para a comunicação de todos os dispositivos da rede e o router, algumas configurações precisam ser padrão em todos os equipamentos:

- O número SSID, que identifica a rede dos equipamentos.
- O protocolo de segurança deverá ser o mesmo em todos os equipamentos.
- O modo de operação da rede local sem fio.
-

6. Conclusões

Através deste trabalho pode-se concluir que esta tecnologia já é uma realidade, que vem mudando a forma de se comunicar.

Depois dos computadores pessoais, criados na década de 80, e a internet, na década de 90, que gerou um aglomerado de informações, agora a tecnologia de rede local sem fio vem proporcionar a mobilidade no acesso a estas informações. As principais vantagens desta tecnologia estão de encontro com as principais necessidades atuais do mundo. A possibilidade de acessar as informações a qualquer momento e de qualquer local que ofereça o acesso sem fio. A alternativa de extensão de rede cabeada, para a transmissão de dados em locais de difícil conexão de redes de computadores através de cabos. E a flexibilidade de operação e localização dos computadores no ambiente da rede.

Esta tecnologia através da constante evolução, no aspecto de velocidade na taxa de transmissão, possibilidade de locomoção entre as células de comunicação sem fio (*roaming*), robustez contra interferências, e principalmente na questão de segurança, está se tornando uma tecnologia muito promissora, sendo adotada em todo o mundo, em diversos ambientes, e em várias aplicações. O custo desta tecnologia esta cada vez mais acessível, em relação ao custo benefício desta rede, em relação à rede convencional.

Diante deste cenário, percebe-se que esta tecnologia será adotada amplamente em aplicações cada vez mais complexas. Assim, deve-se salientar a importância da elaboração de um projeto de implantação, utilizando a metodologia “Site Survey”. Através do estudo de caso apresentado em forma de um projeto de uma rede sem fio, foi possível verificar que através da aplicação dos procedimentos desta metodologia, consegue-se realizar uma análise minuciosa, atingindo com isso uma maior eficiência e redução de custos da rede.

A transmissão de dados em redes de computadores sem fio, além desta rede WLan utilizada para ambientes locais, tende uma abrangência de alcance para patamares de longa distância, através do padrão 802.16, denominado popularmente com Wimax. Tornando esta nova tecnologia uma ótima opção de tema para um futuro trabalho.

7. Referências Bibliográficas

- J. S. Silva, Adailton. Rede Nacional de Ensino e Pesquisas (RPN), As tecnologias de Redes Wireless Disponível em : http://www.rnp.br/newsgen/9805/wireless.html Acesso em : 01mai. 2004

- SUCESU-ES. Sociedade de Usuários de Informática e Telecomunicações do Espírito Santo, Desafio de investir em mobilidade Disponível em : http://www.sucesues.org.br/documentos/index.asp?cod_noticia=454 Acesso em 01 mai. 2004

- Fortes, Débora. Na Freqüência do WI_FI. Revista Info Exame. v.218, p. 42 – 44, mai, 2004.

- Fortes, Débora. O WI-FI Na Vida Real. Revista Info Exame. V.218, p. 49 – 53, mai, 2004

- Fortes, Débora. O WI-FI Na Vida Real. Revista Info Exame. V.218, p. 49 – 53, mai, 2004

- C.C. Ribas, Júlio. Trabalho Individual Pós Graduação, Universidade Federal de Santa Catarina Disponível em http://www.nersd.org/~sartori/Wireless/TI_Julio.doc. Acesso em 01 mai. 2004

- G.U. Garcia, Luis. Redes Locais Sem Fio que atendem ao Padrão 802.11, Universidade Federal do Rio de Janeiro Disponível em www.gta.ufrj.br/grad/01_2/802-mac Acesso em : 01 jun. 2004

- P.S.S. Land, Ana. Redes wireless Acesso Via Rádio Padrão 802.11 Disponível em http://professores.faccat.br/azambuja/teleprocessamento/802_03.htm Acesso em 01 jun. 2004

- E.Abras. Gustavo; C.G Sanches, Jayme. Pontifica Universidade Católica do Paraná, Monografia Wireless Lan Disponível em http://www.ppgia.pucpr.br/~jamhour/Download/pub/ArtigosPos/Monografia%20WLAN.pdf.

- Maia, Roberta. Segurança em Redes Wiereless. GTA – Universidade Federal do Rio de Janeiro. Disponível em http://www.gta.ufrj.br/grad/02_2/wep/ Acesso em 25 Out. 2004.

- P. Mathias, André. Universidade Federal do Rio de Janeiro IEEE 802.11 – Redes Sem Fio Disponível em : http://www.gta.ufrj.br/grad/00_2/ieee/index.html Acesso 05. Set. 2004

- Teleco, Informação para o Aprendizado Contínuo em Telecomunicações, Wlan/WI-fi Disponível em : http://www.teleco.com.br/wifi.asp Acesso em : 05. Set 2004

- UFRJ, IEEE 802.11 As Técnicas de Espalhamento Espectral http://www.gta.ufrj.br/seminarios/semin2003_1/aurelio/2-80211.htm Acesso em : 07.Set. 2004