UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL - UFRGS
INSTITUTO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM COMPUTAÇÃO

WIRELESS LAN
A grande questão: 802.11a ou 802.11b?

por

CARLOS DIONÍSIO HAUENSTEIN

Trabalho de Conclusão submetido como requisito parcial para a obtenção
do grau de Mestre em Informática

Prof. Juergen Rochol
Orientador

Porto Alegre, dezembro de 2002

CIP – CATALOGAÇÃO NA PUBLICAÇÃO

Hauenstein, Carlos Dionísio

Wireless LAN a Grande Questão: 802.11a ou 802.11b? / por Carlos Dionísio Hauenstein. – Porto Alegre: PPGC da UFRGS, 2002.

90 p.: il.

Trabalho de Conclusão (mestrado) – Universidade Federal do Rio Grande do Sul. Programa de Pós-Graduação em Computação, Porto Alegre, BR – RS, 2002. Orientador: Rochol, Juergen.

1. IEEE 802.11. 2. Benefícios. 3. Aplicabilidade. 4. Funcionamento. 5. Hardware 6. Características. 7. Segurança. 8. Tecnologias. 9. Tipos. 10. Infra-estrutura. 11. Sub-camadas. 12. Fabricantes. I. Rochol, Juergen. II. Título.

Agradecimentos

Aos professores da UFRGS, pelo ensinamento teórico e prático.

Aos colegas, pela amizade e partilha do conhecimento adquirido ao longo dos anos de atividades na área profissional, nos mais diversos setores da sociedade.

Ao professor Juergen Rochol, pelo vasto conhecimento repassado, pela visão das tendências tecnológicas e pela motivação nos momentos decisivos desde o início até o término deste trabalho de conclusão.

À todos os conselheiros da Empresa X, onde exerço minhas atividades junto a área de Tecnologia da Informação, pelos investimentos na área de educação.

À minha esposa Miriam e filhas Débora e Deise, presentes em todos os momentos, especialmente nos oito meses e meio em que estive enfermo em 2002.

Sumário

Lista de Abreviaturas

ACLs	Access Control Lists
AM	Amplitude Modulation
AP	Access Point
ASK	Amplitude Shift Keying
ATIM	Ad-Hoc TIM
BDD	Binary Decision Diagrams
BOE	Backoff time Expirado
BOR	Backoff time Residual
BSA	Basic Service Area
BSS	Basic Service Set
BWA	Broadband Wireless Access
CCK	Complementary Code Keying
CSMA/CA	Carrier Sence Multiple Access with Collision Avoidance
CTS	Clear To Send
DBPSK	Differential Binary Phase Shift Keying
DCF	Distributed Coordination Function
DFWMAC	Distributed Foundation Wireless Medium Access Control
DIFS	DCF inter-frame spacing
DQPSK	Differential Quadrature Phase Shift Keying
DS	Distribution Service
DSSS	Direct-Sequence Spread Spectrum
DTIM	Delivery TIM
EHF	Extremely High Frequency
ERB	Estação Rádio Base
ESA	Extended Service Area
ESM	Estação de Suporte a Mobilidade
ESS	Extended Service Set
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FFH	Fast Frequency Hopping
FHSS	Frequency-Hopping Spread Spectrum
FDM	Frequency division multiplexing
FM	Frequency Modulation
FSK	Frequency Shift Keying
GFSK	Gaussian Frequency Shift Keying
HF	High Frequency
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISM	Industrial Scientific and Medical
LAN	Local Area Network
LF	Low Frequency
MAC	Medium Access Control
MANET	Mobile Ad-Hoc Networks
MF	Medium Frequency
MIB	Management Information Base
MIMO-OFDM	Multiple Input, Multiple Output Orthogonal Frequency Division Multiplexing

NAV	Net Allocation Vector
NCC	Network Control Center
NLOS	Non-Line-of-Sight
OFDM	Orthogonal Frequency Division Multiplexing
PBCC	Packet Binary Convolutional Coding
PCF	Point Coordination Function
PCM	Pulse Code Modulation
PDA	Personal Digital Assistants
PDU	Physical Data Unit
PIFS	PCF inter-frame spacing
PLCP	Physical Layer Convergence Procedure
PLW	PLCP_PDU Length Word
PM	Phase Modulation
PMD	Physical Medium Dependent
PPM	Pulse Position Modulation
PRM	Modelo de Referência de Protocolos
PRNG	Pseudo Random Number Generator
PSF	PLCP Signaling Field
QAM	Quadrature Amplitude Modulation
RADIUS	Remote Authentication Dial-In User Service
RF	Rádio Freqüência
RTS	Request To Send
SFD	Start Frame Delimiter
SFH	Slow Frequency Hopping
SHF	Super High Frequency
SIFS	Short inter-frame spacing
SIP	Sistema de Identificação de Produtos
SOHO	Small Office Home Office
SSID	Service Set Identifier
TCP	Transfer Control Protocol
TDMA	Time Division Multiple Access
TIM	Traffic Indication Map
UM	Unidade Movel
VCS	Virtual Carrier Sense
VHF	Very High Frequency
Wi-Fi	Wireless Fidelity
VLF	Very Low Frequency
VOFDM	Vector OFDM
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WOFDM	Wideband OFDM
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network

Lista de Figuras

Lista de Tabelas

Resumo

Este trabalho apresenta, inicialmente, uma análise comparativa detalhada dos dois padrões, IEEE 802.11a e IEEE802.11b, que foram apresentados recentemente pelo IEEE na área de redes sem fio (*wireless*). São apresentadas as principais diferenças tecnológicas dos dois padrões, no que se refere, principalmente, à arquitetura, funções de controle, segurança, desempenho e custo de implementação destas duas tecnologias de redes *wireless*. São avaliados também os aspectos de interoperabilidade, quando estas redes são integradas em redes corporativas fixas, que são baseadas, principalmente, em redes Ethernet, tradicionalmente usadas em redes corporativas. São considerados também, aspectos de custo e flexibilidade de aplicação das duas tecnologias e mostram-se como estas diferenças devem ser levadas em conta em aplicações típicas de um ambiente corporativo.

Finalmente, apresenta-se também, como estudo de caso, uma análise focalizada principalmente na integração da tecnologia *wireless* em aplicações típicas de uma grande empresa local. Consideram-se as vantagens e desvantagens de ambas as tecnologias, como solução para algumas aplicações típicas encontradas nesta empresa, e justifica-se a escolha da solução que foi adotada.

Conclui-se com algumas projeções quanto ao futuro da tecnologia *wireless* no ambiente público e corporativo.

Palavras-chave: Redes *wireless*, IEEE 802.11a e IEEE802.11b. Aplicações *wireless*, Arquiteturas *wireless*, Interoperabilidade de redes *wireless*, Custo de Implementação.

TITLE: “WIRELESS LAN THE GREAT QUESTION: 80211a OR 802.11b?”

Abstract

This research presents, first of all, a detailed comparative analysis of both standards, IEEE 802.11a and IEEE 802.11b, recently released by the IEEE, in the area of wireless LANs. We present the main technological differences between the two standards concerning mainly to architectural aspects, control functions, performance and costs of implementation of these two types of wireless LANs. We also consider the problem of interoperability when we integrate wireless technology with fixed wired LANs based mainly on Ethernet LANs traditionally used in a corporate network. We also analyze some aspects of costs and flexibility in the application of wireless technology and how these differences must be considered in typical applications in a corporate environment.

Finally we present, as a case study, an analysis focused mainly on the integration of wireless technology for typical applications in a big local corporation. We consider the advantages and disadvantages of both technologies as a solution for typical applications in the corporation and we justify the adopted solution.

We conclude with some future projections in the application of wireless solutions in public and corporate environments.

Keywords: WLANS, IEEE 802.11a, IEEE 802.11b, Wireless Applications, Wireless LAN Architectures, Interoperability of Wireless LANs, Implementation costs.

1 Introdução

Esta introdução está dividida em três sessões, a saber:

a) 1.1) histórico da computação movel;

b) 1.2) construção de redes wireless LAN na Empresa X, título dado em substituição ao nome original da empresa que construiu redes wireless no seu ambiente de produção;

c) 1.3) estrutura do trabalho.

1.1 Histórico da computação movel

Computação Movel é o último estágio do desenvolvimento da computação pessoal. Em 1946, Illinois Bell Telephone Company disponibilizou um serviço de telefonia movel, o qual possibilitou usuários na direção de veículos comunicarem-se com o sistema telefônico, tornando-se a primeira iniciativa com sucesso na comunicação bi-direcional sem fio.

Antigamente, até a metade da década de 90, as tecnologias Wireless LAN eram muito lentas e caras. A inexistência de padrões não possibilitavam que fossem interoperacionais e confiáveis. A alocação de freqüências também era um problema, pois as tecnologias proprietárias disputavam faixas do espectro. Adquirir uma tecnologia proprietária sempre foi um investimento de grande risco. Usuários que construíssem as WLANs ficavam numa difícil situação: dependência de um único fornecedor ou tentavam resolver seus problemas de infra-estrutura por conta própria.

Com o objetivo de encaminhar uma solução para este problema o IEEE criou um comitê para padronização do WLAN: o “Working Committe for Wireless LANs”. Em 1997, foi aprovado o padrão 802.11 e designada a faixa de 2.4 GHz para utilização. Em 1999, foram aprovados os padrões 802.11b e 802.11a. A partir daí, a indústria começou a trabalhar na conformidade aos padrões e na interoperabilidade.

Redes com o padrão 802.11b, desenvolveu-se mais rapidamente que o padrão 802.11a, foram construídas nas áreas de manufatura das empresas e nas redes dos setores educacional e institutional. Mais recentemente, particularmente em 2001, quando os preços dos adaptadores e dos pontos de acesso baixaram drasticamente os produtos de rede wireless 802.11b começaram a serem usados em larga escala em escritórios, hospitais, shopping centers, lojas, bares, restaurantes e eventos temporários.

Mark Weiser, um dos papas da computação movel e um dos cientistas brilhantes da Xerox Parc, no seu artigo já clássico, "The Computer for the Twenty-First Century" ("O Computador para o Século Vinte e Um") vislumbra um novo horizonte para o computador pessoal e para a computação sem fio: um mundo sem fio, e ao mesmo tempo um mundo conectado à uma rede onipresente de computadores.

Após termos iniciando este novo século, o 21, estamos assistindo a uma nova revolução: a dos Personal Digital Assistants (Assistentes Pessoais Digitais) ou dos Handheld Computers (Computadores de Mão), como são chamados os pequenos computadores pessoais que cabem na palma da mão. Os PDAs, fabricados por empresas como 3Com, HP, Compaq, Casio e Philips começam a fazer parte do cotidiano das pessoas. Segundo a Microsoft Research, o número de pessoas conectadas a redes sem fio irá ultrapassar a barreira de 1 bilhão no ano 2004.

1.2 Motivação para construção de redes wireless LAN na Empresa X

Freqüentemente as empresas enfrentam dificuldades técnicas quando planejam instalar suas redes de comunicação de dados via cabo. É o caso, por exemplo:

a) de instalações nas quais há uma rua separando os edifícios;

b) de empresas e agências bancárias onde o lay-out dos computadores é alterado muito freqüentemente;

c) de áreas de difícil acesso, ou onde está operacional uma linha de produção 24x7 (poucas paradas programadas) e muitas vezes de grande interferência eletromagnética;

d) de ambientes onde os usuários necessitam mobilidade constante sem perder a conexão com os sistemas da rede corporativa.

Utilizando-se da tecnologia Wireless LAN tem-se uma solução prática e ao mesmo tempo economicamente viável. Todos os casos, acima mencionados, aplicam-se as necessidades da Empresa X, e várias delas já foram encaminhadas. Entretanto, há uma outra necessidade, a qual motivou o estudo e aplicação desta tecnologia, conforme descrito nos tópicos 1.2.1 e 1.2.2, abaixo.

1.2.1 Configuração inicial

Nas diversas áreas de produção estão configuradas bases de dados SQL as quais replicam-se com um servidor de consolidação central, configurado no CPD de cada uma das unidades industrial. A base de dados do servidor central de cada unidade industrial, replica suas informações com o SAP R/3 localizado em Porto Alegre. Este, o SAP R/3, contém as informações de todas as unidades da Empresa X.

Uma aplicação, desenvolvida de forma padrão para todas as unidades da Empresa X, gerencia o processo de produção e carregamento, nas áreas industrial.

O peso real dos produtos é obtido por meio de balanças colocadas em cada máquina produtora, ou em centrais de pesagem, ligadas a coletores de dados e impressoras de códigos de barras. Cada peça produzida tem o seu peso lido das balanças, e além da impressão nas etiquetas, este peso é armazenado nos bancos de dados, os quais possibilitam uma série de consultas sobre a produção.

Quando um caminhão entrava na unidade para realizar um carregamento de cargas fracionadas (diferentes produtos), era necessária a realização de pesagens intermediárias para cada produto. Desta forma o caminhão tinha que se deslocar diversas vezes até a balança da expedição aumentando o seu deslocamento dentro da unidade, esperando na fila de caminhões da balança e retornando a uma mesma frente de carregamento diversas vezes.

1.2.2 Objetivos e resultados esperados

A Empresa X, com suas 105 unidades (industrial, comercial e florestal) instaladas no Brasil, identificou a necessidade de melhorar a qualidade dos serviços do seu Sistema de Identificação de Produtos (SIP) nos seguintes aspectos:

a) controle do tempo de permanência dos caminhões das transportadoras dentro das unidades;

b) fornecimento de uma melhor identificação dos produtos, utilizando-se de etiquetas de PVC;

c) gerenciamento das diversas frentes de carregamento, mantendo o estoque dos produtos atualizado e disponível de forma on-line;

d) aprimoramento da qualidade dos serviços, obtendo o peso real nas etiquetas para os produtos comercializados em quilos, evitando erros de digitação;

e) mobilidade dos operadores dentro das áreas de produção;

f) maior flexibilidade no posicionamento de pontos de coleta fixos e;

g) necessidade de maior rapidez na troca de informações entre o ponto de coleta e as bases de dados dos servidores; pois, os dados a serem usados no ponto de coleta alteram rapidamente, passando a ser de vital importância o uso da informação mais atual;

h) vários operadores executam uma mesma tarefa sendo necessário coordená-los.

O resultado aguardado pelo conselho diretor da empresa é o completo automatismo do processo de carregamento dos caminhões nas *frentes de carregamento*, possibilitando que todos os itens a serem carregados sejam transmitidos para coletores de dados, móveis, por meio de redes wireless LAN, e que todas as etiquetas das peças a serem carregadas sejam lidas e as informações obtidas sejam transmitidas para o módulo de Carregamento do SIP, que as envia para o SAP R/3 - Sistema encarregado da emissão da Nota Fiscal e Certificado de Qualidade.

Para alcançar estes objetivos, decidiu-se projetar, adquirir e implementar uma solução de rede local wireless, que inclua interoperabilidade entre diferentes fabricantes.

1.3 Estrutura do trabalho

Para a Empresa X, que têm sua área de Tecnologia da Informação corporativa e algumas dezenas de administradores de rede nas demais localidades, é de suma importância que todos obtenham conhecimento com relação aos conceitos, os tipos de rede Wireless LAN, as tecnologias empregadas, a arquitetura do sistema e o conhecimento do funcionamento destas redes – MAC, descritos nos capítulos 2, 3, 4, 5 e 6. Por este motivo, tais assuntos exaustivamente pesquisados no IEEE 802.11 e em outras literaturas foram adicionados à este trabalho.

No Capítulo 1, introduzimos nossas considerações com relação a evolução das redes móveis, a motivação para construção de redes wireless LAN na Empresa X e descrevemos a estrutura do trabalho.

No Capítulo 2 apresentamos os objetivos, como funcionam, as características, os benefícios sobre as redes fixas, os conceitos, a comunicação entre as estações numa WLAN e a legislação radiofreqüência no Brasil.

No Capítulo 3 abordamos os tipos de rede WLAN, descrevendo as infra-estruturas fixa e Ad-Hoc, as WLANs com múltiplos pontos de acesso e pontos de extensão, o compartilhamento do acesso a internet, a conexão com as redes fixas e, as redes cliente/servidor com ponto de acesso.

No capítulo 4, são descritas as tecnologias empregadas nas WLANs – Narrow Band, Spread Spectrum e OFDM. São consideradas a Frequency Hopping Spread Spectrum, exemplificando a seqüência de salto FHSS na banda 2,4GHz e o formato do quadro FHSS; a Direct Sequence Spread Spectrum, descrevendo o formato do quadro DSSS e a alocação de banda no DSSS. Faz-se um comparação entre FHSS x DSSS. O capítulo finaliza considerando a transmissão infra-vermelha difusa e os outros sistemas Wireless.

No Capítulo 5 é descrita a arquitetura do sistema WLAN, ou seja, as células e os pontos de acesso, as funções dos APs, as ligações entre células (stand alone e multi-células), o modelo básico de arquitetura, os frames, a fragmentação e rearranjo das mensagens, a conexão de uma estação – como se desenvolvem os processos de autenticação e associação, a criptografia e sua importância, as fontes de interferência e as interfaces.

No Capítulo 6 são apresentados os aspectos relacionados ao MAC (Medium Access Control). É considerada a arquitetura de protocolos, o modelo de referência de protocolos, o DFWMAC-DCF básico (CSMA/CA), o CSMA/CA com o mecanismo RTS/CTS, o DFWMAC-PCF com Polling, os quadros do MAC, a sub-camada MAC, e, o gerenciamento (sincronização, energia, roaming e handoff).

No Capítulo 7 comparamos os padrões 802.11a e 802.11b com relação aos aspectos tomada de decisão, modelo de referência de protocolos, largura de banda, interoperabilidade, aplicabilidade, suporte a canais, interferência e segurança (métodos e regras). Finalizamos considerando os novos desenvolvimentos do padrão 802.11 e com um sumário das tecnologias.

No Capítulo 8, descrevemos: as metas definidas para o atingimento dos objetivos propostos pela Empresa X, as características consideradas no processo de especificação tecnológica, o que foi melhorado no processamento das informações, o laboratório 802.11b desenvolvido pela Empresa X, o laboratório 802.11a que não foi concluído, por falta de componentes no mercado, pela Empresa X e o laboratório 802.11a desenvolvido pela empresa norte-americana Extremetech.

No Capítulo 9, finalizamos o trabalho com um resumo das tecnologias WLANs.

2 Conceitos

Utilizando-se, quase que invariavelmente, da tecnologia de rádio-freqüência, as redes sem fio transmitem dados “pelo ar". Assim sendo, as ondas eletromagnéticas bem como as de rádio-freqüência não necessitam de meio algum para se propagar, ao contrário das ondas sonoras que necessitam de um meio material.

Um ambiente de **computação movel** compreende computadores interligados em rede através de um sistema de ondas de rádio. Vamos chamar de Unidade Movel (UM) o elemento de rede (computador, impressora, etc...) interligado a rede de computação movel. Diversas Unidades Móveis (UMs) conectam-se à uma antena, ou seja, a um Ponto de Acesso, formando uma sub-rede. Não é obrigatoriamente necessária a presença de Pontos de Acesso, então, um ambiente de computação movel pode ser projetado e/ou desenvolvido de forma independente da infra-estrutura fixa, as chamadas redes Ad-Hoc, onde a comunicação entre si ocorre diretamente através das antenas.

A mobilidade, porém, sempre implica em algumas condições típicas do ambiente, as quais devem ser consideradas independente do sistema de acesso, como por exemplo:

a) capacidade de comunicação limitada com largura de banda variável e alta taxa de erros;

b) autonomia de energia condicionada à baterias com limite de consumo, sendo necessário dispender o mínimo de energia com processamento e dispositivos de apoio ao sistema;

c) limites físicos de hardware para garantia de portabilidade, limitando também o poder de processamento e dispositivos.

2.1 Objetivos das WLANs

As primeiras vantagens percebidas no WLAN são: flexibilidade, mobilidade, facilidade de expansão e custo/benefício. Os seguintes objetivos também necessitam ser atendidos:

a) usar ondas de rádio para interconectar usuários num raio de desde algumas centenas de metros até quilômetros;

b) transmitir dados com confiabilidade a taxas comparáveis à LANs convencionais (com cabos);

c) interoperar com tecnologias de rede como Ethernet e ATM, assim como outras tecnologias de wireless;

d) ser escalável, seguro e de fácil manutenção.

2.2 Aspectos de funcionamento

Os sistemas wireless podem ser divididos em sistemas fixos, portáteis e IR.

a) Sistema Wireless Fixo: utiliza freqüência de rádio e possui uma antena fixa. Exemplos: internet via rádio, conexões via satélite.

b) Sistema Wireless Portátil: geralmente utiliza bateria. Exemplos: telefones celulares, notebooks, pagers, PDAs.

c) Sistema Wireless IR: utiliza radiação infra-vermelha para enviar sinais dentro de uma área limite de comunicação. Esses sistemas são usados geralmente em controles remotos de televisão, teclados e mouse sem fios. Com o surgimento de novas tecnologias, sistemas IR podem agora conectar notebooks, desktops e outros dispositivos usados dentro de uma mesma área de rede (WLAN).

2.2.1 Como funcionam?

A princípio, o funcionamento deste tipo de rede é igual ao das redes cabeadas e, dividem-se em três tipos: redes locais, redes locais estendidas e computação movel.

Na maior parte do tempo, a WLAN interage com a Ethernet LAN. Sendo assim, o AP funciona como uma bridge dentro da LAN, permitindo dispositivos WLAN compartilhar os mesmos recursos das estações cabeadas.

Numa Rede sem Fio os dados são enviados "através do ar" em canais de freqüência de rádio, infra-vermelho ou laser. O *infra-vermelho* é pouco usado. Sua faixa de freqüência fica logo abaixo da freqüência da luz visível. Os sinais transmitidos devem ser bem fortes, de alta intensidade para não permitir a interferência da luz externa. Pode-se conseguir altas taxas de transmissão chegando a 10 Mbps. A distância máxima de comunicação não ultrapassa 30 metros mesmo com dispositivos bem potentes da atualidade. Pode-se utilizar a transmissão por infra-vermelho com feixe direto (linha de visada desobstruída), semelhante à comunicação dos controles remotos das televisões caseiras, ou com radiação a todas as direções por reflexão em superfícies e teleponto óptico (lentes) de banda larga [WLA 2001].

Já o *laser* pode alcançar distâncias de 200 a 300 metros com visada direta. Ele pode ser utilizado para conectar duas Redes sem Fio, cada uma cobrindo, por exemplo, um prédio.

As *freqüências de rádio* (radiodifusão) são as mais utilizadas em redes de computadores. Por sua natureza, são adequadas tanto para ligações ponto a ponto quanto para ligações multiponto. As Redes sem Fio, baseadas em radiodifusão, são uma alternativa viável onde é difícil, ou mesmo impossível, instalar cabos metálicos ou de fibra óptica. Seu emprego é particularmente importante para comunicações entre computadores portáteis em um ambiente de rede local movel.

A radiodifusão também é utilizada nas aplicações onde a confiabilidade do meio de transmissão é requisito indispensável. Um exemplo drástico são as aplicações bélicas, onde, o rompimento de um cabo pode paralisar todo um sistema de defesa.

Para a transmissão das informações de um ponto a outro, são utilizadas as ondas eletromagnéticas (rádio ou infra-vermelho), sem a necessidade da existência de uma conexão física. Ondas de rádio são geralmente referidas como *portadoras* de rádio porque simplesmente fazem a função de entregar energia para um receptor remoto.

O dado a ser transmitido é sobreposto a uma portadora de modo a ser corretamente extraído pelo receptor. Isto é geralmente referido como *modulação* da portadora. Uma vez que o dado é sobreposto (modulado) à portadora, o sinal de rádio ocupa mais de uma freqüência simples, desde que a freqüência ou taxa de bits da informação da modulação some-se com a da portadora.

Múltiplas portadoras podem co-existir num mesmo espaço e ao mesmo tempo sem interferir uma nas outras, desde que as ondas de rádio sejam transmitidas em diferentes freqüências de rádio. Para extrair os dados, um receptor de rádio sintoniza-se em uma freqüência de rádio enquanto rejeita todas as outras. Usam-se transceptores, os quais têm a propriedade de receber e transmitir sinais de rádio, e, também placas de rede wireless que fazem uma ponte entre as estações móveis e a base. O dispositivo base (transceptor) é chamado de ponto de acesso, pois por ele as informações chegam e são enviadas para as demais estações, outros pontos de acesso ou até para uma rede cabeada. Há dezenas de métodos de modulação de uma portadora, mas todos introduzem a informação a ser transmitida. Uma vez sobreposta a informação na portadora, o sinal de rádio ocupa mais que uma freqüência se o processo for de FM (freqüência modulada), a base dos métodos mais empregadas.

O projeto de uma rede movel tem três problemas básicos fundamentais: localização das unidades móveis, alocação de freqüências e propagação de sinais. Definida a infra-estrutura, outros dois problemas se destacam: rastreamento de usuários e gerenciamento de energia. Sempre que houver a necessidade de estabelecer uma comunicação com um determinado usuário, o sistema precisa determinar qual dos Pontos de Acesso será utilizado para a conexão. Portanto, o sistema, necessita enviar mensagens curtas (“paging") através dos Pontos de Acesso e aguardar por uma resposta da unidade movel. Este processo impacta em outras dificuldades, tais como:

a) como organizar ou agrupar as células, de forma a facilitar a localização?

b) com que freqüência as unidades móveis enviam mensagens aos Pontos de Acesso informando-os de sua localização atual?

c) quais algoritmos podem ser utilizados, afim de localizar com mais eficiência a célula em que se encontra o usuário?

2.2.2 Topologia

A topologia de uma rede IEEE 802.11 é composta pelos seguintes elementos:

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

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

AP - Access Point - funciona como uma bridge entre a rede wireless e a rede tradicional. Coordena a comunicação entre as STA dentro da BSS.

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

2.3 Benefícios sobre as redes fixas

Como benefícios oriundos das WLANs, podemos citar:

a) *Conforto:* para utilização em qualquer ambiente;

b) *Flexibilidade:* para utilização em diversas aplicações que exijam movimento. Possibilidade de as redes chegarem onde cabos não podem ir;

c) *Robustez:* uma rede sem fio pode sobreviver intacta em caso de um desastre, por exemplo, um terremoto onde a comunicação continuaria garantida;

d) *Disponibilidade:* independente da localização do usuário, combinando conectividade de dados com mobilidade, ou seja, acesso as informações em qualquer lugar de sua organização;

e) *Custo Reduzido:* o custo inicial de uma rede wireless pode ser mais elevado que o de uma rede fixa, entretanto, o custo de manutenção desta rede é significativamente mais baixo;

f) *Escalabilidade:* redes wireless podem ser configuradas segundo diversas topologias, de acordo com as necessidades. As configurações podem ser alteradas facilmente e as distâncias entre as estações adequadas de acordo com as necessidades;

g) *Instalação rápida e simples:* instalar uma rede local sem fio pode ser rápido e fácil, eliminando a necessidade de atravessar cabos através de paredes e andares;

h) *Diversas topologias:* podem ser configuradas numa variedade de topologias para atender a aplicações específicas, sendo as configurações facilmente alteradas.

2.4 Características

Muitos dos objetivos a serem alcançados são conflitantes e devem ser levados em consideração para garantir o sucesso comercial das Redes sem Fio:

a) Operação global: a operação de uma Rede sem Fio depende de uma padronização técnica. E países diferentes podem possuir padronizações diferentes, diminuindo dessa forma os ganhos advindos da economia em escala;

b) Consumo de energia: uma característica intrínseca da comunicação através de uma Rede sem Fio é a falta de conexão das estações móveis com uma infra-estrutura. Daí a necessidade de se construir equipamentos capazes de consumir o mínimo de energia possível, e, de a própria Rede sem Fio ser capaz de otimizar o consumo de energia do sistema;

c) Freqüências: sua utilização deve ser bem gerenciada. Uma questão a ser pesquisada é como se pode utilizar as freqüências disponíveis de modo mais eficiente;

d) Proteção de investimento: muito dinheiro já foi investido nas redes cabeadas. Portanto as novas Redes sem Fio devem ser capazes de interagir com elas; ou seja, os mesmo tipos de dados e serviços devem ser padronizados nas Redes sem Fio;

e) Segurança e robustez: um ambiente sem fio deve garantir transmissões confiáveis sem ruídos e ter métodos de segurança que evitem a recepção das informações por interceptores não autorizados e indesejáveis. Este é um dos aspectos mais preocupantes, mas as redes sem fio oferecem métodos de encriptação de dados que as fazem ser chamadas de WEP (Wireless Equivalent Privacy);

f) Conexão à rede cabeada: é importante que haja interconexão com as estações do backbone da rede cabeada. Nas infra-estruturas sem fio isto é disponibilizado pelo uso de módulos de controle que conectam os dois tipos de rede. Certamente esta é uma característica importante quando do início da implantação numa rede pré-existente ou mesmo para iniciar uma migração;

g) Área de cobertura: é a área de garantia da disponibilidade do serviço da comunicação. Pode ser de, aproximadamente, 30 a 100 metros de diâmetro para equipamentos em ambientes fechados, mas pode chegar a dezenas de quilômetros com equipamentos refinados e caros, geralmente empregados apenas por grandes corporações e empresas;

h) Mobilidade: faz-se necessário que as estações se movam de uma área a outra da mesma rede, mesmo quando se passa de um ponto de acesso a outro. Recursos de roaming são desejáveis;

i) Licença de operação: é preferível o uso de redes que funcionem sem a necessidade de licença para a freqüência de operação. No caso oposto, pode ser mais complexo liberar a operação e os custos envolvidos podem ser mais elevados.

Os ambientes móveis podem ser divididos em dois grupos: Infra-estruturados e *Ad-Hoc.*

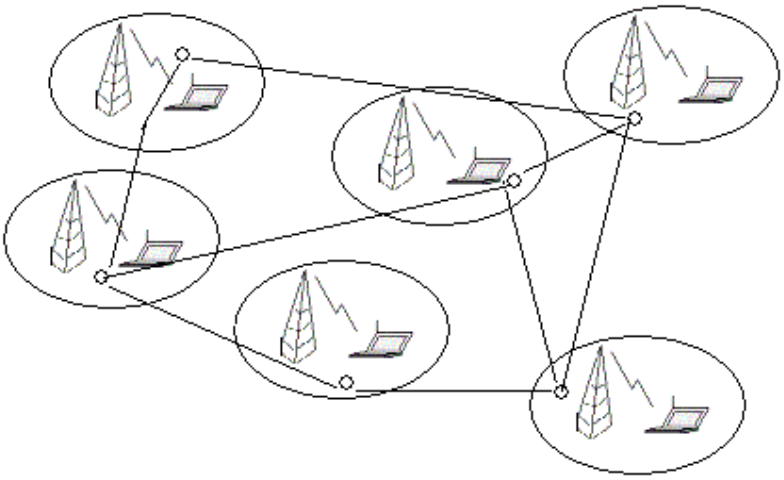

FIGURA 2.1 – Redes Móveis Infra-estruturadas

A maioria das WLANs, atualmente, são **redes com infra-estrutura**. Nelas, a transferência de dados acontece sempre entre uma estação e um ponto de acesso – AP. Os APs são nós especiais responsáveis pela captura e retransmissão das mensagens enviadas pelas estações. A transferência de dados nunca ocorre diretamente entre duas estações. O AP também pode agir como uma ponte para outra rede (cabeada ou sem fio). A (figura 2.2) mostra três APs com suas três áreas de atuação e uma rede cabeada ligando essas três áreas.

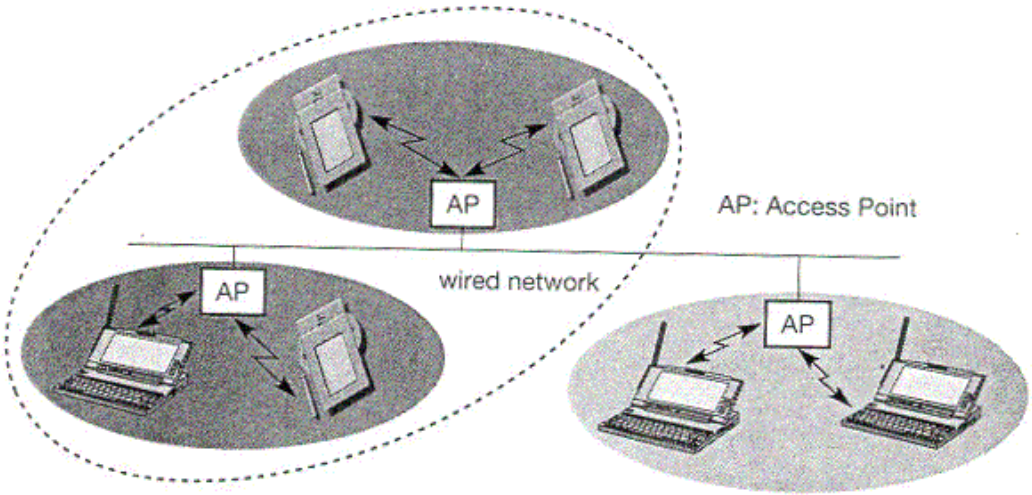

FIGURA 2.2 – Redes wireless conectadas à rede cabeada

Essa estrutura é típica de uma rede com topologia em estrela, onde um elemento central (no caso, o AP) controla o fluxo de toda a rede. Este tipo de rede pode usar diferentes esquemas de acesso, com ou sem colisão. Colisões podem ocorrer se as estações juntas com o AP não são coordenadas. Entretanto, quando somente o AP controla o acesso ao meio, nenhuma colisão é possível. Redes com infra-estrutura perdem um pouco da flexibilidade que as Redes sem Fio podem oferecer, por exemplo, elas ficam inutilizadas no caso de um terremoto que provoque a destruição de toda infra-estrutura da rede.

As redes de telefonia celular, são um caso típico de redes com infra-estrutura, que funcionam através de satélites também possuem uma infra-estrutura – os próprios satélites. Portanto, uma infra-estrutura não implica necessariamente numa rede fixa cabeada.

O segundo grupo é chamado de Redes Móveis *Ad-Hoc* ou Redes Móveis Não-Estruturadas, que não possuem uma ESM. A (figura 2.3) mostra uma rede movel *Ad-Hoc*.

Em MANET as entidades móveis comunicam–se sem o auxílio da ESM. Neste tipo de rede todos os nodos da rede podem se movimentar e comunicar-se com qualquer outro nodo que esteja em sua área de alcance. Esta área de alcance depende de características como potência da antena do nodo, potência da antena do nodo receptor de sinais, possíveis obstáculos entre os nodos, etc.

Ao se pensar em roteamento, é natural termos em mente os modelos tradicionais, inerentes às redes fixas, mas que em geral não se aplicam à realidade de ambientes móveis. Isso ocorre pelo simples fato de que eles não foram projetados levando-se em conta a mobilidade. Além disso, o endereço IP tradicional não pode ser usado no roteamento já que ele não pode ser associado a uma única rede.

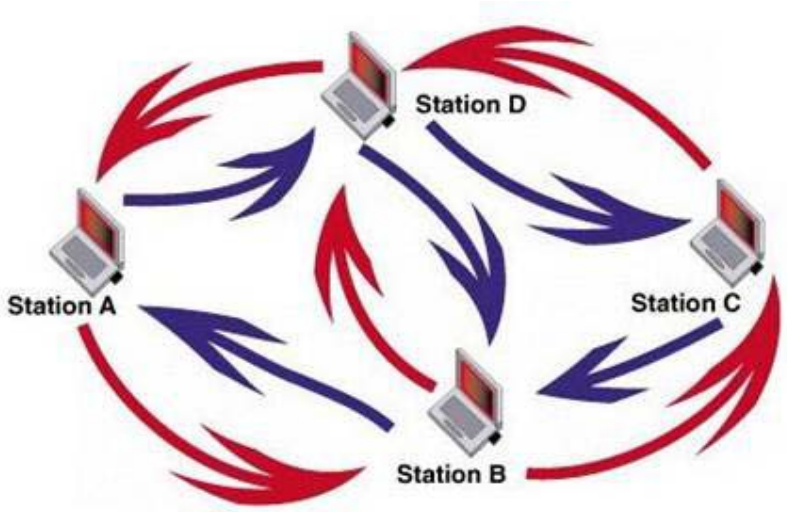

FIGURA 2.3 – Redes Móveis *Ad-Hoc*

Para se obter uma caracterização mais precisa e confiável, normalmente, utiliza-se Simuladores e/ou Métodos Formais.

Os simuladores são ferramentas que comprimem tempo e espaço. Comprimem espaço à medida que colocam lado-a-lado elementos que não estão fisicamente próximos. E comprimem o tempo porque proporcionam a observação de um sistema por um período que normalmente é difícil de observar, como 5 ou 10 anos. Esse poder de compressão do tempo nos permite saltar algumas etapas no processo de "verificação" de um sistema. Infelizmente simuladores não têm total garantia de que seus resultados são absolutamente corretos, pois há "pedaços" do sistema que não são considerados durante esse processo.

Os métodos formais, por sua vez, têm se mostrado bastante eficientes, seguros e têm apresentado grande sucesso na especificação e na verificação de sistemas computacionais bastante diversificados.

Outras considerações sobre métodos formais:

a) são técnicas de modelagem matemática que podem ser aplicadas a diferentes projetos de sistemas de computação tanto de hardware, quanto de software.

b) podem ser usados para especificar e modelar o comportamento de um dado sistema, e também para verificar matematicamente que o projeto, e sua implementação satisfazem propriedades desejadas e/ou necessárias. Não obstante, não há garantia de que o sistema modelado é perfeito [TRE 99].

c) geralmente apresentam bons resultados porque, devido ao seu caracter matemático, faz-se necessário um estudo mais aprofundado do sistema.

d) podem encontrar erros, às vezes não encontrados em simulações, pois se tem uma descrição mais clara e precisa do mundo real. No entanto, propriedades como confiabilidade, disponibilidade são ainda uma grande incógnita no que tange à especificação formal.

É importante perceber que as duas abordagens, simulação e verificação formal, não competem, ao contrário, as duas se completam.

Spin [SPI 97] é um pacote de software distribuído gratuitamente na Internet que suporta verificação formal de sistemas distribuídos. Foi desenvolvido pelo grupo de métodos formais da Bell Labs e é amplamente usado por pesquisadores da área. O Spin usa a linguagem de especificação chamada PROMELA [SPI 97], que é considerada bastante flexível e apresenta boa expressividade.

O MultiKit [MCM 99], ou Model-Checking Kit [SCH 99], é um conjunto de programas que permite modelar um sistema de estados finitos, usando uma grande variedade de linguagens, e verificar o sistema usando vários *Checkers*, incluindo *deadlock-checkers, reachability-checkers,* e *model-checkers* para lógicas temporias CTL e LTL. A mais interessante caracterísitca do Kit é a independência da linguagem de descrição escolhida. Quase todos os *checkers* podem ser aplicados ao mesmo modelo. Desta forma, os contra-exemplos produzidos pelo *checker* são apresentados ao usuário em termos da linguagem de descrição usada para modelar o sistema [SCH 99].

Verus é uma linguagem projetada com o intuito de simplificar o processo de verificação de programas de tempo real. Esta ferramenta é baseada na técnica de BDDs para comprimir os grafos gerados pelos estados do sistema.

As redes Ad-Hoc não necessitam de nenhuma infra-estrutura para funcionar. Cada estação se comunica diretamente com outra estação. Nenhum AP é necessário para controlar o acesso ao meio. Uma estação A só pode se comunicar com uma estação B se B estiver dentro do raio de ação de A ou se existir uma ou mais estações entre A e B que possam encaminhar a mensagem. Entenda-se por raio de ação a área de cobertura de uma estação, ou seja, todos os pontos geográficos onde o sinal desta estação chegue com um mínimo de clareza.

Numa rede Ad-Hoc, a complexidade de cada estação é alta porque toda estação tem que implementar mecanismos de acesso ao meio, mecanismos para controlar problemas com "estações escondidas" e mecanismos para prover uma certa qualidade de serviço.

As duas variantes básicas de Redes sem Fio, rede baseada em infra-estrutura e rede Ad-Hoc, nem sempre aparecem na sua forma pura. Existem redes que contam com AP e serviços básicos de infra-estrutura (exemplo: controle de acesso ao meio), mas também permitem uma comunicação direta entre duas estações sem fio.

O IEEE 802.11 é uma típica rede com infra-estrutura, mas que pode suportar uma rede Ad-Hoc. Entretanto, muitas implementações só funcionam na versão com infra-estrutura.

2.5 Largura de banda

É a diferença entre a maior e a menor freqüência.

Na literatura tradicional de comunicação, o termo largura de banda se refere à habilidade ou capacidade dos equipamentos de telecomunicação ou serviços de rede em termos de bits por segundo. Na terminologia de redes sem fio, largura de banda se refere à quantidade de freqüência oferecida pela FCC.

Pensando em largura de banda como o diâmetro de um tubo, quanto maior a sua largura maior a sua capacidade. Igualmente, quanto maior a freqüência da largura de banda, mais dados ela pode carregar. Por exemplo, TV tem largura de banda de 6000 kHz porque ela carrega áudio, vídeo e outros sinais.

A seqüência de freqüência gera os sons relativos à voz que são transmitidos via rádio ou sistemas com fio. O sinal de rádio é uma onda de energia que no vácuo viaja 297 000 Km/s. A comunicação via rádio atua em um espectro limitado de freqüências, por motivos técnicos, e algumas bandas são nocivas a diferentes espécies inclusive ao homem.

TABELA 2.1 - Espectro de Freqüência Eletromagnética

Freqüência	Banda	Tipo de freqüência
20 kHz para baixo		Audível
Menos de 30kHz		Rádio
30 – 300 kHz	VLF (Very Low Frequency)	Rádio
300 kHz – 3 MHz	LF (Low Frequency)	Rádio AM – 10^5
3 – 30 MHz	MF (Médium Frequency)	Rádio
30 – 300 MHz	HF (High Frequency)	Rádio
300 MHz – 3 GHz	VHF (Very High Frequency)	Rádio FM - 10^8
3 – 30 GHz	SHF (Super High Frequency)	Rádio
Mais de 30 GHz	EHF (Extremely High Frequency	Rádio
100 GHz		Raios-X
Acima de 10^{22} Hz		Raios Cósmicos

A conexão transmissor/receptor se dá por diversos tipos de ondas: As terrestres ou de superfície, que seguem a superfície da terra, em geral exploram baixas freqüências, apresentam longos comprimentos de ondas (10000 m), e são sujeitas a variações topográficas. As ondas espaciais, que trafegam em linha reta, usadas em transmissões de TV e apenas na faixa VHF e SHF, e as ondas celestiais que usam a camada de ionosfera como meio de transporte, atuam na faixa HF, usada para transmissão de rádio, e telefonia de longa distância. Ondas eletromagnéticas por si só não carregam informação.

Modulação é o processo no qual a informação é adicionada a ondas eletromagnéticas. É assim que qualquer tipo de informação, até a voz humana ou transação de dados numa aplicação interativa é transmitida numa onda eletromagnética [DOR 2000]. O transmissor adiciona a informação numa onda básica de tal forma que poderá ser recuperada na outra parte através de um processo reverso chamado demodulação.

Nas modernas redes de telecomunicação, a informação é transmitida, observando-se uma das duas características da onda: a amplitude e a freqüência. A modulação de amplitude AM, usa o sistema de chaveamento de amplitude ASK, e é usada na comunicação de voz, na maioria das transmissões de redes locais LAN. Mas não é indicada para LAN sem fio porque é muito sensível a ruído. A modulação de freqüência FM, usa o chaveamento de freqüência FSK. Outras formas de modulação são Modulação de fase PM, PCM e QAM, usados em sistemas digitais.

Sistemas de micro-ondas de rádio são classificados como analógico e digital dependendo do tipo de técnica de modulação empregada. Intrinsecamente, todas as transmissões de micro-ondas são feitas no sistema analógico. O uso da modulação

(analógico ou digital) é que diferencia. Pela modulação caracterizamos a forma de apresentar a informação que se transforma em tráfego.

2.6 Banda passante

Dá-se o nome de banda passante à faixa compreendida entre a maior e menor freqüência que um equipamento possa transmitir. Pode-se interpretar a banda passante como sendo uma "janela" no domínio das freqüências.

2.7 Banda estreita

Um sistema de rádio de banda estreita transmite e recebe informação do usuário numa freqüência de rádio específica, ajusta a freqüência do sinal do rádio a menor possível apenas para passar a informação.

2.8 Comprimento de onda

Toda comunicação sem fio usa energia eletromagnética para transmitir informação: Rádio, luz, Raios-X, são diferentes formas de radiação magnética. A única diferença está no comprimento de onda e a freqüência. Os sistemas móveis de comunicação se baseiam em sua grande maioria em rádios ou sinais.

Uma onda é caracterizada, conforme especificado abaixo, por: amplitude, freqüência e fase.

2.8.1 Amplitude

A amplitude é a medida da altura da onda para voltagem positiva ou para voltagem negativa. Também definida como crista da onda, a amplitude do sinal digital é igual à diferença da voltagem para o degrau entre 0 e 1. Iniciando na voltagem zero, a onda cresce, atinge a amplitude; decresce, se anula, atinge sua amplitude negativa e volta a crescer até se anular novamente. Essa seqüência compõe um *ciclo*.

2.8.2 Freqüência

A freqüência é o número de cristas por segundo ou o número de ciclos por segundo. Um ciclo também é denominado por 1 Hertz = 1 Hz, medida usual da freqüência, e seus múltiplos: 1 Kilohertz = 1Khz = 10 Hz, 1 Megahertz = 1Mhz = 1000 kHz, 1 Gigahertz = 1Ghz, e 1 Tetrahertz = 1Thz.

2.8.3 Fase

A fase é o ângulo de inflexão em um ponto específico no tempo, medido em graus.

2.9 Capacidade de transmissão

A capacidade de transmissão depende diretamente da freqüência de operação. Quanto maior a freqüência de operação de um sistema, maior será a sua capacidade de transmissão.

2.10 Canal

Um canal representa uma freqüência e uma largura de banda. Geralmente os designers quebram a largura de banda em duas partes: uma para uplink (terminal para rede) e outra para downlink (rede para terminal).

2.11 Pontos de acesso

É uma configuração tipicamente hardware/software, que reside na ou próxima a uma torre de antena. Transmite ou recebe sinais eletromagnéticos de ou para dispositivos numa área específica. A altura, o design e o tamanho da antena são fatores determinantes.

2.12 Repetidores

O alcance de transmissão de um sinal de uma micro-onda de rádio é finito, e é dependente do poder da estação base e a altura da antena. O caminho a ser percorrido pelo sinal e as obstruções ao longo do caminho afetam o alcance. Repetidores são usados para extender as transmissões para grandes distâncias.

Basicamente ele intercepta o sinal de uma antena e depois o retransmite. Alcances variam de acordo com freqüências. Vêr (tabela 2.2).

TABELA 2.2 - Variação de micro-ondas de rádio

Freqüência	Alcance aproximado antes do uso de repetidores
2 – 6 GHz	30 milhas / 50 Km
10 – 12 GHz	20 milhas / 30 Km
18 – GHz	7 milhas / Km
23 GHz	5 milhas / 8 Km

2.13 A comunicação entre as estações em uma Wireless LAN

A comunicação entre as estações numa rede Wireless LAN dentro de um escritório pode ser feita através de um ponto de acesso, instalado no teto do ambiente, transmitindo e recebendo dados das estações wireless pertencentes a rede. O barramento da rede, portanto, passa a ser o sinal irradiado (pode ser freqüência de rádio na faixa de 900 MHz a 6 GHz ou infra-vermelho que utiliza a faixa de freqüência próxima a 100 THz). Neste caso, o alcance ou cobertura varia de 30 a 100 metros, dependendo do tipo de sistema utilizado.

Considerando que as mudanças de locais e a estrutura dentro das empresas de um modo geral, são muito grandes, sendo estimado que 40% dos ambientes internos da empresa mudam de lugar por ano, as redes Wireless apresentam a vantagem de não serem afetadas pelas mudanças do ambiente, o mesmo não acontece com os cabos que devem acompanhar o planejamento e mudanças dos ambientes da empresa.

2.14 Transmissão de dados via radiofreqüência

Conhecido que as ondas eletromagnéticas se propagam a grande velocidade e atravessam vários meios, uma aplicação imediata é a transmissão de informação através das mesmas. A técnica consiste em estabelecer uma fonte, gerando uma onda básica chamada de portadora e variar alguma propriedade desta onda em função dos dados que se querem

transmitir. Este processo é chamado de modulação.

Por exemplo, caso se queira transmitir dados binários, podemos fazer com que a portadora fique na freqüência original f1 quando passe um bit zero e quando passe um bit um o sistema mude a portadora para a freqüência f2.

O receptor fará o processo inverso: quando ele receber a portadora na freqüência f1 ele gerará um bit zero e quando receber a portadora na freqüência f2 ele gerará um bit um. Este processo utilizou a freqüência da onda eletromagnética para transmitir os dados. Por isso ele é chamado modulação em freqüência (figura 2.4).

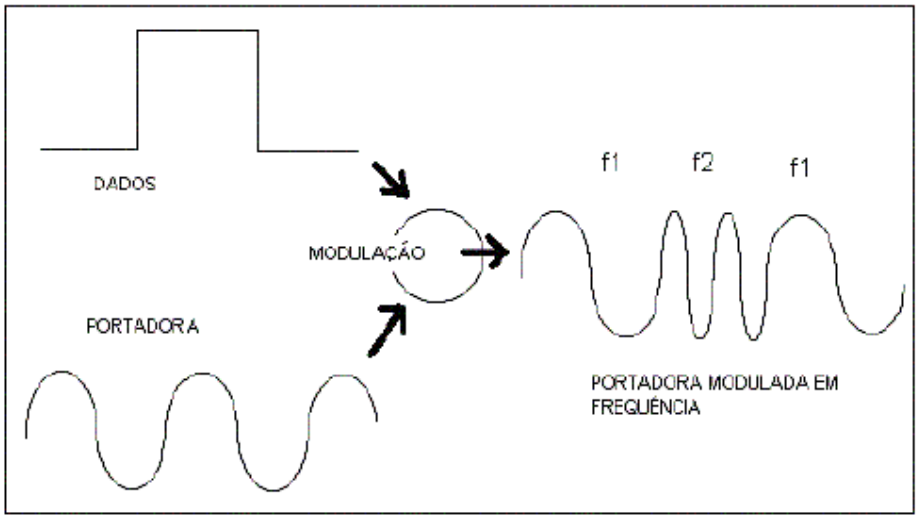

FIGURA 2.4 – Transmissão de dados via radiofreqüência

2.15 Legislação radiofreqüência

Com a proliferação dos meios de comunicação e a invenção de inúmeros aparelhos geradores de RF, o espectro eletromagnético começou a ficar congestionado. Consequentemente, foram criados órgãos internacionais que se dedicam especificamente para definir normas e fiscalizar a utilização do espectro eletromagnético. Estes órgãos dividiram o espectro em faixas atribuindo utilizações específicas para cada faixa.

No Brasil o órgão que tem a função de definir e fiscalizar a utilização das freqüências é a Anatel, pertencente ao Ministério das Comunicações. Qualquer equipamento que utilize RF deve ser submetido a um processo de certificação junto à Anatel, ou seja, deve ser registrado com todas as suas características junto ao Ministério das Comunicações. Em seguida, dependendo das características de transmissão, o cliente deverá obter uma autorização (licenciamento) da Anatel para a utilização do equipamento num local especificado. Entretanto, dependendo das características do equipamento o sistema pode ser isento de licenciamento.

2.16 Transmissão infra-vermelha difusa [IEEE 97]

O comprimento de onda de raios infra-vermelhos varia de 0,75 a 1000 microns, que é maior do que as cores espectrais mas muito menor do que ondas de rádio. O padrão define a utilização de radiação infra-vermelha com comprimento de onda entre 750 e 850 nanometros. O ar oferece a menor atenuação para esta faixa de comprimento de onda.

Neste tipo de rede, um transmissor e um ou mais receptores comunicam-se através de um plano de reflexão, que normalmente é o teto. O transmissor envia seus quadros,

iluminando o teto. Não deve haver qualquer tipo de obstáculo, que seja opaco a raios infra-vermelhos, em relação a qualquer nodo movel, e, todos devem monitorar o plano de reflexão. Entretanto, não é necessário que nodos móveis estejam alinhados entre si para se comunicarem, pois todos comunicam-se através do plano de reflexão. A maior distância entre nodos móveis e o plano de reflexão é de, no máximo, 10 metros.

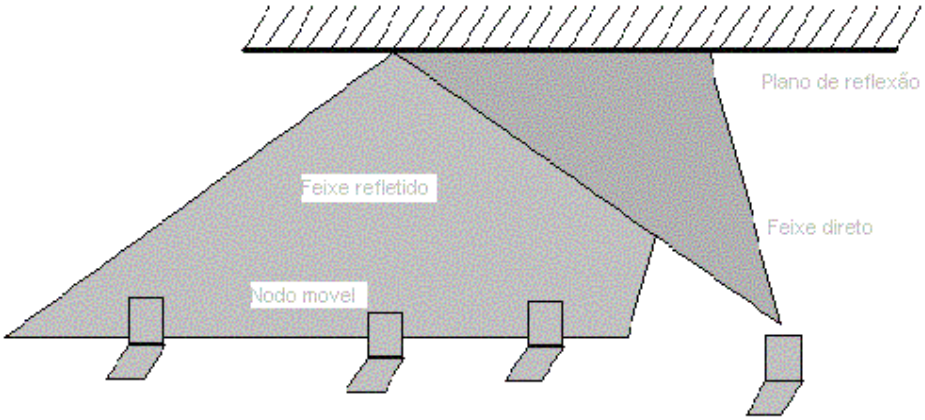

FIGURA 2.5 - Transmissão infra-vermelha difusa

A maior vantagem do infra-vermelho, é a sua habilidade de carregar uma grande largura de banda, podendo atingir velocidades de até 16 Mbps, operando na faixa de 100 THz. Entretanto, o infra-vermelho pode ser facilmente obstruído: a luz não pode atravessar objetos sólidos e opacos como paredes e pode receber interferências de iluminação do ambiente, além de exigir visada direta entre os dois pontos a serem conectados.

TABELA 2.3 – Radiodifusão x infra-vermelho

	Radiodifusão	Infrared
Freqüência	902MHz a 928 MHz; 2.4 GHz a 2.4385 GHz; 5.725 a 5.825 GHz	3 x 10^14 Hz
Cobertura de máximo	105 a 800 pés, ou até 50.000 pés	30 a 80 pés
Linha de visão requerida	Não	Sim
Transmissão de energia	Menos de 1 W	N/A
Requer licença	Não	Não
Uso interno em prédios	Possível com antena	Possível
Velocidade (% de 10 Mbps)	20% a 50%	50% a 100%

3 Tipos de Rede

Precisamos estar cientes que as aplicações de Redes sem Fio, hoje existentes, formam apenas uma pequena parte do cenário que existirá no futuro. Como a "onda" de Redes sem Fio está crescendo rapidamente, muitas outras aplicações serão criadas.

As quatro características de redes de comunicação, possíveis, estão descritas abaixo:

a) Fixa e cabeada: essa configuração descreve um típico computador pessoal dentro de um escritório, acessando a rede.

b) Movel e cabeada: muitos laptops de hoje em dia pertencem a essa configuração, ou seja, os usuários acessam a rede local cabeada quando em seus escritórios e, ao viajarem de um hotel para outro, reconectam-no à rede de sua companhia através do fio de telefone e de um modem.

c) Fixa e sem fio: essa configuração é usada, por exemplo, em construções históricas, para evitar a destruição causada por uma rede cabeada.

d) Movel e sem fio: essa configuração é a mais interessante. Nenhum cabo restringe o usuário, que pode passear por diferentes redes sem fio.

3.1 Rede local sem fio Ad-Hoc

Vários computadores, cada um configurado com placas de interface de rede sem fio. Cada computador pode comunicar-se diretamente com todos os outros. Eles podem compartilhar arquivos, impressoras, mas não acessam os recursos de uma rede fixa [VIC 2002].

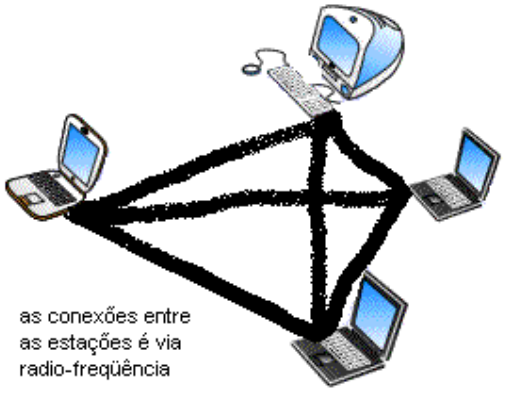

FIGURA 3.1 – Rede Local sem Fio Ad-Hoc

3.2 Rede local sem fio cliente/servidor com ponto de acesso

Uma rede local sem fio pode possuir um ponto de acesso, que funciona como os hubs das outras redes. Esses pontos de acesso podem conectar (como uma bridge) uma rede local sem fio a uma rede local fixa, permitindo aos computadores acessarem os recursos dessa rede [VIC 2002].

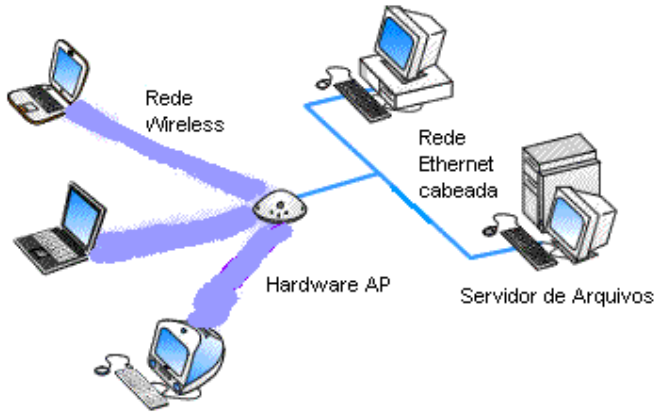

FIGURA 3.2 – Rede Local sem Fio Cliente/Servidor: Ponto de Acesso - HW

Os pontos de acesso podem ser hardwares dedicados (HAP – *Hardware Access Point),* como exemplificado na (figura 3.2), ou softwares rodando em computadores equipados com uma placa de interface de rede sem fio (figura 3.3).

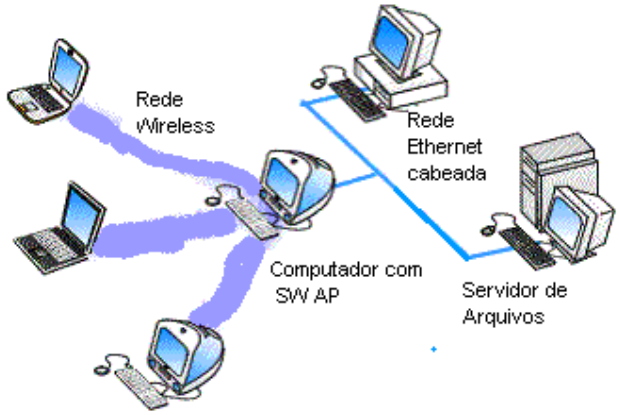

FIGURA 3.3 – Rede Local sem Fio Cliente/Servidor: Ponto de Acesso - SW

3.3 Rede local sem fio com múltiplos pontos de acesso e pontos de extensão

Se uma área é muito grande para ser coberta por um único ponto de acesso, então múltiplos pontos de acesso ou pontos de extensão podem ser utilizados [VIC 2002].

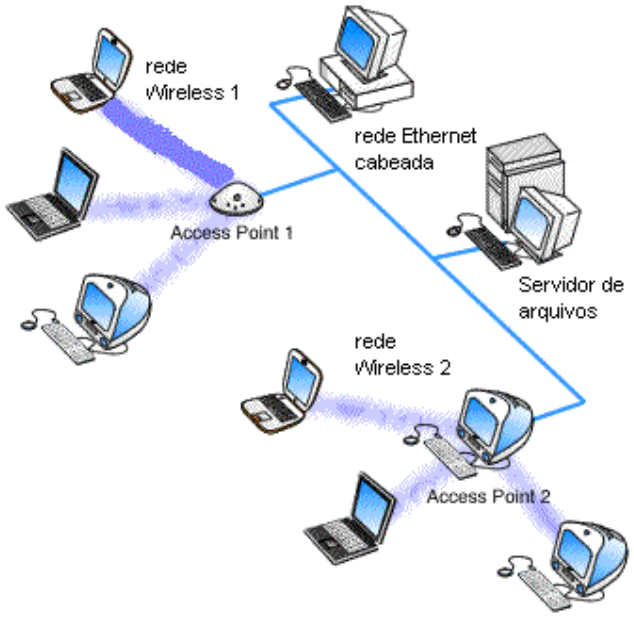

FIGURA 3.4 - Rede Local sem Fio com Múltiplos Pontos de Acesso

Pontos de extensão não foram definidos nos padrões de transmissão sem fio, porém foram desenvolvidos por alguns fabricantes. A principal diferença entre pontos de acesso (figura 3.4) e pontos de extensão (figura 3.5) está no fato de os pontos de extensão não necessitarem de uma rede fixa.

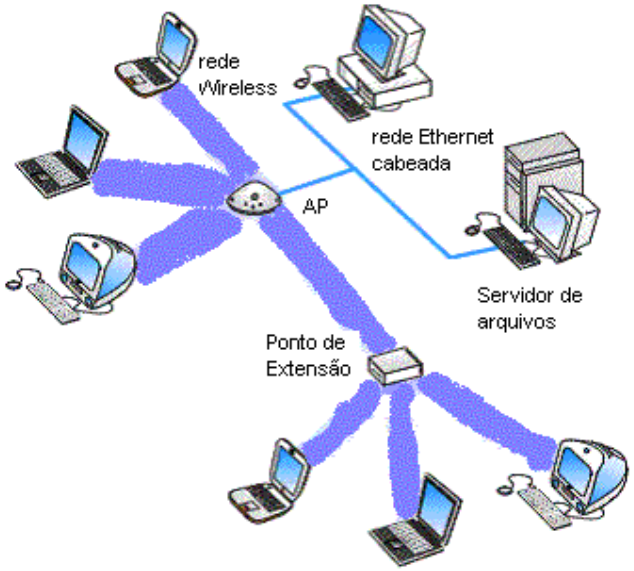

FIGURA 3.5 - Rede Local sem Fio com Múltiplos Pontos de Extensão

3.4 Redes locais sem fio conectando redes locais fixas

Na figura 3.6, dois pontos de acesso foram utilizados para conectar a Rede Ethernet Fixa 1 com a Rede Ethernet Fixa 2. Nesse caso, os pontos de acesso devem estar dentro do alcance de comunicação [VIC 2002].

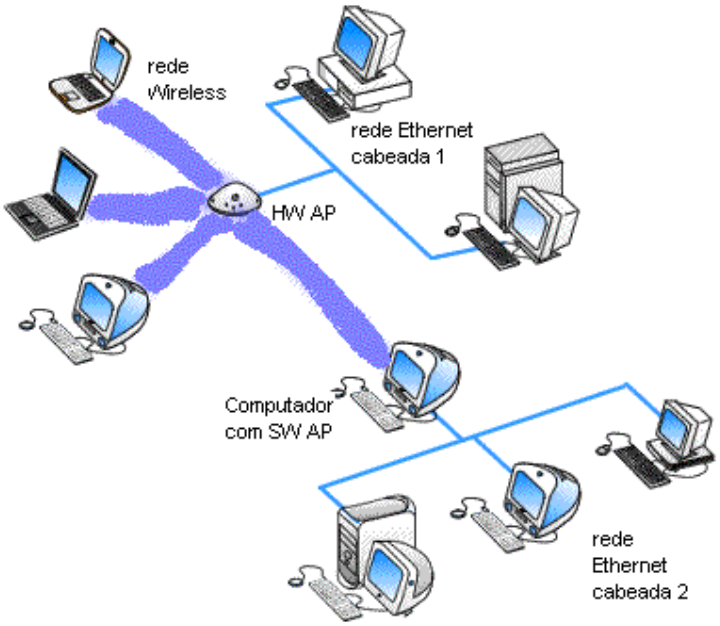

FIGURA 3.6 - Redes Locais sem Fio Conectando Redes Locais Fixas

Na (figura 3.7) duas antenas direcionais foram utilizadas, permitindo que as duas redes fixas estejam a uma distância maior.

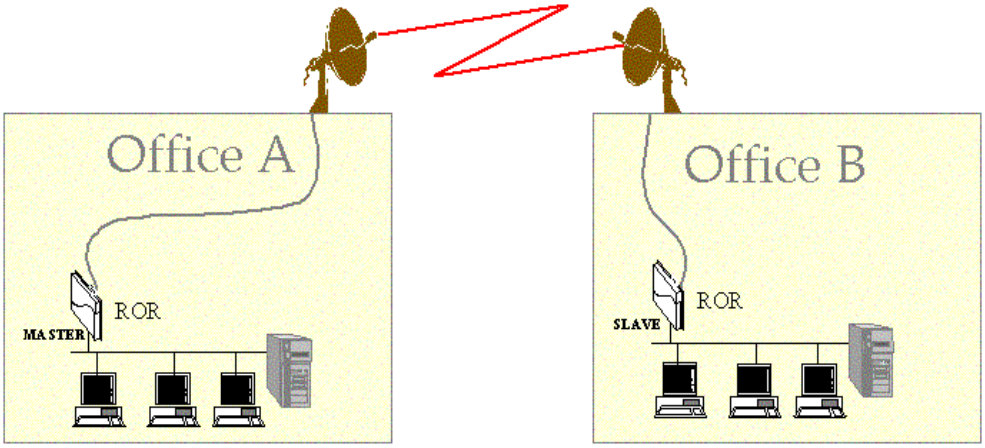

FIGURA 3.7 – Antenas direcionais conectando duas redes fixas

3.5 Rede local sem fio com acesso a internet

Redes locais sem fio podem conectar-se à Internet, sendo que o protocolo 802.11 só padroniza as camadas 1 e 2 da Arquitetura ISO/OSI, e os protocolos de roteamento (como IP) e de transporte (como TCP) são definidos nas camadas 3 e 4 do ISO/OSI, respectivamente [VIC 2002].

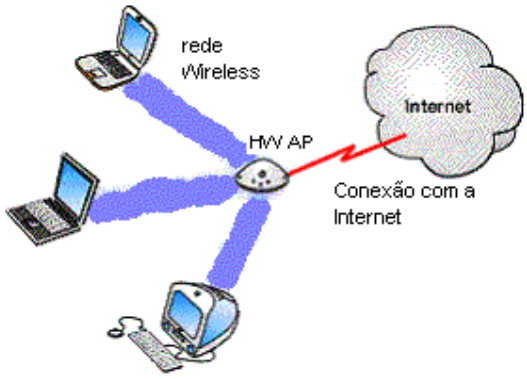

FIGURA 3.8 – Rede Local sem Fio com Acesso à Internet, via HAP

O acesso de redes locais sem fio à Internet pode ser feito tanto por um HAP (figura 3.8) quanto por um computador (figura 3.9).

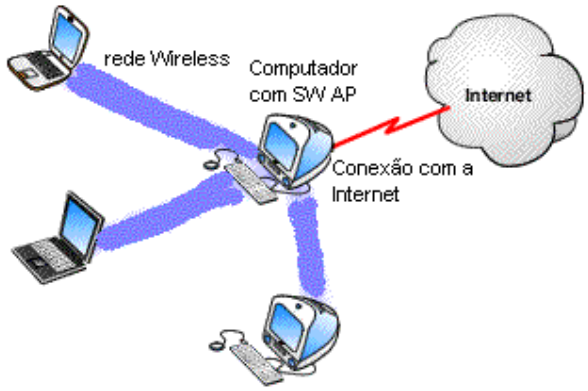

FIGURA 3.9 – Rede Local sem Fio com Acesso à Internet, via computador

3.6 Infra-estrutura fixa x Ad-Hoc

Resumo:

O padrão IEEE 802.11 prevê duas formas de conexão entre redes móveis. As redes de infra-estrutura fixa e as redes independentes ou Ad-Hoc [IEE 97].

a) Redes de infra-estrutura fixa: Neste tipo de rede o ponto de acesso é utilizado para comunicação entre as unidades móveis, de forma que uma unidade movel sempre se comunica com outra somente através de um ponto de acesso. Assim, a rede fixa dá suporte à mobilidade e auxilia em tarefas como roteamento, processamento distribuído, redução de tráfego, adaptabilidade, etc.

b) Redes Independentes ou Ad-Hoc - Nestas redes, não é prevista a existência de qualquer infra-estrutura fixa, e, quando existe, é conhecida pela rede como qualquer outra unidade movel. As unidades móveis comunicam-se diretamente através do meio dispensando infra-estruturas fixas, que podem encarecer o projeto. Se uma unidade deseja se comunicar com outra que não está dentro de seu alcance, ela o faz através de outras unidades móveis, que retransmitem os pacotes até que estes alcancem o seu destino. A maior dificuldade neste caso é o roteamento dos pacotes até o destino.

4 Tecnologias

As transmissões, as quais utilizam-se de radiofreqüência, são amplamente utilizadas nos dias atuais, estando presente em diversos equipamentos eletrônicos, tais como rádios, televisores, portões de garagem, telefones, etc.

Através de várias formas podemos criar uma fonte de energia eletromagnética que irá propagar-se no espaço em todas as direções através de ondas. É como se jogássemos uma pedra num lago (figura 4.1).

As ondas eletromagnéticas podem se propagar através de vários meios tais como o ar, água, alguns tipos de sólidos e até o vácuo.

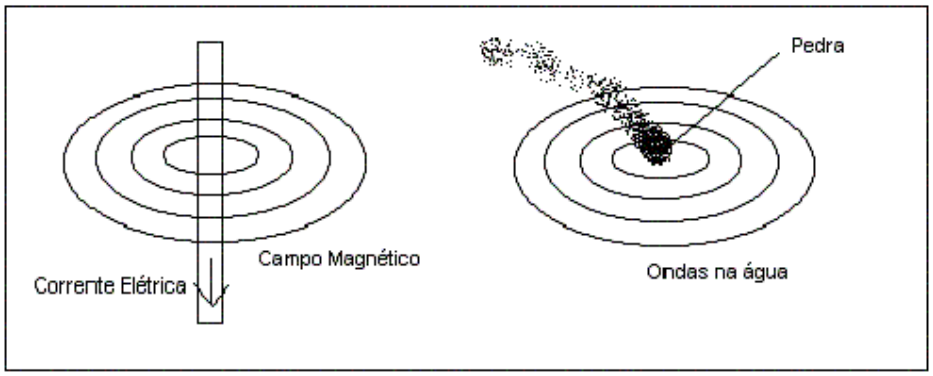

FIGURA 4.1 – Fontes de energia eletromagnética

4.1 Narrow band

Os sistemas Narrow Band, como o próprio nome diz, utilizam uma banda estreita de freqüências para a transmissão dos dados. Esta tecnologia é a mais antiga e mais conhecida.

a) Vantagens: tecnologia simples de implementar, tendo como conseqüência equipamentos de menor custo.

b) Desvantagens: tecnologia susceptível a interferência. Como a faixa é estreita e não há redundâncias em outras freqüências, qualquer interferência dentro da faixa ocasiona grande prejuízo à qualidade do sinal (figura 4.2). A taxa de comunicação é baixa (9600 bps), resultando em tempos de resposta altos e limitando o número de equipamentos.

4.2 Spread spectrum

Também conhecida como CDMA (Code-Division Multiple Access). De fato, esta tecnologia foi originalmente desenvolvida durante a Segunda Guerra Mundial para comunicar mesmo com a presença de sinais interceptores inimigos, com muitos sinais interceptores. Hoje, é utilizada para comunicação de dados no longínquo espaço, onde os níveis de sinal são extremamente fracos e a atmosfera é cheia de sinais de interferência de muitas origens. É também, a tecnologia de transmissão mais utilizada em sistemas de redes locais sem fio, devido ao fato de ser menos sensível a interferências do meio do que as outras tecnologias.

Sendo um sistema cujas ondas de rádio atuam nas freqüências de 902MHz a 928MHz e 2.4GHz a 2.5GHz ISM (Industrial, Scientific, and Medical) – faixas de freqüências de domínio público, este sistema permite transmitir redundâncias dos dados através de freqüências diferentes, evitando assim que uma fonte de interferência numa

freqüência específica comprometa toda a transmissão dos dados. É capaz de superar problemas de interferências como por exemplo o ruído, que degenera qualquer sinal que esteja perto de sua freqüência utilizando múltiplas freqüências da banda. Por exemplo, quando duas estações estão transmitindo ao mesmo tempo, cada uma pega uma freqüência e transmite por certo tempo, mas nunca na mesma freqüência ao mesmo tempo. Também foi designado para definir eficiência de largura de banda com confiabilidade, integridade e segurança. Em outras palavras, mais largura de banda é consumida em relação à transmissão de banda estreita, mas produz um sinal que é, com efeito, mais forte e portanto fácil de detectar, desde que o receptor conheça os parâmetros do sinal *spread spectrum* que está sendo difundido.

A transmissão com tecnologia Spread Spectrum atravessa obstáculos com mais facilidade do que sistemas de microondas, por utilizar freqüências menores, portanto mais fáceis de ultrapassar barreiras como paredes. A (tabela 4.1) especifica um exemplo de equipamento utilizado num rádio com a tecnologia Spread Spectrum:

TABELA 4.1 Equipamento com tecnologia Spread Spectrum

Distâncias entre canais adjacentes	-40 db = 4 MHz
Velocidade assíncrona em bauds	1.2 a 38.4 Kbps simula full duplex - RS-232
Controle	CTS, RTS
Formato dos dados	7 e 8 bits, (par e ímpar) paridade, 1 e 2 parada
Dimensões	(38.6mm x 105.9mm x 127mm)
Faixa dinâmica	-100dBm ~ -30dBm
Faixa de freqüência	902 até 928 MHz
Indicadores	PWR, TxD, RxD
Modulação	Bi-Phase Shift Keying (BPSK)
Modo de operação	Ponto-a-ponto
Temperatura de operação	-20 a +60 graus C (opção para –34 +74C)
Consumo de energia	10 watts máximo
Tensão de alimentação	10.5 a 13.8 VDC
Técnica de rádio	Espectro espalhado (seqüência direta)
Distância mínima aberta	800 pés
Interna	500 a 1500 pés
Externa	12 + milhas com visada
Umidade relativa	0-90 % sem condensasão
Sistema de ganho	120 db
Atraso da transmissão	19 msec (mínimo)
Interface de voz	RJ-11 com microtelefone (325 a 4000 Hz)
Peso	1 Kg

a) Vantagens: grande imunidade à interferências e espionagem.

b) Desvantagens: utilização de equipamentos mais sofisticados. Apesar disto, diversos fabricantes já possuem equipamentos com os respectivos desenvolvimentos amortizados e portanto de baixo custo.

Existem duas técnicas fundamentais para espalhar os sinais uniformemente sobre uma larga faixa de freqüência do espectro - Frequency Hopping Spread Spectrum (FHSS) e Direct Sequence Spread Spectrum (DSSS).

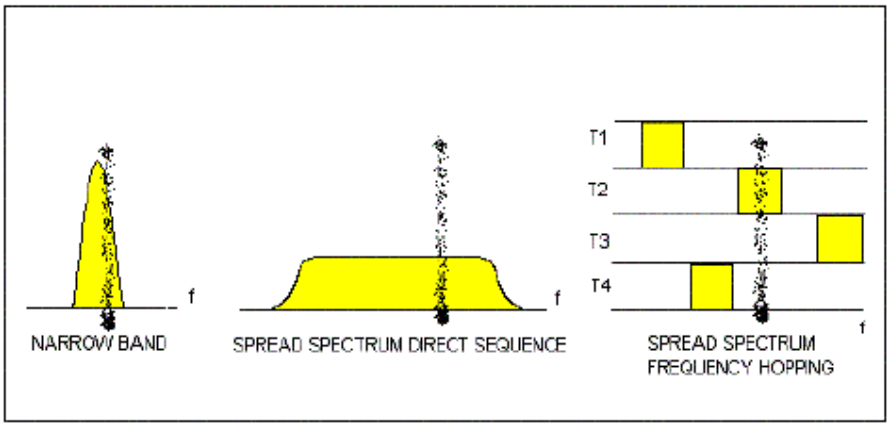

FIGURA 4.2 – Tecnologias

4.2.1 Frequency hopping spread spectrum

Salto de freqüências, pode ser vista como o espalhamento dos dados na banda larga através de vários canais de banda estreita. Os canais são utilizados para transmitir pequenos pedaços de cada mensagem. A transmissão dos dados é feita pelo salto de tempos em tempos (frações de segundo) da portadora em cada canal obedecendo uma seqüência pseudo-aleatória, com o transmissor e o receptor sincronizados. Este método evita a dependência de qualquer um dos canais para o sucesso da comunicação, e de acordo com a FCC (Federal Communications Commission, EUA), os transmissores de Frequency Hopping não devem gastar mais que 0,4 segundos de um canal a cada 20 segundos na banda de 902 MHz e a cada 30 segundos com a banda de 2,4 GHz. Da mesma forma, os transmissores devem poder "saltar" por pelo menos 50 canais na banda de 902 MHz e 75 canais na banda de 2,4 GHz (um canal é uma faixa de freqüências pré-determinada).

Em contraste com o sistema de Direct Sequence, onde a seqüência de Spread é utilizada seqüencialmente (um bit de cada vez), aqui ela é utilizada em paralelo (k bits de cada vez), fornecendo ao sintetizador a cada instante, um número pseudo-aleatório de 0 a 2k – 1, correspondente à freqüência que será gerada. Diz-se que o sistema realiza um salto em freqüência rápida (FFH), quando ele executa vários saltos durante um bit de informação e um salto em freqüência lenta (SFH) quando são transmitidos vários bits de informação em cada salto.

A tecnologia atual permite bandas de salto em freqüência de ordem de vários GHz, que é um valor maior do que aqueles possíveis de serem obtidos para bandas de Spread por Direct Sequence. Com relação à taxa de salto, já encontram-se hoje sistemas capazes de realizar centenas de Ksalto/seg, e outros, em desenvolvimento, já realizam testes de salto maiores do que 1 Msalto/seg.

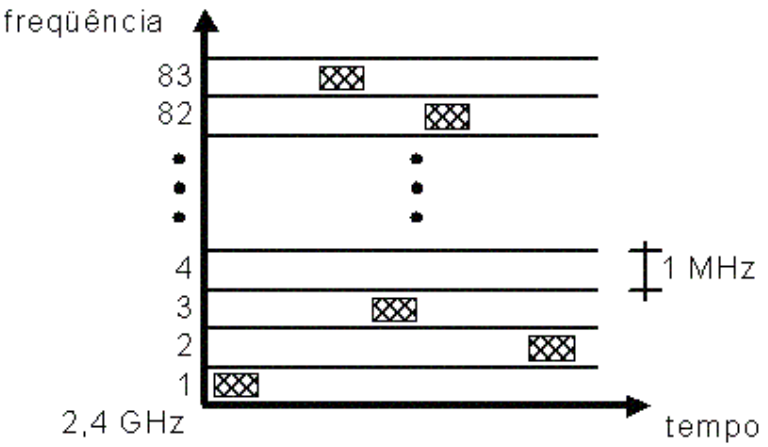

FIGURA 4.3 - Frequency Hopping Spread Spectrum

4.2.2 Formato do quadro FHSS
(sub-nível físico PMD)

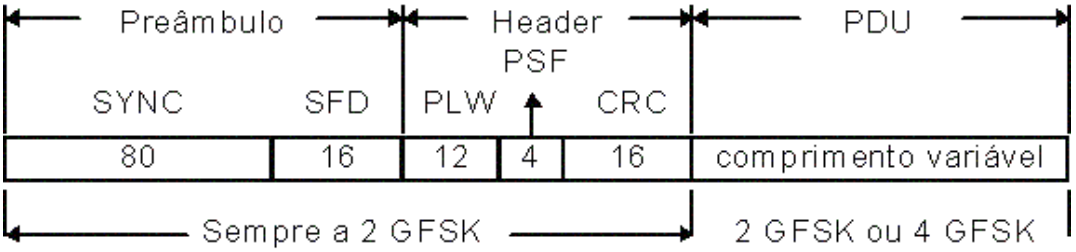

FIGURA 4.4 – Formato de um quadro FHSS

a) SYNC: seqüência de sincronismo, consiste de 80 bits do padrão 0101 e tem como objetivo adquirir o sincronismo, detectar a presença de sinal e resolver a diversidade da antena.

b) SFD (*Start Frame Delimiter*): define 16 bits, a saber: 0000 1100 1011 1101, que provê sincronização de símbolo. Este padrão, além de balanceado, foi projetado para otimizar as propriedades de auto-correlação em conjunto com o padrão 0101 antes dele.

c) PLW (*PLCP_PDU Length Word*) é um campo de 12 bits que indica o tamanho do PDU (*Physical Data Unit*) em octetos, incluindo os 32 bits de CRC ao final do quadro.

d) PSF (*PLCP Signaling Field*) é um campo de quatro bits, com três reservados e um para indicar a vazão da PDU (1 ou 2 Mbit/s).

e) CRC do cabeçalho gerado pelo polinômio CCITT $P(x)=x^{16}+x^{12}+x^5+1$.

f) PDU: campo de dados das camadas superiores.

4.2.3 Direct-sequence spread spectrum

Também conhecida como pseudo noise (pseudo ruído), esta técnica é a que a maioria das WLANs utiliza. Os transmissores utilizados nessa tecnologia, enviam o sinal com a adição de bits redundantes de dados chamados “chips”, ou seja, com um “falso ruído", garantindo a resistência a interferências. São adicionados pelo menos dez chips para cada bit de dado, segundo normas da FCC. O padrão IEEE 802.11 determinou o número de onze chips para a DSSS.

Uma vez que o receptor - precisa conhecer o código de difusão de um transmissor para poder decifrar os dados corretamente - tenha captado todos os sinais de dados, ele usa um correlator, baseado no código de difusão, para remover os chips e truncar o sinal ao tamanho original. O código de difusão é o que permite que diversos sistemas de Direct Sequence Spread Spectrum operem em uma mesma área sem um interferir no outro. Qualquer que seja o método de Spread Spectrum, o resultado final é um sistema extremamente confiável no que diz respeito à intrusão, que não interfere em outros serviços e ainda assim carrega uma razoável largura de banda de dados.

A velocidade máxima dos transmissores de Direct Sequence na banda de 902 MHz é 2Mbps e 80 Mbps na banda de 2.4 GHz. Infelizmente, o número de chips está diretamente relacionado com imunidade do sinal a interferências. Numa área com muita interferência de rádio, é preciso diminuir a velocidade (aumentar os chips) para evitar a corrupção de dados.

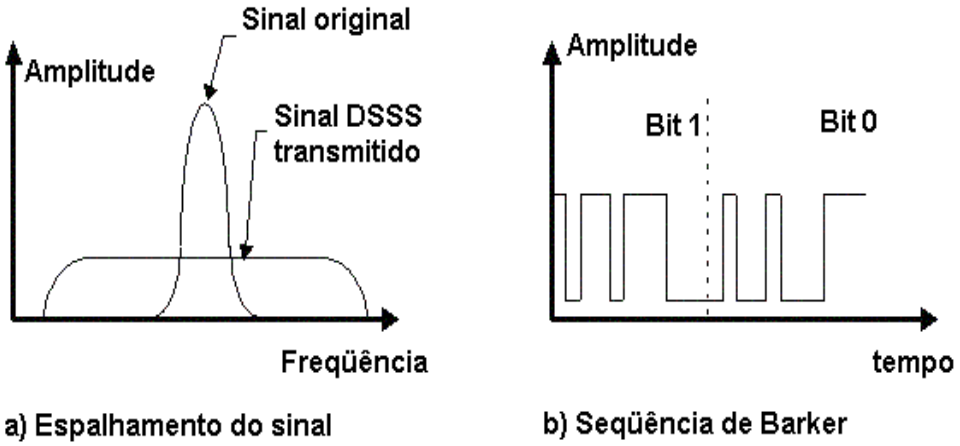

FIGURA 4.5 - Direct Sequence Spread Spectrum

4.2.4 Formato do quadro DSSS

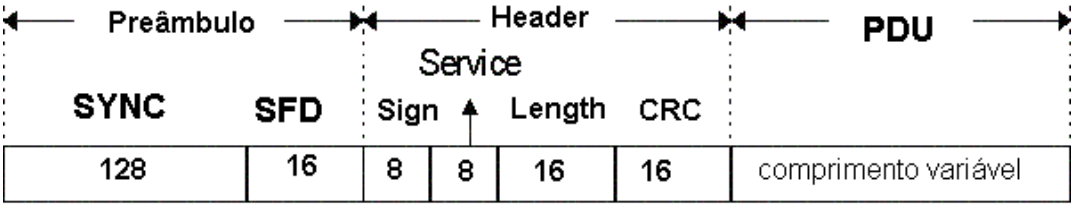

FIGURA 4.6 – Formato do quadro do DSSS

a) SYNC: 128 bits embaralhados em 1, utilizado para sincronismo do receptor (ressalta-se que cada bit é representado pela seqüência de *Barker*, e é esta seqüência que é embaralhada);

b) SFD (*Start Frame Delimiter*): provê a sincronização de quadro e de octeto para o receptor, consistindo de 16 bits com o seguinte conteúdo (do MSB para LSB): 1111 0011 1010 0000. Transmite-se a partir do bit menos significativo;

c) *Signal* (representada por *sign* na figura 4.6): indica qual a vazão de transmissão dos dados do quadro. A velocidade é calculada pelo valor deste campo multiplicada por 100 kbit/s. O padrão define dois valores obrigatórios para este campo, 10 (para 1 Mbit/s) e 20 (2 Mbit/s);

d) *Service*: reservada para uso futuro;

e) *Length*: inteiro de 16 bits sem sinal, indica o número de micros segundos para a transmissão do PDU;

f) CRC do *header* gerado pelo polinômio CCITT $x^{16}+x^{12}+x^{5}+1$.

g) PDU: campo de dados das camadas superiores.

TABELA 4.2 - Freqüências centrais dos canais em DSSS

Identificação do canal	Freqüências do FCC	Freqüências do ETSI	Freqüências do Japão
1	2412 MHz	N/D	N/D
2	2417 MHz	N/D	N/D
3	2422 MHz	2422 MHz	N/D
4	2427 MHz	2427 MHz	N/D
5	2432 MHz	2432 MHz	N/D
6	2437 MHz	2437 MHz	N/D
7	2442 MHz	2442 MHz	N/D
8	2447 MHz	2447 MHz	N/D
9	2452 MHz	2452 MHz	N/D
10	2457 MHz	2457 MHz	N/D
11	2462 MHz	2462 MHz	N/D
12	N/D	N/D	2484 MHz

Legenda:
N/D– não disponível
ETSI– *European Telecommunications Standards Institute*

4.2.5 FHSS x DSSS

Qualquer que seja o método de Spread Spectrum utilizado, o resultado final é um sistema extremamente confiável no que diz respeito à intrusão, que não interfere em outros serviços e ainda assim carrega uma razoável largura de banda de dados.

O FHSS não requer uma contínua alocação de banda, é mais fácil de ser implementado, opera com menos potência, é mais seguro e permite múltiplas transmissões simultâneas. Por outro lado, o DSSS é mais fácil de efetuar "handoff" entre células e possibilita maiores taxas de transmissão em certas circuntâncias.

A escolha sobre que método utilizar depende de qual é a performance deseja, logo ser for necessária uma maior velocidade (11Mbps) e interferências não for o problema, a Direct Sequence é a mais recomendada. Por outro lado, se não houver necessidade de velocidade maior que 2 Mbps, a Frequency Hopping oferece uma solução igualmente confiável. O DSSS e o FHSS, não são interoperáveis, apesar de um mesmo fabricante trabalhar com as duas tecnologias.

4.2.6 Superioridade do FHSS

Apresentamos aqui 4 motivos determinantes que mostram a superioridade do FHSS sobre o DSSS.

a) O FHSS é mais imune à interferências. Redes DSSS podem ser debilitadas por freqüências de mesma faixa por que não tem variação de freqüências, ou seja, a freqüência é pré-selecionada e não pode evitar interferências. Por outro lado, o FHSS varia suas freqüências pela fonte de ruído.

b) O FHSS tem maior valor de banda agregada. No DSSS o máximo de canais não-interferentes é de 3 para um total de 6Mbps. Tipicamente sistemas FHSS provêm mais de 15 canais de 1 Mbps não-interferentes para uma capacidade de 15 Mbps.

c) O FHSS têm maior escalabilidade. Se um sistema FHSS precisar lidar com uma célula adicional, basta adicionar um novo AP (Ponto de Acesso), dobrando a capacidade. Isto porque APs vizinhos são naturalmente não-interferentes, ou interferem muito pouco uns com os outros.

d) Sistemas FHSS requerem menos potência para operar.

4.2.7 Técnica de salto no tempo

Esta técnica também conhecida como transmissão por salvas (burts), consiste na transmissão de informação por blocos de dados (salvas) de mesma duração, que são inicializadas em tempos pseudo-aleatórios, segundo um gerador de código. Em outras palavras, a cada intervalo de tempo T é transmitida uma salva de duração T/n, em uma das n janelas de tempo existentes neste período. A cada janela de tempo corresponde uma seqüência ortogonal do código de Spread, que deverá ser do conhecimento do receptor para que este, através da correlação de seqüências de código com o sinal recebido no período T, identifique a posição exata de salva e assim possa recompor a informação original.

4.3 OFDM - Orthogonal frequency division multiplexing

Como um suplemento ao padrão de IEEE 802.11, o grupo de trabalho do IEEE 802.11 publicou IEEE 802.11a, que especifica o uso de OFDM na faixa 5.8 GHz.

OFDM, algumas vezes chamado multi-portadora ou modulação multi-sinal discreta, é uma técnica de espectro espalhado que distribui os dados sobre um grande número de portadoras que são espaçadas à parte em freqüências precisas. Este espaçamento fornece a ortogonalidade nesta técnica que impede os demoduladores de vêrem outras freqüências que não as suas próprias. É, também, considerada uma técnica eficaz na transmissão digital. Recentemente, sua implementação se tornou tecnicamente viável e o seu custo competitivo.

Ambos, transmissor e receptor podem ser implementados por DSP usando técnicas eficientes de IFFT/FFT. OFDM permite a transmissão de altas taxas de dados e a possibilidade de maximizar sua eficiência adaptando suas variáveis ao comportamento dos canais. Uma vantagem maior pode ser adicionada ao esquema da OFDM incluindo um componente DSSS no sistema.

Os benefícios da OFDM são: alta eficiência spectral, resiliência à interferência de RF, e uma distorção múltiplos-caminhos mais baixa. Isto é útil porque num típico cenário de transmissão terrestre há múltiplos canais, ou seja, o sinal transmitido chega no receptor usando vários caminhos de comprimento diferente. Após as múltiplas versões de sinal interferirem uma nas outras torna-se muito difícil extrair a informação original.

4.4 Rádio-microondas

A tecnologia microondas (figura 4.7) não é exatamente uma tecnologia de LAN. Seu principal uso é interconectar redes locais em diferentes prédios. Devem ser utilizados aparatos para microondas (microwave dish – aparato com o formato de uma antena parabólica) em ambos os lados da conexão. As “microwave dishes” devem ter visada direta (estar na mesma linha de visão) para transmitir e coletar os sinais de microondas.

Os sistemas Wireless que utilizam microondas conseguem ultrapassar pequenos obstáculos como, por exemplo, paredes. Eles operam na faixa de freqüência de 18 GHz e podem atingir velocidades de transmissão máximas de até 15 Mbps.

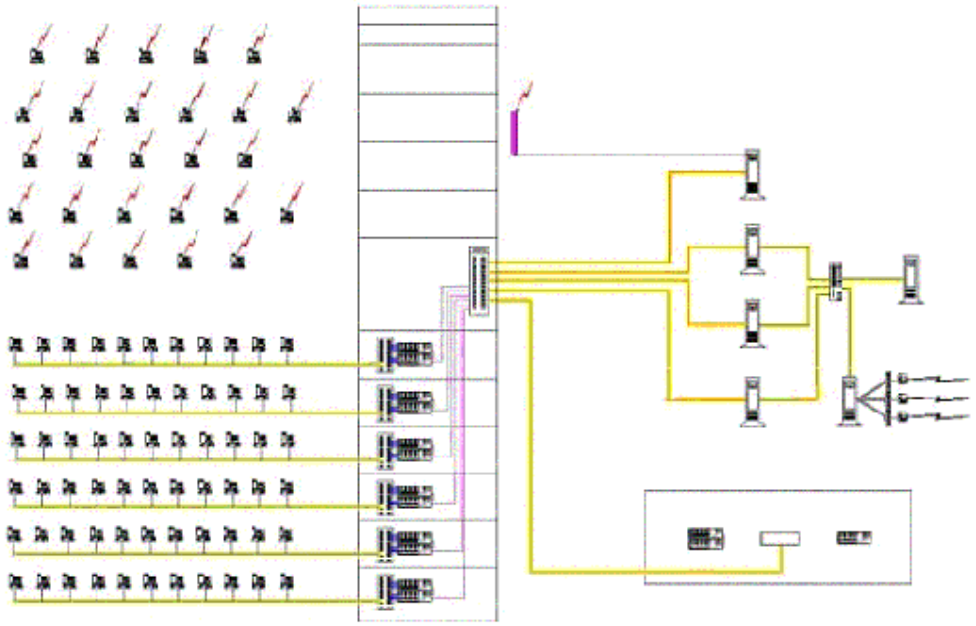

FIGURA 4.7 - Exemplo de utilização de cabeamento tradicional em conjunto com link de rádio omnidirecional a 2 Mbps

A rede local sem cabeamento funciona com uma antena do tipo omnidirecional instalada junto com o servidor, que propaga os sinais Ethernet para as estações que fazem parte daquele barramento de rádio num raio de 360 graus. Cada rede é identificada por um 'Net-ID' de forma a não haver possibilidade de acesso indevido por alguém que não faça parte do workgroup da rede. O alcance da antena omnidirecional conectada no servidor é de até 300 metros em boas condições de transmissão, podendo inclusive atingir vários andares de um mesmo prédio. A freqüência utilizada na transmissão é de 915 MHz.

Em cada micro que faz parte da rede Wireless, é instalada uma placa de rádio e uma antena receptora de pequeno porte que substitui a placa de rede padrão utilizada para conectar o micro na rede. Como cada placa de rádio é configurada com o 'Net-ID' da rede a que pertence, pode haver mais de um barramento de rádio dentro da mesma empresa.

Nestas freqüências as ondas de rádio se comportam praticamente como ondas de luz, desta forma sua propagação segue uma linha reta, de forma que não devem existir obstáculos sólidos em meio a esta linha, também a propagação do sinal é afetada pelas atenuações do espaço livre e as precipitações.

Uma característica importante destes sistemas é que podemos prever o nível do sinal que é recebido pelo receptor distante com uma precisão conhecida.

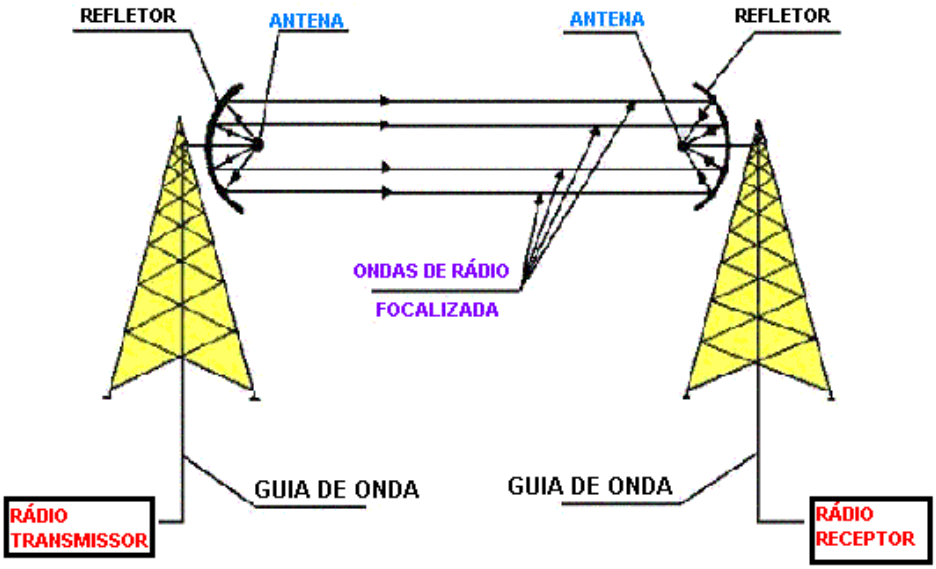

FIGURA 4.8. Elementos de um sistema rádio-microondas

a) Torre: A torre tem a função de suporte da antena de microondas, tem que ser bem sólida para poder suportar as dificuldades meteorológicas, ventos fortes, chuvas torrenciais, sismos etc, porque são estas as que freqüentemente interrompem a transmissão. A altura da torre de microondas vai depender da visibilidade das duas antenas, porém, sempre considerando que as distâncias máximas entre as duas antenas é de 50 até 80 Km. Um método bem prático é fazer uso de um espelho e refletir os raios de luz na outra ponta, para se obter uma boa aproximação.

b) Antena: As antenas de microondas tem por sua vez dois elementos: o refletor que devido a sua forma chama-se refletor parabólico, e a própria antena que é um dipolo eletromagnético. As microondas focalizadas pela parábola transmissora incidem diretamente sobre a parábola receptora que por sua vez focaliza as ondas no seu ponto central, onde está a antena receptora. Dessa antena as ondas são levadas por uma guia de onda até o rádio receptor. Cada antena de microondas com sua respectiva parábola, geralmente serve para transmitir e/ou receber mais de um canal. As dimensões típicas de uma antena microondas variam desde 50 cm até 1.5 m de diâmetro.

c) Guia de Onda: O guia de onda é na realidade uma linha de transmissão, mas não é um cabo coaxial como a maioria dos sistemas de comunicação, neste caso é um tubo quadrangular ou triangular feito de alumínio, ele está entre a antena e o equipamento de rádio. O desenho é feito desta forma, para obter-se uma boa reflexão na superfície e evitar os ruídos eletromagnéticos e interferências devido a distância típica entre uma antena e o equipamento de rádio, que é de 25 a 40 metros, sendo que é por este motivo que existem perdas de sinal. Em equipamentos leves com torres pequenas e lugares com baixo ruído o guia de onda pode ser um cabo coaxial de alta qualidade.

d) Rádio Transmissor/Receptor: É o equipamento que recebe ou transmite os sinais e também faz a modulação, ele deve estar programado para operar na freqüência própria. O rádio trabalha com baterias e se está num lugar distante, por exemplo, um morro, será sempre necessário possuir materiais para a manutenção dos equipamentos.

4.5 Laser

Os sistemas a laser são mais utilizados para conexões ponto-a-ponto de longa distância, como por exemplo, a interligação de duas LANs em prédios separados. A distância entre os pontos de conexão é um dos principais pontos que diferenciam a utilização de sistemas Wireless laser e sistemas Wireless infra-vermelho. O primeiro, como já fora observado, é adequado à longas distâncias, enquanto o segundo é mais utilizado em ambientes internos (escritórios, oficinas, etc...), onde as distâncias entre os pontos de conexão são bem menores em relação às encontradas em ambientes externos.

Os sistemas baseados em tecnologia laser necessitam de visada direta entre os pontos para poder operar, isto é, o receptor deve estar na mesma linha do transmissor para haver comunicação entre os pontos de conexão. Estão sujeitos a interferência climáticas, como chuvas e nevoeiros que podem interromper a transmissão.

5 Arquitetura

A arquitetura adotada pelo projeto IEEE 802.11, baseia-se na divisão da área coberta pela rede em células. As células são chamadas BSA (Basic Service Area). Um grupo de estações que se comunica em uma BSA, constitui um BSS (Basic Service Set). O tamanho da BSA depende das características do ambiente e dos transmissores/receptores usados nas estações [LIN 2001]. Para permitir a construção de redes cobrindo áreas maiores que uma célula múltiplas BSAs são interligadas através de um sistema de distribuição, que pode ser uma rede baseada em outro meio de transmissão, por exemplo, fios metálicos ou fibra óptica via APs.

Os APs são responsáveis pela captura das transmissões realizadas pelas estações de sua BSA destinadas a estações localizadas em outras BSAs, retransmitindo-as, usando o sistema de distribuição. Os BSAs interligados por um sistema de distribuição através de APs definem uma ESA (Extended Service Area). O conjunto de estações formado pela união dos vários BSSs conectados por um sistema de distribuição define um ESS (Extended Service Set). Cada ESS é identificado por um ESS-ID. Dentro de um ESS, cada BSS é identificado por um BSS-ID. Estes dois identificadores formam o Network-ID de uma rede sem fio IEEE 802.11.

Um ESS formado pela interconexão de múltiplos BSSs constitui uma rede local sem fio com infra-estrutura (figura 5.1). A infra-estrutura consiste nos APs e no sistema de distribuição que interliga os APs. O sistema de distribuição, além de interligar os vários APs, pode fornecer os recursos necessários para interligar a Rede sem Fio a outras redes.

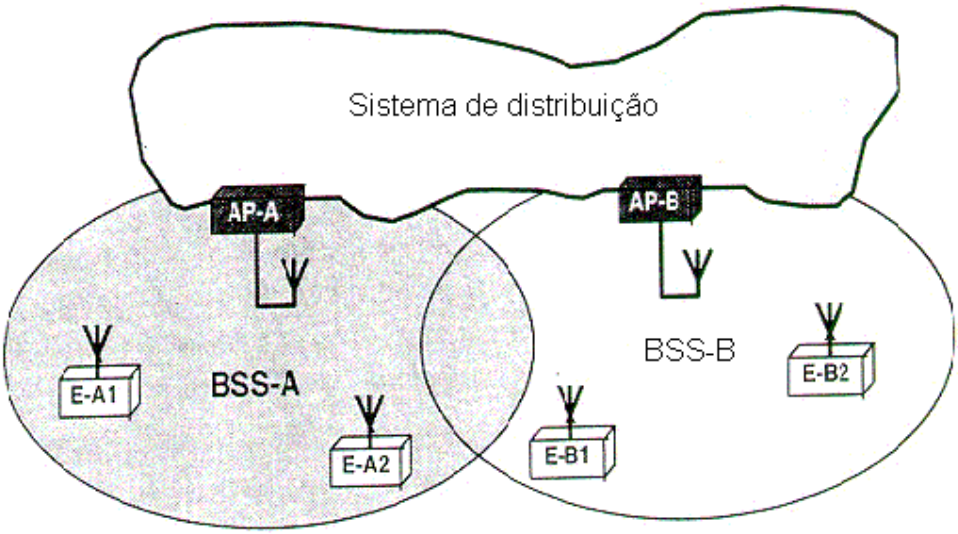

FIGURA 5.1 – Rede local sem fio com infra-estrutura

A arquitetura do sistema de distribuição não é especificada no IEEE 802.11. Entretanto os serviços do sistema de distribuição são padronizados.

5.1 Células e pontos de acesso

A área coberta por uma WLAN simples é denominada célula. O Ponto de Acesso (AP) conecta a célula à outras células e às LANs. Ele deve sincronizar todas as estações com

a célula para que elas possam fazer a sequência de saltos dos canais no tempo e freqüência corretos, coordenando o tráfego intra e inter-rede.

5.2 Nós escondidos

Uma estação escondida é aquela que não percebe todas as transmissões dentro de sua célula. Normalmente, uma barreira ou obstáculo gera perda de sinal entre duas estações dentro de uma célula.

Imaginemos os seguintes cenários:

Cenário 1: A estação C está no limite da área de cobertura de uma célula. A estação A transmite para a estação B mas a estação C não detecta a transmissão. Assim sendo, a estação C também inicia uma transmissão e uma colisão ocorre.

Cenário 2: Ambas as estações - A e C - podem contactar o Access Point. Entretanto, elas não conseguem detectar a transmissão uma da outra, e, uma colisão ocorre. Normalmente, uma barreira ou obstáculo gera perda de sinal entre duas estações dentro de uma célula.

A solução para o problema é usar RTS/CTS, como exemplificado no cenário 3.

Cenário 3: A estação A envia um RTS para o Access Point: Eu quero transmitir por 10 micro segundos. O Access Point recebe o RTS e transmite um (CTS). Todas as demais estações, agora sabem que o meio não está livre por um período de tempo inserido no pacote CTS. O AP envia um broadcast para todas as estações: A estação A irá transmitir por 10 micro segundos. A estação A transmite para a estação B e após todas as outras estações serem informadas da transmissão, via CTS, nenhuma colisão deverá ocorrer. A estação B envia um ACK para a estação A: transmissão bem sucedida, indicando para todas as demais estações que o meio está desobstruido.

Questões RTS/CTS

a) Modo de operação padrão setado para o estado off, sendo capaz de ser ligado quando problemas com nós escondidos ocorrerem. Sendo que pacotes RTS/CTS consomem a banda, a largura de banda disponível para transmitir pacotes de dados “normais” será diminuída.

b) Após o AP transmitir a maioria do tráfego de dados durante a operação normal, nós escondidos não são mais um problema. Por esta razão, o modo de operação RTS/CTS deve ser usado somente quando existir um problema com nós escondidos e quando for absolutamente requerido.

5.3 Ligação entre células

As células podem ser conectadas de quatro formas fundamentais: como células stand alone, como células ligadas em uma configuração multi-célula, como parte de uma LAN ou conectadas a uma LAN remota através de uma “ Wireless Bridge” [WLA 2001].

5.3.1 Células stand alone

Uma célula stand alone consiste do AP e de todas as estações wireless associadas. O número máximo de estações depende da natureza do tráfego de dados. Nos nossos testes, observamos que se houverem muitos dados trafegando na célula, faz-se necessário limitar o número máximo de estações entre 15 e 20. Para as aplicações que geram menor tráfego (somente texto), um número máximo de até 50 estações poderá ser configurado.

O diâmetro da célula depende de muitos fatores, mas de uma forma geral pode chegar a 200 metros num ambiente indoor e 1 quilômetro em ambientes outdoor.

5.3.2 Multi-células

Dá-se o nome de multi-células para os casos em que várias células estão sobrepostas numa mesma área física. Através do uso de algoritmos formais, há a possibilidade de ser definido qual dos APs está melhor posicionado para comandar a comunicação na WLAN desde um ponto de transmissão até um ponto de recepção.

A cobertura em multi-células é bastante útil na presença de tráfego intenso, pois além de propiciar redundância no sistema, assegura uma operação sem falhas.

5.3.3 Bridges remotas

As células podem ser ligadas às WLANs através de bridges remotas. Apesar de não fazerem parte do padrão 802.11 estas bridges conseguem um alcance de quilômetros, com uma alta taxa de transferência de dados, possibilitando que WLANs se transformem em WMANs.

5.4 Conexões de células

Quando o número máximo de estações ou o diâmetro da célula forem excedidos, faz-se necessário disponibilizar mais células. Estas células precisam estar interligadas, possibilitando a comunicação mútua. Quando um usuário passar da área de cobertura de uma célula para a área de cobertura de outra célula, os APs necessitarão realizar um handoff do sinal de uma célula para a outra, sem que o usuário perceba que passou pela área limite de duas células.

5.5 Modelo de arquitetura básica

O padrão 802.11 define uma rede celular. A célula básica é chamada Basic Service Set (BSS). Várias estações (STAs), pertencentes a uma mesma BSS, comunicam-se através de um AP. Um AP é denominado Portal, quando conecta-se com outra rede do tipo 802. Apesar do padrão 802.11 não exigir, normalmente, o AP e o portal fazem parte de um mesmo dispositivo físico. A conexão do tipo 802 é chamada de DS (Distribution Service). O conjunto de BSSs e DSs formam um ESS (Extended Service System).

5.6 Fragmentação e rearranjo das mensagens

No caso das WLANs, existem motivos, especificados abaixo, para que os pacotes sejam menores do que os das LANS:

a) apresentam uma maior taxa de erro dos bits, característica esta herdada da rádio-transmissão;

b) menor custo nas retransmissões (pacotes pequenos);

c) no FHSS, a freqüência muda a cada 100 ms, o que limita o tamanho do burst.

5.7 Frames

Na seqüência, são descritas as informações contidas no frame:

a) último fragmento;
b) número do fragmento;
c) elementos presentes – o frame não está vazio;
d) retransmissão;

e) duração em microsegundos;
f) campos de endereço (6 bytes);
g) endereço de origem;
h) endereço de destino;
i) endereço do AP;
j) endereço da estação transmissora;
k) endereço da estação receptora;
l) controle seqüencial;
m) controle de diálogo;
n) tamanho do frame (de 0 a 2304 bytes);
o) controle de erro CRC.

Existem 4 intervalos inter-frames que separam as ações dentro da mensagem:

5.7.1 SIFP (Short inter frame spacing)

É o tempo máximo – 28 microsegundos - que o transmissor necessita aguardar por uma resposta (por exemplo, um CTS requerido por um RTS).

5.7.2 PIFS (PCF inter frame spacing)

É o tempo usado pelo AP para obter acesso ao meio, antes de qualquer outra estação. Seu valor é um SIFP + 1 slot time ou aproximadamente 78 microsegundos.

5.7.3 DIFS (Distributed inter frame spacing)

É o tempo que uma estação aguarda para iniciar uma transmissão. Seu valor é um PIFS + 1 slot time ou 128 microsegundos.

5.7.4 EIFS (Extended inter frame spacing)

É o tempo que a estação necessita aguardar para transmitir nas situações em que não entender uma mensagem. Caso contrário, os pacotes a serem enviados colidirão com os que estão chegando.

5.8 Backoff exponencial

O método de backoff usado no padrão 802.11 é similar ao Ethernet. Usando o conceito de slot time (tempo em que a estação escuta o meio para saber se o mesmo está ocupado, ou aproximadamente 64 microsegundos), cada estação usa um número aleatório de timeslots (entre um mínimo e um máximo) e espera. Se o meio estiver ocupado, o seu número de timeslots será incrementado do número máximo de timeslots e continuará tentando até obter sucesso. No padrão 802.11, o backoff é executado nas seguintes situações:

a) a estação está pronta para a transmissão, entretanto, verifica que o meio está ocupado;
b) após cada retransmissão;
c) após cada transmissão bem-sucedida.

5.9 Conexão de uma estação

A estação precisa ingressar numa BSS quando ligada. Isto pode ocorrer de duas maneiras:

Passive Scanning – A estação espera por um frame-guia vindo do AP. Este frame-guia, carrega informações de sincronismo, é enviado periodicamente pelo AP com a finalidade de encontrar novas estações.

Active Scanning – A estação envia um frame de requisição para o AP com a finalidade de que este reconheça sua existência. Após isto a estação aguarda por um frame de resposta, até que seja reconhecida. Caso contrário, ela passa ao próximo canal e continua tentando.

5.10 Autenticação

Após o ingresso da estação na célula o AP e a estação entram num processo de autenticação, instante em que trocam informações relacionadas a conta do usuário e a senha.

5.11 Associação

Após uma bem-sucedida autenticação, a estação passa para o processo de associação, quando troca e registra informações sobre suas características com o AP. Somente após concluido este processo é que a estação estará apta para transmitir e receber dados.

5.12 Criptografia

O algoritmo padrão, PRNG (Pseudo Random Number Generator) baseado no algoritmo RSA RC4, possibilita que cada mensagem seja criptografada. Este método é considerado extremamente confiável, pois cada mensagem contém um novo vetor de inicialização que gera um novo PRNG. Portanto, para quebrá-lo faz-se necessário um grande esforço.

5.13 Conectividade com PCs

Laptops e desktops são conectados à WLAN através de um NIC (Network Interface Card) como por exemplo um cartão PCMCIA ou um cartão PCI. Nesta implementação, os NICs para redes Ethernet são substituídos por um NIC próprio para redes wireless. Normalmente o conector utilizado é o RJ-45.

5.14 Fontes de interferência

As três maiores fontes de interferência são: a propagação por multi-percursos, equipamentos de microondas e interferências provenientes das redes ISM (Industrial, Scientific and Medical) que operam localmente em bandas não são licenciadas.

5.15 Interfaces

A arquitetura WLAN além de ser um padrão 802.11, possibilita conexões abertas com interfaces padrão de LAN - 802.3 Ethernet. Interagem de forma transparente com protocolos comuns de rede tais como IP, IPX, Apple Talk, Netbeui, Decnet, SNMP e outros.

6 Medium Access Control

O padrão IEEE 802.11, que especifica as camadas mais baixas do modelo OSI - física e enlace - mantém a mesma interface com as camadas superiores possibilitando a conectividade das WLANs com as redes cabeadas tradicionais.

6.1 Arquitetura dos protocolos

A (figura 6.1) descreve o cenário de uma WLAN IEEE 802.11 conectada a uma rede Ethernet por uma ponte. A camada de aplicação não percebe nenhuma diferença relacionada as camadas inferiores das duas redes (uma possível diferença seria o tempo de acesso maior em relação à WLAN) [LIN 2001]. Consequentemente, as camadas mais altas (aplication, TCP, IP) "vêem" as estações sem fio ou as estações cabeadas de igual modo.

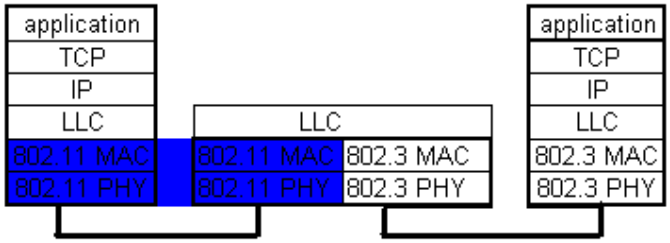

FIGURA 6.1 – WLAN IEEE 802.11 conectada a uma LAN Eth p/uma Bridge

a) o MAC de uma Rede sem Fio é diferente do MAC de uma rede cabeada;
b) a sub-camada LLC (Logical Link Control) equaliza essas diferenças;
c) em muitas das redes atuais nenhuma camada explícita LLC é visível.

6.2 Gerenciamento da camada física

A função da entidade de gerência do nível físico é anotar as estatísticas para a MIB da camada física [IEEE 97].

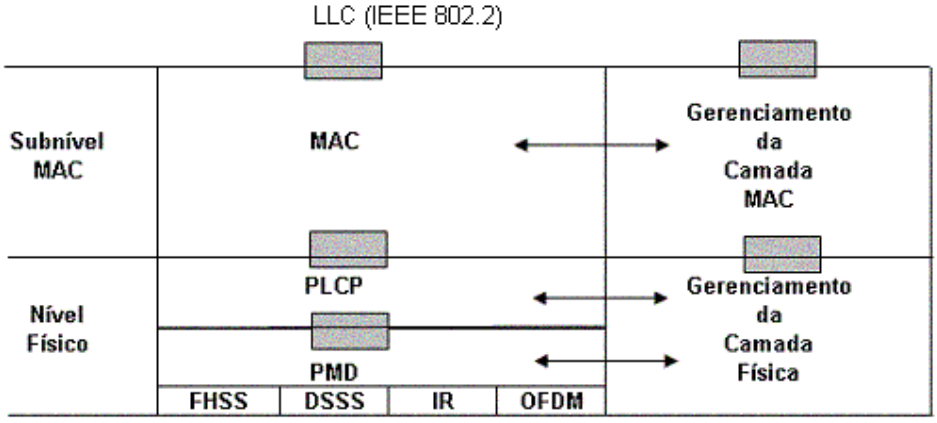

FIGURA 6.2 – LLC (IEEE 802.2)

O nível físico é dividido em duas sub-camadas:

a) inferior, PMD – *Physical Medium Dependent*, responsável pelas diferentes técnicas de transmissão (modulação e codificação do sinal);

b) superior, PLCP – *Physical Layer Convergence Procedure* que fornece aos pontos de acesso serviços comuns relacionados com o nível físico.

O nível físico utiliza quatro métodos de transmissão:

a) S*pread Spectrum*, do tipo F*requency Hopping Spread Spectrum* (FHSS);

b) S*pread Spectrum,* do tipo D*irect Sequence Spread Spectrum* (DSSS);

c) *Orthogonal Frequency Division Multiplexing* (ofdm);

d) transmissão *infra-vermelha difusa*

6.3 Gerenciamento da camada MAC

A sub-camada MAC, é responsável pelo mecanismo de acesso básico ao meio, e pelas funções de fragmentação e encriptação dos dados.

A camada MAC executa diversas tarefas, sendo que a primeira delas é controlar o acesso ao meio, porém, esta camada também oferece suporte para roaming, autenticação e gerenciamento de energia.

Os mecanismos do MAC são chamados de DFWMAC. O DFWMAC suporta dois métodos de acesso, a saber: um método distribuído básico, obrigatório, e um método de acesso centralizado, opcional. Os dois métodos de acesso podem co-existir. Na realidade o método de acesso distribuído forma a base sobre a qual é construído o método centralizado. Os dois métodos, ou "funções de coordenação" [MOB 00], são usados para dar suporte a transmissão de tráfego assíncrono ou com retardo limitado (time bounded).

No IEEE 802.11, uma função de coordenação é um mecanismo que determina quando uma estação específica recebe permissão para transmitir. Se a função de coordenação for distribuída (DCF – conhecida como CSMA/CA), a decisão de quando transmitir é tomada individualmente pelas estações, o que pode resultar em transmissões simultâneas (colisões). Por outro lado, quando a função de coordenação é pontual (PCF), a decisão é centralizada num ponto, sendo este ponto quem determina qual estação deve transmitir e em que momento, evitando a ocorrência de colisões.

Em todos os métodos de acesso, o tempo de espera para que uma estação acesse o meio é fundamental. A (figura 6.3) mostra três diferentes parâmetros que definem a prioridade de acesso ao meio. O meio pode estar ocupado (tanto por um quadro de dados ou por um quadro de controle) ou livre. Durante o período de contenção muitas estações podem tentar acessar o meio.

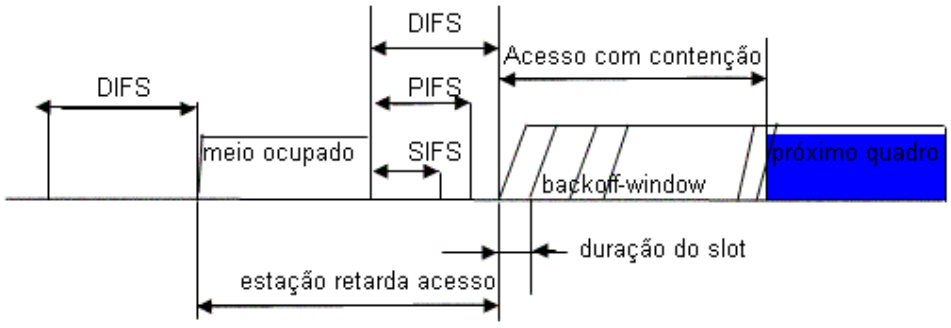

FIGURA 6.3 – Parâmetros que definem o acesso ao meio

a) DCF inter-frame spacing (DIFS) – espaço entre quadros da DCF (Função de Coordenação Distribuída): este parâmetro denota o maior tempo de espera e, portanto, a menor prioridade de acesso ao meio;

b) PCF inter-frame spacing (PIFS) – espaço entre quadros da PCF (Função de Coordenação Pontual): um tempo de espera entre o DIFS e o SIFS (e portanto de prioridade média) é usado para o serviço de acesso com retardo limitado;

c) Short inter-frame spacing (SIFS) – espaço entre quadros curto: o menor tempo de espera para acesso ao meio (e portanto o de maior prioridade) é definido para mensagens de controle curtas, como o ACK (acknowledgement).

6.3.1 DFWMAC-DCF básico (CSMA/CA)

O método de acesso básico do DFWMAC é uma função de coordenação distribuída (DCF) conhecida como CSMA/CA com reconhecimento. Consiste de uma interface definida pelo padrão 802.11 compatível com o Ethernet cabeado, sendo uma variação do CSMA/CD usado no Ethernet. Faz-se necessário destacar que o protocolo CD requer que os rádios sejam capazes de transmitir e receber mensagens ao mesmo tempo, fato este que aumentaria o custo e a complexidade dos equipamentos.

O mecanismo básico do CSMA/CA será mostrado na (figura 6.4) e descrito, como segue:

a) caso o meio esteja inativo por pelo menos a duração de DIFS, uma estação poderá acessá-lo imediatamente. Isto possibilita um atraso de acesso curto, enquanto o tráfego estiver pequeno. Mas, tão logo mais e mais estações tentarem acessar o meio, outros mecanismos de controle serão necessários.

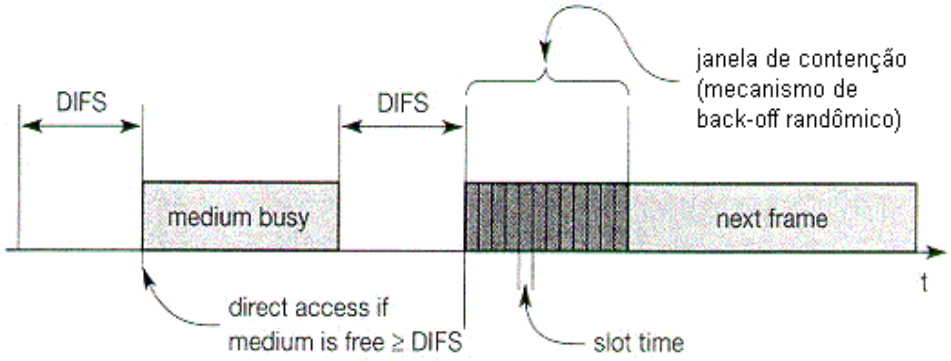

FIGURA 6.4 – Mecanismo básico do CSMA/CA

b) caso o meio esteja ocupado, as estações necessitam esperar pela duração de DIFS, e depois necessitam entrar numa fase de contenção. Cada estação escolhe um backoff time aleatório, dentro de uma janela de contenção, e tenta acessar o meio depois de passado esse intervalo de tempo aleatório. Se, passado esse intervalo de tempo, o meio estiver ocupado, essa estação perdeu este ciclo e tem que esperar até a próxima oportunidade, ou seja, até o meio estar inativo novamente por um período de pelo menos DIFS. Mas, caso contrário, se passado o intervalo de tempo aleatório, o meio estiver ainda inativo, essa estação poderá acessar o meio imediatamente.

c) esse tempo de espera aleatório é escolhido como sendo um múltiplo de um slot time (dentro de um tamanho máximo da janela de contenção). O slot é derivado do atraso de propagação do meio, atraso da transmissão e outros parâmetros dependentes do meio físico.

d) obviamente, o mecanismo básico do CSMA/CA não é justo, cada estação possui as mesmas chances de transmitir no próximo ciclo, e foi por este motivo o IEEE 802.11 acrescentou um contador de backoff. Assim sendo:

d.1) cada estação escolhe um tempo aleatório.

d.2) caso uma determinada estação não conseguir acessar o meio no primeiro ciclo, ela para seu contador de backoff, espera o canal ficar inativo novamente por um período DIFS, e, então reinicia seu contador de backoff.

d.3) quando o contador expirar, esta estação acessará o meio.

Isso significa que esta estação não precisará escolher um tempo aleatório outra vez – passa a ser utilizado o tempo que sobrou no seu contador. Portanto, estações que estão tentando acessar o meio a alguns ciclos têm prioridade em relação as estações que estão iniciando este processo.

A (figura 6.5) mostra esse mecanismo em funcionamento com cinco estações tentando enviar mensagens nos pontos marcados com uma flecha. A estação3 é a primeira a requisitar o meio, espera por DIFS e acessa o meio. A estação1, a estação2 e a estação5 necessitam aguardar até que o meio fique inativo por pelo menos DIFS depois que a estação3 parar de transmitir. Após este instante, as três estações escolhem um backoff time dentro da janela de contenção e começam a decrementar seus contadores.

A (figura 6.5) mostra o backoff time das estações1 e 5 como a soma de BOE (backoff time expirado) e BOR (backoff time residual). A estação2 tem somente o BOE e portanto obtém acesso ao meio, primeiro. Os contadores de backoff das estações 1 e 5 param, e essas estações armazenam seus BORs. Enquanto uma nova estação tem que escolher um backoff time dentro de toda janela de contenção, as duas estações "antigas" têm estatisticamente valores de backoff menores, pois utilizam seus valores do ciclo anterior.

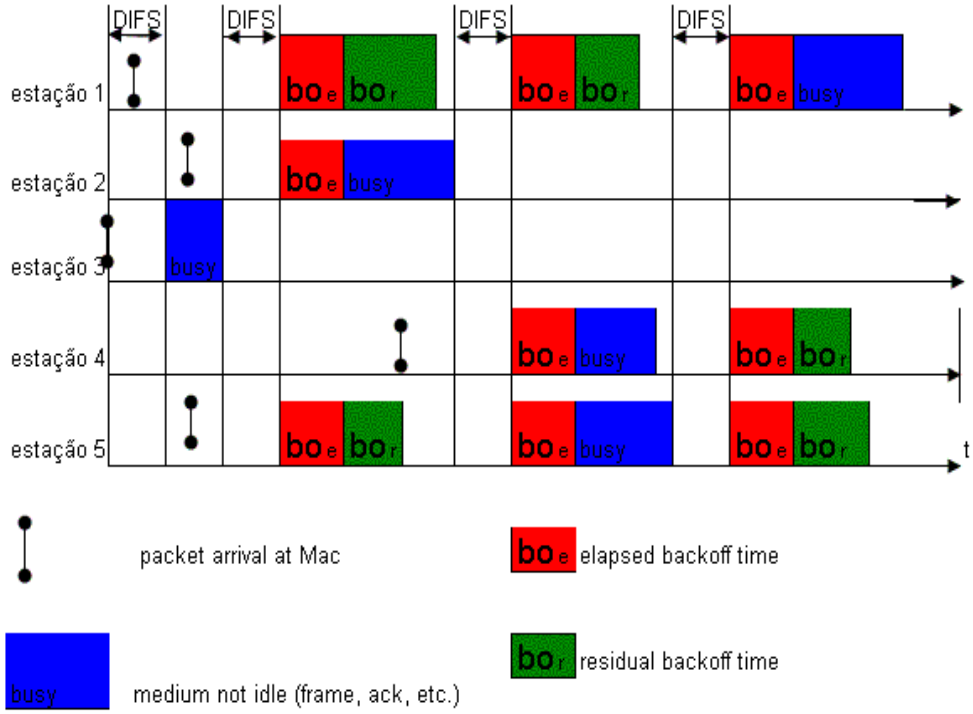

FIGURA 6.5 – Contador de backoff

Agora, a estação 4 quer transmitir. Assim sendo, depois de um período de tempo DIFS, três estações tentam acessar o meio. É possível que aconteça, como mostrado na (figura 6.5), que duas estações acidentalmente tenham o mesmo backoff time, não

importando se ele é do ciclo anterior ou de uma nova escolha. O resultado deste procedimento será uma colisão no meio, ou seja, o quadro transmitido será destruído requerendo-se uma retransmissão com uma nova escolha aleatória do backoff time. A estação1 armazena seu backoff time residual, novamente, e no último ciclo mostrado na (figura 6.5), finalmente consegue acesso ao meio, enquanto que a estação4 e a estação5 necessitam aguardar.

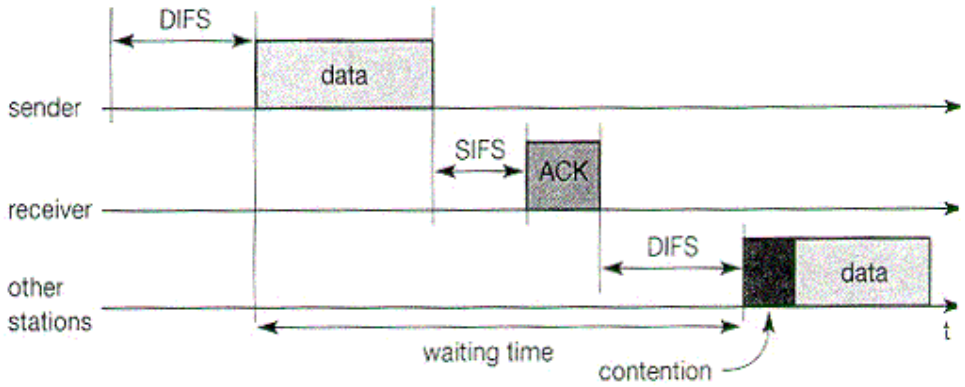

FIGURA 6.6 – Waiting time

6.3.2 CSMA/CA com o mecanismo RTS/CTS

Nem sempre uma estação está numa posição tal que lhe seja possível enxergar todas as demais estações. Por este motivo, o padrão 802.11 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 6.7) mostra o uso do RTS e CTS.

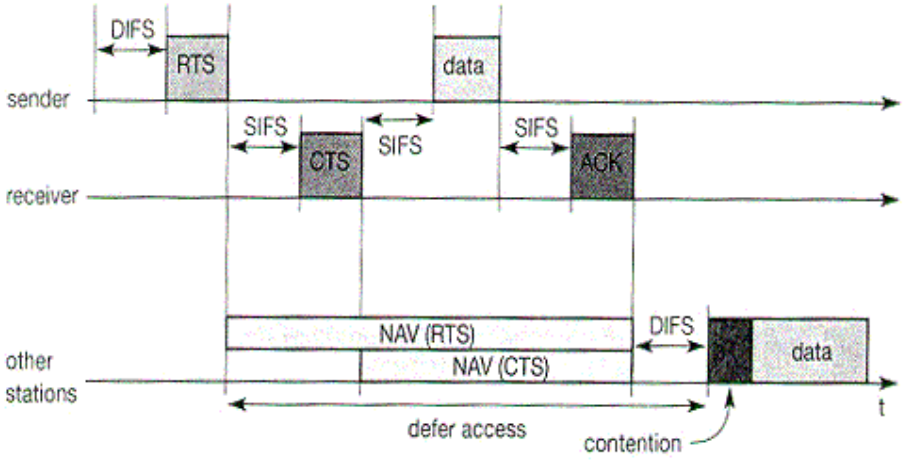

FIGURA 6.7 – RTS e CTS

Após esperar por DIFS (mais um backoff time aleatório se o meio estiver ocupado), o emissor estará apto a emitir um RTS. Este – o RTS - não possui nenhuma prioridade em relação as outras mensagens e nele está incluso o destinatário e o tempo previsto para

transmissão dos dados que 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 poderá tentar acessar o meio novamente.

O receptor da mensagem (aquele com quem o emissor quer se comunicar) recebe o RTS, aguardar por SIFS e responde com um CTS o qual contém, novamente, o tempo previsto para transmissão da mensagem. Neste instante, todas as estações que receberem o CTS do receptor necessitam ajustar os seus NAV. É importante destacar que o conjunto de estações que receberam o CTS não é, necessariamente, o mesmo conjunto de estações que receberam o RTS. Assim sendo, 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. Finalmente, após aguardar por SIFS, o emissor está apto a enviar a mensagem propriamente dita. O receptor recebe a mensagem, espera por SIFS e envia o sinal ACK, caso a transmissão esteja correta. Agora, a transmissão está finalizada e o NAV em cada estação indica que o meio está inativo e o ciclo padrão pode recomeçar.

Com esse mecanismo, 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 delay elevado. Por este motivo, este mecanismo, a princípio, só é utilizado quando do envio quadros grandes.

A taxa de erros de transmissão em Redes sem Fio é geralmente muito maior que em redes cabeadas - fibra óptica por exemplo. Uma metodologia utilizada para diminuir a probabilidade de erros dos quadros é a utilização de quadros pequenos. Neste caso, a taxa de erros na transmissão será a mesma e apenas quadros pequenos serão destruídos. Porém, o mecanismo de fragmentação necessita ser invisível para o usuário e além disso, a camada MAC precisa conseguir ajustar o tamanho do quadro com a taxa de erros específica daquele meio. Para encaminhar estas necessidades, o padrão IEEE 802.11 especificou um modo de fragmentação, mostrado na (figura 6.8).

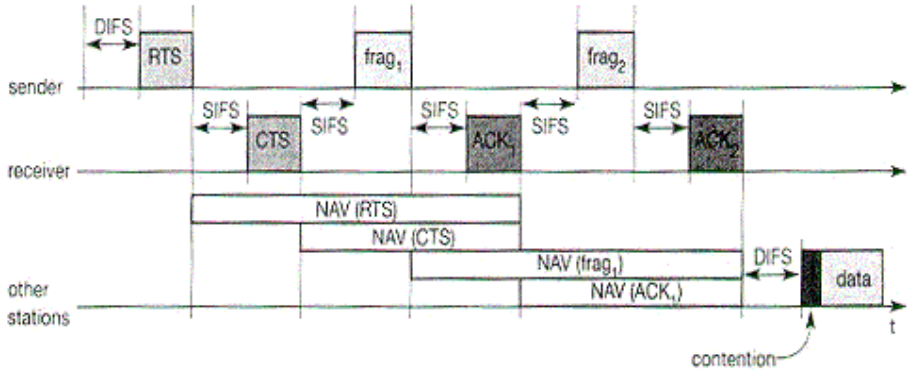

FIGURA 6.8 – Modo de fragmentação

Novamente o emissor envia o RTS e o receptor responde com o CTS. Na seqüência, o emissor envia o primeiro quadro de dados (frag1). A novidade nesse caso, é que, dentro do frag1 há um campo onde está armazenado o tempo previsto para o segundo quadro mais o sinal de ACK do receptor. Outra vez, várias estações irão reajustar seus NAV. O conjunto de estações que farão este reajuste pode ou não ser igual ao conjunto de estações que receberam o RTS, dependendo da ação de cada estação do sistema. Depois de receber frag1, o receptor

envia o sinal de ACK, que neste caso também armazena o tempo previsto para o segundo quadro mais o segundo sinal de ACK. Esse sinal será recebido pelo conjunto de estações que estão dentro do raio de ação do receptor da mensagem. Caso existissem mais quadros para serem enviados, o procedimento se repetiria após o envio do frag2.

6.3.3 DFWMAC-PCF com polling

Os dois mecanismos de acesso apresentados nas duas seções anteriores (CSMA/CA básico e CSMA/CA com RTS/CTS) não são determinísticos, ou seja, não garantem (com 100% de chance) que uma estação vai conseguir acessar o meio. Para oferecer um serviço determinístico (com retardo limitado), o padrão suporta opcionalmente uma função de coordenação pontual (PCF) centralizada, construída sobre a função de coordenação distribuída (DCF). Usando PCF, um Access Point controla o acesso ao meio determinando, a cada instante, qual estação deve transmitir. Redes Ad-Hoc não podem usar essa função sendo que não possuem um nó central controlador.

As duas funções de coordenação – pontual e distribuída – são integradas com a utilização do conceito de superquadro. Quando implementa a função de coordenação pontual, o 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); no segundo, controlado pela DCF, o acesso baseia-se na disputa pela posse do meio (podem ocorrer colisões). A (figura 6.9) mostra como são construídos os superquadros e mostra também muitas estações (todas na mesma linha) e os NAVs das estações (também na mesma linha).

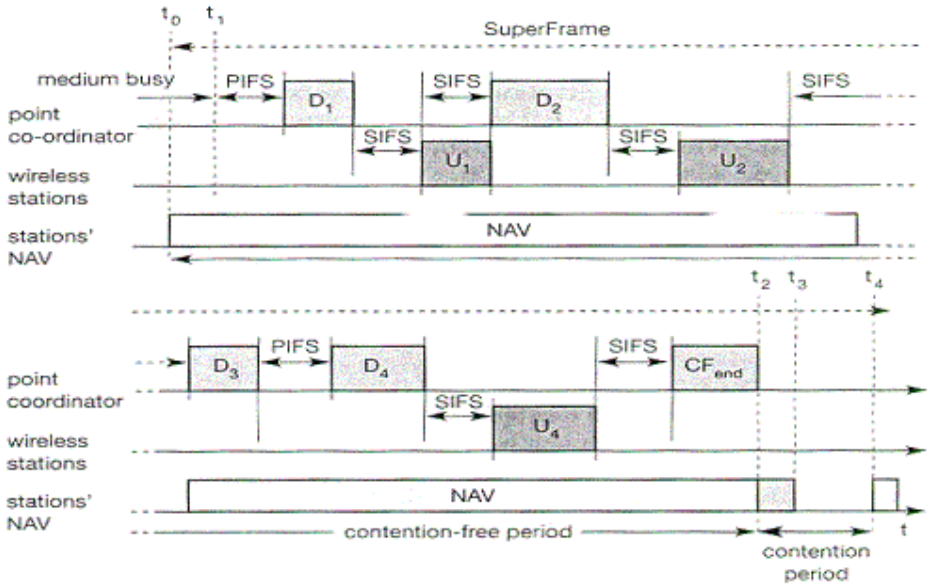

FIGURA 6.9 – Como são construídos os superquadros

No tempo t0, o período livre de contenção do superquadro deveria ter sido 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, a não existência de 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 - observar a (figura 6.9). Depois de esperar SIFS novamente, o AP pode requerer a transmissão da segunda estação. 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.

Após aguardar 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 reinicia com um outro superquadro.

Se, somente o PCF for usado, ou seja, se não houver período de contenção, então a banda passante é distribuída uniformemente entre todas as estações. Neste caso, há uma semelhança com o sistema de transmissão TDMA. Este método pode levar a um overhead elevado se algumas estações não possuirem nada para enviar (apesar do AP continuar requisitando-as para transmitir permanentemente).

A função de coordenação pontual pode permitir a transmissão de tráfego assíncrono no período livre de contenção dos superquadros. Uma estação que utiliza o período sem contenção para transmitir quadros assíncronos, também pode utilizar o período com contenção para trasmitir este tipo de tráfego. Nesse caso, a utilização do período livre de contenção tem o objetivo de aumentar o desempenho da estação. O período sem contenção do superquadro só pode ser utilizado para transmissão de tráfego assíncrono caso os requisitos do tráfego com retardo limitado tenham sido atendidos.

6.3.4 Quadros do MAC

A (figura 6.10) mostra a estrutura básica de um quadro da camada MAC do padrão IEEE 802.11.

Controle do quadro	Duração ID	end. 1	end. 2	end. 3	Controle Seqüência	end. 4	dado	CRC

FIGURA 6.10 – Estrutura básica de um quadro da camada MAC

a) controle do quadro (2 bytes): os dois primeiros bytes servem para muitas coisas, portanto contém muitos sub-campos. Estes campos indicam a versão do protocolo, o tipo de quadro (controle, dados, gerenciamento), se o quadro está fragmentado, informações privadas, e os 2 bits DS (distribution system) que indicam o significado dos quatro campos de endereço.

b) duração ID (2 bytes): para o mecanismo de reserva virtual usando RTS/CTS e fragmentação. O campo de duração contém o período de tempo que o meio ficará ocupado.

c) endereços 1 a 4 (6 bytes cada): os quatro campos contém o endereço MAC padrão IEEE 802.11 - como eles são conhecidos nos outros padrões 802.x LANs. O significado de cada endereço depende dos bits DS do campo de controle de quadro e será explicado mais adiante.

d) controle de seqüência (2 bytes): uma seqüência de números é usada para evitar quadros de ACK duplicados.

e) dado (0 até 2312 bytes): contém um número de bytes arbitrário, que é transferido transparentemente do emissor para o receptor ou receptores.

f) CRC (4 bytes): checksum – é usado para proteger o quadro de possíveis erros na tranmissão.

Os quadros podem ser transmitidos entre estações, entre estações e um AP, e entre um AP e um sistema de distribuição (DS). Dois bits dentro do campo de controle do quadro, "to DS" e "from DS", diferenciam estes casos e então controlam o significado dos quatro endereços usados. A (tabela 6.1) mostra exatamente isso.

TABELA 6.1 – Transmissão de quadros

To DS	From DS	End. 1	End. 2	End. 3	End. 4
0	0	DA	SA	BSSID	-
0	1	DA	BSSID	SA	-
1	0	BSSID	SA	DA	-
1	1	RA	TA	DA	SA

O endereço 1 identifica o receptor físico do quadro. Baseado nesse endereço, uma estação ou AP pode decidir se o quadro é relevante ou não para ele. O endereço 2 representa o emissor físico do quadro. Essa informação é importante porque o emissor é também o receptor do sinal de ACK. Os outro dois endereços representam o emissor ou receptor lógico do quadro.

Rede Ad-Hoc: se ambos os bits DS estão zerados, o quadro constitui uma mensagem que é enviada entre dois nós sem fio sem um sistema de distribuição envolvido. DA (destination address) indica o endereço do destinatário e SA (source address) indica o endereço da fonte do quadro, que são identificados pelo receptor físico e pelo emissor físico, respectivamente. O endereço 3 indica o BSS, que é representado pelo BSS-ID. O quarto endereço não é usado.

Consideremos os seguintes exemplos:

a) de um AP para uma rede com infra-estrutura: se somente o bit from DS está setado, o quadro é originado fisicamente de um AP. DA é o receptor lógico e físico. O segundo endereço identifica o BSS e o terceiro especifica o emissor lógico, o endereço da fonte do quadro. Este caso é um exemplo de um pacote enviado de um emissor através de um AP.

b) de uma rede com infra-estrutura para um AP: se uma estação envia um pacote para outra estação através do AP, somente o bit to DS é setado. Agora o endereço1 representa o receptor físico do quadro (AP) através do indentificador BSS. O endereço2 é o emissor lógico e físico do quadro, enquanto que o endereço3 indica o receptor lógico.

c) rede com infra-estrutura, dentro de um DS: para pacotes transmitidos entre dois APs através de uma sistema de distribuição, ambos bits são setados. O endereço1 indica o endereço do receptor (RA-receiver address) que representa o endereço MAC do AP receptor. Da mesma maneira, o endereço2 identifica o AP emissor (TA-transmitter address) dentro de um sistema de distribuição. Os outros dois endereços são necessários para identificar o destinatário original (DA) do quadro e a fonte original (AS) do quadro.

6.3.5 Sincronização

A sincronização do relógio é necessária para o gerenciamento de energia e também para coordenação do PCF. Usando PCF, o relógio local de uma estação pode prever o início de um superquadro.

Dentro de uma BSS, a temporização é coberta por uma transmissão (quase) periódica de um quadro de 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 tempos em tempos o relógio interno deve ser ajustado. A transmissão do quadro de beacon não é sempre periódica já que ela é adiada se o meio estiver ocupado. A (figura 6.11) mostra exatamente isso.

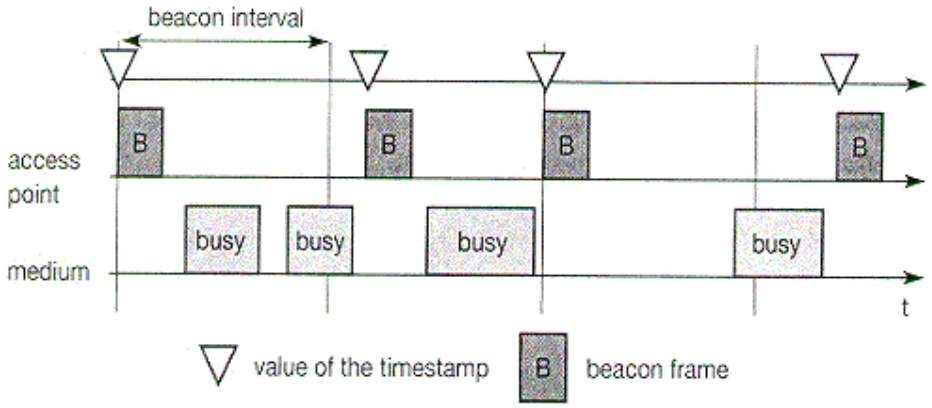

FIGURA 6.11 – Sincronização de tempo

Já numa rede Ad-Hoc a situação é mais complicada, sendo que não existe um AP para transmitir o quadro de beacon. Nesse caso, cada estação mantém sua própria temporização e a sincronização é estabelecida pela transmissão de uma das estações (a que conseguir transmitir seu quadro depois de concorrer com as outras pelo acesso ao meio).

6.3.6 Economia de energia

A grande maioria das WLANs possuem como estações de usuários: handhelds, laptops, palmtops, desktops e uma série de outros equipamentos periféricos. Um componente chave do padrão IEEE 802.11 define um modo stand-by, no qual as estações permanecem inertes até que recebam uma requisição de um AP. Com isto, há um aumento significativo do tempo de operação das baterias e uma utilização otimizada das estações de trabalho.

Os protocolos padronizados para LANs assumem que as estações estão sempre prontas para receber dados, embora os receptores estejam a maior parte do tempo sob um tráfego baixo. Entretanto, essa permanente observação do meio é crítica quando os equipamentos funcionam com baterias com limitada vida útil.

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 consegue saber quando o transceptor tem que estar ativo, ele necessita ligar o transceptor periodicamente. O desligamento do transceptor deve ser transparente para os protocolos e deve ser flexível o 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.

Economizar energia inclui dois estados de uma estação, inativo e ativo e armazenamento de dados do emissor. Se um emissor desejar 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 necessita 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. Manter-se ativa até o momento certo requer a função de sincronização de tempo (que foi explicada na seção Sincronização). Todas as estações tem que ser ativadas ou estarem ativadas ao mesmo tempo.

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

A função de sincronização de tempo assegura que uma estação inativa vai ativar-se periodicamente e receber o TIM. Caso o TIM indicar que uma determinada estação é receptora de quadros armazenados no AP, então essa estação deverá permanecer ativa para receber a transmissão. Para transmissões multicast/broadcast, as estações permanecerão sempre ativas. Uma outra razão para uma estação permanecer ativa é a transmissão de dados dessa estação para o AP. A função de sincronização de tempo continua funcionando normalmente mesmo que a estação estiver inativa.

A (figura 6.12) mostra um exemplo com um AP e uma estação. O estado do meio também é indicado. Novamente, o AP transmite um quadro de beacon a cada intervalo beacon. Este intervalo é agora o mesmo que um intervalo TIM. Além disso, o AP mantém um intervalo de mapa indicativo de tráfego de entrega (DTIM) para enviar quadros broadcast/multicast. O intervalo DTIM é sempre um múltiplo do intervalo TIM.

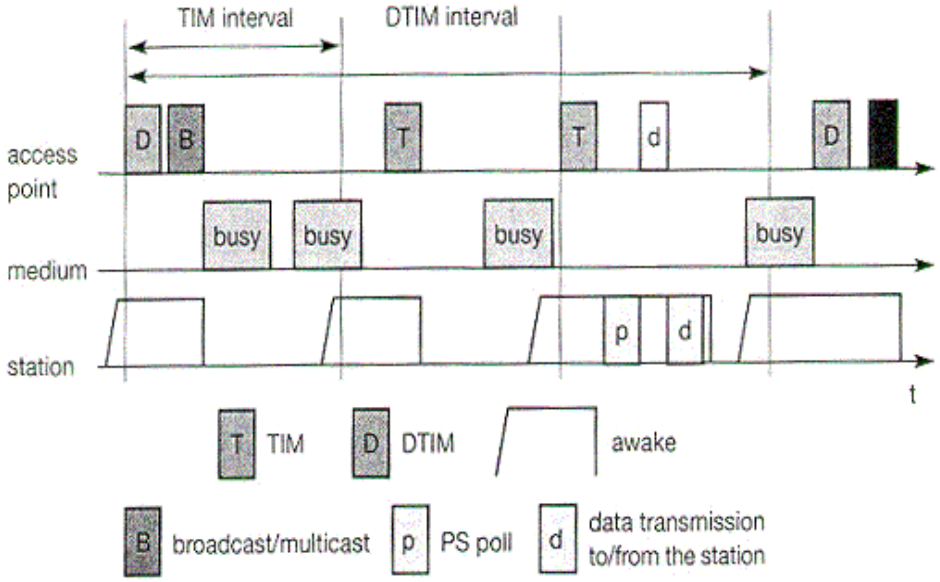

FIGURA 6.12 – Função de sincronização de tempo: um AP e uma estação

Todas as estações (no exemplo, apenas uma é mostrada) são ativadas previamente para receber TIM ou DTIM. No primeiro caso, o AP tem que transmitir um quadro broadcast e a estação deve permanecer ativa para receber esse quadro. Depois disso, ela retorna para o modo inativo. A estação volta a ficar ativa depois do próximo TIM. Dessa vez

(figura 6.12) o TIM é atrasado porque o meio está ocupado, e portanto, a estação permanece ativa. O AP não tem nada para enviar e a estação volta a ficar inativa.

No próximo intervalo TIM, o AP indica que a estação é destinatária de um quadro armazenado. Agora a estação responde com um PS (power saving) poll e permanece ativa para receber o quadro. O AP então transmite o quadro para a estação. Nesse momento a estação envia um sinal de ACK (figura 6.12) e pode ou não enviar algum dado (no exemplo ela envia). Depois disso a estação volta a ficar inativa novamente.

Finalmente, o AP tem mais dados broadcast para enviar no próximo intervalo DTIM, que é novamente adiado porque o meio está ocupado.

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 desejar 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.

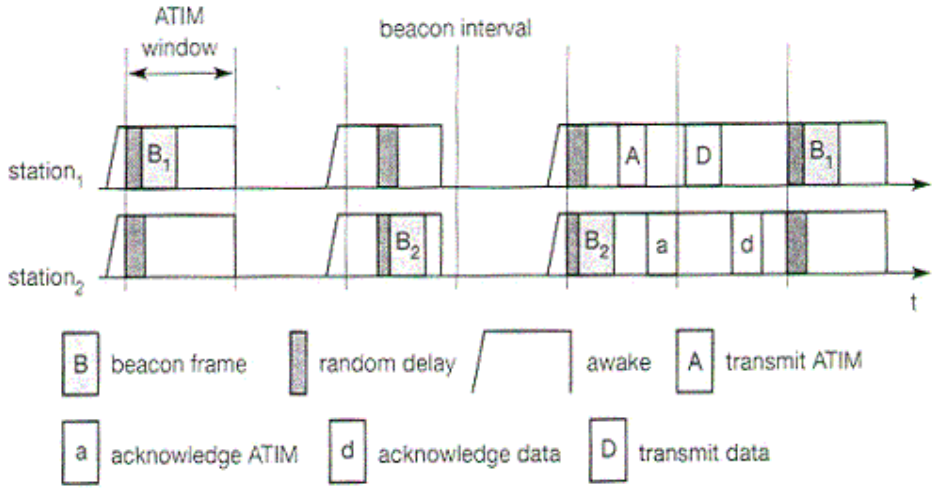

FIGURA 6.13 – Rede Ad-Hoc com duas estações

A figura 6.13 mostra uma simples rede Ad-Hoc com duas estações. Novamente, o intervalo de beacon é determinado por uma função de distribuição (diferentes estações podem enviar o beacon). Entretanto devido a sincronização, todas as estações dentro da rede Ad-Hoc serão ativadas ao mesmo tempo. Todas as estações permanecem ativas durante o intervalo ATIM. Nos primeiros dois intervalos mostrados na (figura 6.13) nenhum quadro foi armazenado, por este motivo as estações voltam a ficar inativas. No terceiro intervalo a estação1 tem dados armazenados para a estação2. Isso é indicado através da transmissão de ATIM pela estação1. A estação2 confirma o recebimento de ATIM e permanece ativa para receber os dados. Depois do intervalo ATIM window, a estação1 pode transmitir o quadro de dados, e a estação2 confirma o recebimento.

Um problema desse mecanismo ocorre quando muitas estações dentro de uma rede Ad-Hoc operam no modo power-save, pois muitas estações podem querer transmitir seus ATIMs dentro do intervalo ATIM window. Isso faz com que aumente o número de colisões.

6.3.7 Roaming e handoff

Roaming é a capacidade que as estações tem de se mover de uma célula para outra, tanto em topologia de células ligadas quanto na concepção de multi-células. Os APs devem fazer o handoff do sinal, além de realizar o sincronismo apropriadamente.

Um fator de grande importância na hora da escolha de um fornecedor para este tipo de serviço é saber como são tratados os assuntos referentes a roaming e sincronização dos APs, pois não há uma padronização sobre estes aspectos.

Redes sem fio típicas dentro de prédios requerem mais que apenas um AP para cobrir todos os ambientes. Dependendo do material com que são feitas as paredes, um AP tem um raio de transmissão que varia de 20 a 50 metros, para que uma transmissão seja de boa qualidade. Se um usuário passeia com uma estação sem fio, a estação tem que se mover de um AP para outro. Os passos para um roaming entre APs são descritos abaixo:

a) uma estação decide quando uma conexão com um determinado AP está muito ruim. Essa estação, então, começa a procurar por outro AP.

b) a procura envolve uma busca ativa por outra BSS. 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 à uma sonda contém a informação necessária para a estação se unir ao novo BSS.

c) 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.

d) o novo AP responde com uma resposta de associação. Se a resposta é positiva, a estação é tranferida para o novo AP. Caso contrário ela continua procurando por outro AP.

e) o AP aceitando o requerimento de associação informa 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.

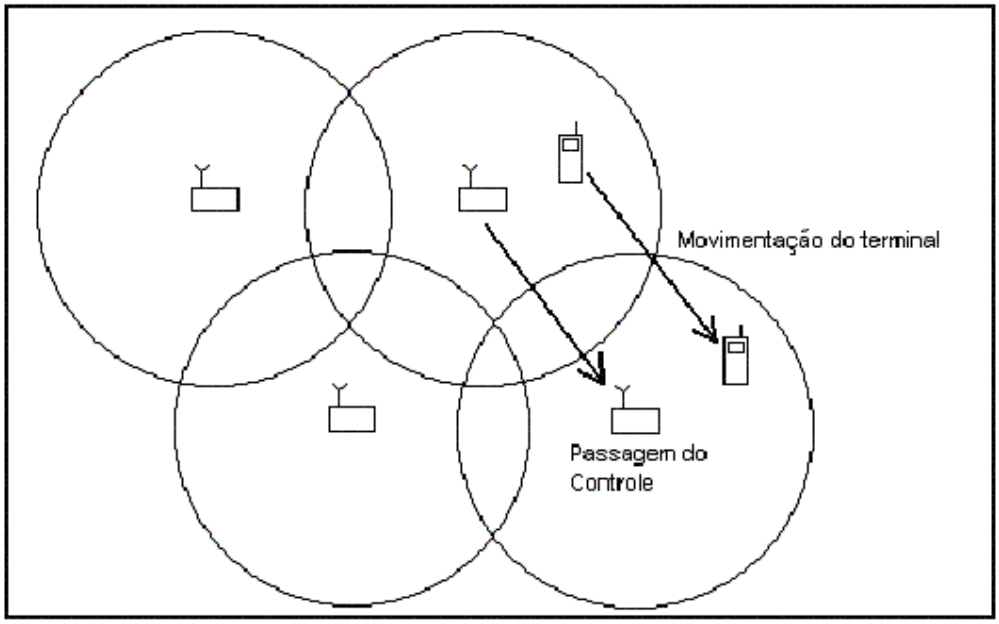

FIGURA 6.14 - Passagem de equipamento entre células

7 A grande Questão: 802.11a ou 802.11b?

O primeiro objetivo do padrão 802.11, definido pelo IEEE em 1997, foi a especificação de uma simples e robusta WLAN capaz de oferecer serviços síncronos e assíncronos. Além disso, a camada MAC necessita interagir com várias camadas físicas, cada uma exibindo diferentes "sensores do meio" e diferentes características de transmissão. A exemplo dos demais padrões 802.x, preserva a mesma interface com as camadas mais altas, portanto mantendo a conectividade com as redes cabeadas típicas.

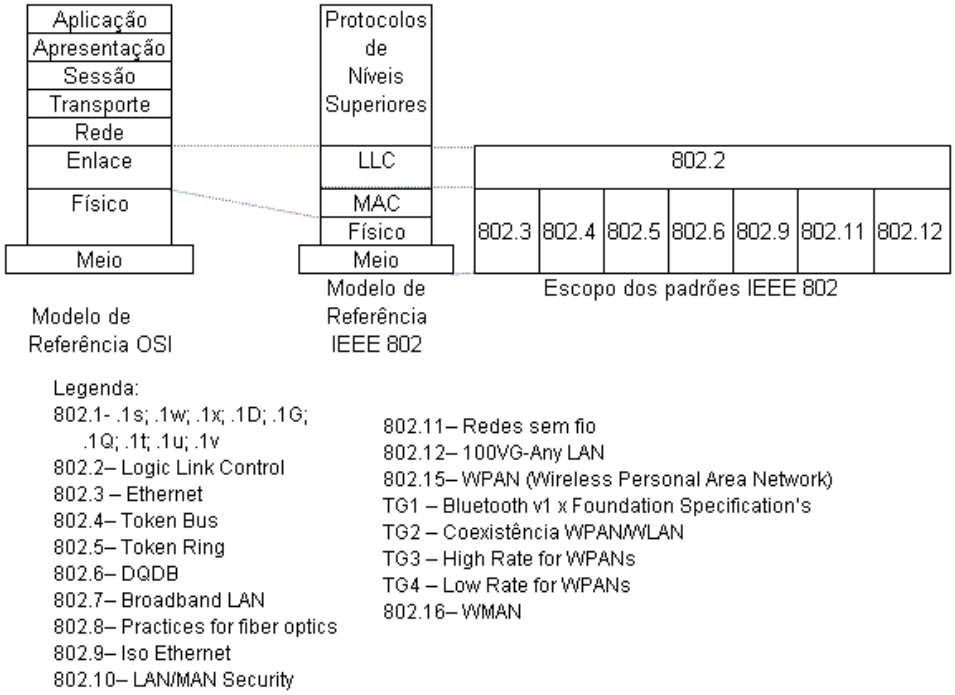

FIGURA 7.1 – Padrões IEEE 802.x

As redes wireless não foram aceitas inicialmente por três razões:

a) o throughput (1Mbps/2Mbps) era muito baixo se comparado ao padrão 10Mbps Ethernet;

b) os adaptadores e os pontos de acesso wireless eram significativamente mais caros do que as placas de rede e os switches;

c) os primeiros produtos wireless não trabalhavam bem juntos com produtos wireless de outros fabricantes.

Durante os últimos anos, após a especificação das normas 802.11a e 802.11b todos estes três interesses foram encaminhados.

a) os produtos que seguem o padrão IEEE 802.11b têm uma banda de rede de 11Mbps equivalente à 10Mbps Ethernet;

b) os interesses de interoperabilidade estão sendo coordenados pelo programa de certificação WECA's Wi-Fi em que os produtos são submetidos para testes de interoperabilidade. Um programa similar denominado Wi-Fi5, mais recentemente, foi desenvolvido para testar a interoperabilidade dos produtos 802.11a;

c) as forças de mercado incluindo a competição e volumes vastamente aumentados reduziram os custos dos equipamentos wireless 802.11b.

Dos três fatores que impulsionaram a aceitação das rede wireless, o Wi-Fi foi provavelmente o mais significativo, pois assegurou aos compradores de grandes volumes que eles não estariam presos a soluções proprietárias.

O diagrama a seguir mostra uma rede típica 802.11:

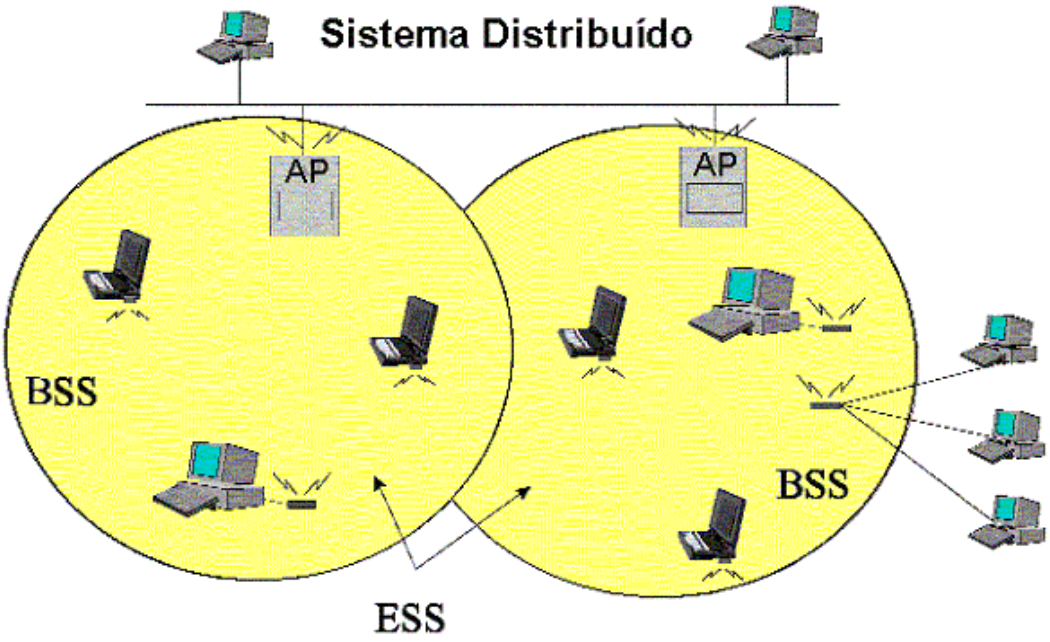

FIGURA 7.2 – Rede típica 802.11

A especificação 802.11a não foi escrita para resolver os problemas do padrão 802.11b. De fato ambas as especificações foram publicadas em 1999 pelos coordenadores dos padrões IEEE, entretanto, o padrão 802.11b foi disponibilizado no mercado mais rapidamente.

Se você estiver planejando implementar uma WLAN, precisará definir qual padrão implementará, pois 802.11a e 802.11b definem cada um uma camada física diferente. Os rádios 802.11b transmitem em freqüência 2.4GHz e enviam dados até 11Mbps usando a modulação DSSS, enquanto que os rádios 802.11a transmitem em 5GHz e enviam dados até 54Mbps usando OFDM.

Recentemente, foram feitas demonstrações de rádio 802.11a que entregam 54Mbps com distâncias de aproximadamente 60 pés, as quais são bem menores que os 300 pés disponíveis com sistemas 802.11b. Comparando com a solução 802.11b, você necessitará um número muito maior de pontos de acesso 802.11a [GEI 2001].

Uma diferente radiofreqüência e tipos de modulação fazem com que os padrões 802.11a e 802.11b tornem-se inoperantes. Por exemplo, um usuário final equipado com um cartão de rádio 802.11a não será capaz de conectar-se com um ponto de acesso 802.11b. O padrão 802.11 não oferece provisão de interoperabilidade entre as diferentes camadas físicas.

Naturalmente o desempenho superior do 802.11a oferece excelente sustentação para aplicações que precisam de largura de banda, mas operando-se a freqüência mais altas, conseqüentemente temos um alcance relativamente mais curto. Mantenha sempre em mente que a largura de banda disponível pode ser vista de perspectivas diferentes:

a) quanto conteúdo você pode transmitir dentro de um dado período de tempo;
b) quão rapidamente você pode transmitir uma quantidade dada de conteúdo;

c) quantos usuários podem eficazmente usar a largura de banda disponível simultaneamente.

Há diversos fatores chaves a considerar na avaliação das várias tecnologias wireless, incluindo velocidade, canais simultâneos, interoperabilidade, interferência, e aceitação internacional.

A seguir apresentaremos algumas diretrizes que o ajudarão na tomada da decisão:

7.1 Considerações usando 802.11b

Atualmente, a tecnologia 802.11b é a nítida vencedora nos negócios de rede wireless LAN. Operando na faixa de freqüência 2.4GHz, 802.11b tem uma taxa de dados nominal máxima de 11Mbps, com o potencial de três canais simultâneos. 802.11b tem uma grande vantagem porque é aceita mundialmente.

Devido ao fato da tecnologia wireless de 11Mbps (802.11b) já ocupar as instalações das empresas, há muito interesse nos produtos que permitirão que 802.11a e 802.11b co-existam.

Uma das desvantagens mais significativas do 802.11b é que a banda de freqüência está cheia, e sujeita à interferência de outras tecnologias de rede, fornos de microonda, telefones sem fio (2.4GH - um mercado enorme), e Bluetooth. Há alguns inconvenientes na tecnologia 802.11b, tais como a falta de interoperabilidade com dispositivos de voz, e nenhuma provisão de QoS para conteúdo multimídia. Além destes aspectos há três problemas principais: limitada largura de banda, interferência de rádio de outros dispositivos e redes, e segurança preocupante.

7.1.1 Largura de banda

Mesmo que a performance 802.11b equipare-se a rede Ethernet 10Mbps, overhead, configuração, e fatores de segurança podem baixar o throughput real para 4 a 7Mbps. Essa velocidade é muito boa para suportar os usuários que na maioria das vezes movem textos através da rede. Aplicações que exigem mais demanda, como por exemplo, tráfego multimídia podem facilmente esgotar o throughput do 802.11b, particularmente nos casos em que houver uma grande disputa pela largura de banda por muitos usuários. As companhias e as organizações que necessitam suportar muitos usuários, principalmente se todos eles estão verificando o E-mail, podem rapidamente achar que 802.11b está sobrecarregado.

Uma alternativa para estes casos é adicionar mais pontos de acesso e atribuir canais a grupos de usuários, mas mesmo assim a performance da rede baixará quando muitos usuários convergirem para uma área pequena (em um hall de leitura ou em um local de conferência, por exemplo).

Não há nenhum conflito no que diz respeito a largura de banda porque as duas tecnologias usam partes muito diferentes do spectrum de rádio, mas, as companhias que já investiram na tecnologia 802.11b hesitariam em jogar fora seu parque existente e substituí-lo por novos componentes que suportem a tecnologia 802.11a.

O sinal 802.11b pode extender-se de 100 a 150 pés dentro dos edifícios, trafegando através das paredes e dos tetos, e acima de 1000 a 1500 pés em ambientes abertos. Se seu escritório ou vizinhos residenciais estiverem usando a mesma tecnologia de rede ou algum dos outros dispositivos wireless no spectrum 2.4GHz seu throughput pode diminuir.

7.1.2 Interferência

As questões da interferência são o principal problema para as redes 802.11b, um fator que pode piorar agora que os dispositivos de Bluetooth se tornaram finalmente disponíveis. Ambos, Bluetooth e 802.11b, usam o spectrum 2.4GHz de rádio. Outras fontes de interferência para 802.11b são sistemas wireless antigos e os dispositivos caseiros de controle que usam o padrão X-10.

7.1.3 Configuração básica de segurança spread spectrum

Comunicações sem fio, especialmente a tecnologia *spread spectrum*, foram desenvolvidas durante a Segunda Guerra Mundial para aplicações militares. O objetivo inicial dessas técnicas de transmissão era prover comunicação de voz segura e confiável. Uma das primeiras definições de *spread spectrum* especificava um rádio *frequency-hopping* para guiar torpedos aos seus alvos.

As comunicações sem fio 802.11 não podem ser recebidas – e muito menos decodificadas – por simples rastreadores, receptores de ondas curtas, etc. Isto está baseado na concepção comum de que comunicações sem fio não podem ser acessadas por qualquer um [KOL 2001]. Porém, invasão é possível usando equipamentos especiais.

Como Craig Ellison demonstrou num de seus artigos, Explorando e Protegendo Redes Wireless [ELL 2001], muitas instalações de rede wireless estão totalmente abertas porque os padrões configurados pelos fabricantes nos equipamentos, nunca são alterados após a instalação. Assim sendo, se você não instituir e não usar boas práticas de segurança, sua rede será vulnerável quer esteja baseada em cabos ou em wireless.

O objetivo principal com relação a segurança em *spread spectrum* é impedir que ocorram interferências no sinal e recepção não autorizada, intencional ou não.

A maioria dos produtos *spread spectrum* possuem quatro modos básicos de segurança:

a) usam baixos níveis de força na transmissão, restringindo o alcance das ondas;

b) usam alguma técnica para embaralhar o sinal: transmissores efetivamente embaralham os dados, enviando-os em múltiplas freqüências de rádio;

c) usam endereços únicos e específicos para cada usuário;

d) usam codificação de espectro: o controlador seleciona um único código *spread spectrum* e o AP e os equipamentos operam com aquele código; o próximo AP tem um código diferente e ainda não pode comunicar (ou roubar) dados.

Adicionalmente, observa-se, atualmente, que muitos curiosos casuais não comprarão um rastreador ou um receptor de rádio para capturar um sinal de um produto específico. Enfim, é muito mais difícil para um hacker entrar em um prédio carregando um receptor sem fio do que utilizar um *nutcracker* para acessar uma rede fixa.

7.1.4 Suporta tipicamente até 3 canais

O DSS PHY para U.S. especifica 11 freqüências centrais, com afastamento de canais mínimo de 25 MHz na banda de 2.4 a 2.4835 GHz ISM.

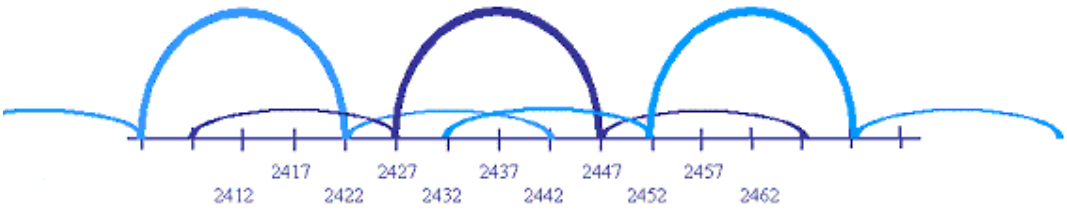

FIGURA 7.3 – DSS PHY – freqüências centrais

7.2 Considerações usando 802.11a

A chave do sucesso inicial do 802.11a no mercado corporativo será construir uma ponte sobre as tecnologias que ajude a 802.11a e a 802.11b co-existirem.

As maiores vantagens do 802.11a comparado ao 802.11b incluem taxas mais elevadas do throughput e o aumentado suporte a canais, ambos resultando em uma largura de banda maior.

A velocidade nominal para 802.11a é 54Mbps, mas, atualmente, sua largura de banda real máxima varia entre 22 e 26Mbps. Dentro da especificação do IEEE para 802.11a existe um modo de velocidade mais elevada que pode ser implementado para aumentar a largura de banda - alguns fabricantes denominam-o de modo "turbo" e outros de modo "2X" - com o qual é esperada uma melhoria aproximada de 25% a de 50%. É importante destacar que enquanto o modo normal do 802.11a é especificado para garantir interoperabilidade, o módulo de alta velocidade não está padronizado. Assim sendo a interoperabilidade entre chipsets e igualmente entre os produtos de OEM usando o mesmo chipset não são garantidos no modo turbo ou 2X.

Observam-se, hoje, argumentos a favor do uso do 802.11a nas aplicações SOHO, tais como a velocidade total e a capacidade média de transferência, mas indubitavelmente a maioria das primeiras instalações serão implementadas em conjuntos empresariais.

Uma estratégia acertada para alguém que está considerando configurar uma rede wireless doméstica ou SOHO é esperar até que os preços do 802.11a baixem. A ampla largura de banda para transferência de vídeo e a impossibilidade de ocorrem interferências oriundas dos forno microondas e telefones 2.4GHz devem ser razão suficiente para os usuários domésticos, em particular, adotarem 802.11a como a rede wireless padrão.

7.2.1 Largura de banda superior

802.11a, como 802.11b pode operar em diferentes níveis de velocidade. É possível ajustar os drivers de ambos os cartões (AP e estações) para rodarem numa velocidade apenas, ou, mais usualmente, para cair para taxas mais lentas quando a potência do sinal diminuir. Enquanto a velocidade máxima do padrão 802.11b é 11Mbps podendo retroceder para 5.5, 2, e 1Mbps, a velocidade máxima do padrão 802.11a é 54Mbps podendo retroceder para 48, 36, 24, 18, 12, 9, e 6Mbps.

TABELA 7.1- Tabela de padrões aprovados pelo IEEE

	802.11a	802.11b	802.11
Padrão aprovado	Set/99	Set/99	Jul/97
Largura de banda disponível	300MHz	83.5MHz	83.5MHz
Freqüências de operação não-licenciadas	5.15-5.35GHz, 5.725-5.825GHz	2.4-2.4835GHz	2.4-2.4835GHz
Número de canais não-sobrepostos	4 (Indoor) 4 (Indoor/Outdoor) 4(Indoor/Outdoor)	3 (Indoor/Outdoor)	3 (Indoor/Outdoor)
Taxa de dados por canal	6, 9, 12, 18, 24, 36, 48, 54 Mbps	1, 2, 5.5, 11Mbps	1, 2Mbps
Tipo de modulação	OFDM	DSSS	FHSS, DSSS

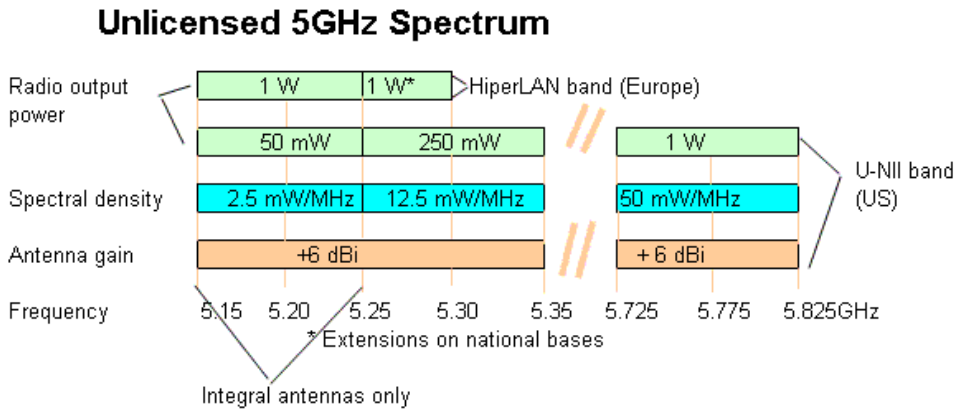

FIGURA 7.4 – Unlicensed 5GHz Spectrum

7.2.2 Canais de transmissão adicional

Uma segunda razão para maior largura de banda total com 802.11a é o suporte a canais. Com 802.11b, três canais estão disponíveis para operação simultânea dentro da banda de freqüência 2.4-2.4835GHz (existem onze núcleos de freqüências especificadas 2.412, 2.417, 2.422, 2.427, 2.432, 2.437, 2.442, 2.447, 2.452, 2.457, e 2.462 GHz, mas porque existe um espaçamento requerido de 25MHz entre os canais ativos, somente três são tipicamente usados de cada vez). No 802.11a, entretanto, oito canais podem operar simultaneamente nas duas bandas mais baixas do spectrum 5GHz usado nos U.S., 5.15-5.25GHz e 5.25-5.35GHz. Os pontos centrais para os oito canais, cada um dos quais com largura de 20MHz podem suportar 52 sinais de portadora: 5.18, 5.2, 5.22, 5.24, 5.26, 5.28, 5.30, e 5.32 GHz. A alta banda do não-licenciado spectrum 5GHz (5,725 a 5.825GHz), está disponível, mas é mais comumente usada para aplicações wireless prédio a prédio.

7.2.3 Spectrum e alocação de canais

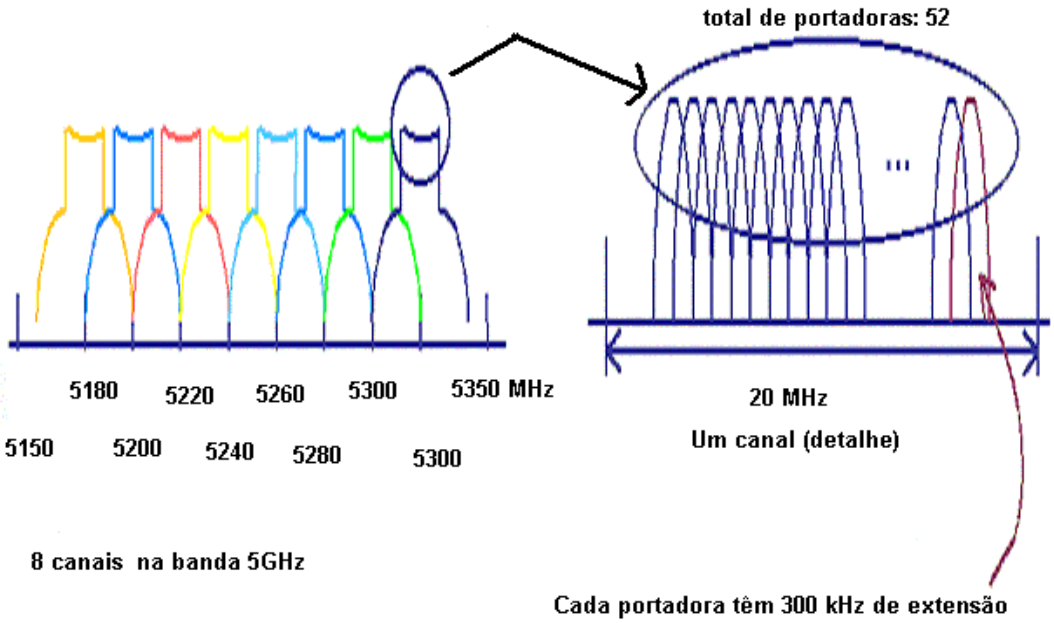

FIGURA 7.5 – Spectrum e Alocação de Canais – 802.11a

a) O canal de 20 MHz é dividido em 52 portadoras (48 carregam dados, 4 áreas de sinais piloto).

b) Todas as 52 portadoras são usadas sempre e cada portadora têm ~300kHz de largura de banda

c) As taxas de dados FRM, 6Mb/s à 54Mb/s, são suportadas pela variação da modulação e código de correção de erros

d) Capacidade interna para crescimento das redes

e) Densidade mais elevada de usuários

f) 802.11a tem 8 canais não sobrepostos

g) Permite quase três vezes mais pontos de acesso numa área fechada

h) Suporta mais usuários simultâneos em áreas densas

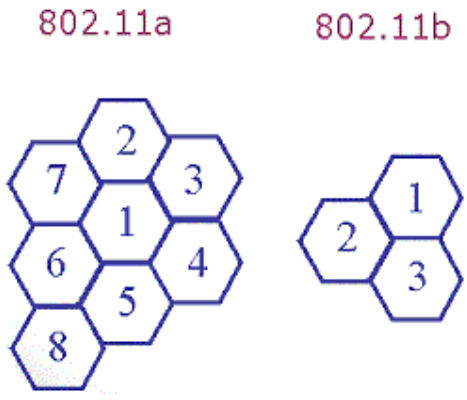

FIGURA 7.6 – 8 Canais não sobrepostos

Não obstante o número de canais disponíveis, um ponto de acesso 802.11a usa somente um canal de cada vez, o qual se gerenciado corretamente pode lhe ajudar a obter a maior largura de banda disponível. Se você tiver múltiplos pontos de acesso, você pode suportar mais usuários do que com um ponto de acesso atribuindo os canais específicos aos usuários associados com os pontos de acesso específicos. Se uma outra companhia, departamento, ou vizinho que também usam 802.11a estiverem dentro da faixa de sua rede, ajuste seus pontos de acesso para usar canais específicos para diminuir a disputa da largura de banda.

Note que há algumas oportunidades para que os fabricantes desenvolvam tecnologias de balanço de carga para espalhar automaticamente a carga assim que um canal estiver começando a superlotar enquanto outros estejam disponíveis. Os fabricantes, desenvolveram a tecnologia de balanço de carga para o 802.11b e continuarão encaminhando o gerenciamento, o desempenho, e as questões da banda para o padrão 802.11a.

O problema da interferência com as redes 802.11b devido aos telefones sem fio 2.4GHz, aos fornos de microonda, aos dispositivos caseiros de controle X-10, e os dispositivos Bluetooth não são um problema com 802.11a. Porque 802.11a opera na faixa de freqüência 5GHz não está sujeito à interferência dos dispositivos 2.4GHz ou das redes.

7.3 Potenciais melhorias na interoperabilidade

A interoperabilidade entre 802.11a e 802.11b será melhorada consideravelemente. Por exemplo, Synad, uma companhia de engenharia localizada em Londres, anunciou recentemente seu desenvolvimento de um chipset duplo 802.11a/b. Isto permitirá desenvolvedores do produto disponibilizar rádios WLAN que operem em ambos os padrões: 802.11a e 802.11b.

Como conseqüência, um rádio 802.11a/b dentro de um dispositivo de usuário final será automaticamente reconhecido se o ponto de acesso for 802.11a ou 802.11b e então comunicar-se-á. Igualmente, um AP pode ativar uma solução dual 802.11a/b, permitindo interoperabilidade com dispositivos de usuários finais equipados com um rádio 802.11a ou 802.11b. Com isto em mente, possivelmente, sua decisão será adquirir ambas as soluções: 802.11a e 802.11b [GEI 2001]!

7.4 Aplicação

As redes WLANs, em expansão e cada vez mais adquirindo popularidade, estão sendo utilizadas em segmentos como saúde, varejo, manufatura e educação. Por este motivo, incluiremos neste tópico exemplos de algumas oprtunidades de utilização deste tipo de rede.

a) na Empresa X está em uso nas áreas de produção de 11 unidades instaladas no Brasil. Aplicações que trocam informações com bancos de dados em ambientes hostis, tais como: controle dos processos industriais, apontamento de mão-de-obra, estatística de utilização e parada dos equipamentos, controle do carregamento dos produtos nas frentes de carregamento e identificação de produtos utilizam-se dos serviços desta rede;

b) os pesquisadores da University of Washington, estão desenvolvendo uma tecnologia de rede capaz de possibilitar a qualquer computador movel o reconhecimento e adaptação a ambientes externos, transmitindo para o usuário informações relativas ao ambiente. Assim sendo, ao chegar numa nova cidade um turista poderá ter seu PDA automaticamente atualizado com o mapa e principais atrações turísticas daquela localidade;

c) na Universidade Federal de Minas Gerais está sendo desenvolvido um protótipo de servidor Web sem fio que vai permitir, entre outras coisas, a monitoração de pacientes à distância;

d) em hospitais: sistemas de prontuário de pacientes fornecendo acesso on-line a informação médica no atendimento, prescrição de medicação e dieta em cada leito, etc;

e) gerentes de redes de computadores em ambientes dinâmicos, realizando alterações de lay-out e ampliando redes num curto espaço de tempo;

f) grupos de estudos em universidades com fácil acesso e/ou troca de informações, facilitando a aprendizagem;

g) configuração de redes em prédios históricos;

h) controle de iluminação sem fio, gerenciamento de energia, e outras aplicações para prédios inteligentes;

i) em aeroportos: sistemas de abastecimento, check-in de passageiros, localização de bagagem, etc;

j) em lojas: comunicação de PDVs sem fio permitindo grande flexibilidade, inventário de produtos, auditoria de preços de gôndola, apoio à execução do cronograma, geração de pedidos de mercadorias para a área de venda, etiquetas eletrônicas, etc;

k) em depósitos: para apoio as operações de recebimento, armazenamento, picking, expedição, inventário, etc.

7.5 Novos desenvolvimentos do padrão 802.11

Três grandes questões no mundo wireless LAN estão sendo consideradas, atualmente:

a) por quanto tempo 802.11b prevalecerá sobre 802.11a nos negócio de redes wireless LAN;

b) os interesses, que envolvem os fornecedores de equipamentos, relacionados ao padrão 802.11a versus o padrão 802.11g;

c) a conclusão da definição do padrão 802.11e - promete trazer QoS (qualidade de serviço - essencial para multimídia) para o mundo 802.11.

Após a série de reuniões do IEEE 802.11 Committee Working Group G na Australia, em 2001, sobressaiu a impressão de que o padrão 802.11g corria riscos de ser abandonado, mas em 15 de Novembro de 2001 a aprovação da especificação do padrão 802.11g foi garantida - firmada num comprimisso apartir de propósitos específicos juntamente com as empresas Texas Instruments e Intersil. Baseado nesta aprovação, a corrida pelas redes wireless de alta velocidade, então, foi iniciada ou pelo menos proposta.

Um aspecto animador da competição das rede wireless é que os maiores fabricantes de produtos wireless comercial construirão e venderão produtos para qualquer padrão que seja aprovado, visando atender a demanda dos clientes.

A empresa Intersil Corp., já líder nos chips 802.11b, foi a grande vencedora com a adoção do padrão 802.11g. A empresa Texas Instruments demonstrou chips 802.11g 22Mbps no estande da Linksys na Comdex/2001 e também espera ter o novo chip 802.11g, de acordo com o padrão acordado, ainda em 2002. A empresa Atheros Comunicações Inc., a primeira companhia a fabricar o chip 802.11a, provavelmente preferiria que o padrão 802.11g permancesse na mesa de discussão por mais tempo enquanto suas companhias sócias iniciassem as vendas dos equipamentos com a tecnologia 802.11a. Como a adoção e o desenvolvimento das redes wireless devem aumentar muito nos próximos cinco anos, as apostas são muito elevadas, neste jogo.

7.5.1 802.11g

Nas primeiras considerações acerca da tecnologia 802.11g, que opera na freqüência 2.4GHz com obrigatória compatibilidade com 802.11b mas com uma taxa de dados máxima

de 54Mbps, ficou evidenciado que está sendo dado um passo importante no sentido de melhorar a performance das redes wireless, mantendo-se a compatibilidade com Wi-Fi. A proposta 802.11g encontrou significativa resistência e muitos predisseram que seria abandonada, deixando o campo de redes wireless de alta velocidade para 802.11a. É importante observarmos que esta tecnologia ainda está em fase de aprovação de uma especificação, e que não terá sua aprovação final até que as versões trabalhadas estejam testadas e 90% dos votantes no comitê, votem afirmativamente.

O padrão opera inteiramente na freqüência 2.4GHz, mas usa um mínimo de dois modos (ambos mandatórios) com dois modos opcionais. Os modos mandatórios de modulação/accesso são o mesmo modo CCK usado pelo 802.11b (em virtude disto a compatibilidade com Wi-Fi) e o modo OFDM usado pelo 802.11a (mas neste caso na faixa de freqüência 2.4GHz). O modo mandatório CCK suporta 11Mbps e o modo OFDM um máximo de 54Mbps. Há também dois modos que usam métodos diferentes para alcançar uma taxa de dados de 22Mbps – TI's PBCC-22, qualificado para 6 a 54Mbps) e modo Intersil's CCK-OFDM (com uma taxa máxima qualificada de 33Mbps).

A vantagem óbvia do padrão 802.11g é que mantém a compatibilidade com o padrão 802.11b oferecendo, também, taxas de dados mais rápidas quando comparado com o padrão 802.11a. O número de canais disponíveis, entretanto, não foi aumentado e nesta questão o padrão 802.11a vence com seus oito canais, comparados com os três canais disponíveis no 802.11b ou 802.11g. Uma outra desvantagem do 802.11g é que a freqüência 2.4GHz ficará cada vez mais congestionada.

As companhias que queiram uma performance mais rápida agora podem não ter muitas escolhas, mas, para fazer upgrade, ou ampliam as redes existentes utilizando o padrão 802.11a, ou pressionam para que padrão 802.11g seja disponibilizado em breve.

8 Laboratórios WLAN

As atividades desenvolvidas e descritas neste capítulo contribuíram significativamente, na decisão final da Empresa X, para o encaminhamento dos assuntos descritos nos tópicos 1.2.1 e 1.2.2 deste trabalho. O capítulo está sub-dividido em tópicos, de acordo com a relação abaixo:

a) metas definidas pela Empresa X para alcançar os objetivos propostos;
b) características consideradas no processo de especificação tecnológica;
c) site survey;
d) laboratórios 802.11b e 802.11a, executados pelas Empresa X e Extremetech;
e) laboratório transferência de dados, executado pela empresa Extremetech;
f) dicas de configuração de segurança;
g) o que foi melhorado no processamento das informações na Empresa X.

8.1 Metas definidas para atingir os objetivos propostos

a) proceder uma análise teórica do estado da arte em sistemas *wireless LAN*;

b) analisar as ferramentas de monitoração disponíveis que suportem a simulação de ambientes *wireless* heterogêneos;

c) avaliar as soluções de HW e SW das Wireless LANs, disponíveis no mercado e, estar capacitado tecnicamente para a configuração de um ambiente de rede Wireless;

d) modelar e implementar um ambiente de simulação heterogêneo que possibilite avaliar o comportamento das conexões e, que verifique e ecoe pacotes de dados entre um coletor de dados wireless e um Access Point. Nesta troca de dados as funções de recuperação de erros do protocolo devem estar desativadas, de forma a permitir uma avaliação precisa das condições de comunicação.

e) simular as piores condições possíveis em termos de interferência à propagação de radiofreqüência, obtendo-se assim a melhor configuração indicada de antenas e rádio-bases;

f) analisar os resultados das simulações para auxiliar na especificação da solução mais compatível com a realidade do ambiente industrial da Empresa X;

g) estudar e testar os aspectos de segurança disponíveis.

8.2 Características consideradas no processo de especificação tecnológica

a) suporte ao padrão IEEE 802.11 (802.11a e 802.11b), considerando os aspectos de funcionamento descritos no capítulo anterior;

b) aprovar uma arquitetura de bridge, a qual possibilite caminhos de comunicação entre múltiplos segmentos de rede, sejam eles cabeados ou RF;

c) assegurar uma grande resistência a interferências. Foram consideradas a Rádio Freqüência Spread Spectrum por Direct Sequence e a OFDM;

d) suporte a ltas taxas de comunicação;

e) baixo consumo de energia, ou seja, suporte a modo de operação PSP (Power Save Polling) do padrão IEEE 802.11;

f) gerenciamento através de protocolo SNMP;

g) suporte a diversidade de antenas de radiofreqüência;

h) obtenção de tempos de resposta baixos;

i) suporte a um grande número de equipamentos (mais de 100); e

j) possibilidade de ampliação da capacidade do sistema pela adição de novos APs.

8.3 Site survey

Nos laboratórios que desenvolvemos, concluímos que neste tipo de rede faz-se necessária a realização de um site survey. Por este motivo, descreveremos as etapas para a execução de um correto site survey:

a) o primeiro passo é elaborar um plano descrevendo todas as etapas, usando um desenho detalhado da localização.

b) o administrador da rede necessita ter em mãos as seguintes informações sobre o local onde a rede wireless será instalada:

b.1) localização de possíveis fontes de interferência;

b.2) lay-out da rede cabeada, existente;

b.3) redes wireless em áreas próximas (potenciais fontes de interferência);

b.4) conhecer as exigências de rede dos usuários, tais como largura de banda, localizações e necessidades de roaming.

8.3.1 Materiais recomendados:

a) deesenho detalhado da localização;

b) vários Access Points (os que serão configurados no local);

c) um notebook com o software utilitário cliente e com um wireless PC card instalado;

d) wireless PC cards para todos os Access Points.

8.3.2 Fase de planejamento:

Uma vez que todos os requerimentos da rede são conhecidos, use os parâmetros de cobertura básicos para uma célula de rede wireless, e, na planta do site faça uma suposição quanto a onde colocar os Access Points. Esta suposição deverá levar em consideração:

a) áreas de cobertura – compreensão da área de cobertura ideal e área de cobertura atual (muito provavelmente serão diferente);

b) conectividade de Rede - deve estar distante no máximo 100 metros (328 pés) ou a conexão de rede deve ser extendida, com por exemplo o uso de um repetidor.

Após a conclusão do planejamento, instale os Access Points nos locais desejados. A opção teste de link, do software utilitário cliente, auxiliará na obtenção das informações necessárias, descritas logo abaixo, e requeridas para a verificação da área de cobertura da rede wireless:

a) relação Sinal-Ruído entre a estação e o Access Point;
b) taxa de dados entre a estação e o Access Point;
c) associação Access Point-estação.

8.3.3 Verificando a área de cobertura:

Com o laptot, lentamente inspecione a área de cobertura e verifique os níveis de operação da rede, usando a opção teste de link do software de gerenciamento cliente. Ajuste a localização do Access Point até alcançar a cobertura desejada.

Na planta do site, anote as seguintes informações:

a) fronteiras da célula wireless (quando o SNR atinge zero);
b) mudança da taxa de dados (alta, média, padrão, baixa).

8.3.4 Documentando o site survey:

a) com todas as informações documentadas na planta do site, a área de cobertura para a célula de wireless é agora conhecida;

b) compare a área de cobertura atual com a área de cobertura desejada, dando atenção especial à taxas de dados suportadas bem como aos requerimentos dos usuários;

c) mova o Access Point se necessário, e execute a inspeção do site novamente até que a requerida cobertura seja alcançada;

d) uma vez finalizada a inspeção da primeira célula, complete o processo nas demais células.

8.4 Laboratórios

Para comparar as tecnologias 802.11a e 802.11b, considerando as metas e as características propostas nos dois primeiros tópicos deste capítulo, foram utilizados:

a) notebooks configurados com Windows 2000 Professional;
b) APs 802.11a e 802.11b da Symbol, Cisco e Enterasys;
c) cartões de rádio wireless 802.11a e 802.11b da Symbol, Cisco e Enterasys.

Os APs, quando os testes desenvolveram-se no modo infra-estrutura, estavam conectados a rede LAN (cabeada) possibilitando o acesso das estações ao servidor Windows configurado com DHCP.

Inicialmente, alteramos o nome e a senha do user Admin, o SSID default dos equipamentos configurados e habilitamos o protocolo de encriptação WEP. Um completo site survey foi executado dentro de uma área de produção, determinando o número total de APs e suas localizações, considerando a desejada área de cobertura bem como as taxas de dados suportadas em todos os locais.

8.4.1 Laboratório 802.11b

No ambiente industrial da Empresa X enfrentamos situações adversas, devido a limitada largura de banda desta tecnologia, quando muitos operadores (aproximadamente 40) convergiam para uma mesma área da frente de carregamento. A taxa real de transferência dos arquivos de dados baixava para menos de 3Mbps. Constatamos que a altura das pilhas dos produtos armazenados e a interferência de outras redes industriais fazia com que o sistema retrocedesse para taxas inferiores (5.5Mbps em distâncias entre 20 e 30m e 2Mbps em distâncias entre 50 e 60m).

Nas áreas de maior consumo dos recursos da rede, foi-nos necessário adicionar mais pontos de acesso e atribuir canais a grupos de usuários, com o que melhoramos a performance da rede. No 802.11b está disponível a tecnologia de balanço de carga, para espalhar automaticamente a carga assim que um canal estiver começando a superlotar enquanto outros estejam disponíveis, isto não está disponível no 802.11a, ainda. Cinco canais de separação são requeridos para que não ocorra interferência entre canais numa área de cobertura, específica.

Teoricamente, o número de usuários suportados por um AP é 250. Entretanto, em nossos laboratórios constatamos que o número, razoável, de usuários para aplicações que trafegam arquivos de dados está entre 25 e 50.

Para obter melhor desempenho dos APs, limitamos a taxa de multicast, alteramos a configuração de full bridge para workgroup bridge e desabilitamos os protocolos que não são utilizados na rede da Empresa X. Com esta configuração obtivemos melhores resultados na transferência de arquivos de dados.

Configuramos 4 chaves de criptografia e definimos qual delas seria a padrão para proceder nas transmissões. O adptador de rede (NIC) dos notebooks também foi configurado com criptografia. É fundamental observar que:

a) a chave do AP usada para transmissão necessita ser configurada nas estações;

b) as chaves nas estações necessitam estar na mesma ordem do AP;

c) as chaves criptografadas devem ser alfanuméricas e são case sensitive;

d) uma estação, configurada com o conjunto de criptografia incorreto mesmo assim será capaz de associar-se com um AP.

O sinal 802.11b, com boa qualidade, extendeu-se de 35m a 80m (dependendo da altura das pilhas dos produtos) dentro dos prédios industriais, trafegando através das paredes e dos tetos, e acima de 300m à 500m fora dos prédios. Sugerimos a execução dos seguintes procedimentos nos casos em que ocorrerem problemas com o link de comunicação wireless:

a) verifique se o link está ativo;

b) execute um site survey;

c) indique qual velocidade o link suporta para uma data localização;

d) localize fontes de interferência. Interferências reduzem a área de cobertura, degradam a performance, perdem pacotes os quais precisam ser retransmitidos.

Nos laboratórios desenvolvidos, constatamos que quando os equipamentos retrocediam para taxas inferiores, os motivos sempre foram os mesmos:

a) fatores como quantidade e presença de paredes, equipamentos de metal e altura das pilhas dos produtos;

b) as distâncias entre notebooks/coletores de dados e APs;

c) equipamentos e/ou materiais geradores de interferência;

d) os modelos dos computadores e os sistemas operacionais usados.

Quando a qualidade do sinal cai para níveis inaceitáveis (10db, com auto-ajuste das taxas), o sistema automaticamente retrocederá para a próxima velocidade. Isto se faz necessário para suportar a taxa de dados que está sendo usada. Assim sendo, operar numa taxa de dados inferior faz com que o sistema porte-se melhor, onde há qualidade de sinal pobre. Após 10 transmissões consecutivas com sucesso, a estação tentará transmitir na velocidade imediatamente superior e se tiver sucesso, mudará a velocidade de operação. Uma dica importante relacionada a este assunto é que você precisa comparar tecnologias usando os mesmos computadores, nos mesmos locais e as mesmas aplicações.

Nosso maior interesse, nos testes de performance no modo infra-estrutura, consistia em saber quanto tempo levaríamos para transferir pastas com 10MB, 50MB e 100MB entre dois computadores usando as tecnologias 802.11a e 802.11b. Para dentro das pastas copiamos arquivos MP3 de 10MB, 50MB, e 100MB. Em todos os casos, a performance da tecnologia 802.11a foi de 3 a 4 vezes superior.

Para testar o throughput máximo no modo Ad-Hoc colocamos dois notebooks com os cartões wireless separados por 1,65m. Executamos cada teste pelo menos duas vezes para obter resultados consistentes e então achar o tempo médio para cada transfência de diferentes pastas de dados. Também testamos o desempenho numa distância moderada, movendo um dos notebooks para uma distância aproximada de 13m. Não houveram alterações significativas quando comparadas ao modo infra-estrutura, sendo que a tecnologia 802.11b teve um throughput máximo entre 4 a 7Mbps e a tecnologia 802.11a entre 23 e 26Mbps, dependendo da distância dos noteobooks.

É importante destacarmos que as aplicações que necessitam maior largura de banda (tráfego multimídia, por exemplo), rapidamente esgotaram o throughput da rede 802.11b, chegando inclusive a não serem inicializadas. Para finalizar os testes com esta tecnologia, procuramos acessar um vídeo remotamente, e obtivemos muitas dificuldades, pois o mesmo apresentou pausas, alterações no áudio (espaçado) e por fim desistimos.

8.4.2 Laboratório 802.11a

Como argumentos favoráveis a tecnologia 802.11a destacamos a velocidade total, a capacidade média de transferência e a inexistência de conflito no que diz respeito a largura de banda porque as duas tecnologias usam partes muito diferentes do spectrum de rádio.

Configuramos os drivers dos cartões para baixarem para taxas mais lentas quando a potência do sinal diminuia, e tudo funcionou corretamente.

Ajustamos cada ponto de acesso 802.11a para acessar um canal de cada vez e atribuímos os canais específicos aos usuários associados aos APs. Com esta configuração obtivemos maior largura de banda disponível (33Mbps) pois a disputa pela largura de banda diminuiu e conseguimos suportar mais usuários (aumentou de 45 para 55).

Nos laboratórios que desenvolvemos, investigamos as seguintes expectativas prometidas da tecnologia 5GHz:

a) medimos a performance 802.11a de acordo com configurações similares ou idênticas as do 802.11b, e constatamos que há ganhos significativos de performance.

b) testamos o throughput puro (foi medido pelo tempo requerido para transferir arquivos grandes) e a capacidade de tráfego multimídia (trailers de filmes DVD não criptografados e vídeos de música). Basicamente nós assistimos e escutamos o playback tocar sem pausas, saltos, ou travamento.

c) na medição do throughput, avaliamos a performance na distância máxima e a performance relativa para distâncias diferentes na modalidade Ad-Hoc.

d) testamos também a performance da rede wireless-to-wireless e wireless-to-wired PC no modo infra-estrutura usando um ponto de acesso;

e) para o throughput e testes multimídia, nós observamos, também, a capacidade da tecnologia de manter um link de rede enquanto os notebook foram movidos dentro das dependências do escritório e para os diferentes pavimentos no edifício.

Os resultados dos testes com o modo 2X/turbo não foram consistentes, ocorreram erros com os cartões de rede wireless. Ao consultar os fornecedores obtivemos a resposta que isto estava acontecendo (junho de 2002) porque seus drivers estavam ainda em desenvolvimento.

Ao concluirmos nossa primeira análise da tecnologia 802.11a, obtivemos amplas evidências favoráveis a adoção desta tecnologia. Procuramos desenvolver o mesmo laboratório desenvolvido pela empresa Extremetech (laboratório transferência de dados) e não foi-nos possível, pois no momento, setembro/2002, a tecnologia estava sendo disponibilizada pelos fabricantes e ainda existiam dificuldades no que se refere a configuração dos drivers (estava na versão beta) das estações.

8.5 Laboratório Transferência de dados

As informações contidas neste tópico (planilhas, gráficos e comentários) são o resultado da análise, destas duas tecnologias, desenvolvida e fornecida pela empresa norte-americana Extremetech.

TABELA 8.1 – Transferência de dados – Ad-Hoc e Infra-estrutura

802.11a vs 802.11b Transferência de Dados

	Modo Ad-Hoc - wireless to wireless						Modo infraestrutura - wireless to wireless			Modo infraestrutura - wireless to wired Ethernet		
	1,65m			13m								
	10MB	50MB	100MB	10MB	50MB	100MB	10MB	50MB	100MB	10MB	50MB	100MB
Proxim 802.11a PC Cards (média/ segundos)	**4,9**	**21,2**	**42,6**	**7,4**	**33,7**	**93,7**	**8,7**	**40,4**	**80,2**	**5**	**21,7**	**43,2**
Referência 802.11b PC Cards (media/ segundos)	**19,8**	**99,3**	**196,9**	**19,1**	**94,3**	**196,6**	**36,1**	**177,2**	**353,7**	**18,9**	**91,7**	**183,6**
Velocidade relativa (quantas vezes 802.11a foi mais rápido que 802.11b?)												

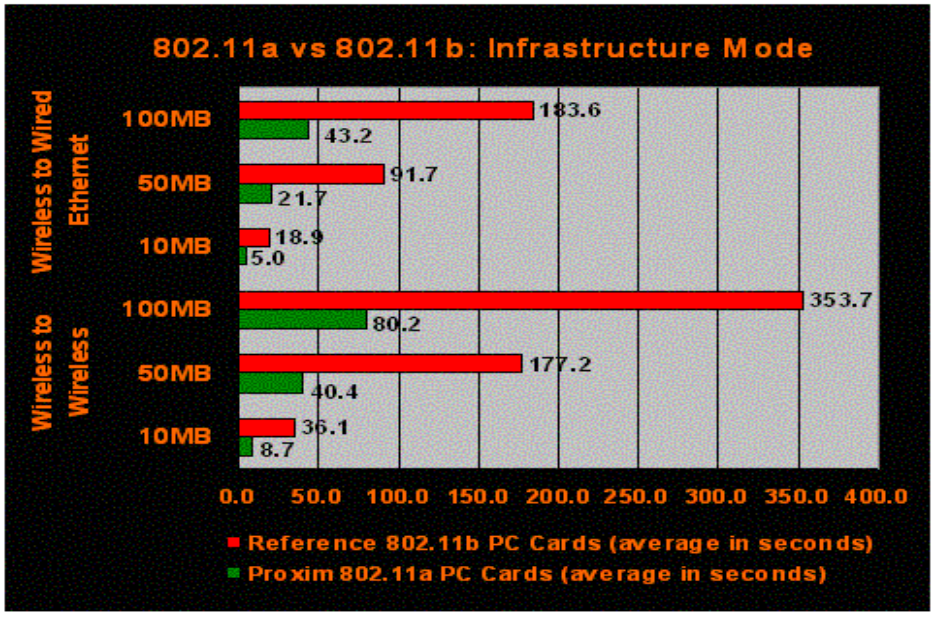

FIGURA 8.1 – 80.211a vs 802.11b: Modo Infra-estrutura

TABELA 8.2a – 802.11a vs802.11b Transferência de Dados

802.11a vs 802.11b Transferência de Dados

		Ad-Hoc - wireless to wireless								
		1X – 1,65m			1X – 13m			2X – 1,65m		
		10MB	50MB	100MB	10MB	50MB	100MB	10MB	50MB	100MB
802.11a		Todos os tempos são medidos em segundos								
Actiontec	Teste 1	5,9	25,7	48,8	4,8	26,9	62	3,7	17	34,5
(beta)	Teste 2	5,7	27,7	46,8	4	30,7	66	3,8	16,5	33,2
	Média	**5,8**	**26,7**	**47,8**	**4,4**	**28,8**	**64**	**3,8**	**16,8**	**33,9**
Atheros	Teste 1	6,2	23	46,7	11,2	47,5	99,4	3,8	17	34,8
(beta)	Teste 2	5,1	23	46,4	11,2	42	96	4,1	15,5	31
	Média	**5,7**	**23**	**46,6**	**11,2**	**44,8**	**97,7**	**4**	**16,3**	**32,9**
Proxim	Teste 1	5,02	21,4	42,24	7,25	31,1	92,44	6,23	27,2	60,7
	Teste 2	4,72	21,06	42,9	7,59	36,3	95,04	6,2	37,8	53,4
	Média	**4,9**	**21,2**	**42,6**	**7,4**	**33,7**	**93,7**	**6,2**	**32,5**	**57,1**
TDK	Teste 1	6,5	22,7	43,5	50,4	96	209	5,9	20,7	44,9
(beta)	Teste 2	5,6	23,2	42,4	46	156	195	4,5	20	53
	Média	**6,1**	**23**	**43**	**48,2**	**126**	**202**	**5,2**	**20,4**	**49**
	Média para 802.11a	**5,6**	**23,5**	**45**	**17,8**	**58,3**	**114,4**	**4,8**	**21,5**	**43,2**
802.11b										
Actiontec	Teste 1	19,9	101	202	20,3	101	202,5	N/A	N/A	N/A
(beta)	Teste 2	20	101	201	20,58	101	210	N/A	N/A	N/A
	Média	**20**	**101**	**201,5**	**20,4**	**101**	**206,3**	N/A	N/A	N/A
Atheros	Teste 1	18,6	89	176,5	18,9	90	176	N/A	N/A	N/A
(beta)	Teste 2	18,2	88,8	176,8	17,5	82	188	N/A	N/A	N/A
	Média	**18,4**	**88,9**	**176,7**	**18,2**	**86**	**182**	N/A	N/A	N/A
Proxim	Teste 1	20,5	107	215	18,7	92	182	N/A	N/A	N/A
	Teste2	21,5	109	210	18,6	100	221	N/A	N/A	N/A
	Média	**21**	**108**	**212,5**	**18,7**	**96**	**201,5**	N/A	N/A	N/A
	Média para 802.11b	**19,8**	**99,3**	**196,9**	**19,1**	**94,3**	**196,6**	N/A	N/A	N/A

TABELA 8.2b– 802.11a vs 802.11b Transferência de Dados (cont.)
Considerar como se estivesse a direita da (tabela 8.2.a)

802.11a vs 802.11b Transferência de Dados

		Ad-Hoc wireless to wireless			Infraestrutura - wireless to wireless			Infraestrutura - wireless to Ethernet		
		2X 13m			1X 1,65m			1X 1,65m		
		10MB	50MB	100MB	10MB	50MB	100MB	10MB	50MB	100MB
802.11a										
Actiontec	Teste 1	3,7	16,4	33,4	9,4	40,8	81,8	5,1	22,5	44,7
(beta)	Teste 2	3,5	15,4	30,7	8,7	40,9	80,7	4,6	22,2	45
	Média	**3,6**	**15,9**	**32,1**	**9,1**	**40,9**	**81,3**	**4,9**	**22,4**	**44,9**
Atheros	Teste 1	8	17,9	42,3	8,3	39	74,6	4,5	21,9	43,7
(beta)	Teste 2	10,5	21,4	44,4	7,5	36,8	73,7	4,1	21,4	42,7
	Média	**9,3**	**19,7**	**43,4**	**7,9**	**37,9**	**74,2**	**4,3**	**21,7**	**43,2**
Proxim	Teste 1	10,1	42,3	68,1	9,5	40,9	80,1	5,2	21,9	43,7
	Teste 2	8,4	39,5	48,5	7,9	39,8	80,3	4,7	21,4	42,7
	Média	**9,3**	**40,9**	**58,3**	**8,7**	**40,4**	**80,2**	**5**	**21,7**	**43,2**
TDK	Teste 1	não pode ser			8,9	39,6	78,9	5,9	22,1	43,5
(beta)	Teste 2	completado			8,5	39,1	78,6	4,6	21,5	42,6
	Média				**8,7**	**39,4**	**78,8**	**5,3**	**21,8**	**43,1**
	Média para 802.11a	**7,4**	**25,5**	**44,6**	**8,6**	**39,6**	**78,6**	**4,8**	**21,9**	**43,6**
802.11b										
Actiontec	Teste 1	N/A	N/A	N/A	35,9	176,6	342,8	18,7	90,8	181
	Teste 2	N/A	N/A	N/A	34,5	172,6	352,1	18,1	90,1	180
	Média	**N/A**	**N/A**	**N/A**	**35,2**	**174,6**	**347,5**	**18,4**	**90,5**	**180,5**

Não foram feitos testes, com o modo 2X ou turbo, no modo infra-estrutura pois não tínhamos nenhum cartão 802.11a para associar com o AP quando setamos o modo de alta velocidade. Porque os drivers de alta velocidade ainda estavam em desenvolvimento e também porque cada fabricante pode alterar a maneira de trabalhar com o modo de alta velocidade.

Observando os números acima conclui-se, que a performance dos cartões 11a e 11b são relativamente consistentes no modo Ad-Hoc (pelo menos no modo 1X em 1,65m), mas observa-se maior variação no modo 2X em distâncias mais longas. É também importante observar que os três pares de cartões 802.11b tiveram performance razoavelmente consistente. Note que não há nenhum teste 2X para 802.11b porque a especificação não tem tal modo.

Os resultados dos testes foram os seguintes:

a) em distâncias próximas (1,65m) 802.11a foi quatro vezes melhor que a velocidade do 802.11b;

b) em distâncias moderadas (13m) 802.11a foi aproximadamente 2,5 vezes mais rápido que 802.11b;

c) transferência de dados entre dois notebooks wireless-to-wireless é mais rápida no modo Ad-Hoc que no modo infra-estrutura para ambas as tecnologias: 802.11a e 802.11b;

d) transferência de dados para clientes wireless-to-wired no modo infra-estrutura foi mais rápido que transferência de dados wireless-to-wireless fig (8.1), e quase igual para transferência Ad-Hoc wireless-to-wireless (fig 8.2).

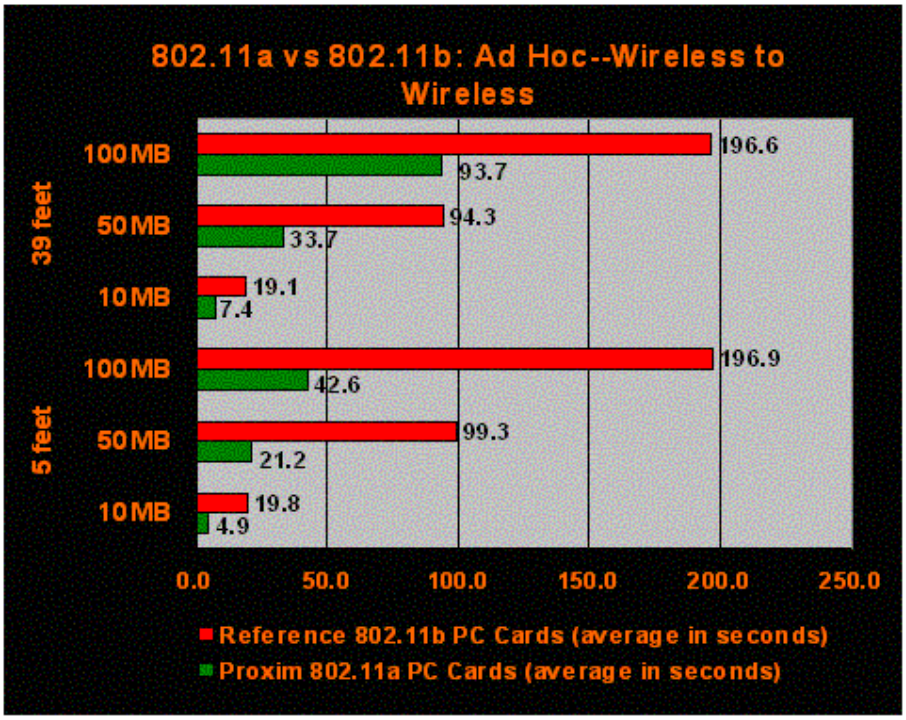

FIGURA 8.2 – 802.11a vs 802.11b: Ad-Hoc – Wireless to Wireless

No laboratório transferência de vídeo multimídia, as diferenças entre 802.11b e 802.11a foram consideráveis. Colocamos os notebooks distantes 1,65m e 13m nos modos Ad-Hoc e infra-estrutura quando trafegando vídeo entre eles. Na tecnologia 802.11b o conteúdo do tráfego DVD via mídia 802.11b foi picado e quebrado. Ocorreram muitas pausas de audio e vídeo, mesmo quando consideramos que as condições eram ótimas (1,65m de distância entre os notebooks e nenhum outro tráfego) a experiência foi terrível. Com a tecnologia 802.11a, entretanto, o conteúdo de tráfego DVD foi satisfatório - embora não perfeito – de modo que foi possível apreciar assistir a um filme.

Com o objetivo de avaliar a área de cobertura da rede, instalamos os APs para ambas as tecnologias no meio do pavilhão atrás da parede e, movemos idênticos notebooks (um com um cartão 802.11b e o outro com um cartão 802.11a) para vários locais e ao redor de nosso escritório (caminhamos para fora do prédio).

Sendo que a freqüência 5GHz da tecnologia 802.11a tem uma onda de rádio mais curta do que 2.4GHz 802.11b, esperávamos que o alcance para 802.11b fosse visivelmente superior, mas ficou provado não ser o caso.

Abrimos o Internet Explorer para surfar na web e usamos o Windows Explorer para procurar novos sub-diretórios nas várias máquinas de nossa rede.

Conseguimos manter uma conexão de rede externa, na frente do prédio - 3,5m à 7m, outra vez com níveis quase iguais para ambas as redes. Note que porque os APs foram colocados no primeiro piso do prédio, a taxa externa foi maior. Caso a colocação dos APs tivesse sido no porão, isto significaria que quando fossemos para a frente do prédio os sinais teriam que passar através das paredes, tetos, concreto, e terra.

Nós não executamos testes de transferência em todos os locais mas, achamos que quando nos movíamos para próximo dos diferentes compartimentos tanto do primeiro como do segundo piso do prédio, que normalmente, em todos os lugares onde podíamos iniciar uma boa conexão com 802.11b também podíamos nos conectar com o 802.11a.

8.6 Configuração de segurança wireless

Para invadir uma WLAN faz-se necessário conhecer a freqüência de banda, o nome da rede e as chaves de criptografia.

Primeiramente, você deve controlar quem têm acesso a rede – autenticação - e então proteger a informação que está trafegando – encriptação [COM 2002].

O WEP com chave de 40 bits, considerado um esquema de segurança fraco, foi o primeiro sistema de criptografia wireless (RC4). Seus principais problemas são:

a) escalabilidade - não pode ser "escalado" para grandes corporações;

b) gerenciamento - não existe distribuição de chaves, falta um esquema de autenticação e não há como prever "seqüestro" de conexão (kidnapping/spoofing).

Por este motivo as empresas viram-se forçadas a adotar medidas de segurança para proteger suas WLANs.

A (figura 8.3) apresenta a pilha de protocolos WLAN e a segurança:

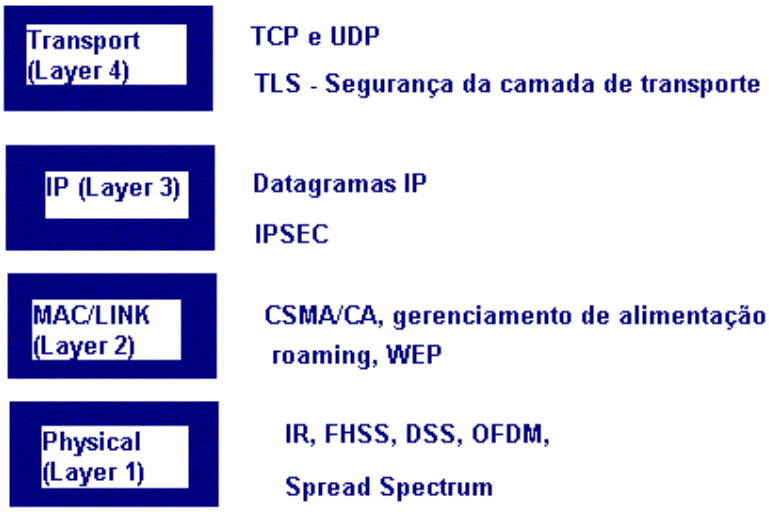

FIGURA 8.3 – pilha do protocolo WLAN e a segurança

As principais medidas de segurança recomendadas pela Symbol e que foram adotadas pela Empresa X, são:

a) adoção dos mesmos padrões de VPN's;

b) autenticação com Kerberos/EAP/TLS ou Radius (gerenciadores de autenticação);

c) autenticação mútua de *todos* os agentes da rede;

d) ACLs (Listas de Controle de Acesso) as quais liberam o acesso a rede somente para os MAC registrados;

e) criptografia TKIP/SSN, Keyguard (MCM ou PCM) e WEP 128 RC4-128.

O WEP com chave de 128 bits é um sistema de criptografia aprimorado, que já tem sua implementação corrigida para evitar nova "quebra" com revisão para algorítmo RC4-128.

Com a implementação do Kerberos - gerenciador de chaves e autenticação - todos os equipamentos da rede necessitam autenticar-se num servidor (KDC) o qual gerencia o processo de distribuição e validade de chaves de uso único e com tempo de vida curto.

8.6.1 Evolução da segurança:

1ª geração
a) SSID único para cada cliente/site;
b) quem não tinha o SSID não conseguia se conectar à WLAN;
c) lista de controle de Acessos MAC (ACL).

2ª geração
IEEE 802.11 Wired Equivalent Privacy (WEP), com encriptação 40 bits RC4.
Funcionamento do WEP:
Padrão IEEE 802.11 de 1999 dividido em duas partes:
a) autenticação: (que garante o controle de acesso)
a.1) sistema aberto – autenticação sem chave - (somente ESSID);
a.2) chave compartilhada – autenticação com uma chave secreta compartilhada globalmente;
b) encriptação: "por pacote": para garantir a privacidade dos dados.

3ª geração
a) métodos para autenticação;
b) novas criptografias, chaves descartáveis;
c) técnicas iguais às de VPN;
d) IEEE 802.11e (IEEE Task Group e).

IEEE Task Group "e" – aprimorando a segurança:
O IEEE e as indústrias de Wireless participantes definiram a questão da segurança para os padrões 802.11. Enfocaram as fraquezas existentes na autenticação, gerenciamento de chaves e criptografia. A última geração de WLANs utiliza protocolos conhecidos e já existentes, tais como descritos os abaixo:
a) 802.1x (segurança de portas);
b) EAP (Extensible Authentication Protocol)*;*
c) Kerberos ou RADIUS (gerência de autenticação).

Benefícios do Task Group "e" de segurança:
a) distribuição de chaves por link que é o oposto de chaves globais compartilhadas;
b) gerência de chaves através do Kerberos;
c) propicia a distribuição remota de chaves, de duas maneiras:
c.1) autenticação mútua
- da estação movel para o AP e do AP para a estação movel;
- evita ataques tipo "espião no meio" e AP no estacionamento (Rogue AP).

c.2) níveis aperfeiçoados de encriptação
- larger initialization vector (128-bits);
- sequência numérica, evitando repetições;
- campos de hash/autenticação evitando desordenamento;
- novos algorítimos de criptografia (opcionais).

8.6.2 Opções atuais de segurança:

camada 2 ISO (Link) - 802.11 WEP
a) 64 Bits;
b) 128 bits (implementação dos fabricantes).

camadas 3/4 – segurança "end to end"

a) VPNs – IPSec;
b) SSL/TLS;
c) Kerberos (KDC).

Esquematização do EAP:

EAP proporciona uma ponte flexível de ligação a esquemas de segurança. Atualmente, dispomos de métodos EAP baseados nos padrões IETF

a) protocolo de "encapsulamento";
b) sem dependência do protocolo IP;
c) ACK/NAK, sem "windowing";
d) sem suporte a fragmentação;
e) poucas pressuposições na camada "link";
f) pode "rodar" sobre qualquer protocolo da camada "link" (PPP, 802., etc);
g) não assume que o link é fisicamente seguro;
h) são usados "métodos" para obter o link de segurança;
i) assume que não precisa reordenamento de pacotes;
j) pode "rodar" sobre mídias com ou sem perdas de pacotes;
k) responsabilidade pela retransmissão é do "autenticador" (desnecessário para 802.1x ou 802.11);

(TLS) Segurança na Camada de Transporte (suportada no Windows 2000)

a) GSS_API (incluindo Kerberos Server)

Autenticação kerberos:

a) desenvolvido pelo MIT – Projeto Athena;
b) baseado em padronização (V5.0);
c) suportado no Windows 2000, Linux, Unix;
d) modelo client/server que se ajusta às atuais redes corporativas;
e) proporciona autenticação mútua de todos os agentes;
f) troca de chave por sessão, absolutamente segura
f.1) chaves "descartáveis", uso único e com duração curta;
g) encriptação rápida com chaves secretas compartilhadas versus chaves globais compartilhadas;
h) roaming seguro, sem comprometer mobilidade
h.1) usuários são pré-autenticados com o AP;
i) ganho principal: mantém mobilidade com o mais alto nível de segurança.

8.6.3 Resumo de segurança wireless:

a) os padrões 802.11 requerem atenção cuidadosa aos mecanismos de segurança;
b) os atuais padrões IEEE oferecem boa segurança com WEP 128 e ACL's
b.1) tem que ser especificamente habilitado;
b.2) tem que ser RC4-128;
c) maiores níveis de segurança são atingidos com protocolos de maior nível na camada ISO. Kerberos e IPSec são exemplos;
d) o IEEE já resolveu e ainda está evoluindo na solução dos problemas do WEP (Ex: RC4-128);

e) os fabricantes oferecem soluções de segurança adicionais (ex. Kerberos KDC, RADIUS) [COM 2002].

Unifique sua política de segurança

A segurança para as redes wireless não requer uma infra-estrutura separada com procedimentos e protocolos diferentes. Desenvolva uma política de segurança que abranja ambas as redes (sem fio e cabeada) para alavancar o gerenciamento e as vantagens de custo. Por exemplo, integre a requisição de identificação de usuário e senha para os usuários que estão acessando a rede, através de sua infra-estrutura cabeada ou wireless.

Regras gerais de acesso a serviços:

a) não confie em qualquer nó sem que ele prove quem é;
b) uma vez provado para mim quem você é, eu também tenho que provar quem sou;
c) após nos reconhecermos, aí sim, podemos "conversar".

8.7 O que foi melhorado no processamento das informações

Foi configurada uma rede wireless LAN, complementar a rede local cabeada, utilizando-se de equipamentos adquiridos da Symbol e da Enterasys. Ambas as redes – cabeada e sem fio - estão interligadas, possibilitando a atualização das bases de dados SQL, a impressão do código de barras nas etiquetas, o carregamento dos produtos através de coletores de dados móveis e a mobilidade das estações de trabalho (chamadas pontos de visão do processo).

Com esta implementação, garantimos que nenhum produto será carregado sem estar com a sua especificação técnica correta. Através do coletor de dados, o operador faz a busca na base de dados do servidor dos itens a serem carregados para aquela ordem de embarque; lê o código do produto na etiqueta do produto conferindo-o na base de dados SQL, e somente após este procedimento carrega os produtos no caminhão. Neste momento, o estoque e os demais sistemas residentes nos servidores da empresa são atualizados.

A redução do tempo de permanência dos caminhões na unidade foi alcançada eliminando-se as pesagens intermediárias. O caminhão retorna a balança da Expedição somente para pesar o peso bruto final, passar por uma rápida conferência e ter a nota fiscal e o certificado de qualidade emitidos.

Além do processo de carregamento, a gestão da permanência dos caminhões na unidade também é auxiliada pelo módulo de monitoração do carregamento, que informa em tempo real, como está avançando o processo de carregamento.

A rastreabilidade dos produtos é melhorada com o SIP, pois o número do lote (principal instrumento de rastreabilidade) é automaticamente impresso nas etiquetas e nos códigos de barras.

Na área de produção ***Y*** o número do lote que será produzido é informado no módulo de identificação do SIP e nos processos seguintes (áreas de produção ***V, W*** e ***Z***), a etiqueta da peça que entra para ser processada é lida e o número do lote é obtido e automaticamente impresso nas peças produzidas.

Outro instrumento auxiliar de rastreabilidade é o número de série que fornece uma identidade única para cada peça, permitindo obter-se diversas informações sobre o processo de produção.

Um segundo motivo, fez com que a Empresa X aprovasse a implementação de redes wireless LAN: há diversos pontos nas unidades onde não é possível a instalação de cabeamento devido a existência de equipamentos que estão indisponíveis por pouco tempo,

para rápidas manutenções e com alto grau de periculosidade. Nestes locais estão sendo configurados APs e estações notebook e/ou desktop wireless.

Recentemente, uma terceira meta foi proposta: implementar uma rede wireless LAN no ambiente administrativo das unidades industriais e nas filiais da Empresa X. Para tal finalidade, um projeto piloto será desenvolvido na área de Informática corporativa, utilizando-se da tecnologia 802.11a, assim que todos os componentes desta tecnologia estiverem disponíveis no mercado.

9 Conclusão

As wireless LANs, que são uma nova opção de configuração de redes, propiciam a seus usuários acesso as informações compartilhadas em qualquer local dentro de sua área de cobertura.

Assim como acontece com todas as novas tecnologias, o crescimento da computação movel também enfrenta desafios. No campo dos desafios técnicos, um dos principais é a capacidade de armazenamento de energia - ainda pequena - dos equipamentos disponíveis. Outro desafio é a confiabilidade da utilização da computação sem fio em operações que requerem elevado grau de segurança, sendo que as informações são transmitidas pelo ar através de ondas eletro-magnéticas. Enfim, requer-se um sistema onde o processamento portátil de transações *on-line* e a passagem transparente das unidades móveis entre as células de rádio (*seamless roaming*).

O projeto de uma rede movel tem que considerar três aspectos básicos, porém, de suma importância: a localização das estações de rádio, a alocação de freqüências e a propagação de sinais. Definida a infra-estrutura, outros dois aspectos necessitam ser considerados: o rastreamento de usuários e o gerenciamento de energia.

A definição final da localização das unidades móveis deve ocorrer após a execução de um detalhado site survey. Faz-se necessário destacar que sempre que for estabelecida uma comunicação com uma determina estação, o sistema precisará determinar qual dos APs será utilizado para a conexão. Portanto é imprescendível organizar e/ou agrupar as células de forma a facilitar a localização, definir com que freqüência as unidades móveis enviam mensagens para os APs informando-os de sua localização atual, e, conhecer quais algoritmos podem ser utilizados para localizar com mais eficiência a célula em que se encontra o usuário.

A implementação, inicial, de uma rede Wireless não é tudo. Por este motivo, planejar antecipadamente as mudanças na rede (lay-out, alteração nas aplicações, população usuária, ...) possibilitando identificar e controlar os fatores que impactam a qualidade de serviços oferecidos, exigem atividades específicas de gerência da rede que se somam ao projeto da implementação da rede.

O gerenciamento das wireless LANs facilmente é integrado aos sistemas de gerenciamento de redes das empresas - para esta finalidade, basta habilitar o protocolo SNMP nos APs. As redes wireless LANs suportam, também, os principais tipos de protocolos em frames Ethernet IEEE-802-3 (TCP/IP, IPX, NetBEUI).

A tecnologia 802.11a é muito mais rápida que a 802.11b, com uma taxa de dados máxima de 54Mbps (atualmente crescendo para 72Mbps ou 108Mbps num não padronizado modo de velocidade dupla, dependendo dos fabricantes), e o seu padrão de interoperabilidade, Wi-Fi5, opera na faixa de freqüência 5GHz, possibilitando a utilização de oito canais simultâneos.

Uma grande desvantagem da tecnologia 802.11b em relação a 802.11a é que ela opera na freqüência 2.4GHz, a qual está cada vez mais congestionada. O crescente uso de telefones wireless a 2.4GHz e dispositivos Bluetooth estão aglutinando o spectrum de rádio dentro de sua faixa e decrementando significativamente a performance das redes 802.11b.

Uma desvantagem da tecnologia 802.11a em relação a 802.11b é que ela está disponível somente na metade da largura de banda no Japão (para um máximo de quatro canais) e não foi aprovado para uso na Europa, onde HiperLAN2 é o padrão. Um outro grupo do IEEE, 802.11h, está trabalhando na especificação de uma tecnologia que possibilitará 802.11a trabalhar perto de alguns canais 5GHz usados pelas forças armadas na Europa.

Existindo a necessidade de desempenho mais elevado, ou seja, se for necessário suportar aplicações mais pesadas como vídeo, voz, e transmissão de imagens grandes e arquivos, opte pela tecnologia 802.11a. A tecnologia 802.11b provavelmente não será capaz de suportá-las.

Para os casos onde os usuários finais estejam densamente concentrados, como por exemplo aeroportos e centros de convenções, e competindo pelo mesmo ponto de acesso, o uso da tecnologia 802.11a irá remanejar uma maior concentração de usuários finais oferecendo uma maior largura de banda total.

Atualmente, os fornecedores estão preocupados em disponibilizar uma solução, única, que seja compatível com as duas tecnologias. Para solucionar este impasse, recomendamos que nos casos em que as duas tecnologias co-existam que ambos os APs (802.11a e 802.11b) sejam conectados num switch (preferencialmente) ou num hub da sua rede e ambas as tecnologias trabalharão juntas.

O completo automatismo do processo de carregamento dos caminhões nas *frentes de carregamento* – possibilitando que todos os itens a serem carregados sejam transmitidos para coletores de dados, móveis, por meio de redes wireless LAN, e que todas as etiquetas das peças a serem carregadas sejam lidas e as informações obtidas sejam transmitidas para o módulo de Carregamento do SIP, que as envia para o SAP R/3 - aguardado pelo conselho diretor da Empresa X, foi plenamente alcançado.

A Empresa X implementou e aprovou o uso de redes wireless. Entendemos, também, que não há nenhuma dúvida que as redes wireless de alta velocidade estejam chegando rapidamente.

Bibliografia

[COM 2002] COMEAU, Bruce. **Channel Viewpoint. Top 10 wireless security.** Disponível em: <http://w2knews.com/rd/rd.cfm?id=020624TB-WLAN_Security>. Acesso em: 20 jan. 2002.

[DOR 2000] DORNAN, Andy. **The Essential Guide to Wireless Communications Application.** New York: Prentice-Hall Computers Books, 2000.

[ELL 2001] ELLISON, Craig. **Exploiting and Protecting 802.11b Wireless Networks.** Disponível em: <http://extremetech.com/article2/0,3973,13084,00.asp>. Acesso em: set. 2001.

[GEI 2001] GEIER, Jim. **Wireless LANs:** Implementing High-Performance IEEE 802.11 Networks. New York: Sams, 2001.

[IEE 99] IEEE. **High Rate, direct sequence spread spectrum PHY specification Spread Spectrum Scene Online,** Std. 802.11-1999. Piscataway, 1999.

[IEE 97] IEEE. **Higher-Speed Physical Layer Extension in the 2.4 GHz Band,** Std. 802.11-1997. Piscataway, 1997.

[IEE 99a] IEEE. **FH PHY interoperability with the High Rate PHY,** Std. 802.11-1999. Piscataway, 1999.

[KOL 2001] KOLESKI, Fábio. Paging: o remédio veio tarde. **Revista TELETIME**. Disponível em: <http://teletime.com.br/revista/30/paging.htm>. Acesso em: mar. 2001.

[LIN 2001] LIN, Yi-Bing; CHLAMTAC, Imrich. **Wireless and Mobile Network Architectures.** [S. l.]: John Wiley & Sons, 2001. 532p.

[RAP 95] RAPPAPORT, Theodore. S. **Wireless Communications (Principles & Practice).** [S. l.]: IEEE Press: Prentice Hall PTR, 1996. 638p.

[SCH 2000] SCHILLER, Jochen H. **Mobile Communications.** Harlow: Addison-Wesley, 2000. 394p.

[SOU 2000] SOUZA, Lindenberg Barros de. **Redes de Computadores:** dados, voz e imagem. São Paulo: Érica, 2000. p. 407-422.

[IEE 99b] IEEE. **Spreading sequences and modulation for CCK modulation at 1, 2, 5.5 and 11 Mbit/s,** Std. 802.11-1999. Piscataway, 1999.

[ISO 99] ISO/IEC. **Wireless LAN Medium Access Control and Physical Layer Specifications,** Std. 802.11-1999. Piscataway, 1999.

[ANS 99] ANSI/IEEE. **Supplement to ANSI/IEEE Std. 802.11,** Std. 802.11-1999**.** Piscataway, 1999.

[WLA 2001] WLANA. **What is a Wireless LAN?** Disponível em: <http://wlana.com/learn/educate.htm>. Acesso em: nov. 2001.

[SPI 97] THE SPIN Model Checker. **IEEE Transactions on Software Engineering,** New York, v. 23, n. 5, p. 279-295, May 1997.

[TRE 99] TRETMANS, Jan; WIJBRANS, Klaas; CHAUDRON, Michel. Software Engineering with Formal Methods: the Development of a Storm Surge Barrier Control System – Seven Myths of Formal Methods Revisited. **Formal Aspects of Computing:** the International Journal of Formal Methods, [S.l.], v. 10, n. 5/6, 1998. Trabalho apresentado no ERCIM Workshop on Formal Methods for Industrial Critical Systems, 1999.

[VIC 2002] VICOMSOFT. **KnowledgeShare – White Papers.** Disponível em: http://vicomsoft.com/knowledge/reference/wireless1.html. Acesso em: jul. 2002.