

PAULO ALEXANDRE SERRA COUCELLO DA FONSECA

**CONSIDERAÇÕES SOBRE LANS E WLANS: UMA
PROPOSTA PARA UM CENTRO CULTURAL**

PORTO VELHO - RO

2001

**UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA
COMPUTAÇÃO**

PAULO ALEXANDRE SERRA COUCELLO DA FONSECA

**CONSIDERAÇÕES SOBRE LANS E WLANS: UMA PROPOSTA
PARA UM CENTRO CULTURAL**

Tese submetida à Universidade Federal de Santa Catarina como parte dos requisitos para a obtenção do grau de Mestre em Ciência da Computação.

Orientador: PROF. JOÃO BOSCO DA MOTA ALVES

PORTO VELHO, Fevereiro/2001.

CONSIDERAÇÕES SOBRE LANS E WLANS: UMA PROPOSTA PARA UM CENTRO CULTURAL

PAULO ALEXANDRE SERRA COUCELLO DA FONSECA

Esta Dissertação foi julgada adequada para a obtenção do título de Mestre em Ciência da Computação Área de Concentração de Sistemas de Computação e aprovada em sua forma final pelo Programa de Pós-Graduação em Ciência da Computação.

Prof. Fernando A. Ostuni Gauthier, Dr.

Banca Examinadora

Prof. Rogério Cid Bastos, Dr

Prof. João Bosco Da Mota Alves, Dr.

Prof. Luiz Fernando Jacintho Maia, Dr.

EPÍGRAFE

Nada se pode ensinar a um homem. Pode-se apenas ajudá-lo a descobrir coisas dentro de si, pois se ele não for melhor que hoje no dia de amanhã, então para que precisará de amanhã? Porque para que se faça grandes coisas não se deve estar acima dos homens mas junto deles.

Galilei, Rabbi Nahman de Brastav, Montesquieu

DEDICATÓRIA

À minha falecida mãe, D. Otilia, por toda a força, disposição e apoio que me deu em todas as fases de minha vida. Sem a força que ela me transmitiu não poderia ter ultrapassado mais este degrau em minha busca por conhecimento.

AGRADECIMENTOS

Meus agradecimentos à minha esposa Edilene, a meu filho Victor, ao meu amigo Jackson e família, e, por último, a todos aqueles que direta ou indiretamente me ajudaram a realizar esta etapa de minha vida.

Sumário

LISTA DE FIGURAS	XI
RESUMO	XII
ABSTRACT	XIII
CAPÍTULO 1 – INTRODUÇÃO	1
1.1 OBJETIVO DA DISSERTAÇÃO	1
1.2 ORGANIZAÇÃO DA DISSERTAÇÃO	2
CAPÍTULO 2 – REDES SEM FIO	3
2.1 HISTÓRIA DAS WLAN'S.....	4
2.2 URGÊNCIA PARA A NORMA IEEE 802.11.....	6
2.3 OBJETIVOS DAS WLANS.....	7
2.4 O NOVO PARADIGMA WIRELESS	8
2.5 POR QUE ESCOLHER REDES WIRELESS?.....	8
2.6 O NEGÓCIO PARA AS REDES WIRELESS	10
CAPÍTULO 3 - WLANS – O ASPECTO TECNOLÓGICO.....	12
3.1 TECNOLOGIAS DE DIFUSÃO DE ESPECTRO (SPREAD SPECTRUM)	12
3.2 CSMA/CA	15
3.3 ARQUITETURA WLAN	16
3.3.1 Conexões Ethernet.....	16
3.3.2 Células e Pontos de Acesso	16
3.3.3 Nós Escondidos	17
3.3.4 Células autônomas	18
3.3.5 Células acopladas	18
3.3.6 Multi-células.....	19
3.3.7 Roaming e Comutação.....	19
3.3.8 Pontes remotas (remote bridges).....	20
3.3.9 Conectividade com PC	20
3.3.10 Fontes de interferência.....	21
3.3.11 Outras considerações	21
CAPÍTULO 4 - IEEE 802.11: A NORMA PARA AS NOVAS REDES SEM FIO.....	23
4.1 MODELO DE ARQUITETURA BÁSICA DA IEEE 802.11	25
4.2 DESCRIÇÃO DA CAMADA IEEE 802.11.....	25
4.3 FRAGMENTAÇÃO E REMONTAGEM	27
4.4 ESPAÇAMENTO INTER-FRAMES (INTER FRAMES SPACING).....	28
4.5 BACK OFF EXPONENCIAL.....	30
4.6 COMO UMA ESTAÇÃO SE CONECTA	30
4.7 PROCESSO DE SINCRONIZAÇÃO.....	31
4.8 O PROCESSO DE AUTENTICAÇÃO	31
4.9 O PROCESSO DE ASSOCIAÇÃO.....	31
4.10 ROAMING	31
4.11 ESCUTA CLANDESTINA	32
4.12 ECONOMIA DE ENERGIA	33
4.13 ESTÁGIO ATUAL DA 802.11	33
4.14 CONCLUSÃO DO CAPÍTULO	33
CAPÍTULO 5 - BLUETOOTH	35
5.1 INTRODUÇÃO.....	35
5.2 SIG BLUETOOTH.....	36

5.3 PORQUÊ BLUETOOTH?	36
5.4 VISÃO DA ARQUITETURA BLUETOOTH	38
5.5 A ESTRATÉGIA DA ARQUITETURA BLUETOOTH	38
5.6 PERFIS E MODELOS DE UTILIZAÇÃO BLUETOOTH	40
5.6.1 GAP	41
5.6.2 SDAP	41
5.6.3 SPP	42
5.6.4 GOEP	42
5.7 MODELOS DE UTILIZAÇÃO BLUETOOTH	42
5.7.1 Transferência de Arquivos	43
5.7.2 Ponte para Internet (Internet Bridge)	43
5.7.3 Acesso a Redes Locais	43
5.7.4 Sincronização	43
5.7.5 Telefone três-em-um	44
5.7.6 Fone de ouvido	44
5.8 PROTOCOLOS CENTRAIS DO BLUETOOTH	45
5.8.1 Banda-base	45
5.8.2 Audio	45
5.8.3 HCI	45
5.8.4 LMP	46
5.8.5 L2CAP	46
5.8.6 SDP	47
5.9 PROTOCOLO DE SUBSTITUIÇÃO DE CABOS	47
5.9.1 RFCOMM	47
5.10 PROTOCOLO DE CONTROLE DE TELEFONIA	48
5.10.1 Controle Binário de Telefonia	48
5.10.2 Comandos AT - Controle de Telefonia	48
5.11 PROTOCOLOS ADOTADOS	48
5.11.1 PPP	49
5.11.2 TCP/UDP/IP	49
5.11.3 Protocolo OBEX	49
5.11.4 WAP	50
5.12 A INTERFACE AÉREA BLUETOOTH	50
5.12.1 A técnica de salto de frequência	51
5.12.2 Modulação/Transmissão e definição de pacote	52
5.12.3 Redes Bluetooth	53
5.12.4 Parâmetros de rádio	54
5.12.5 Tipos de link	55
5.12.6 Scatternet e Piconet	56
5.12.7 Estabelecendo conexões de rede	57
5.12.8 Modos de economizar energia	58
5.12.9 Scatternet	58
5.12.10 Segurança Bluetooth	59
5.13 PONTOS FORTES DO BLUETOOTH	60
5.14 O FUTURO PRÓXIMO DO BLUETOOTH	61
CAPÍTULO 6 - WAP	62
6.1 REQUISITOS	63
6.2 DEFINIÇÕES	64
6.3 O PROTOCOLO WAP	65
6.3.1 Conceitos	65
6.4 A ARQUITETURA WAP	66
6.4.1 O modelo WWW (World-Wide Web)	66
6.4.2 O Modelo WAP - Wireless Application Protocol	68
6.4.3 Exemplo de uma Rede WAP	70
6.4.4 Modelo de Segurança	70
6.5 COMPONENTES DA ARQUITETURA WAP	71
6.5.1 Componentes para ambiente wireless	71

6.5.2 Camada de Aplicação WAE (<i>Wireless Application Environment</i>)	72
6.5.3 Camada de Sessão WSP (<i>Wireless Session Protocol</i>).....	73
6.5.4 Camada de Transação WTP (<i>Wireless Transaction Protocol</i>)	73
6.5.5 Camada de Segurança WTLS (<i>Wireless Transport Layer Security</i>).....	74
6.5.6 Camada de Transporte WDP (<i>Wireless Datagram Protocol</i>).....	74
6.5.7 Bearers (<i>Serviços de Entrega</i>).....	75
6.5.8 Outros Serviços e Aplicações.....	75
6.5.9 Configurações da Tecnologia WAP.....	75
6.6 CONCLUSÃO DO CAPÍTULO	76
CAPÍTULO 7 - WLANS EM AÇÃO.....	78
7.1 BREEZENET NO SUPER BOWL	78
CAPÍTULO 8 - UMA PROPOSTA PARA UM CENTRO CULTURAL.....	80
8.1 OBJETIVOS DA WLAN	80
8.2 ÁREAS ENVOLVIDAS.....	81
8.3 SOLUÇÃO PROPOSTA	81
CAPÍTULO 9 - CONCLUSÃO	82
CAPÍTULO 10 - GLOSSÁRIO	83
CAPÍTULO 11 – BIBLIOGRAFIA	88
11.1 REFERÊNCIAS BIBLIOGRÁFICAS	90
11.1.1 Livros.....	90
11.1.2 Internet.....	90

LISTA DE FIGURAS

Figura 1.1	Representação de transmissão em FHSS	13
Figura 1.2	Célula básica	16
Figura 1.3	Nós Escondidos	17
Figura 1.4	Multi-células	19
Figura 1.5	Escopo do Padrão IEEE 802.11	23
Figura 1.6	Tipos de Topologia	24
Figura 1.7	Protocolo básico de conexão	27
Figura 1.8	Campos básicos do quadro	28
Figura 2.1	A pilha de protocolos do Bluetooth	38
Figura 2.2	O perfil do objeto PUSH	39
Figura 2.3	Os perfis Bluetooth	40
Figura 2.4	Salto de frequência por divisão de tempo	52
Figura 2.5	Um pacote com múltiplos slots	53
Figura 2.6	A seleção de saltos	54
Figura 2.7	O formato do pacote Bluetooth	54
Figura 2.8	Requisitos para transmissão de dados	61
Figura 3.1	Modelo WWW	67
Figura 3.2	Modelo WAP	68
Figura 3.3	Rede WAP	70
Figura 3.4	Camadas do protocolo WAP	71
Figura 3.5	Ambiente de Interação do WAE	72
Figura 3.6	WAP e outras tecnologias wireless	76

Resumo

A flexibilidade e a mobilidade das redes sem fio fazem com que elas sejam tanto extensões efetivas como alternativas atraentes às redes com fio convencionais.

As redes sem fio fornecem todas as funcionalidades das redes com fios convencionais sem as restrições físicas do fio propriamente dito. Elas serão o próximo estágio de evolução das redes computacionais, isto é, a possibilidade do usuário poder acessar os recursos de um sistema (serviços, servidores, impressoras, etc.) a qualquer tempo, bastando ao mesmo estar localizado dentro dos limites de uma infra-estrutura de comunicações sem fio.

As configurações de redes sem fio disponíveis variam de topologias ponto-a-ponto simples até complexas redes oferecendo conectividade de dados distribuídos e roaming.

Além de oferecer mobilidade ao usuário final dentro de um ambiente de rede, as redes sem fios facilitam a existência de redes portáteis, permitindo que as redes se movam acompanhando os seus usuários.

O presente estudo visa mostrar que na implementação de redes locais, metropolitanas ou, até mesmo, de longo alcance, as redes sem fio (wireless lan's – WLAN's) surgem como uma alternativa com grandes vantagens em relação às redes convencionais com fios.

Como ilustração é apresentada uma proposta de transição de uma rede convencional com fio para uma rede sem fio usando, como referência, um centro cultural composto de diferentes ambientes que necessitam ser interconectados.

Abstract

Flexibility and mobility make Wireless Lans both effective extensions and attractive alternatives to wired networks.

Wireless Lans provides all the functionality of wired lans, without the physical constraints of the wire itself. They will be the next stage of evolution of the computer networks, i.e, the possibility of the user access all the resources of a system (services, servers, printers, etc.) at any time, since the user is located within the limits of a wireless communication infrastructure.

Wireless Lan configurations range from simple peer-to-peer topologies to complex networks offering distributed data conectivity and roaming.

Besides offering end-user mobility within a networked environment, Wireless Lans enable portable networks, allowing LANS to move with his users.

The present study intends to show that when implementing LAN's, MAM's or, even, WAN's, the wireless lan's appears as an alternative that has great advantages considering wired networks.

As ilustration is shown a proposition of transition from a conventional wired network to a wireless lan using, as a reference, a cultural center composed of diferent environments that need to be interconnected.

Capítulo 1 – Introdução

Na última década do século XX, as pessoas ficaram cada vez mais dependentes e confortáveis com as comunicações sem fio. A facilidade de se portar telefones celulares e pagers, a qual permite que as pessoas se comuniquem localmente ou a longas distâncias, aumentou o apelo das comunicações de dados sem fio. Isto é evidente no rápido crescimento do uso das WLAN's para suportar os modelos de negócios contemporâneos. Estas redes apresentam várias vantagens importantes sobre os sistemas com fio. Elas permitem rápida expansão, suporte para mobilidade pessoal, uso em locações temporárias ou industriais e possuem uma notável eficiência de custo. As WLAN's são um complemento natural às redes com fio e, em alguns casos, seu substituto natural - principalmente quando usadas em redes de alcance empresarial - já que soluções usando hubs e/ou switches sem fio são mais facilmente expansíveis que em soluções com fio. Adicionalmente, a mobilidade acrescenta uma camada de facilidade no gerenciamento das estações a serem implementadas onde os dados são gerados. No passado, contudo, houve resistência no uso de redes sem fio de alcance global em função da falta de padronização das indústrias. Esta barreira foi dramaticamente removida com a adoção recente da nova norma de redes sem fio IEEE 802.11. Com esta norma, os gerentes de redes podem, agora, considerar as wireless lan's como uma opção completa para prover a tarefa das redes corporativas.

1.1 Objetivo da dissertação

O mundo das telecomunicações cresce a cada dia e, junto com essa expansão surgem novas tecnologias para atender a grande demanda do setor. E, como nessa área praticamente tudo é novo, faz com que as pessoas e, principalmente, as empresas não possuam o conhecimento adequado sobre essas tecnologias que lhes permita considerá-las como opções viáveis.

Uma conexão sem fio (wireless) é qualquer forma de conexão entre um emissor e um receptor que não necessite o uso de fios. Nesse caso, usam-se frequências de rádio ou sinais luminosos (normalmente, o infra-vermelho) para estabelecer essas

comunicações. Exemplos dessas conexões, entre outros, são os telefones celulares e os controles remotos.

O fato de não existirem conexões físicas entre os dispositivos de comunicação permite que seja oferecida uma mobilidade inexistente anteriormente.

Essa característica, em conjunto com as definições que oferecem bons níveis de segurança na conexão, permite apresentar as redes sem fio como alternativas viáveis e eficientes para a implementação e/ou substituição das redes de computadores, que é o objetivo maior desta dissertação.

1.2 Organização da dissertação

A dissertação é organizada na forma que segue. No Capítulo 2, tem-se uma definição das redes de computadores e seu histórico, bem como das redes sem fio (Wireless Lans – WLANS), seu histórico e sua utilização nos tempos atuais. No Capítulo 3, discute-se o aspecto tecnológico das WLANs e a sua arquitetura. O Capítulo 4, descreve e discute a norma IEEE 802.11 que veio para regulamentar as comunicações sem fio. O Capítulo 5, apresenta o padrão e as tecnologias Bluetooth, os quais visam a fornecer os meios para a substituição de cabos usando um link de rádio universal de baixo alcance. No Capítulo 7, discute-se o WAP (Wireless Application Protocol – Protocolo de aplicações sem fio), cuja importância está relacionada às comunicações móveis disponibilizada pelas comunicações sem fio e com o acesso à Internet, cada vez mais difundido. No Capítulo 8, apresenta-se um caso real da utilização das WLANs. O Capítulo 9, apresenta uma proposta de aplicação da tecnologia na expansão da rede de computadores de um centro cultural. Finalmente, o Capítulo 10 apresenta as conclusões e as recomendações para trabalhos futuros.

Capítulo 2 – Redes sem fio

Em Março de 1971, Gordon Moore e Robert Noyce, fundadores de uma empresa no Vale do Silício, anunciaram que o seu microprocessador Intel 4004 estava plenamente funcional e pronto para ser liberado. Essa invenção, o descendente direto do transistor de Shockley inventado uma década antes, começou uma revolução que está propulsionando o mundo dos negócios com uma aceleração cada vez maior. Concomitantemente com este rápido crescimento, as redes computacionais e telefônicas, usando microprocessadores, também se desenvolveram a uma taxa acelerada. Com a adição do vídeo e com a colocação das várias tecnologias na mesma infra-estrutura binária, assiste-se agora à convergência dessas tecnologias em uma simples e unificada força, força essa que está revolucionando os negócios e a sociedade. O desenvolvimento geral da computação distribuída nas empresas mudou a forma de se fazer negócios. O novo modelo econômico requer redução de custos, prazos de entrega menores, melhor acesso pelos clientes e uma grande ênfase na qualidade. Todas estas pressões estão forçando as empresas a irem onde os dados estão sendo gerados: o cliente. Considere-se, como exemplo, o fato de que o uso cada vez maior de computadores portáteis mudou a forma como as aplicações processam dados remotos. Indo à origem dos dados e capturando-os “in situ”, ao invés de entrar com esses dados manualmente num formulário a ser remetido a um mainframe, consegue-se atingir as metas do novo modelo de negócios. Estas mesmas vantagens são alcançadas pelas WLAN’s.

As comunicações sem fio são o ponto final lógico para a invenção de Moore e Noyce. A mudança de mainframes para cliente/servidor traz o computador para mais perto de onde os dados são gerados: o cliente. Adicionalmente, as forças econômicas que norteiam as empresas, estão forçando mudanças constantes em todos os aspectos dos negócios. As pessoas estão sendo constantemente realocadas. Companhias de classe mundial são caracterizadas pela sua habilidade de criarem pequenos grupos de trabalho rapidamente e pela habilidade de rearrumar rapidamente esses grupos para novas iniciativas. Organizações que estejam atreladas a redes com fio, físicas e estáticas, irão competir com as redes sem fio (WLAN’s) quase tão bem quanto as caixas registradoras mecânicas o fizeram com as caixas registradoras com microprocessadores, nos anos 70. Adicionalmente, existem locais onde o cabeamento tradicional não é possível ou tenha

um custo proibitivo. Alguns exemplos típicos incluem salas de emergência de hospitais, escritórios médicos, salas de aula, salas de conferências, pequenas empresas de comércio, ambientes abertos e a casa dos empregados. De fato, o ambiente com fios é a anomalia aqui: ela força o usuário a ir onde o fio se encontra, da mesma forma que se era obrigado a ir até ao mainframe antes do advento do PC.

Se as redes sem fio têm um custo tão baixo e uma performance equivalente às redes tradicionais então não haveria razão para a instalação de fios. Como se verá mais tarde, tais condições estão bem próximas de ser alcançadas. A habilidade de equipar, com um baixo custo, os usuários com dispositivos portáteis (notebook, palmtops, etc.) confere uma enorme vantagem estratégica nos mercados altamente competitivos da atualidade. O usuário, municiado de um palmtop, pode capturar os dados na origem. No ambiente de trabalho, o usuário pode-se conectar à rede sem fio em qualquer parte do edifício. Finalmente, novos dispositivos podem ser conectados a qualquer momento ou em qualquer local sem o caro atraso da instalação de novas camadas de cabos.

Por que tal tecnologia não foi desenvolvida até agora? Uma das razões é que as tecnologias sem fio antigas eram muito lentas. Além disso, sem padrões industriais uniformes, as antigas tecnologias eram caras, sem interoperabilidade e, frequentemente, não confiáveis. Contudo, tais barreiras estão sendo derrubadas. Com o advento de protocolos padronizados por fóruns envolvendo usuários e fornecedores tais como a IEEE 802.11, o Bluetooth e o WAP, está se tornando cada vez mais comum a utilização da tecnologia sem fio em todas as áreas relacionadas ao dia a dia de cada um de nós.

2.1 História das WLAN's

As WLAN's já estão por aí faz bastante tempo. De fato, elas antecederam as redes com fio. ALOHA, a discutível primeira rede de computadores e base para a Ethernet, era baseada em rádio. A primeira rede a utilizar comutação de pacotes em canais de rádio-frequência foi desenvolvida no Havaí, EUA, em 1971, para interligar sete campus, distribuídos por quatro ilhas, com o computador central da ilha de Oahu. Ironicamente, nasceu desta experiência a tecnologia amplamente utilizada em redes locais fixas: a Ethernet. Limitações na largura de banda e na tecnologia de transmissão

não permitiram que o projeto resultasse na utilização, em massa, das redes sem fio. Porém, dois fenômenos consolidados ao longo da última década - miniaturização de componentes eletrônicos e comunicações pessoais sem fio - devolveram às redes locais sem fio um grande interesse em termos de pesquisa e desenvolvimento, que culminou com o aparecimento das primeiras redes sem fio comerciais no início dos anos 90.

As primeiras redes locais sem fio de rádio-frequência implementaram ou a transmissão *spread spectrum* (difusão de espectro), ou a transmissão infravermelha difusa [GEI96]. A transmissão *spread spectrum* nestas redes utilizava a banda ISM (*Industrial, Scientific and Medical* - Médica, Científica e Industrial), compostas por três faixas, de 902 a 928 MHz; de 2,40 a 2,4835 GHz e de 5,725 a 5,85 GHz. Todavia, estas redes apresentavam baixa interoperabilidade, pois cada rede possuía um conjunto de características único, já que os fabricantes desenvolviam os produtos para as suas redes conforme critérios próprios. É possível encontrar redes com vazões e alcances diferentes, empregando diversos critérios de segurança e definindo os algoritmos da subcamada MAC (*Medium Access Control*) com abordagens particulares.

Assim, a evolução das redes usando técnicas sem fio ficou bem para trás em relação às redes baseadas em fios. Estas últimas evoluíram recentemente das velocidades de 10-100 megabits por segundo para a faixa de gigabits por segundo considerando-se aquelas baseadas em padrões Ethernet e WANs ATM SONET. Em contraste, a forma mais comum de comunicação sem fio atualmente, ligações por modem usando conexões celulares analógicas, disponibiliza taxa de transmissão de alguns Kbps apenas. As LANs que usam raios infravermelhos, uma das tecnologias alternativas, também têm limitações em função dos problemas dramáticos de interferência causados pela luz do sol e pela luz artificial. Além disso, e isto é primeiramente um paradigma do ponto-a-ponto, o que significa que para usar raios infravermelhos na construção de uma WLAN se torna necessária a instalação de um grande número de pontos de acesso. Finalmente, qualquer forma de rádio-comunicação necessita da alocação de um espectro de frequência, uma área lotada de tecnologias concorrentes que competem por espaço. De forma semelhante, muitos conjuntos de produtos foram baseados em tecnologias proprietárias não-padrão. Fazer um estudo de caso de negócio baseado em tecnologia de comunicação de propriedade de um único fornecedor é um risco extremo.

2.2 Urgência para a norma IEEE 802.11

Similarmente, a indústria da WLAN não providenciou um conjunto de produtos estratégicos unificados que pudessem interoperar entre os vários fornecedores. Adicionalmente, os fornecedores de redes com fio, ao invés de projetarem seus produtos para serem completos, baseavam seus componentes (bridges, roteadores, etc.) e conjuntos de produtos na tecnologia de adaptação. Assim, usuários que quisessem usar WLANs eram colocados na difícil situação de ou serem dependentes de um único fornecedor ou então terem que resolver os problemas de infra-estrutura por si mesmos. Convencer um administrador de rede, acostumado com o excesso de protocolos de rede com fio totalmente padronizados e integrados de vários fornecedores, a considerar uma solução sem fio não padrão e fragmentada, era uma tarefa árdua.

Esta falta de padronização emperrou o desenvolvimento e, sobretudo, a adoção de redes locais sem fio. Em maio de 1991, foi submetido ao IEEE, organização responsável, entre outras atividades, pela elaboração dos padrões adotados em redes locais e metropolitanas, um pedido de autorização para formar o Grupo de Trabalho 802.11, cujo objetivo seria definir uma especificação para conectividade sem fio entre estações de uma área local.

Reconhecendo isto, a IEEE constituiu uma nova subcomissão para o processo de normatização 802, o Comitê de Trabalho 802.11 para redes sem fio (802.11 Working Committee for Wireless LANs), para produzir um padrão para a faixa de 2.4 GHz das WLANs. À medida em que se elaborava o padrão, os fabricantes de equipamentos de rede passaram a formular planos de migração de seus produtos, de acordo com as exigências feitas pela norma 802.11. O atraso na elaboração do padrão, juntamente com um mercado aquecido, determinou que muitos produtos fossem lançados no mercado, com garantias de uma transição suave para as especificações IEEE 802.11. A lentidão de tal grupo em produzir uma norma atrasou a aceitação das WLANs no início da década de 90. Contudo, em 26 de Junho de 1997, o Grupo de Trabalho 802.11 ratificou finalmente a especificação 802.11. Foi definido que o mecanismo básico de controle de acesso ao meio (MAC) seria o CSMA/CA (*Carrier Sense Medium Access with Collision*

Avoidance – Acesso ao meio com detecção de portadora e prevenção de colisão). Com base neste mecanismo, construiu-se um algoritmo de *polling* que permite que dados trafeguem no canal sem o risco de eventuais colisões. A partir daí a indústria de redes sem fio começou a trabalhar imediatamente em interoperabilidade e conformação.

Espera-se que este padrão aberto seja o catalisador para que o mercado unifique suas ofertas e apresente aos seus clientes, um conjunto maduro e completo de produtos que irão introduzir uma nova mudança no paradigma das redes de computadores, a rede sem fio – a WLAN.

2.3 Objetivos das WLANs

Quais são os objetivos das WLANs? Os objetivos imediatos são oferecer, ao cliente, flexibilidade, mobilidade, facilidade de expansão e baixo custo.

Claramente, a WLAN necessita usar ondas de rádio para interconectar usuários num raio de várias centenas de metros e transmitir dados confiáveis a taxas comparáveis às das redes com fio. Também necessita prover conectividade para redes com alcances de vários quilômetros. Finalmente, deve interagir com tecnologias de rede com fio padrão tais como Ethernet e ATM. Para serem bem sucedidas de uma forma geral, as WLANs devem ser onipresentes, capazes de se integrarem de forma transparente com as tecnologias com fio e devem ser baseadas em padrões abertos. Adicionalmente, devem ser robustas, capazes de transmitir dados a taxas na faixa de megabits, no mínimo, devem ser escaláveis, seguras, de fácil manutenção e devem ser construídas usando-se um conjunto de produtos integrados. E, claro, devem ter preços competitivos com as LANs com fio.

Em adição a todos esses objetivos, as WLANs têm que competir com uma tecnologia de redes que é madura, na qual os usuários se acostumaram a esperar respostas quase instantâneas além de atender à maioria dos objetivos acima citados. No passado, as WLANs não conseguiam atingir muitos desses objetivos e, por esse motivo, eram pouco empregadas. Os únicos casos em que elas poderiam ser usadas seriam aqueles onde alguma unidade, por decisões locais e táticas, optou pela aquisição de uma WLAN por razões específicas. Têm havido nichos de aceitação: laboratórios, redes

industriais, científicas e médicas que operam na banda de frequência, não licenciada, de 902-928 MHz e com velocidades superiores a 100Kbps. Os satélites têm fornecido taxas semelhantes há anos. Três novos satélites irão, brevemente, fornecer Serviços de Comunicação Pessoais (PCS - Personal Communications Services), mas, novamente, as taxas serão baixas (64 Kbps). Adicionalmente, como os serviços de telefonia celular se espalham cada vez mais, pode-se esperar que os serviços wireless o façam também, mesmo que eles também operem, inicialmente, na faixa de kilobits. Contudo, até recentemente, nenhuma tecnologia wireless fornecia um conjunto de serviços que satisfizesse todas as condições acima.

2.4 O novo paradigma wireless

Com a aceitação da norma IEEE 802.11, uma condição necessária e importante foi atingida: interoperabilidade. Fornecedores estão agora fabricando produtos que são maduros e baratos. Conjuntos de produtos oferecendo soluções completas permitem que os administradores de redes construam WLANs customizadas e as integrem com suas redes convencionais com fio. A tecnologia é madura e tem preços competitivos. Por causa da abertura do padrão, a competição está fazendo com que os preços caiam. O gerente da empresa pode agora considerar as WLANs como uma opção estratégica tanto para complementar as redes com fio como para substituí-las em circunstâncias apropriadas.

2.5 Por que escolher redes wireless?

Quando se deve escolher uma rede wireless e por que? Existem pelo menos quatro situações nas quais as redes wireless são uma opção apropriada: cenários onde há mobilidade; a necessidade de utilização por curtos períodos de tempo; rapidez de expansão; e, a necessidade de sobrepor as dificuldades típicas da instalação de fios.

- Mobilidade – A habilidade de acessar informação em tempo real enquanto negocia com clientes, é realçada com uma WLAN. Em hospitais, por exemplo, fornecedores de atendimento médico podem melhorar a qualidade dos cuidados com os pacientes. Com uma WLAN, a entrada de dados e a tomada de decisão imediata podem reduzir o ciclo de vezes de atendimento ao paciente. Da mesma forma, a redução de erros pela manutenção de dados uma só vez é significativa.

Em um escritório, a habilidade de se mover pelo edifício enquanto processa as informações é uma vantagem. Similarmente, empregados de vendas podem circular livremente enquanto atendem os clientes. Agentes de seguros podem capturar dados diretamente a partir das premissas dos clientes e receber processamento analítico online e em tempo real. Se existe vantagem do negócio em ir de encontro ao cliente ao invés de fazer com que o cliente venha até você, então a adoção da wireless pode ser obrigatória.

Finalmente, WLANs permitem que aplicações móveis sejam disparadas. Considere-se o estudante habilitado na WLAN a qual pode fazer com que ele, através de seu laptop, mude de leitura para leitura e permaneça conectado, em qualquer tempo, a seus arquivos e aplicações. De fato, tal ambiente está agora em andamento na Universidade Carnegie-Mellon, a qual instalou uma WLAN com alcance para todo o campus que tem mais de 100 APs interconectados.

- Utilização por curtos períodos de tempo – Similarmente ao item mobilidade, a conectividade por tempo determinado permite aos usuários desenvolverem capacidades numa base do quando necessário sem se preocupar com a justificação de custos para soluções com fio. Auditores fiscais, por exemplo, podem simplesmente se conectar pelo tempo necessário para fazer a auditoria. Isto permite uma flexibilidade operacional significativa e facilita a criação de grupos de trabalho “ad-hoc”. Estar apto a se conectar à rede por um curto período de tempo, desta maneira, provê uma vantagem competitiva.

- Rapidez de expansão – As WLANs permitem uma rápida conectividade a uma rede. A formação e desmonte de grupos de trabalho podem ser executados facilmente com as WLANs. A complexidade e longo ciclo de tempo necessários para a inclusão ou exclusão de nós em uma rede com fio, introduz custos operacionais altos em comparação com a flexibilidade da ligação wireless, onde os custos operacionais são quase zero.
- Dificuldade em instalar fios – Muitas situações não permitem a fácil instalação de fios. Edifícios históricos ou edifícios mais antigos fazem com que a instalação de fios seja ou impossível ou extremamente cara. Tentar implementar redes em ambientes externos é virtualmente impossível com as redes convencionais. Considere-se situações em parques infantis ou complexos esportivos onde se queira instalar uma rede temporária para, logo em seguida, a retirar. Existem outras situações onde a instalação de WLANs é vital. O resgate de desastres, por exemplo, pode fazer uso imediato de WLANs em campo, para recolher dados e coordenar ações de socorro. O uso de WLANs em campos de batalha é óbvio. Finalmente, existem situações onde os fios não podem ser instalados, por exemplo, cruzando ruas ocupadas. Da mesma maneira, a conexão de edifícios é facilitada naquelas situações onde não existe a possibilidade de cabeamento subterrâneo. A utilização de bridges wireless, para conectar LANs fisicamente separadas, pode ser muito efetivo.

2.6 O negócio para as redes wireless

O preço das NIC (Network Interface Cards – Placas de Interface de Rede), para redes wireless, está caindo rapidamente em comparação com as Ethernet com fio. Além disso, as taxas de transferência de dados, mesmo que atualmente menores que as das Fast e Gigabit Ethernet, são comparáveis às velocidades Ethernet padrão. Quando considerando fatores de custo e a necessidade de fácil expansão, tem que se considerar todos os custos associados com os sistemas baseados em fios e não somente os custos

do adaptador do nó. (Foi estimado que o custo inicial de compra de uma rede baseada em fio é somente 20% do custo total de operação de tal LAN). Em muitos casos, os custos de gerenciamento das mudanças e os atrasos de tempo, tornam o uso da WLAN obrigatório.

Alguns produtos para WLAN, especialmente aqueles que usam tecnologias proprietárias, são mais complexos que os da rede com fios média e, usualmente, mais caros. Contudo, existem várias linhas de produtos para WLAN, no mercado, que foram desenvolvidas por usuários finais em função dos menores custos de instalação e configuração em comparação com um esquema completamente baseado em fio. O custo total de instalação mais alto para um sistema com fio é especialmente verdadeiro quando é difícil alcançar a cabeção já existente ou, até mesmo, quando a mesma não existe. Benefícios adicionais das WLANs incluem a máxima utilização dos dispositivos móveis dos clientes. Em geral, as empresas pagam um prêmio por dispositivos portáteis ou móveis e depois perdem o benefício principal de tal portabilidade ao amarrá-los a uma rede, forçando o usuário a se tornar completamente estacionário. Por causa de sua flexibilidade e potencial de se tornarem ainda mais competitivos a nível de custo, o mercado de WLAN é esperado crescer 40% ao ano, levando para um mercado de bilhões de dólares em dois anos. Como é comum em tecnologia da informação, isto, em conjunto com a norma 802.11, irá encorajar a competição para baixar os preços dramaticamente.

Capítulo 3 - WLANs – O aspecto tecnológico

Uma WLAN é como uma rede com fio só que nela os cabos são substituídos por sinais do espectro de rádio-frequência. Os componentes fundamentais da arquitetura WLAN são descritos em seguida. Primeiro, necessita-se de uma linha de visão para as comunicações por rádio. As ondas de rádio ocupam um subconjunto do espectro eletromagnético que também inclui rádio, televisão, informações de controle de tráfego aéreo, etc. De fato, o espectro de frequências de rádio não só é um local ocupado como é um recurso escasso. Assim, os agentes reguladores têm distribuído algumas bandas de frequência para propósitos específicos de forma a evitar colisões desnecessárias, já que o espectro é um meio compartilhado. Estas bandas podem ser licenciadas ou não. Acesso a bandas licenciadas é restrito a empresas de controle mas o acesso a bandas não licenciadas é aberto. As bandas das WLANs são não-licenciadas. Vinte anos atrás, a banda de 900 MHz era reservada para o uso ISM. Então, as agência reguladoras alocaram a banda de 2,4-2,483 GHz para o tráfego das WLANs nos Estados Unidos. O FCC, em particular, restringiu a potência de saída, dos dispositivos que operassem na banda de 2,4 GHz, em até 4 watts. Contudo, a história é mais complicada que somente considerar as limitações do rádio impostas pelas restrições de potência. Ondas de rádio a tais frequências ricocheteiam bastante, refletindo-se em objetos sólidos. Reflexões ou múltiplas transmissões do mesmo sinal têm que ser levadas em consideração. Além disso, existem outros equipamentos eletrônicos que também geram sinais nessas frequências. Tais sinais são ruídos para uma célula WLAN. Por tudo isso, os projetistas têm que encontrar uma forma eficiente de reduzir a interferência dessas fontes de ruído aleatórias e compensar as múltiplas reflexões. Consequentemente, é mais complicado projetar um produto para uma WLAN que para um sistema único baseado em fio.

3.1 Tecnologias de difusão de espectro (SPREAD SPECTRUM)

A maneira óbvia de começar o projeto de uma arquitetura WLAN seria fixar o sinal em uma determinada frequência e usá-la como se fosse o “fio” para comunicação.

Contudo, os problemas de ruído são tão graves que um método alternativo deve ser escolhido: a chamada solução de difusão de espectro. O ruído tem sua própria frequência e irá destruir qualquer sinal que seja enviado através dessa nuvem de ruído. Contudo, a difusão de espectro, como o nome indica, usa múltiplas frequências na banda para aumentar a imunidade a ruídos em qualquer frequência específica. Hoje, duas abordagens são usadas para implementar a difusão de espectro para transmissões WLAN: Frequency Hopping Spread Spectrum (FHSS) e a Direct Sequence Spread Spectrum (DSSS). A FHSS usa um grande número de canais de frequência, 80, com o transmissor enviando um sinal de ruptura “burst” sobre o canal e pulando “hopping” para outro canal.

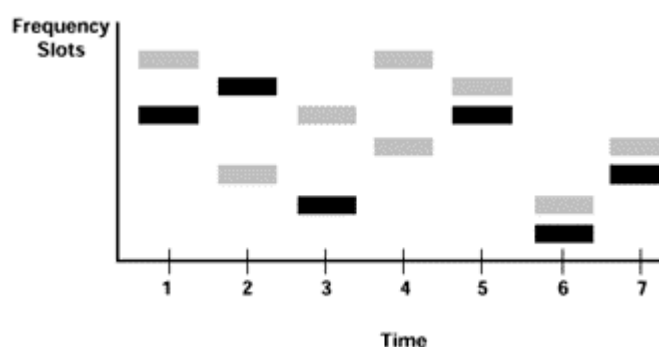


Figura 1.1 - Representação de transmissão em FHSS

Como pode ser visto na figura 1.1, duas estações estão transmitindo ao mesmo tempo. Cada uma pega uma frequência e transmite nela por um período (slot) de tempo especificado. Ao final dessa fatia de tempo, ambas as estações mudam ou “pulam” para outra frequência. A sequência exata dos “pulos” deve ser conhecida tanto pelo transmissor quanto pelo receptor em cada canal. A largura de banda típica do sinal de informação é de 1 MHz e o período de tempo é de um décimo de segundo. O diagrama ilustrado na Figura 1.1 é uma simplificação extrema, já que a sequência atual usada na norma 802.11 deve ter 79 faixas (slots) de frequências. Tanto o número de “pulos” quanto o tempo máximo de “residência” são determinados pelas agências reguladoras, como o FCC no caso dos Estados Unidos. Têm que haver, no mínimo, 75 camadas e o tempo de “residência” não deve superar os 400 milissegundos. A sequência das camadas é quase aleatória mas é conhecida pelo transmissor e pelo receptor. Existe um número de sequências fixas (26) que podem ser selecionadas pelo instalador. Se ocorrer ruído, o

pior caso é aquele em que um pacote pode ser ligeiramente corrompido em uma frequência necessitando ser retransmitido no próximo “pulo”.

Uma tecnologia alternativa de difusão de espectro é a abordagem DSSS. Esta usa um sinal banda-base e substitui a mensagem por blocos de código de tamanho fixo, expandindo a largura de banda por um grande fator. O receptor conhece a sequência de decodificação e recupera a mensagem original. A DSSS é a tecnologia mais antiga e tem sido, gradualmente, substituída pela FHSS. É importante notar que as duas não são interoperáveis, mesmo que alguns fornecedores fabriquem ambos os conjuntos de produtos.

Algumas das vantagens da FHSS, em relação à DSSS, é que a FHSS não necessita da alocação de uma banda de frequências contígua, é mais simples e mais barata de se implementar, é mais segura e permite transmissões simultâneas múltiplas. Por outro lado, na DSSS é mais fácil de se comutar de uma célula para outra e pode fornecer maiores taxas de transferência ponto-a-ponto, em certas circunstâncias.

Hoje, quase todos os fornecedores escolheram o método FHSS, o qual é superior ao DSSS em vários sentidos. Por exemplo:

- A FHSS é mais imune a interferências no sinal. Redes com DSSS podem ser prejudicadas por interferências externas dentro da mesma faixa de frequência já que o DSSS não tem uma agilidade de frequência. A frequência é pré-selecionada e não se pode evitar interferências na banda pré-selecionada. A FHSS, por outro lado, “pula” rodeando a fonte de ruído.
- A FHSS tem uma maior capacidade total de agregação. O número máximo de canais DSSS de 1 Mbps não sobrepostos é 3, de uma capacidade total de 6 Mbps. Tipicamente, o sistema FHSS pode dispor de até 15 canais de 1 Mbps não sobrepostos para uma capacidade de 15 Mbps.
- A FHSS é mais escalonável. Se a FHSS necessitar lidar com atividade adicional em uma célula, basta somente se acrescentar um AP (Access Point – Ponto de Acesso) adicional dobrando, portanto, a capacidade da célula. Já que os APs co-localizados são, naturalmente, de frequências não sobrepostas, eles interferem muito pouco entre si.

- Sistemas FHSS têm algumas vantagens físicas. As unidades FHSS são, tipicamente, mais leves que as DSSS. As unidades DSSS também requerem maior potência para operar.

3.2 CSMA/CA

Como se verá mais tarde, a norma 802.11 define uma camada de interface MAC que é compatível com a Ethernet com fio. Contudo, ao invés de usar o padrão Ethernet CSMA/CD (Carrier Sense Multiple Access / Collision Detect – Acesso Múltiplo com Percepção de Portadora e com Detecção de Colisões) usa uma variação chamada CSMA/CA (Collision Avoidance – Evitando Colisões). O protocolo CD iria requerer que os rádios sem fio fossem capazes de enviar e receber ao mesmo tempo, o que aumentaria o preço e complexidade do produto. Também, com estações wireless, nem sempre é o caso em que todas as estações possam estar posicionadas de forma a “escutar” todas as estações restantes. Para minimizar a possibilidade das estações não serem capazes de “ouvir” as outras, a norma 802.11 define a noção de Percepção de Portadora Virtual (Virtual Carrier Sense). A estação transmissora primeiramente envia um pacote muito pequeno, chamado de pacote RTS (Request To Send – Solicitação para Envio), o qual contém os endereços de origem e destino e a indicação da duração da mensagem pretendida. Se o meio está livre, o receptor irá responder com um pacote CTS (Clear To Send – Pronto Para Enviar). Na recepção deste pacote, a transmissão começa. A utilização do protocolo CSMA/CA reduz as chances de colisões. Se o meio está ocupado, os transmissores irão executar um “backoff” similar às suas contrapartidas com fio. Assim, a 802.11 usa um protocolo chamado de reconhecimento positivo (positive acknowledge). Quando uma estação quer transmitir, ela primeiro verifica o meio para apurar se o mesmo está livre, da mesma forma que ocorre em ambientes com fio. Caso esteja livre, ela transmite. A estação receptora, depois de receber a mensagem e constatar que a mesma não está corrompida, manda uma confirmação (acknowledgement). Se a estação emissora não recebe esta confirmação então ela assume que a comunicação não foi completada e, assim, ela retransmite a mensagem.

3.3 Arquitetura WLAN

3.3.1 Conexões Ethernet

Em cerca de 98% do tempo, a WLAN se interliga com LANs Ethernet com fio. Neste ambiente, o ponto de acesso (AP) age como uma ponte (bridge) para a LAN, permitindo que os dispositivos WLAN compartilhem os mesmos recursos da LAN da mesma forma que as estações da LAN conectadas por fio. Ambientes SOHO (Small Office Home Office – Pequenos Negócios / Negócios Caseiros), por outro lado, são usualmente suportados por um sistema wireless somente mas também podem usar um ponto de acesso em redes ponto-a-ponto (peer-to-peer). Uma WLAN ponto-a-ponto pode ser configurada mas tem um uso muito limitado.

3.3.2 Células e Pontos de Acesso

A área coberta por uma única WLAN é chamada de célula. As estações que compreendem a WLAN em si, estão localizadas dentro da célula. Todas as comunicações dentro e fora da célula devem ser coordenadas por uma única unidade chamada de Ponto de Acesso (AP). O AP conecta a célula com outras células e com LANs com fio. O AP deve também sincronizar todas as estações da célula, de forma que elas possam executar o “pulo” de frequência no tempo certo e para a frequência correta.

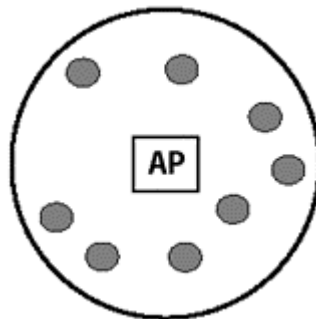


Figura 1.2 - Célula básica

A Figura 1.2 mostra uma célula básica. Dentro da célula, teoricamente cada estação pode “ouvir” todas as outras. Na prática, nem todos os nós podem “ouvir” os outros. Neste caso, a célula necessita ter um controlador mestre chamado Ponto de Acesso (AP). O AP deve ser capaz de “ouvir” todos os nós e coordenar todo o tráfego interno e externo da célula.

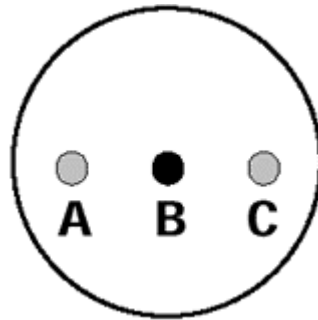


Figura 1.3 - Nós Escondidos

3.3.3 Nós Escondidos

Suponha-se que A queira mandar uma mensagem para B, conforme ilustrado na Figura 1.3. A escuta para garantir que não haja portadora; ao nada escutar e assumindo que tudo está livre, ela transmite. Ao mesmo tempo, C, que não pode “ouvir” A, também quer transmitir para B. Toma a mesma decisão que A mas ambos os pacotes colidem em B. Isto é o problema do nó escondido nas WLANs. Se isto ocorre, as retransmissões irão reduzir a taxa de transmissão efetiva. Ao invés de facilitar, a norma IEE 802.11 acrescenta uma ligeira complicação no protocolo. Ela força A a mandar um pacote RTS (Request To Send) primeiro, indicando o momento e a quantidade de dados que pretende enviar. O nó B, se pretender se conectar, responde com um pacote CTS (Clear To Send) o qual também é “ouvido” por C. Isto faz com que C retarde sua transmissão em função da informação recebida sobre A. Assim, as colisões são reduzidas significativamente. Esta adição faz com que o protocolo seja mais complicado e introduz um atraso adicional. Contudo, muitos projetistas o escolhem para uma melhor performance no geral e, como se verá mais tarde, é uma opção no protocolo 802.11.

As células podem ser conectadas de quatro maneiras fundamentais:

- como células autônomas;
- como células acopladas em configurações de multi-células;
- como um elemento em um ambiente Ethernet com fio; e,
- a uma LAN remota através de uma ponte wireless.

3.3.4 Células autônomas

Uma célula autônoma consiste em um Ponto de Acesso e todas as estações wireless associadas. O número máximo de estações depende da natureza do tráfego de dados. Se houver uma grande quantidade de dados se deslocando então 15 (quinze) estações seria o limite máximo enquanto que um ambiente menos intenso pode suportar até 50 (cinquenta) estações. Em tais situações, não existe necessidade de instalação de fios. O diâmetro da célula depende de muitos fatores, mas pode-se considerar um alcance de até 200 metros em áreas fechadas e de até 4 quilômetros ao ar livre.

3.3.5 Células acopladas

Quando o número máximo de membros da célula é excedido ou quando o diâmetro da célula é extrapolado, mais células podem (e devem) ser criadas. Estas células devem se sobrepor para permitir comunicações sem emendas entre elas. Quando um usuário se desloca da área de cobertura de uma célula para outra, os Pontos de Acesso envolvidos devem comutar o sinal de uma célula para a outra sem que o usuário perceba que atravessou os limites das duas células, este processo é conhecido como *roaming*. Essas células são chamadas de células acopladas (linked cells), mas a comutação é tão suave que o usuário nem percebe que passou para outra célula. Combinada com uma conexão de suporte principal (backbone), um campus universitário completo pode ser “conectado”.

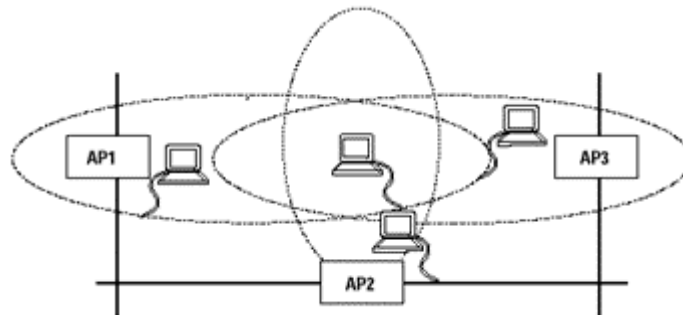


Figura 1.4 - Multi-células

3.3.6 Multi-células

Se várias células sobrepõem a mesma área física, então esta configuração é chamada de multi-células. Com algoritmos inteligentes, os APs podem decidir qual deles é o melhor posicionado para comandar as comunicações entre o emissor e o receptor na WLAN. Quando se espera tráfego pesado, isto é uma grande vantagem. Tal cobertura, chamada de cobertura multi-célula, não só diminui a carga do tráfego entre células mas também fornece redundância para assegurar operações de recuperação confiáveis.

3.3.7 Roaming e Comutação

O roaming é a capacidade das estações portáteis se moverem livremente entre células sobrepostas, ou numa topologia acoplada ou numa topologia multi-célula. O roaming é semelhante no fato de que o usuário não percebe nenhuma interrupção quando se deslocando de uma célula para outra. Os APs devem comutar o sinal e fazer o sincronismo apropriado. Algumas diferenças chave entre os fornecedores podem ser vistas na forma como eles tratam o roaming e a sincronização do AP. Elas não foram padronizadas e o usuário deve se informar, junto aos fornecedores, sobre como é que isso é tratado.

O roaming e a comutação rápida são importantes. Como um teste extremo, pode-se perguntar ao fornecedor qual a velocidade que um veículo, contendo um laptop, pode

ter para se deslocar através de um ambiente multi-células. Claramente, se a WLAN estiver funcionando bem, pode-se esperar que a WLAN possa lidar com velocidades na faixa de vários quilômetros por hora. Similarmente, pode-se perguntar como é que as diferentes estações se comunicam com APs diferentes, de forma a avaliar a qual AP elas estão correntemente associadas. Esta é uma decisão dinâmica e que depende da localização da estação e dos padrões de tráfego naquele instante.

Uma questão relacionada é aquela de como a diminuição da carga é alcançada, em se tratando de células adjacentes de uma WLAN. Se existir um tráfego significativo entre as células sobrepostas talvez seja melhor, para a WLAN, realocar algumas das estações para o AP com menor carga e executar os procedimentos necessários para assegurar que a estação não fique “pulando” de AP para AP.

3.3.8 Pontes remotas (remote bridges)

Finalmente, as células podem ser conectadas a WLANs remotas através do uso de bridges wireless. Mesmo não sendo parte da norma 802.11, tais bridges podem estender o alcance para vários quilômetros, com altas taxas de transferência, transformando WLANs em WMANs se necessário.

3.3.9 Conectividade com PC

Os laptops e os PCs desktop são conectados à WLAN através de placas NIC, tais como placas PCMCIA e ISA. Nesta implementação, o NIC padrão Ethernet é substituído pelo NIC wireless, o qual é instalado nos mesmos slots de I/O do dispositivo do cliente. Adicionalmente, todos os drivers necessários devem ser instalados bem como devem ser configuradas todas as interrupções de hardware, da mesma forma que ocorre com as placas de rede com fio. Outra abordagem para criar um cliente wireless é usar um transceiver wireless externo que, simplesmente, é conectado na placa de rede convencional ou na porta do dispositivo do cliente e que fornece acesso sem fio instantâneo, sem a necessidade de drivers adicionais ou de qualquer outro software. Esses dispositivos podem possuir uma ou mais conexões RJ-45. Esta abordagem

fornece a flexibilidade de se conectar virtualmente qualquer dispositivo Ethernet à WLAN.

3.3.10 Fontes de interferência

Os projetistas também tentam minimizar as fontes de interferência as quais, com o corrompimento do sinal, causam retransmissões e, portanto, reduzem as taxas de transferência e performance. As três maiores fontes de interferências são a propagação por múltiplos caminhos, os dispositivos de microondas e as das redes ISM.

Como já evidenciado, as ondas de rádio “pulam” bastante causando reflexões e múltiplas instâncias do mesmo sinal. Antenas especialmente desenhadas são usadas para reduzir o efeito destas fontes. O modem, se adequadamente construído, irá selecionar o sinal mais forte numa base quadro-a-quadro. A técnica FHSS também difunde o sinal por 79 camadas (hops) usando bandas de 1 MHz cada. As camadas são mudadas de 8 a 30 vezes, por segundo, numa ordem pré-definida. As estações emissora e receptora devem usar a mesma sequência de camadas com a mesma sincronização de espaços de tempo. Assim, em caso de interferência, somente um único canal irá sofrer seus efeitos e por um curto período de tempo. Outra vantagem desta técnica é que ela fornece uma segurança excelente contra ouvintes indesejados ou hostis. Isto essencialmente faz com que as WLANs sejam tão seguras quanto as LANs baseadas em fio. Fornos de microondas são um incômodo de pouca importância a pequenas distâncias, nas quais eles podem gerar interferência na faixa de 2.4 GHz. Finalmente, equipamentos médicos e científicos podem estar usando transmissões ISM periódicas de baixa potência, as quais podem, ocasionalmente, ser interpretadas como ruído pelas WLANs instaladas.

3.3.11 Outras considerações

As arquiteturas WLAN, em adição ao fato de estarem padronizadas na norma 802.11, devem permitir conexões com interfaces LAN padrões, tais como a Ethernet 802.3. A WLAN deve trabalhar, de uma forma transparente, com os protocolos comuns de rede tais como IP, IPX, AppleTalk, Netbeui, DECnet e outros. Os protocolos de

gerenciamento padrão devem ser seguidos, tais como o SNMP. Um bom fornecedor irá suportar “MIBS” como MIBII e bridge MIB e também prover um MIB privado para suas unidades.

Finalmente, a maioria das WLANs irão ter laptops, hand-helds ou palm-tops como suas estações usuárias, além dos PCs desktop, estações de trabalho de grande potência baseadas em processadores 68000 e vários tipos de dispositivos periféricos. Os dispositivos portáteis, tais como os laptops, palmtops ou handhelds, são, por definição, baseados em baterias. Assim, um componente chave da norma IEEE 802.11 foi definir um modo de stand-by no qual as estações poderiam permanecer num estado de espera, hibernando, ativando-se a partir de um sinal do AP. Tais estratégias irão estender significativamente a vida operacional das baterias e a utilidade da estação para os usuários.

Capítulo 4 - IEEE 802.11: A norma para as novas redes sem fio

Como em qualquer outro padrão IEEE 802.x, o padrão IEEE 802.11 define as regras relativas às sub-camada MAC e camada física [Figura 1.5]. Desta forma, a sub-camada LLC (*Logic Link Control - Controle de Ligação Lógico*) e os níveis superiores não percebem as particularidades da sub-camada MAC e de seus possíveis níveis físicos.

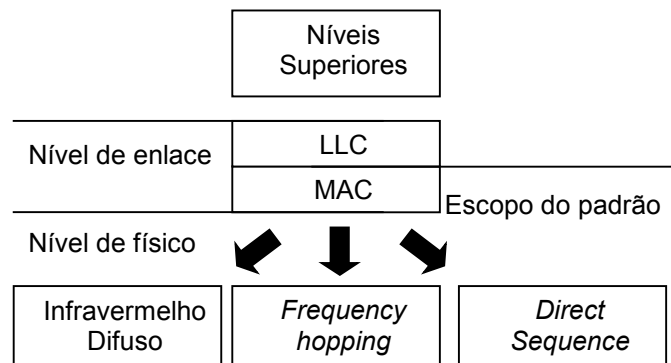


Figura 1.5 - Escopo do Padrão IEEE 802.11

O padrão define três tipos de tecnologia de transmissão sem fio. Isto visa atender necessidades diferentes, porque as primeiras redes sem fio apresentavam-se com essa variedade de nível físico [DAY97]. Duas destas formas de transmissão são de técnicas de difusão de espectro, que é uma exigência nos Estados Unidos para utilização da banda ISM de 2,4 GHz. A outra forma de transmissão é a radiação infravermelha difusa. A vazão nominal destas redes é de 1 a 2 Mbit/s, mas há grupos de trabalho definindo vazões maiores [CHA96].

Observa-se que a transmissão sem fio possui características únicas quando comparadas às das redes fixas, ressaltando-se a alta taxa de erros conjugada a uma vazão limitada. As características do meio podem variar abruptamente no tempo, ou seja, as características de propagação do sinal alteram-se muito rapidamente [CHE94]. Acresce-se que a largura de banda é limitada, tanto por imposição de órgãos regulamentadores, quanto pelas limitações técnicas dos dispositivos de transmissão e recepção. Além disso, a detecção de portadora (essencial para o funcionamento da subcamada MAC pois esta define um algoritmo CSMA) não é confiável e nem rápida

[BAU95]. Por fim, o meio é de domínio público, estando sujeito a interferências e problemas de segurança.

Quanto à segurança, o padrão possibilita autenticação e criptografia dos quadros MAC. Para tanto, define um algoritmo denominado WEP (*Wired Equivalent Privacy*). O WEP utiliza o algoritmo RC4 PRNG da companhia RSA Data Security, Inc [IEE97].

Outros dois problemas graves que constituem desafios a serem resolvidos para a adoção de redes sem fio 802.11: a polêmica levantada sobre problemas de saúde, possivelmente ocasionados pela radiação eletromagnética em alta frequência, que também se aplica a redes sem fio; e, o consumo de energia. Não há ainda conclusões definitivas sobre malefícios originados pela transmissão celular, e muitos estudiosos acreditam que estes problemas não se aplicariam a dispositivos sem fio, uma vez que a transmissão ocorre a uma distância segura do cérebro dos usuários [DAY97].

O consumo de energia torna-se um problema na medida em que: (i) não se prevê aumento significativo em armazenagem de energia até o ano de 2005 (um máximo de 20% em relação às capacidades das baterias em 1995) [SOU97]; (ii) os computadores sem fios (laptops) possuem cada vez mais dispositivos, multimídias inclusive, com processadores mais potentes, aumentando o consumo de energia destes dispositivos. Para aliviar a demanda de energia, o padrão prevê mecanismos de economia de energia, em que os dispositivos de transmissão passam a consumir significativamente menos (estado *stand-by*).

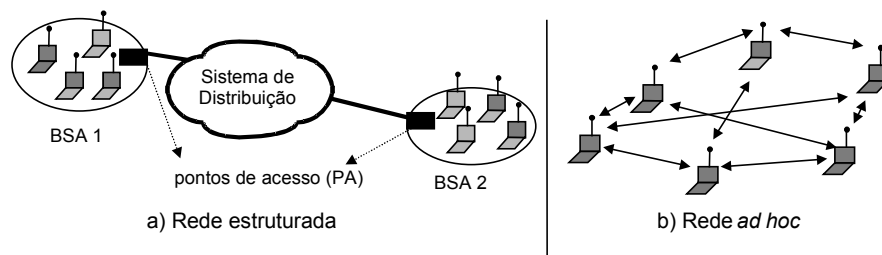


Figura 1.6 - Tipos de Topologia

Redes sem fio 802.11 podem apresentar-se fisicamente de dois modos: redes estruturadas e redes *ad hoc*. Redes estruturadas [Figura 1.6a] caracterizam-se por possuir dois tipos de elementos: estações móveis e pontos de acesso (AP). Cada ponto de acesso é responsável pela conexão das estações móveis de uma área de cobertura

(BSA – *Basic Set Area*) com a rede fixa. O AP desempenha tarefas importantes na coordenação das estações móveis: aceita ou não a inserção de uma nova estação à rede, colhe estatísticas para melhor gerenciamento do canal e ajuda a definir quando uma estação deve ou não ser controlada por outro ponto de acesso. Cada estação está associada a apenas um ponto de acesso em um determinado instante de tempo. Também é nos pontos de acesso que é executada a rotina responsável pela transmissão livre de contenção.

Redes *ad hoc* [Figura 1.6b] caracterizam-se por não possuírem qualquer infraestrutura de apoio à comunicação. São diversas estações móveis confinadas em uma pequena área que estabelecem comunicação *ponto-a-ponto* entre si. Contudo, as características de propagação do sinal não permitem assumir que todas as estações possam comunicar-se sempre entre si.

4.1 Modelo de arquitetura básica da IEEE 802.11

A 802.11 define uma rede celular. A célula básica é chamada de BSS (Basic Service Set – Conjunto de Serviços Básicos). Cada BSS irá conter várias estações (STAs) com uma estação principal chamada de Ponto de Acesso (AP). Se o AP se conecta com outra rede 802 (como uma Ethernet), ele é chamado de Portal. A rede 802 em questão é chamada de DS (Distribution Service – Serviço de Distribuição). Coleções de BSSs e DSs formam um conjunto chamado de ESS (Extended Service System – Sistema de Serviços Estendidos). Apesar da norma não requerer, o AP e o Portal estão, normalmente, no mesmo dispositivo físico.

4.2 Descrição da camada IEEE 802.11

A especificação da camada MAC da 802.11 se encaixa abaixo da parte superior da Camada de Link de Dados (DLL - Data Link Layer) da 802.2, do modelo IEEE padrão. Abaixo disso, três especificações de camadas físicas são definidas:

- FHSS (Frequency Hopping Spread Spectrum), DSSS (Direct Sequence Spread Spectrum) e IR infravermelho - Da FHSS e da DSSS espera-se que operem em 1 ou 2 Mbps nominais. Em adição à funcionalidade normal da camada MAC, a camada MAC da 802.11 também atenta para a fragmentação, remontagem de pacotes e confirmações. Ela também define dois métodos de acesso diferentes: DCF (Distributed Coordination Function – Função de Coordenação Distribuída) e PCF (Point Coordination Function – Função de Coordenação de Ponto).

O método de acesso básico, chamado de DCF, é similar ao Ethernet. Usando uma técnica CSMA/CD, ele executa o CSMA, escutando para sentir se o meio está livre. Se sim, transmite, se não, adia. Contudo, não existe a detecção de colisões (CD – Collision Detect) e, ao invés, é usado o protocolo que evita as colisões (CA – Collision Avoidance). Assim, o protocolo da camada MAC é chamado de CSMA/CA. Existem duas razões pelas quais a abordagem CSMA/CD não foi usada: a primeira é que iria requerer que as estações envolvidas fossem full-duplex, o que iria aumentar o custo significativamente e, a segunda, é que não pode ser assumido que todas as estações possam ouvir todas as outras em todas as situações (como comparado com a Ethernet baseada em fio). Só porque uma estação está pronta para transmitir e percebe que o meio está livre ao seu redor, não significa que o meio esteja liberado ao redor do receptor. Adicionalmente, a norma define um termo chamado VCS (Virtual Carrier Sense – Percepção de Portadora Virtual). De forma a reduzir a probabilidade de que uma estação esteja “escondida” (e, portanto, não possa ouvir), o transmissor envia uma pequena mensagem, RTS, ao receptor, indicando o assunto e o tempo de duração aproximado. O receptor irá responder com um CTS, se for apropriado. Todas as estações que percebam este processo, irão marcar seu NAV (Network Allocation Vector – Vetor de Alocação de Rede) indicando que acusaram o “uso” da portadora virtual. Tal negociação irá reduzir as probabilidades de colisões e a probabilidade de uma estação não ouvir corretamente. A norma define um parâmetro de limite para o RTS de forma a que pequenas mensagens não experimentem um aumento de carga. Finalmente, se o transmissor detecta ocupação do meio, ele recua, como visto mais adiante. Em termos

de seqüências de tempo, o protocolo básico se comporta como o mostrado na Figura 1.7.

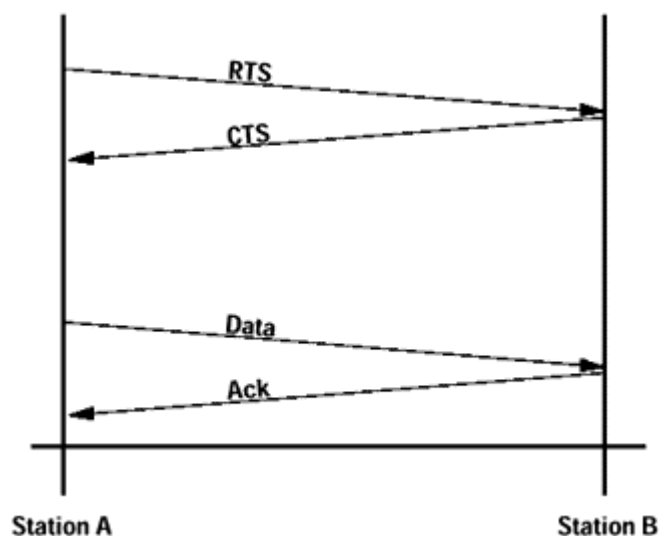


Figura 1.7 - Protocolo básico de conexão

4.3 Fragmentação e Remontagem

Os pacotes Ethernet podem variar, no tamanho, até ao limite de 1518 bytes e, de fato, para maximizar sua taxa de transferência, deve-se usar os pacotes tão grandes quanto possível. Isto nem sempre é o caso com a 802.11. Existem boas razões para fazer com que o tamanho dos pacotes das WLANs sejam menores. Elas incluem o inerentemente mais alto BER (Bit Error Rate – Taxa de Erros de Bit) da transmissão de rádio, os menores custos de retransmissão de pacotes menores e, no caso da FHSS, a frequência é tipicamente mudada a cada 100 milissegundos. Além disso, os fornos de microondas possuem um ruído de 4 milissegundos e um ciclo de canal livre de, também, 4 milissegundos, o qual tem aproximadamente o tamanho de um pacote completo Ethernet, fazendo-o assim altamente suscetível à ocorrência de colisões, forçando a retransmissão. Assim, o protocolo força abordagens de fragmentação do frame, de remessa do frame e de espera. Portanto, parte do protocolo MAC é usado para dividir o frame em vários fragmentos e enviar os vários fragmentos até que toda a mensagem seja recebida.

4.4 Espacejamento inter-frames (Inter Frames Spacing)

Os formatos básicos do frame, definidos pela norma, se parecem com aqueles mostrados na Figura 1.8.

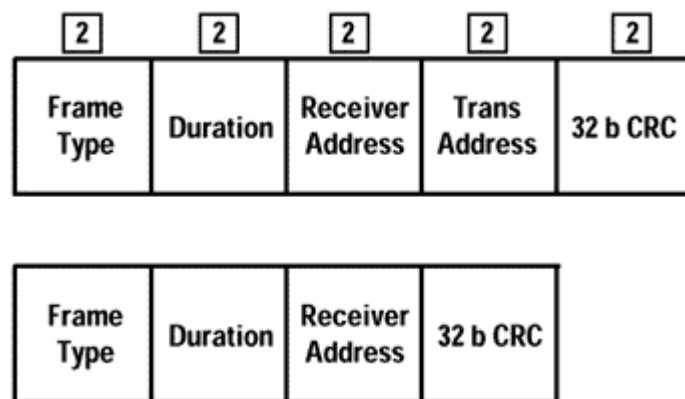


Figura 1.8 - Campos básicos do quadro

Os detalhes precisos dos tamanhos dos campos e de seu conteúdo são explicados na norma. Citam-se, a seguir, os elementos mais importantes para dar uma idéia do teor da camada MAC. Os elementos do frame incluem:

- Último fragmento;
- Re-tentativa - se o frame é uma retransmissão;
- Presença de elementos – o frame não está vazio;
- Duração em microssegundos – para nós escondidos;
- Campos de endereço – todos os 6 bytes;
- Endereço de origem;
- Endereço de destino;
- Endereço do AP;
- Endereço da estação transmissora;
- Endereço da estação receptora;

- Controle de sequência;
- Controle de diálogo;
- Número do fragmento;
- Corpo do frame (de 0 a 2304 bytes de tamanho); e,
- Controle de erro – CRC.

Existem quatro tempos inter-frames especificados para separar as interações da mensagem. Eles são:

1. SIFP (Short Inter Frame Spacing – Espaçamento Inter-Frames Curto) – Este é o tempo máximo que o transmissor tem que respeitar ao esperar uma resposta (por exemplo, de um RTS para um CTS). Para a camada física FS, o valor é de 28 microssegundos.
2. PIFS (Point Coordination Inter Frame Spacing – Espaçamento Inter-Frames por Ponto de Coordenação) – Este é o tempo usado pelo AP para garantir acesso ao meio antes de qualquer outra estação. É definido para ser um SIFP acrescido de um espaço de tempo ou cerca de 78 microssegundos.
3. DIFS (Distributed Inter Frame Spacing – Espaçamento Inter-Frames Distribuído) – Este é o tempo que uma estação espera quando quer iniciar uma conversação. Ele é um PIFS acrescido de um espaço de tempo ou 128 microssegundos.
4. EIFS (Extended Inter Frame Spacing – Espaçamento Inter-Frames Estendido) – Este é o tempo que uma estação deve esperar se não entendeu uma mensagem de definição de tempo, antes de mandar qualquer outra coisa. Caso contrário, a mensagem da estação iria provavelmente colidir com outros pacotes que estejam chegando.

4.5 Back Off Exponencial

O método de Backoff usado na 802.11 é similar ao da Ethernet. Usando a definição de espaço de tempo (o tempo no qual uma estação pode verificar se o meio está em uso ou cerca de 64 microssegundos), cada estação seleciona um número aleatório de espaço de tempo entre 1 e um máximo, e o usa para esperar para uma nova tentativa. Se o meio ainda está ocupado, ela incrementará este tempo pelo máximo (por isso o uso da palavra “exponencial”). Na 802.11, o backoff exponencial é executado quando:

- A estação percebeu que o meio está ocupado no momento que se prepara para transmitir;
- Após cada retransmissão; e,
- Após cada transmissão com sucesso.

A única vez que uma estação não executará um backoff exponencial será quando o meio estiver liberado por um tempo superior a um DIFS e tem algo mais a enviar.

4.6 Como uma estação se conecta

Uma estação necessita se conectar a uma BSS quando ela é ligada pela primeira vez. Ela pode fazer isso de duas formas:

- Scaneamento passivo (passive scanning) – A estação espera por uma mensagem de quadro Beacon (Beacon frame) vinda do AP. Esta mensagem é enviada periodicamente para verificar por uma informação de sincronização nova ou incluída.
- Scaneamento ativo (active scanning) – A estação envia um quadro de requisição de sonda (Probe Request Frame), o qual é uma requisição para o AP para reconhecimento de sua existência. Então espera um quadro de

resposta de sonda (Probe Response Frame). Em caso negativo, a estação salta então para o próximo canal e tenta de novo.

4.7 Processo de sincronização

A sincronização para os saltos é crucial bem como o são outros sinais de temporização necessários. O AP faz isto através do envio de um quadro Beacon, o qual contém um sinal de tempo originário do AP. Note-se que este é o tempo atual em que o quadro é transmitido e não o tempo em que ele é enfileirado, o qual pode ser significativamente diferente em função do algoritmo de colisão. As estações receptoras alteram então seus clocks de acordo com o novo valor.

4.8 O processo de autenticação

Qualquer dos dois métodos acima é aceitável para a inclusão na célula. Após a conexão inicial, o AP e a estação entram no processo de autenticação, no qual eles trocam senhas e outras informações pertinentes.

4.9 O processo de associação

Quando a estação for autenticada, o AP começa o processo de associação. As capacidades básicas de cada um são trocadas e registradas. As características da estação são gravadas e trocadas com o AP. Somente após este processo ter sido completado é que a estação pode transmitir e receber dados.

4.10 Roaming

O roaming é um processo de movimentação de uma BSS (célula) para outra, sendo a comutação feita de uma forma suave. Ele é similar ao roaming em telefones celulares, exceto que o roaming em uma WLAN é feito em função dos limites dos pacotes. O modo como isto é feito não é definido pela norma mas deixado para os fornecedores definirem em suas ofertas proprietárias. Conseqüentemente, deve-se tomar cuidado com soluções que envolvam muito fornecedores em face da possibilidade de problemas de interoperabilidade. Outro item relacionado a implementações diversas diz respeito à velocidade de comutação no roaming. Algumas implementações são mais rápidas que outras, o que também contribui para problemas de interoperabilidade.

Além disso, outros dois itens se fazem importantes notar:

- Segurança por que a WLAN é sem fio - A segurança é de extrema importância. O comitê definiu o termo WEP (Wired Equivalent Protection – Proteção Equivalente ao Fio), para forçar a que uma WLAN seja tão segura quanto uma LAN.
- Restrição de acesso – A idéia aqui é fornecer algo semelhante à chave física usada na LAN. É assumido que áreas de acesso serão protegidas com um mecanismo similar.

4.11 Escuta clandestina

Cada mensagem é encriptada usando um gerador de números pseudo-randômico padrão (PRNG – Pseudo-Random Number Generator), baseado em um software que usa o algoritmo RSA RC4. Esse método é considerado razoavelmente forte já que seria necessário um esforço considerável para tentar quebrá-lo. O fato de que cada mensagem contém um novo Vector de Inicialização (Initializing Vector), o qual gera um novo PRNG, faz com que seja ainda mais difícil de ser quebrada. Seria mais fácil copiar a chave para o laboratório.

4.12 Economia de Energia

As WLANs dão ênfase ao uso de dispositivos portáteis. Estes usam baterias e a energia das baterias é um recurso bem escasso. Assim, a norma foi longe tentando definir um modo de economia de energia. Basicamente, permite que uma estação “vá dormir”. O AP mantém registro de quaisquer mensagens, armazenando-as até que a estação “acorde”.

4.13 Estágio atual da 802.11

A norma 802.11 define assim uma camada MAC compatível com a 802, que pode interoperar com outras tecnologias padrão 802. Três normas físicas são definidas: a FHSS, a DSSS e o Infra-vermelho. No momento, o foco da norma é para a banda de 2,4 GHz mas isto deverá mudar para bandas mais altas logo que as mesmas sejam liberadas para uso aberto. Essencialmente, a norma 802.11 fornece redes assíncronas abertas que necessitam de uma função de controle distribuída. As taxas de transferência são de 1 ou 2 Mbps; contudo, fornecedores de WLANs, que sejam criativos e que possuam peritos em processamento de sinais digitais e de rádio, podem produzir produtos com taxas superiores a 3 Mbps, e mesmo que sejam usados em velocidades mais baixas para conversar com dispositivos 802.11 continuarão sendo compatíveis com a 802.11.

4.14 Conclusão do capítulo

Com o acordo para a norma IEEE 802.11, existe uma nova norma que permite a implementação de WLANs. Pode-se esperar que muitos fornecedores tragam produtos compatíveis com a 802.11 para o mercado em números cada vez maiores e com menores custos. Mais, os fornecedores irão prover soluções completas que irão permitir a construção de WLANs e também integrar as LANs com fio existentes com os novos

componentes. Usando protocolos padrão de gerenciamento, tais como o SNMP, os usuários serão capazes de integrar seus componentes wireless com seus sistemas legados e, assim protegendo suas antigas LANs, enquanto alavancam vantagens a partir das novas capacidades dos produtos emergentes das WLANs. Como já notado no início, a transformação original do poder da computação completa finalmente sua evolução dos mainframes, ambientes não amigáveis aos clientes, para situações amigáveis ao cliente e que colocam o poder computacional e das redes aonde ele deve estar: com o cliente.

Concluindo, quando se considera o custo total de propriedade, incluindo o sempre crescente custo de manutenção e o custo das oportunidades perdidas, o negócio com as WLANs se torna uma opção obrigatória para análise. O gerente de redes da empresa deve entender tanto a tecnologia quanto o negócio envolvido nas redes sem fio (WLANs).

Capítulo 5 - Bluetooth

5.1 Introdução

Os padrões e tecnologias Bluetooth fornecem os meios para a substituição dos cabos que conectam um dispositivo a outro, usando um link de rádio universal de baixo alcance. A tecnologia foi originalmente desenvolvida para substituir cabos, mas já evoluiu para viabilizar a possibilidade de conexão entre várias unidades.

Um estudo foi iniciado na Ericsson em 1994 para descobrir uma interface por rádio com baixo custo e de baixa potência entre telefones móveis e seus acessórios. As especificações referentes a preço, capacidade e tamanho foram definidas para que a nova técnica pudesse ter o potencial de substituir todas as soluções usando cabos entre dispositivos móveis. Inicialmente, uma interface adequada de rádio com a faixa de frequência correspondente tinha que ser definida. A unidade de rádio tinha que ser tão pequena e consumir tão pouca energia que pudesse ser colocada em dispositivos portáteis com suas próprias limitações. O conceito tinha que lidar com dados e voz e também precisaria funcionar em qualquer parte do mundo.

O estudo logo mostrou que a solução com rádio era factível. Quando os projetistas da Ericsson começaram a trabalhar num chip de transmissão logo constataram que necessitariam de ajuda para desenvolver a técnica. Os associados trabalhariam não só para melhorar as soluções técnicas mas também para obter um grande e sólido suporte de mercado nas áreas de hardware de PCs, computadores portáteis e telefones móveis.

Ericsson, Intel, IBM, Toshiba e Nokia formaram um Grupo de Interesse Especial (Special Interest Group - SIG) em 1998. Este grupo representava o suporte de mercado diversificado necessário para viabilizar a nova tecnologia. Em maio do mesmo ano, o consórcio Bluetooth foi anunciado. A intenção do SIG Bluetooth é definir um padrão de fato para interface aérea e para o software que a controla. O objetivo é atingir interoperabilidade entre dispositivos diferentes de diferentes fornecedores de computadores portáteis, telefones móveis e outros dispositivos.

O nome Bluetooth vem de um rei viking dinamarquês, Harald Blåtand (Bluetooth, em inglês), que viveu no final do século X. Harald Blåtand uniu e controlou a Dinamarca e a Noruega.

5.2 SIG Bluetooth

Em fevereiro de 1998 foi fundado o SIG Bluetooth. No começo consistia das cinco empresas citadas acima. Atualmente, mais de 2000 empresas já se associaram ao SIG de forma a trabalhar em um padrão aberto para o conceito Bluetooth. Assinando um acordo com custo zero, empresas podem se associar ao SIG e se qualificar para uma licença, livre de encargos, para construir produtos baseados na tecnologia Bluetooth.

Uma pesquisa da Cahners In-Stat Group estima que, já neste ano, serão vendidos 15 milhões de dispositivos Bluetooth no mundo. Mas esse número deve crescer para quase 1 bilhão em 2005.

Para evitar diferentes interpretações do padrão Bluetooth relativas à forma como um tipo específico de aplicação deva ser mapeada para o Bluetooth, o SIG definiu uma série de modelos e perfis de protocolos. Estes são descritos em mais detalhes na seção intitulada Perfis e Modelos de Utilização Bluetooth.

O SIG também trabalha com um processo de qualificação. Este processo define critérios para a qualificação dos produtos Bluetooth o qual assegura que os produtos que passem neste processo obedecem à especificação Bluetooth.

5.3 Porquê Bluetooth?

A remoção das conexões por cabo entre o telefone móvel e seus acessórios foi a origem do conceito Bluetooth. Esta tecnologia pretende ligar instantaneamente os dispositivos mais variados numa distância entre 10 e 100 metros. Um computador conectado a um teclado, um mouse, um par de alto-falantes, um PDA e outros, é uma situação onde uma solução sem fio seria proveitosa. A necessidade de diferentes

dispositivos serem colocados lado a lado também pode ser eliminada. Ao contrário, a localização dos dispositivos é somente limitada pela localização da fonte de energia.

Outro motivo para a tecnologia Bluetooth são os problemas com a conexão e configuração de dispositivos móveis. Para conectar um novo dispositivo se torna necessário um cabo, normalmente específico para aquele dispositivo. Quando a conexão física é estabelecida, normalmente se segue uma complicada configuração da conexão. Com as técnicas de substituição de cabos existentes, a segurança na transmissão de dados é insuficiente. Estas dificuldades estão também contempladas no desenvolvimento da técnica Bluetooth.

A introdução do Nokia Communicator 9000 tem sido descrita como um evento que aumentou o interesse no desenvolvimento do Bluetooth. O Communicator reduziu a complexidade na conexão de um telefone móvel com um computador através da construção de uma unidade dois-em-um para resolver o problema. A combinação de dois dispositivos em um surgiu como uma ameaça aos grandes fabricantes de computadores portáteis. E se as pessoas comessem a comprar comunicadores dos fornecedores de telefones móveis ao invés de PC's portáteis da IBM ou Toshiba?

Outros motivos para uma nova técnica de substituição de cabos são:

- O número de usuários de PC's portáteis está aumentando. Isto implica um maior mercado para conexões sem fio de dispositivos.
- A constante diminuição do tamanho dos PC's portáteis tem levado para soluções onde os dispositivos, drives de CD-ROM por exemplo, são externos e necessitam ser conectados suavemente ao PC.
- Os computadores móveis estão competindo com os computadores de mesa em termos de performance. A necessidade de um computador fixo no escritório e de um computador portátil para viajar está diminuindo.

A técnica Bluetooth fornece uma solução para os problemas descritos acima. A solução elimina os aborrecidos cabos e suas limitações concernentes a flexibilidade e alcance. Mas, o Bluetooth significa mais que isso. A técnica provê os meios para conectar várias unidades entre si se as mesmas forem qualquer tipo de dispositivo

Bluetooth. Uma diversidade de cenários podem ser descritos. Eles demonstram possibilidades que vão bem além da eliminação do cabo ponto-a-ponto.

5.4 Visão da arquitetura Bluetooth

Aqui se descreve a arquitetura Bluetooth. A pilha de protocolo completa compreende, como visto na figura 2.1, protocolos específicos para Bluetooth e protocolos não específicos para Bluetooth. Os protocolos não específicos estão hachurados.

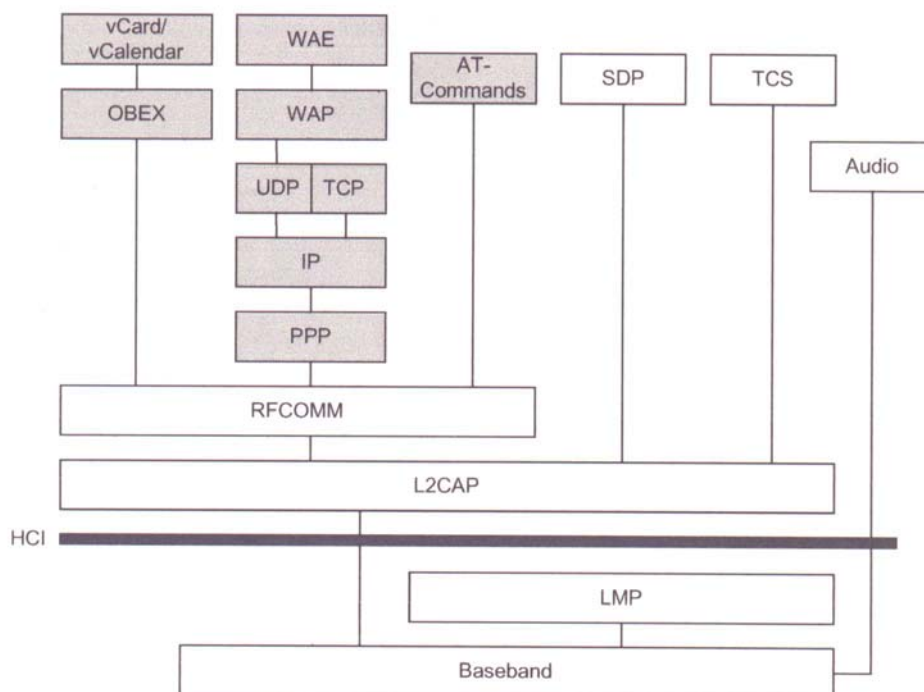


Figura 2.1 - A pilha de protocolos do Bluetooth

5.5 A estratégia da arquitetura Bluetooth

Uma diversidade de perfis foi definida pela organização de padronização do Bluetooth. Estes perfis foram desenvolvidos de forma a descrever como a implementação dos modelos de utilização deve ser elaborada. Os modelos de utilização

descrevem uma série de cenários onde o Bluetooth executa a transmissão por rádio. Estes perfis especificam como as aplicações e dispositivos serão mapeados considerando o conceito Bluetooth.

Um perfil define uma seleção de mensagens e procedimentos em conformidade com as especificações Bluetooth e faz uma descrição inequívoca da interface aérea para serviços especificados e estudo de casos. Um perfil pode ser descrito como uma fatia vertical da pilha de protocolo. Ele define opções, em cada protocolo, que são mandatórios para o perfil. Ele também define uma série de parâmetros para cada protocolo. O conceito de perfil é usado para diminuir o risco de problemas de interoperabilidade entre produtos de diferentes fornecedores.

O perfil definido para a troca de informações vCard é ilustrada na Figura 2.2, onde uma aplicação, vCard, é definida para operar sobre um certo subconjunto (OBEX, RFCOMM e seguintes) da pilha de protocolo Bluetooth. Alguns dos modelos de utilização e seus perfis são descritos na seção de Perfis e Modelos de Utilização Bluetooth.

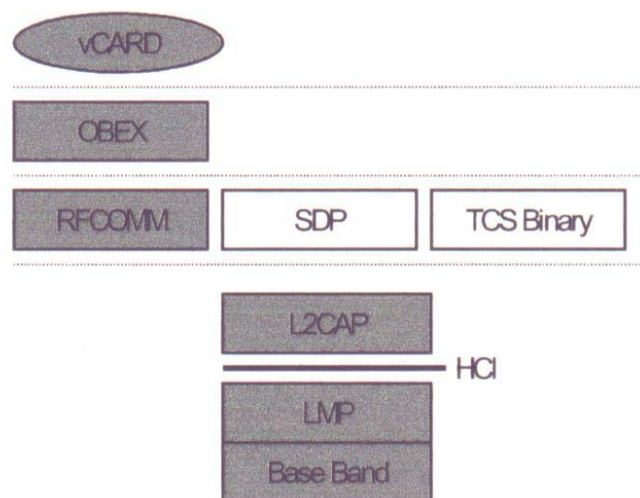


Figura 2.2 - O perfil do objeto vCARD

Existem quatro perfis genéricos definidos, sobre os quais alguns dos modelos de utilização de mais alta prioridade e seus perfis são baseados diretamente. Estes quatro modelos são: o GAP (Generic Access Profile - Perfil de Acesso Genérico); o SPP

(Serial Port Profile - Perfil de Porta Serial); o SDAP (Service Discovery Application Profile - Perfil de Aplicação de Descoberta de Serviço); e, o GOEP (Generic Object Exchange Profile - Perfil de Troca de Objeto Genérico).

Protocolos como o OBEX e UDP foram incluídos na arquitetura do protocolo para facilitar a adaptação das aplicações que usem tais protocolos. Isto possibilita, por exemplo, que as aplicações baseadas em UDP tenham uma interface com o Bluetooth.

5.6 Perfis e Modelos de Utilização Bluetooth

Nesta seção, são discutidos os quatro perfis gerais: GAP, SPP, SDAP e GOEP. Uma série de modelos de utilização são identificados pelo SIG Bluetooth como fundamentais e, portanto, são destacados na documentação Bluetooth. Alguns destes modelos de utilização e seus perfis respectivos são descritos nesta seção. Note-se que para cada modelo de utilização existe um ou mais perfis correspondentes. Os perfis Bluetooth e seus relacionamentos são mostrados na Figura 2.3.

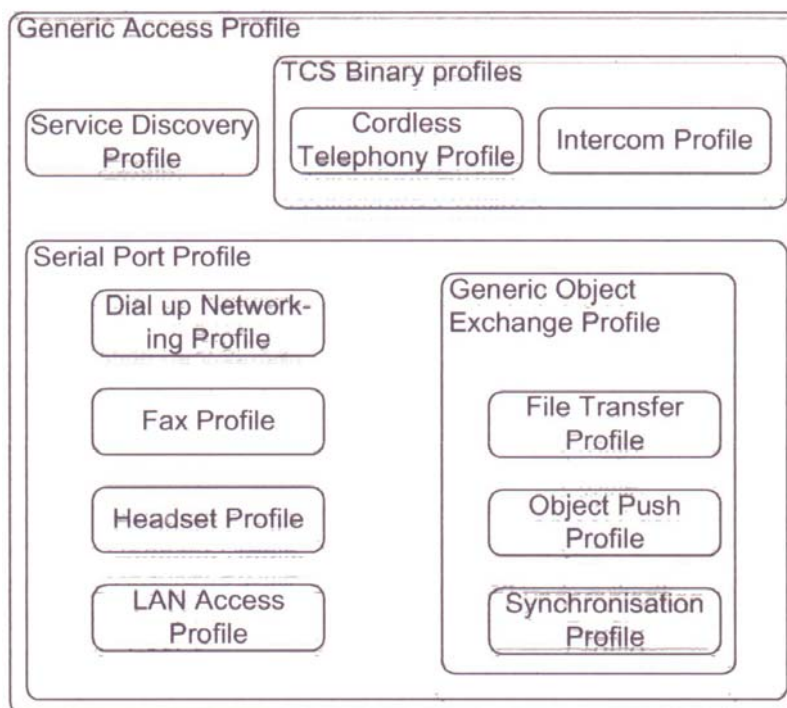


Figura 2.3 - Os perfis Bluetooth

Os quatro perfis descritos nesta seção formam a base para os modelos de utilização e seus perfis. Os perfis também fornecem as fundações para modelos de utilização futuros e seus perfis.

5.6.1 GAP

O Perfil de Acesso Genérico, GAP, define como duas unidades Bluetooth descobrem e estabelecem uma conexão entre si. O GAP gerencia a descoberta e estabelecimento de conexão entre unidades desconectadas. O perfil define operações que são genéricas e pode ser usado por perfis que referenciem o GAP e por dispositivos que implementem perfis múltiplos.

O GAP assegura que duas unidades Bluetooth quaisquer, independentemente de fornecedor ou aplicação, possam trocar informações através do Bluetooth visando descobrir que tipo de aplicações a unidade suporta. Unidades Bluetooth que não estejam em conformidade com qualquer outro perfil Bluetooth devem suportar, pelo menos, o GAP de forma a assegurar interoperabilidade e coexistência básica.

5.6.2 SDAP

O Perfil de Aplicação de Descoberta de Serviço, SDAP, define a investigação de serviços disponíveis para uma unidade Bluetooth. O perfil gerencia a procura por serviços específicos e conhecidos bem como a busca de serviços genéricos.

O SDAP envolve uma aplicação, a Aplicação Usuária de Descoberta de Serviço, a qual é necessária, em uma unidade Bluetooth, para localizar serviços. Esta aplicação faz a interface entre o Protocolo de Descoberta de Serviço, que manda e recebe consultas de serviço, das unidades Bluetooth envolvidas. Assim, o SDAP descreve uma aplicação que faz interface com um protocolo Bluetooth específico para tirar vantagem total do mesmo e, portanto, beneficiar diretamente o usuário final.

O SDAP é dependente do GAP, isto é, o SDAP reutiliza partes do GAP.

5.6.3 SPP

O Perfil de Porta Serial, SPP, define como criar portas seriais virtuais em dois dispositivos e como conectá-las com o Bluetooth. A utilização deste perfil fornece às unidades Bluetooth uma emulação de um cabo serial usando a sinalização de controle padrão RS232 (RS232 é um padrão de interface comum usado em equipamentos de comunicação de dados). O perfil assegura que taxas de transferência de até 128 Kbps podem ser usadas.

Este perfil, da mesma forma que o SDAP, é dependente do GAP e, portanto, reutiliza partes do GAP.

5.6.4 GOEP

O Perfil de Troca de Objeto Genérico, GOEP, define o conjunto de protocolos e procedimentos a ser usado pelas aplicações que gerenciem trocas de objetos. Uma série de modelos de utilização, descritas na seção Modelos de Utilização Bluetooth, são baseados neste perfil. São exemplos, a Transferência de Arquivos (File Transfer) e a Sincronização (Synchronisation). Unidades típicas Bluetooth que usam este perfil são os notebooks, os laptops, os palmtops, os PDAs, os telefones móveis e os telefones inteligentes.

Aplicações que usam o GOEP assumem que os elos e canais estão estabelecidos, como definido pelo GAP. O GOEP descreve o procedimento necessário para trafegar dados de uma unidade Bluetooth para outra.

O GOEP é dependente do Perfil de Porta Serial.

5.7 Modelos de Utilização Bluetooth

Nesta seção são descritos alguns modelos de utilização Bluetooth. Para cada modelo de utilização existe um ou mais perfis correspondentes definindo camadas de protocolo e funções a serem usadas.

5.7.1 Transferência de Arquivos

O modelo de transferência de arquivos (File Transfer) oferece a capacidade de transferir objetos de dados de um dispositivo Bluetooth para outro. Arquivos, pastas inteiras, diretórios e formatos de mídia por streaming são suportados por este modelo. O modelo também possibilita paginar o conteúdo das pastas em um dispositivo remoto. Além disso, operações de troca também são suportados por este modelo como, por exemplo, a troca de dados de cartões de negócios usando o formato vCard. O modelo de transferência de arquivos é baseado no GOEP.

5.7.2 Ponte para Internet (Internet Bridge)

O modelo de ponte para internet descreve como um telefone móvel ou um modem sem fio disponibiliza, para um PC, capacidades de rede através de recursos dial-up sem a necessidade de conexão física com o PC. Este cenário de rede requer um protocolo de duas camadas, uma para os comandos AT que controlam o telefone móvel e outra para transferir os dados.

5.7.3 Acesso a Redes Locais

O modelo para acesso a rede local é similar ao modelo de ponte para internet. A diferença é que o modelo para acesso a rede local não utiliza os protocolos para os comandos AT. O modelo descreve como terminais de dados usam um ponto de acesso da rede como uma conexão sem fio a uma LAN. Quando conectado, os terminais de dados operam como se eles estivessem conectados à LAN através de uma rede dial-up.

5.7.4 Sincronização

O modelo de sincronização fornece os meios para a sincronização automática entre, por exemplo, um PC de mesa, um PC portátil, um telefone móvel e um notebook. A sincronização requer que as informações referentes a tarefas e calendário, por

exemplo, sejam transferidas e processadas pelos computadores, telefones celulares e PDA's usando um protocolo e formato comum.

5.7.5 Telefone três-em-um

O modelo de telefone três-em-um descreve como uma base de telefone pode ser conectada a três provedores de serviços distintos. O telefone pode operar como um telefone sem fio se conectando à rede pública de telefone em casa, como se fosse um telefone fixo. Este cenário inclui a elaboração de chamadas através de uma estação base de voz e fazendo chamadas diretas entre dois terminais usando a estação base. O telefone também pode se conectar diretamente com outros telefones operando como um "walkie-talkie" ou extensão. Finalmente, o telefone pode operar como um telefone celular conectado à infra-estrutura celular. Os cenários de intercomunicação e sem fio usam a mesma pilha de protocolos.

5.7.6 Fone de ouvido

O modelo de fone de ouvido define como um fone de ouvido sem fio Bluetooth pode ser conectado para operar como uma unidade de rádio remota para interface de entrada e saída. A unidade é, provavelmente, um telefone móvel ou um PC que tenha entrada e saída de áudio. Da mesma forma que na ponte para internet, este modelo requer duas camadas de protocolo: uma para os comandos AT que controlam o telefone móvel e outra para a transferência de dados, por exemplo, voz. Os comandos AT controlam o telefone no que diz respeito, por exemplo, à resposta e término das chamadas.

5.8 Protocolos centrais do Bluetooth

5.8.1 Banda-base

A banda-base e a camada de controle de link habilitam o link físico de rádio-frequência entre as unidades Bluetooth formando uma piconet. Esta camada controla a sincronização das unidades Bluetooth e a transmissão da sequência de salto de frequência. Os dois tipos diferentes de links do Bluetooth: SCO (Synchronous Connection Oriented - Síncrona Orientada a Conexão) e ACL (Asynchronous Connectionless - Assíncrona Sem Conexão), descritas na seção Tipos de Links, são também gerenciados por esta camada.

Os links ACL, para dados, e os links SCO, principalmente para áudio, podem ser multiplexados para usar o mesmo link de rádio-frequência.

5.8.2 Áudio

Transmissões de áudio podem ser executadas entre uma ou mais unidades Bluetooth usando diversos modelos. O áudio não passa através da camada L2CAP (descrita mais abaixo), mas trafega diretamente, após a abertura de um link Bluetooth, entre duas unidades Bluetooth.

5.8.3 HCI

A HCI (Host Controller Interface - Interface de Controle de Host), provê um método de interface uniforme para acessar recursos de hardware Bluetooth. Ele contém uma interface de comando para o controlador de banda-base e gerenciador do link e para acesso ao estado do hardware. Finalmente, ele contém registros de eventos e de controle.

5.8.4 LMP

O LMP (Link Manager Protocol - Protocolo de Gerenciamento de Link) é responsável pelo acionamento do link entre unidades Bluetooth. Ele gerencia o controle e negociação do tamanho dos pacotes usados na transmissão de dados. O LMP também lida com o gerenciamento dos modos de energia, consumo de força e estado de uma unidade Bluetooth em uma piconet. Finalmente, esta camada trata da geração, troca e controle das chaves para link e encriptação visando autenticação e encriptação.

5.8.5 L2CAP

O L2CAP (Logical Link Control and Adaptation Protocol - Protocolo de Adaptação e Controle de Link Lógico) está situado acima da camada da banda-base e do LMP. Ela fornece serviços de dados orientados a conexão e sem conexão às camadas superiores.

As quatro principais tarefas do L2CAP são:

- Multiplexação - O L2CAP deve suportar a multiplexação de protocolos já que diversos protocolos (por exemplo, SDP, RFCOMM e TCS) podem operar sobre o L2CAP.
- Segmentação e remontagem - Pacotes de dados que excedem a MTU (Maximum Transmission Unit - Unidade de Transmissão Máxima) devem ser segmentados antes de serem transmitidos. Tanto esta como a sua funcionalidade reversa, a remontagem, são executados pela L2CAP.
- Serviços de Qualidade (QOS) - O estabelecimento de uma conexão L2CAP permite a troca de informações concernentes ao serviço de qualidade corrente para a conexão entre as duas unidades Bluetooth.
- Grupos - A especificação do L2CAP suporta uma abstração de grupo que permite implementações para o mapeamento de grupos numa piconet.

Uma implementação L2CAP deve ser simples e implicar em baixa carga já que deve ser compatível com os recursos computacionais limitados numa pequena unidade Bluetooth.

5.8.6 SDP

O SDP (Service Discovery Protocol - Protocolo de Descoberta de Serviço) define como uma aplicação cliente Bluetooth deve se comportar para descobrir os serviços servidores Bluetooth disponíveis e suas características. O protocolo define como um cliente pode procurar por um serviço baseado em atributos específicos sem que o cliente conheça nada sobre os serviços disponíveis. O SDP provê meios para descobrir novos serviços que venham a estar disponíveis quando o cliente entrar em uma área onde um servidor Bluetooth estiver operando. O SDP também fornece funcionalidades para detectar quando um serviço não está mais disponível.

5.9 Protocolo de substituição de cabos

5.9.1 RFCOMM

O protocolo RFCOMM é um protocolo de emulação de portas seriais. O protocolo cobre aplicações que façam uso das portas seriais da unidade. O RFCOMM emula os sinais de controle e dados padrão RS-232 sobre a banda-base Bluetooth. Ele provê capacidades de transporte para os serviços de nível superior. Por exemplo, o OBEX usa uma linha serial como mecanismo de transporte.

5.10 Protocolo de Controle de Telefonia

5.10.1 Controle Binário de Telefonia

O protocolo de controle de telefonia binário, TCS binary ou TCS BIN, é um protocolo orientado a bit, que define a sinalização de controle para o estabelecimento e liberação de chamadas por voz e dados entre unidades Bluetooth. Bem como a sinalização para facilitar o tratamento de grupos de unidades Bluetooth. Além disso, o protocolo provê funcionalidades para a troca de informações sinalizadoras não relacionadas ao progresso das chamadas.

O estabelecimento de uma chamada por voz ou dados numa configuração ponto-a-ponto bem como numa configuração ponto-a-multiponto é coberto neste protocolo (note-se que, após o estabelecimento da chamada, a transmissão é feita ponto a ponto). O TCS BIN é baseada na recomendação ITU-T Q.931.

5.10.2 Comandos AT - Controle de Telefonia

Uma série de comandos AT são suportados para a transmissão de sinais de controle de telefonia. Estes usam a emulação de portas seriais, RFCOMM, para a transmissão.

5.11 Protocolos Adotados

Esta seção descreve uma série de protocolos que estão definidos para serem adotados pela pilha de protocolo Bluetooth.

5.11.1 PPP

O Protocolo Ponto-a-Ponto, PPP, na tecnologia Bluetooth, é designado para acontecer na RFCOMM de forma a completar as conexões ponto-a-ponto. O PPP é um protocolo orientado a pacote e, por isso, deve usar seus mecanismos seriais para converter um fluxo de dados empacotado em um fluxo de dados serial.

5.11.2 TCP/UDP/IP

Os padrões TCP/UDP/IP são definidos para operar em unidades Bluetooth permitindo-lhes que se comuniquem como outras unidades conectadas, por exemplo, à Internet. Dessa forma, a unidade Bluetooth pode operar como uma ponte para a Internet. A configuração de protocolo TCP/IP/PPP é usada para todos os cenários de ponte para a Internet, na Bluetooth 1.0 e para o OBEX, descrito adiante, em versões futuras. A configuração UDP/IP/PPP está disponível como transporte para o WAP.

5.11.3 Protocolo OBEX

O IrOBEX, abreviadamente OBEX, é um protocolo opcional da camada de aplicação projetado para habilitar as unidades a suportar as comunicações por infravermelho visando a troca de uma grande variedade de dados e comandos de uma forma padronizada. O OBEX usa um modelo cliente-servidor e é independente do mecanismo e da API de transporte. O protocolo também define um objeto que permite a paginação do conteúdo de pastas em um dispositivo remoto. A camada RFCOMM é usada como a camada de transporte principal para o OBEX.

5.11.4 WAP

O protocolo de aplicações sem fio, WAP, é uma especificação de protocolo sem fio, que trabalha com uma grande variedade de tecnologias de rede sem fio de grande alcance, que traz a Internet para os dispositivos móveis. O Bluetooth pode ser usado como outras redes sem fio no que diz respeito ao WAP e também pode ser usado para prover um suporte (transportador) para o transporte de dados entre o cliente WAP e o seu servidor WAP adjacente. Além disso, as capacidades de rede "ad-hoc" do Bluetooth possibilitam ao cliente WAP possibilidades de mobilidade únicas comparadas com outros transportadores WAP.

A forma tradicional das comunicações WAP envolve um dispositivo cliente que se comunica com um dispositivo servidor usando protocolos WAP. Espera-se que o Bluetooth forneça um serviço transportador como especificado pela arquitetura WAP.

A tecnologia WAP suporta técnicas de push. Se isto for usado em conjunto com Bluetooth, se abrem novas possibilidades para a distribuição de informações a dispositivos de mão em bases locais. Por exemplo, lojas podem disponibilizar ofertas de preços especiais para clientes WAP que estejam ao alcance do Bluetooth.

5.12 A interface aérea Bluetooth

Para atender aos requisitos da interface aérea foi escolhida a faixa de frequência entre 2,4 e 2,5 GHz. Assim, os requisitos referentes à operação de alcance mundial, suporte para dados e para voz e as limitações concernentes às características físicas (tamanho e consumo de energia) foram atendidos. Esta faixa de rádio-frequência é a banda ISM e varia, na Europa e nos Estados Unidos, de 2,400 a 2,4835 GHz (na França e na Espanha somente partes deste intervalo estão disponíveis). Como resultado, os dispositivos Bluetooth devem ser capazes de atuar na faixa de frequência definida e devem poder selecionar o segmento da banda ISM na qual irão trabalhar. A banda ISM está aberta para qualquer sistema de rádio. Telefones sem fio, controles para abertura de

portões e fornos de microondas operam nesta banda, sendo que os fornos de microondas são as maiores fontes de interferências.

As unidades Bluetooth se conectam entre si formando as chamadas *piconet*, compostas de até oito unidades Bluetooth ativas.

5.12.1 A técnica de salto de frequência

Interferências são evitadas pelo uso do salto de frequência, FH, na tecnologia spread spectrum. Esta tecnologia é bem adequada para implementações de rádio de baixo custo e de baixa potência e é usada em alguns produtos de rede sem fio. A principal vantagem com a escolha de parâmetros do Bluetooth é a maior taxa de saltos, 1600 saltos por segundo, ao invés de somente alguns poucos saltos por segundo. O tamanho de pacote menor da tecnologia Bluetooth é outro benefício.

A faixa de frequência em sistemas FH é dividida em uma série de canais de salto. Cada canal de salto é uma fração da faixa de frequência total. No Bluetooth um canal é usado por 625 microssegundos seguido por um salto, numa ordem pseudo-aleatória, para outro canal para mais 625 microssegundos de transmissão, o que se repete constantemente. Desta forma os saltos espalham o tráfego Bluetooth por toda banda ISM e um sistema com uma boa proteção contra interferências é alcançado. Se uma das transmissões é prejudicada por, por exemplo, uma onda de um forno de microondas, a possibilidade de interferência no próximo canal utilizado é bem baixa. Algoritmos de correção de erros são usados para corrigir a falha causada por transmissões com interferências.

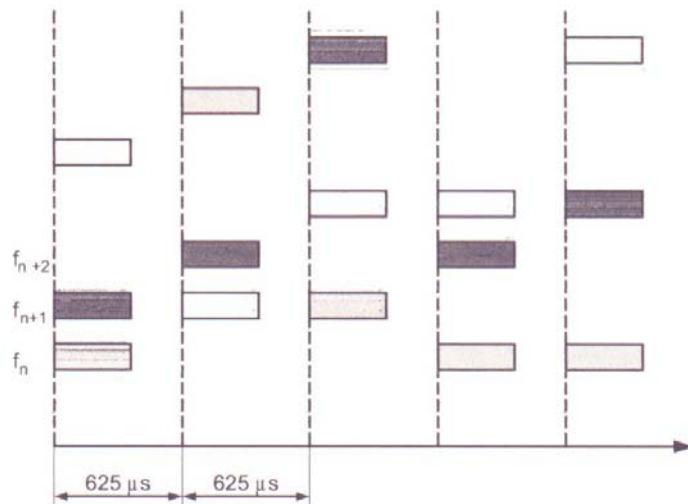


Figura 2.4 - Salto de frequência por divisão de tempo

5.12.2 Modulação/Transmissão e definição de pacote

Uma modulação FSK binária é usada para reduzir a complexidade de transmissão/recepção nas unidades Bluetooth. A capacidade de transmissão full duplex é alcançada pela utilização do duplex por divisão de tempo e slots subsequentes são usados para transmitir e receber. O protocolo de banda-base Bluetooth é uma combinação de comutação de pacotes e circuitos. A reserva de slots pode ser feita para pacotes síncronos. Um pacote usualmente utiliza um slot, mas um método de múltiplos slots é também definido nas especificações Bluetooth. Pacotes de múltiplos slots podem usar três ou cinco slots. Pacotes são sempre remetidos em um canal com salto simples. Isto significa que quando pacotes de múltiplos slots são transmitidos, a frequência de salto é reduzida e não existe salto até que todo o pacote seja remetido. Isto é ilustrado na Figura 2.5. O canal usando o pacote branco começa a sequência ilustrada com um pacote de múltiplos slots cobrindo três slots. Ressalte-se que o canal seguinte, após o pacote de múltiplos slots, é o mesmo (comparando-se com a Figura 2.4) como se não tivesse existido um pacote de múltiplos slots.

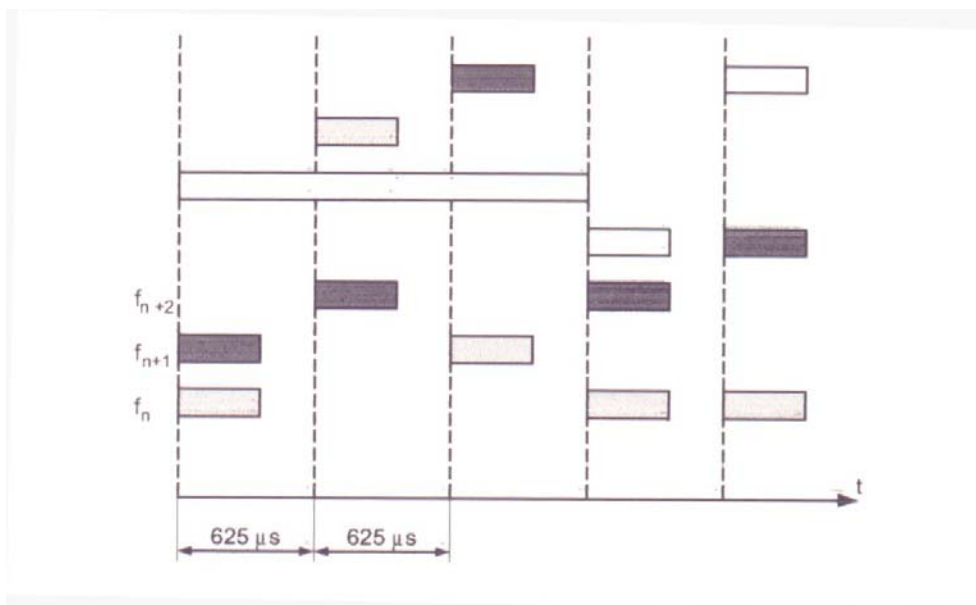


Figura 2.5 - Um pacote com múltiplos slots

5.12.3 Redes Bluetooth

Quando unidades Bluetooth se comunicam, uma delas é a mestre e as restantes se comportam como escravas. O clock de sistema da unidade mestre e a identidade mestre são as partes centrais na tecnologia de salto de frequência. O canal de salto é determinado pela sequência de salto e pela fase nesta sequência. A identidade da mestre determina a sequência e o clock de sistema da unidade mestre determina a fase. Na unidade escrava, um incremento pode ser adicionado ao seu clock de sistema para criar uma cópia do clock mestre. Desta maneira, cada unidade na conexão Bluetooth guarda os clocks sincronizados e a identidade mestre o que identifica de forma única a conexão. Saltos sincronizados com a mestre podem, portanto, ser alcançados como descrito na Figura 2.6. Foram definidas 79 possibilidades de salto para a tecnologia Bluetooth exceto na França e na Espanha onde existem somente 23 possibilidades, isto porque a banda ISM, nesses países, é mais limitada.

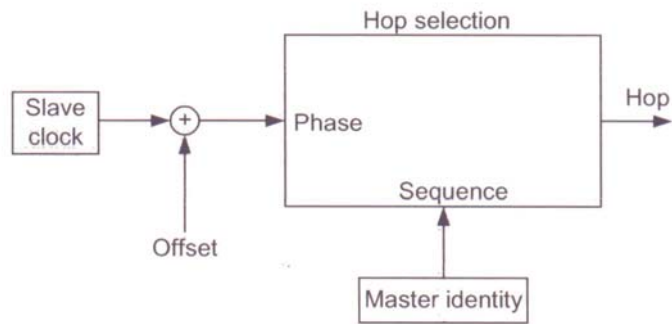


Figura 2.6 - A seleção de saltos

Os pacotes Bluetooth têm um formato fixo. Um código de acesso de 72 bits vem no início do pacote. O código de acesso é baseado na identidade e clock de sistema do mestre, provendo os meios para sincronização. Este código é único para o canal e é usado por todos os pacotes transmitidos num canal específico. Um cabeçalho de 54 bits segue o código de acesso. Este cabeçalho contém informações de correção de erros, retransmissão e controle de fluxo. A informação de correção de erros pode ser usada para corrigir falhas na carga útil e no próprio cabeçalho. Finalmente se segue o campo de conteúdo com qualquer coisa entre 0 e 2.745 bits ou cerca de 340 bytes.

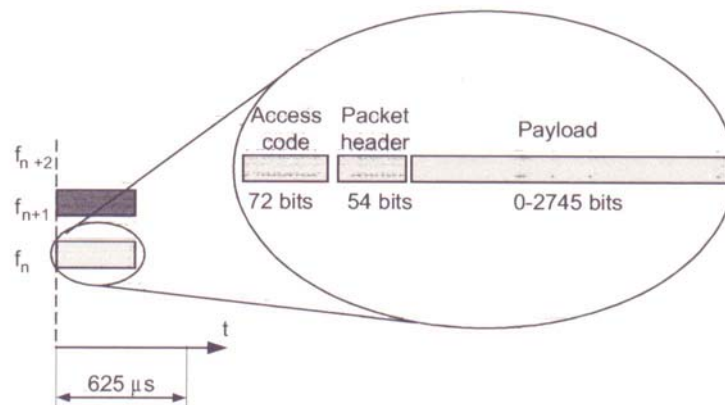


Figura 2.7 - O formato do pacote Bluetooth

5.12.4 Parâmetros de rádio

Unidades Bluetooth operam na banda ISM em 2,45 GHz. A potência de transmissão está compreendida entre 1 e 100 mW. Os transmissores de rádio-freqüência

são bem pequenos. O módulo de rádio Bluetooth de 1 mW, da Ericsson, mede somente 10,2x14x1,6 mm. O baixo consumo de potência implica que uma unidade Bluetooth pode operar com uma pequena bateria por longos períodos (meses). Estas características de hardware tornam possível encaixar uma unidade Bluetooth em vários dispositivos elétricos. O alcance máximo Bluetooth é de 10 metros, com a possibilidade de ser estendido a até 100 metros.

A máxima taxa de transferência é de 1 Mbit/s. A máxima carga útil efetiva é baixa porque as diferentes camadas de protocolo usam dados na carga útil para sinalizar suas camadas correspondentes na unidade com a qual o dispositivo está se comunicando. Estimativas têm indicado taxas de transferência de até 721 Kbit/s.

5.12.5 Tipos de link

Dois tipos de link foram definidos, o ACL e o SCO. Quando duas unidades Bluetooth se comunicam, estabelecem uma piconet (capaz de lidar com até oito dispositivos Bluetooth). Um dos dispositivos da piconet sempre exerce o papel de mestre. Pares mestre-escravo diferentes, na mesma piconet, podem usar diferentes tipos de links. O tipo de link pode ser modificado durante a sessão. Os links SCO suportam conexões simétricas, por comutação de circuitos e ponto-a-ponto e são, portanto, primariamente usados para tráfego de voz. Dois espaços de tempo consecutivos, em cima e em baixo, a intervalos fixos são reservados para um link SCO. A taxa de transferência para links SCO é de 64 Kbit/s.

Os links ACL são definidos para a transmissão de dados em rajadas, primariamente pacotes de dados. Eles suportam conexões simétricas e assimétricas, por comutação de pacotes e ponto-a-multiponto. Pacotes de múltiplos slots usam o tipo de link ACL e podem alcançar a taxa máxima de transferência de 721 Kbit/s em uma direção e 57.6 Kbit/s na outra direção, se nenhuma correção de erros for usada. A unidade mestre controla a largura de banda do link ACL e decide quanto de uma largura de banda, em uma piconet, um escravo pode usar. A mestre também controla a simetria do tráfego. Mensagens de radiodifusão são suportadas pelo link ACL, por exemplo, do mestre para todos os escravos em uma piconet.

Pacotes de dados são protegidos por um esquema ARQ (Automatic Retransmission Query - Consulta de Retransmissão Automática). Este esquema implica que a cada recepção de um pacote uma verificação de erros é executada. Se um erro é detetado, a unidade receptora indica isto no pacote de retorno; assim, pacotes perdidos ou com erros somente causam um atraso correspondente a um slot. Desta maneira, a retransmissão é seletiva, pois somente os pacotes com erro são retransmitidos.

Já que retransmissão não é adequada para transmissões de voz, devido sua vulnerabilidade a atrasos, um esquema de codificação de voz é usado. Este esquema é altamente resistente a erros de bit. Os erros que não podem ser corrigidos resultam num aumento do ruído de fundo.

5.12.6 Scatternet e Piconet

Quando um dispositivo Bluetooth fica ao alcance de um outro dispositivo Bluetooth pode ser estabelecida uma conexão chamada ad-hoc. Quando tal tipo de conexão se estabelece, uma piconet se forma. Sempre existe uma unidade mestre e uma escrava. Uma piconet pode ser formada por até oito unidades ativas, sendo que a piconet é definida pelo canal que as unidades compartilham. O número de dispositivos em uma piconet é, atualmente, ilimitado apesar de só poderem existir oito dispositivos ativos simultaneamente em um dado momento qualquer. Não existe diferença de hardware ou de software entre um mestre e um escravo, assim qualquer unidade pode se tornar mestre. A unidade que estabelece a piconet se torna a unidade mestre. Os papéis em uma piconet podem ser trocados porém nunca pode existir mais de um mestre.

A unidade mestre controla todo o tráfego em uma piconet. Ela aloca capacidade para o link SCO e gerencia um esquema de prioridades para links ACL. Unidades escravas só podem mandar no slot escravo-mestre após terem sido endereçadas no slot mestre-escravo precedente. Se a mestre não possui nenhuma informação para mandar no slot mestre-escravo, um pacote com somente código de acesso e cabeçalho é mandado. Isto é, toda unidade escrava é endereçada numa ordem específica, mediante sua prioridade, e só pode mandar algo após ser endereçada. Desta forma, colisões de pacotes entre unidades escravas emissoras são eliminadas.

5.12.7 Estabelecendo conexões de rede

Antes de uma unidade ser associada a uma piconet ela se encontra em modo de espera (stand-by). Neste modo, uma unidade desconectada "acorda" periodicamente a cada 1,28 segundos para escutar por mensagens. Mensagens de paginação são transmitidas em 32, dentre as 79 (16 das 23 na Espanha e na França) portadoras de salto, as quais são definidas como as portadoras usadas para o processo de despertar (wake-up) (a identidade da unidade determina qual das portadoras será utilizada). Uma conexão é feita por uma mensagem de página se o endereço já é conhecido, ou por uma mensagem de consulta seguida por uma mensagem de página caso o endereço seja desconhecido.

A sequência de despertar é transmitida pela mestre nas 32 portadoras definidas para tal fim. Inicialmente, as 16 primeiras portadoras são usadas, se não houver resposta então as portadoras restantes são usadas. O clock do escravo determina a fase da sequência de despertar. O escravo escuta 18 slots da portadora de despertar e compara o sinal recebido com o código de acesso derivado de sua própria identidade. Se existir uma semelhança, a unidade chama um procedimento de estabelecimento de conexão e passa para o modo de conectada. A unidade mestre necessita saber a identidade e clock da unidade escrava. Isto é requerido para calcular o código de acesso apropriado e sequência de despertar e para prever a fase da sequência de despertar. Para manter registro dos clocks dos escravos, um procedimento de paginação é definido para a unidade mestre. Ele define como as identidades são transmitidas entre as unidades mestre e escravo e como os clocks correntes dos escravos são entregues ao mestre.

Para conectar unidades com endereços desconhecidos é, primeiramente, enviado um sinal de consulta. O sinal é usado para informar à unidade mestre qual a identidade do escravo que esteja ao alcance para transmissão. A unidade de paginação manda uma consulta de código de acesso. As unidades, recebendo esta mensagem, respondem com sua identidade e seu clock de sistema. A mensagem de consulta é tipicamente usada para procurar dispositivos Bluetooth tais como: impressoras públicas, máquinas de fax e dispositivos similares com endereços desconhecidos.

5.12.8 Modos de economizar energia

Três diferentes modos de economia de energia foram definidos: *Hold*, *Sniff* e *Park*. Eles podem ser usados caso não exista tráfego de dados na piconet. Um escravo pode solicitar para ser colocado no modo *Hold* ou pode ser colocado neste modo através da unidade mestre. No modo *Hold* somente um relógio interno estará funcionando. A transferência de dados recomeça instantaneamente quando a unidade sai do modo *Hold*. Este modo é usado quando conectando várias piconets ou quando gerenciando um dispositivo de baixa potência como, por exemplo, um sensor de temperatura. No modo *Sniff*, um dispositivo escravo atende à piconet em taxas reduzidas diminuindo, desta forma, seu ciclo de trabalho. No modo *Park*, uma unidade permanece sincronizada na piconet porém não participa do tráfego de dados.

5.12.9 Scatternet

Para otimizar o uso do espectro disponível, várias piconets podem existir na mesma área. Isto é chamado de *scatternet*. Em uma *scatternet* todas as unidades compartilham a mesma faixa de frequência mas cada piconet usa sequências de salto diferentes e transmite em diferentes canais de salto de 1 MHz. Assim, uma maneira de otimizar a capacidade de transmissão de dados é manter as piconets pequenas (poucas unidades). Todas as piconets compartilham a banda de 80 MHz e cada piconet usa 1 MHz. Portanto, contanto que as piconets utilizem frequências de salto diferentes, não ocorrerá compartilhamento dos canais de 1 MHz.

Consequentemente, se um usuário móvel quer conectar uma série de unidades Bluetooth ao seu telefone móvel, a melhor forma de conseguir alta capacidade de transmissão é através da formação de tantas piconets quanto possível em uma só *scatternet*. Cada conexão estará usando a capacidade máxima de uma piconet (721 Kbit/s). A lei das probabilidades determina que o número de colisões resultante é tão pequeno que é possível ter até 8 piconets em uma *scatternet*.

5.12.10 Segurança Bluetooth

A introdução da tecnologia Bluetooth como uma técnica de substituição de cabos expõe a necessidade de esquemas de segurança para as soluções sem fio. Com a substituição dos cabos e a introdução de sinais de rádio existe a necessidade de que o dispositivo Bluetooth tenha segurança embutida de forma a prevenir escutas clandestinas e a falsificação do originador da mensagem. Assim, funcionalidades para autenticação e encriptação foram adicionadas na tecnologia Bluetooth. A autenticação é usada para prevenir acesso não-autorizado aos dados e para prevenir a falsificação do originador da mensagem. A encriptação é usada para prevenir as escutas clandestinas. Estas duas técnicas combinadas e o alcance de transmissão limitado da unidade Bluetooth, usualmente 10 metros, dá à tecnologia uma maior proteção contra as escutas clandestinas.

Já que a necessidade de segurança é dependente do tipo de aplicação que é executada, três níveis de segurança são definidos no conceito Bluetooth:

1. Não seguro - este modo desconsidera as funcionalidades para autenticação e encriptação.
2. Segurança a nível de serviço - os procedimentos de segurança não são iniciadas até que um canal L2CAP seja estabelecido.
3. Segurança a nível de link - os procedimentos de segurança são iniciados antes que o estabelecimento do link, na camada LMP, seja completado.

5.12.10.1 Segurança a nível de serviço

No modo de segurança a nível de serviço, é sugerido a introdução de um gerente de segurança (Security Manager) que controle os acessos aos serviços e unidades. Este modo de segurança fornece a possibilidade de definir níveis de acesso para os serviços e unidades usados, respectivamente. O acesso é restrito de acordo com os níveis de acesso definidos.

5.12.10.2 Segurança a nível de link

O modo de segurança a nível de link é baseado no conceito de chaves de link. Estas chaves são números randômicos secretos de 128 bits, armazenados individualmente para cada par de dispositivos de uma conexão Bluetooth. A cada vez que duas unidades Bluetooth se comunicam é usada uma chave de link para autenticação e encriptação.

5.13 Pontos fortes do Bluetooth

O conceito Bluetooth oferece vários benefícios comparado com outras técnicas. As principais vantagens do Bluetooth são:

- Dimensões mínimas de hardware
- Baixo preço dos componentes Bluetooth
- Baixo consumo de potência para conexões Bluetooth

As vantagens tornam possível introduzir suporte para Bluetooth em vários tipos de dispositivos a baixos preços. A diversidade de produtos oferecidos (telefones móveis, PDA's, computadores, hardware de computadores, notebooks, etc.) pelas companhias integrantes do SIG Bluetooth e o suporte por elas oferecido para a técnica criam uma posição única no mercado. Tanto os fabricantes de hardware quanto de dispositivos irão trabalhar para a introdução do Bluetooth em vários dispositivos.

A figura 2.8 indica em que áreas o conceito Bluetooth pode ser utilizado. A definição de modelos de utilização específicos e perfis correspondentes combinados com os quatro perfis gerais irão, muito provavelmente, levar para uma situação de mercado onde aplicações cobertas pelos modelos de utilização irão usar os modelos definidos e seus perfis. Mais além, é provável que aplicações novas venham a usar os perfis padrão e, assim, evitar problemas de interoperabilidade entre diferentes fabricantes.

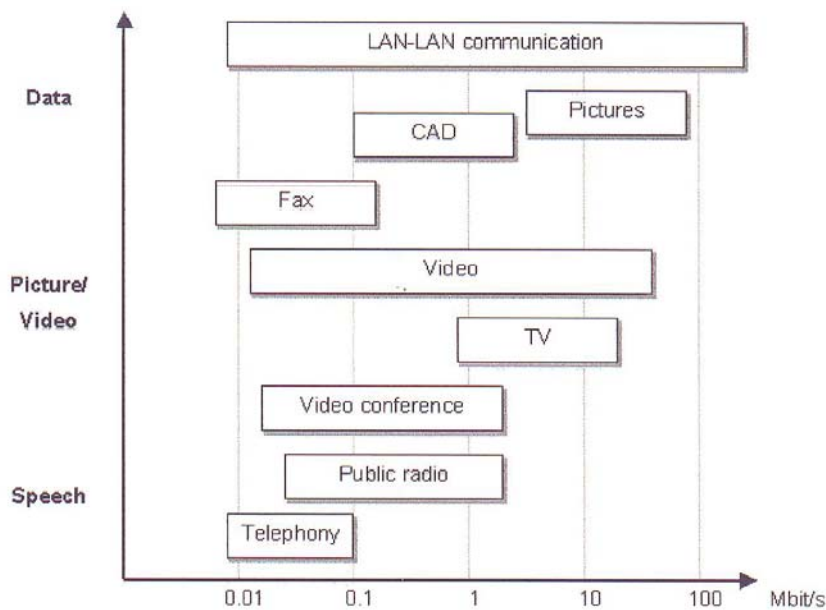


Figura 2.8 - Requisitos para transmissão de dados.

5.14 O futuro próximo do Bluetooth

Estima-se que antes de 2002, o Bluetooth venha a ser um item disponível em mais de 100 milhões de telefones móveis e em vários milhões de outros dispositivos de comunicação, variando de fones de ouvido a PC's portáteis a computadores de mesa e notebooks. Os primeiros produtos Bluetooth serão, provavelmente, produtos básicos de substituição de cabos. Contudo, quando os chips Bluetooth começarem a ser produzidos em massa e forem disponibilizados em uma grande variedade de dispositivos, diversos novos mercados se abrirão para as soluções Bluetooth. Alguns SDK (Software Development Kit - Kit de Desenvolvimento de Software) foram lançados no mercado. Maior competição no mercado de SDK e menores preços dos chips Bluetooth tornarão mais fácil convencer os fabricantes a inserir suporte Bluetooth em seus produtos. As dimensões do hardware Bluetooth e o seu método uniforme para a construção de aplicações irão assegurar um mercado Bluetooth com implementações similares independentemente de marca ou de para que país o produto foi projetado.

Capítulo 6 - WAP

O WAP está sendo introduzido, em meio a duas tecnologias que ainda estão em desenvolvimento: as comunicações móveis e a Internet, que crescem rapidamente e, a cada dia, ganham milhares de usuários.

O crescimento explosivo da Internet propiciou a criação de serviços de informação novos e emocionantes. Esta tecnologia desenvolvida foi projetada para computadores de pequeno, médio e grande porte, ligados através de redes de dados confiáveis e potentes.

Em contrapartida, os dispositivos móveis sem fio tendem a ter (por causa das limitações fundamentais de potência):

- CPUs de processamento mínimo;
- Pouca memória ROM e RAM;
- Baixa potência de consumo; e,
- Visores pequenos (micro-browsers) e dispositivos de entradas diferentes (teclado de um telefone).

Similarmente, as redes móveis possuem ambientes de comunicação mais compactos quando comparados às redes tradicionais.

Devido a estas limitações de potência, as redes móveis tendem a ter:

- Menor banda passante
- Maior latência
- Menor estabilidade nas conexões
- Menores taxas de disponibilidade

As redes móveis estão crescendo na complexidade e no custo, para dar suporte aos serviços que estão surgindo, adaptando-se às exigências dos operadores da rede móvel. Para tanto, as seguintes características são essenciais [WAP 98]:

- **Interoperabilidade** - os terminais dos diferentes fabricantes devem poder comunicar-se com os serviços na rede móvel de maneira uniforme;
- **Escalabilidade** - os operadores de rede móveis devem implementar serviços de acordo com as necessidades do cliente;
- **Eficiência** - fornecer qualidade do serviço de acordo com o comportamento e as características da rede móvel;
- **Confiança** - fornecer uma plataforma consistente e confiável para serviços e aplicações móveis;
- **Segurança** - habilitar serviços seguros em ambientes desprotegidos; garantir a preservação dos dados dos usuários; e, proteger os dispositivos e os serviços de problemas de segurança como a negação de serviço.

Muitas operadoras de redes móveis possuem serviços avançados que podem ser oferecidos aos usuários finais. Por exemplo, seria possível ao usuário escolher que tipo de mídia iria ser utilizada na comunicação com o interlocutor em virtude do status da carga da rede.

6.1 Requisitos

Os requisitos da arquitetura [WAP 98] do protocolo WAP são:

- Definir uma arquitetura flexível, escalonável e extensível;
- Suportar diferentes tipos de redes sem fio;
- Otimização do sinal para agentes da banda estreita;
- Usar de maneira eficiente os recursos dos dispositivos móveis (baixo consumo de memória, CPU e potência);
- Fornecer sustentação para aplicações e comunicação seguras;

- Permitir a criação de MMIs (Man Machine Interfaces), com flexibilidade e funcionalidade; e,
- Fornecer um modelo de programação para serviços e integração da telefonia móvel.

6.2 Definições

Alguns termos utilizados na especificação do protocolo WAP [WAP 98] :

Author - é uma pessoa ou programa que escreve ou gera WML, WMLScript ou outros padrões.

Bytecode - é um padrão codificado que contém uma série de instruções que controlam um dispositivo móvel.

Client - um dispositivo (ou aplicação) que solicita uma conexão com o servidor.

Client Server Communication - uma comunicação entre um cliente e um servidor. Geralmente, o servidor executa uma tarefa (tal como acessar ou processar informações) em nome do cliente. Os resultados da tarefa são enviados ao cliente em um formato padronizado.

Content - sinônimo para objeto de dados.

Content Format - é a representação atualizada de um content.

Content Generator - um serviço que gera ou padroniza content, geralmente é executado nos servidores.

Device - uma entidade da rede que seja capaz de solicitar e receber pacotes de informação e possua um endereço único. Um dispositivo pode agir como um cliente e um servidor, tendo a capacidade de fornecer serviços a um número de clientes (como um servidor), e ser cliente de outro servidor.

JavaScript - uma linguagem padrão que é utilizada dentro de documentos HTML. JavaScript foi originada do ECMAScript.

Origin Server - é o servidor que oferece recursos ou informações, também chamado de servidor web.

Peer-to-peer - é a comunicação direta entre dois terminais clientes, sem a interferência de um servidor intermediário.

Resource - um objeto ou um serviço dos dados da rede que pode ser identificado por um URL. Os recursos podem estar disponíveis em representações múltiplas (em diferentes linguagens, formatos de dados, tamanho e definições).

Server - um dispositivo (ou a aplicação) que espera passivamente pedidos de conexão de um ou mais clientes. Um servidor pode aceitar ou rejeitar um pedido de conexão de um cliente.

Terminal - um dispositivo usado tipicamente por um usuário para solicitar e receber a informação, chamado também de terminal ou estação móvel.

Transcode - é conversão de padrões, por exemplo, conversão de UCS-2 para UTF-8.

User - é a pessoa que interage com um User Agent para visualizar, ouvir ou utilizar de outra maneira um recurso.

User Agent - é todo o software ou dispositivo que interpreta um padrão (por exemplo, o WML). Isto pode incluir browsers de texto ou voz , etc.

WMLScript - uma linguagem script que auxilia na programação do dispositivo móvel. WMLScript é um subconjunto estendido da linguagem XML do JavaScript.

6.3 O Protocolo WAP

6.3.1 Conceitos

O protocolo de aplicação para redes sem fio (WAP) é o resultado dos esforços comuns do fórum WAP (www.wapforum.org) de forma a promover as especificações para a tecnologia de comunicação móvel, permitindo a interação de aplicações e serviços entre redes móveis e a Internet .

O WAP especifica a estrutura e os protocolos de rede para dispositivos móveis tais como telefones celulares, pagers, PDAs (Personal Digital Assistant), etc. As especificações são amplas e atingem todas as tecnologias de redes sem fio (wireless lans) e as tecnologias Internet (tais como XML, URLs, script, etc.). A meta é dar

suporte tecnológico aos operadores, fabricantes e desenvolvedores, permitindo-lhes a execução e a implementação de serviços na rede móvel, de maneira rápida e flexível [WAP 98].

Os objetivos do fórum WAP são [WAP 98]:

- Permitir aos dispositivos móveis o acesso ao conteúdo da Internet, bem como os serviços nela implementados.
- Criar um protocolo de redes móveis capaz de se comunicar com as demais tecnologias e dispositivos móveis.
- Permitir a criação de padrões de conteúdo e aplicações que possam ser interpretados por diferentes tipos de dispositivos móveis.
- Ampliar-se ou adaptar-se aos padrões de tecnologias, aonde for possível e apropriado.

A especificação da arquitetura do WAP também atua como modelo para a compreensão das tecnologias de redes móveis, servindo de referência e especificação de novos detalhes técnicos adicionais.

6.4 A Arquitetura WAP

A seguir, um breve descrição do modelo WWW, que fornece um modelo de comparação similar ao modelo WAP.

6.4.1 O modelo WWW (World-Wide Web)

A arquitetura WWW fornece um modelo de programação muito flexível e poderoso (Figura 3.1). As aplicações e os conteúdos são apresentados em formatos padronizados, e visualizados através de aplicações conhecidas como navegadores (browsers) da WEB. O browser é uma aplicação cliente, que faz solicitações de maneira padronizada para um servidor, que aceita ou não a solicitação através de um formato

padronizado [RFC2068 97].

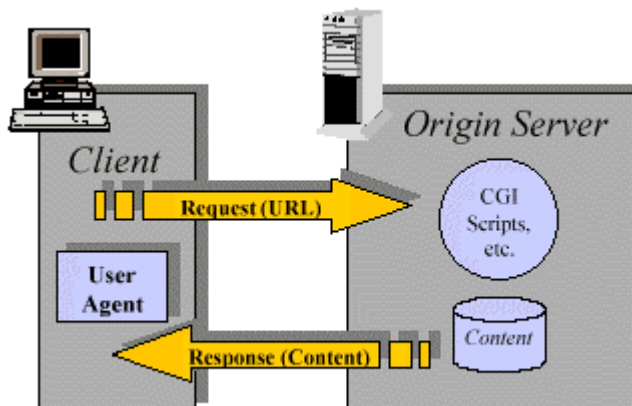


Figura 3.1 - Modelo WWW

Os padrões da W3C [W3C] especificam muitos dos mecanismos necessários para a construção de um ambiente WWW, alguns exemplos são:

- **Standard naming model** - as páginas e servidores WWW possuem um endereçamento próprio, chamado de URL (Uniform Resource Locator) [RFC 1738 94, RFC 1808 95].
- **Content typing** - as páginas WWW especificam a versão em que foram desenvolvidas, o que permite ao browser uma correta interpretação na leitura das páginas. [RFC 2045 96, RFC 2048 96].
- **Standard content formats** - os browsers suportam uma gama diferente de versões da linguagem HTML (*HyperText Markup Language*) [HTML4 97], a linguagem *JavaScript* [ECMAScript 97, JavaScript 97] e outros padrões.
- **Standard Protocols** - os protocolos permitem que os browsers comuniquem-se com qualquer servidor WEB. O protocolo mais utilizado é o HTTP (*HyperText Transport Protocol*) [RFC 2068 97].

O modelo WWW permite que os usuários acessem um grande número de aplicações e serviços na rede mundial. Permite, também, que os desenvolvedores criem aplicações e serviços para a comunidade mundial.

Os protocolos de WWW definem três classes de servidores:

- **Servidor WWW** – Onde as respostas às solicitações estão armazenadas ou são criadas.
- **Proxy** - um programa intermediário que age como um servidor e um cliente, com a finalidade de fazer pedidos em nome de outros clientes. O proxy reside, geralmente, entre o cliente e o servidor. Os pedidos são repassados pelo proxy ao servidor direcionado. O proxy deve atender às exigências do cliente e do servidor e também às especificações de WWW.
- **Gateway** – é um servidor que atua como um intermediário para outro servidor. Ao contrário do proxy, um Gateway recebe os pedidos como se fosse o servidor destino e os transmite para o servidor destino. O cliente, geralmente, não percebe que está se comunicando com um Gateway.

6.4.2 O Modelo WAP - Wireless Application Protocol

O modelo de programação do WAP é similar ao modelo de programação de WWW, oferecendo facilidades aos desenvolvedores no modelo de programação, na arquitetura e adaptações aos serviços e aplicações já existente na Internet. Foram implementadas otimizações e extensões no modelo WAP, a fim de combinar as características com o ambiente wireless [WAE 99].

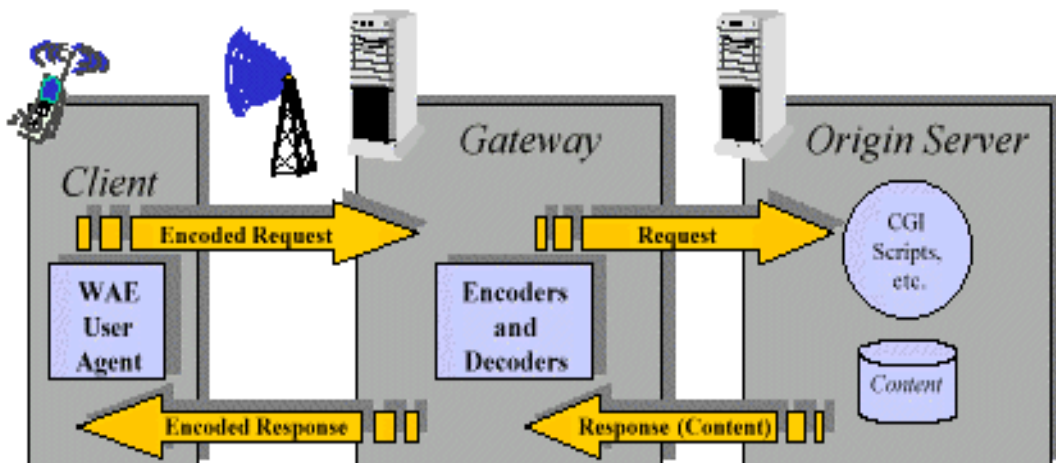


Figura 3.2 - Modelo WAP

O modelo WAP, exposto na Figura 3.2, trata os conteúdos WAP dentro de uma

recomendação semelhante aos já definidos no ambiente WWW. Aqueles são resolvidos através do mesmo esquema de protocolos de comunicação utilizados num servidor WEB. Um microbrowser [WAP 98], assim chamados os browsers dos dispositivos móveis, é a interface do usuário, da mesma maneira que o browser padrão da WWW.

Em função disto, o protocolo WAP define um conjunto de recomendações que permitem uma comunicação entre terminais e servidores, dentre elas [WAP 98]:

- **Standard naming model** – as URLs são utilizadas para localizar o conteúdo WAP no servidor.
- **Content typing** – os conteúdos WAP seguem uma recomendação, facilitando o correto processamento de leitura aos dispositivos móveis.
- **Standard content formats** – os conteúdos WAP são baseados na tecnologia de WWW e incluem algumas de suas características funcionais, o conceito de corpo da página, links, imagens e linguagem script.
- **Standard communication protocols** - os protocolos de comunicação do WAP permitem a interação do microbrowser do terminal móvel com o servidor WEB.
- **Protocol Gateway** - o dispositivo que traduz as solicitações dos protocolos WAP (WSP, WTP, WTLS, e WDP) para os protocolos HTTP e TCP/IP.
- **Content Encoders and Decoders** – transformam o conteúdo WAP em formatos codificados compactos para reduzir o tamanho dos dados sobre a rede.

O modelo WAP permite aos usuários e desenvolvedores um grande alcance na utilização dos serviços e aplicações nas WLANs. O proxy WAP possibilita a hospedagem de conteúdos WAP nos servidores WEB, além do processamento de requisições WAP, através de tecnologias como o CGI. Conexões seguras podem ser implementadas pelo proxy WAP, uma vez que compartilha os mesmos requisitos de segurança do servidor WEB [RFC2068 97].

6.4.3 Exemplo de uma Rede WAP

Um exemplo da rede Wap é mostrado na figura 3.3, o cliente WAP comunica-se com os dois servidores na WLAN. O proxy WAP traduz os pedidos do cliente WAP para o ambiente WWW, submetendo-os ao servidor WEB. O proxy codifica as respostas do servidor WEB e os devolve ao cliente, no padrão WML [WAE 99]. Se o servidor WEB gerar um conteúdo WML, o proxy envia-o diretamente ao cliente, porém se for HTML, um filtro (HTML Filter) é utilizado para traduzi-lo para o padrão WML.

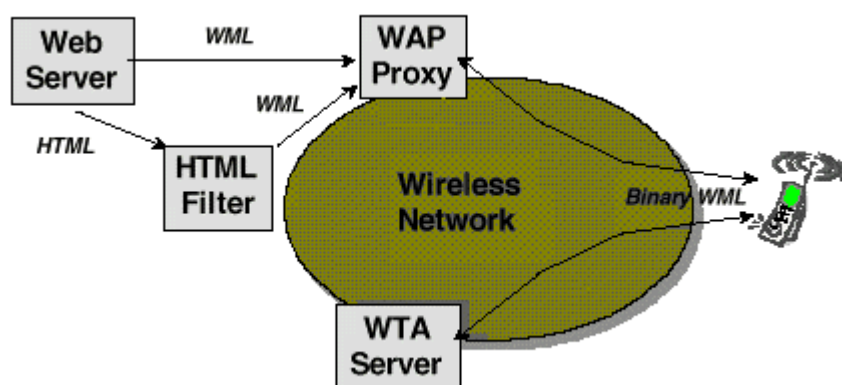


Figura 3.3 - Rede WAP

O servidor WTA (*Wireless Telephony Application*) é um exemplo de servidor WAP ou Gateway WAP que responde diretamente aos pedidos de um cliente WAP. O servidor WTA é o provedor fundamental de suporte à infra-estrutura das WLANs [WAE 99].

6.4.4 Modelo de Segurança

O protocolo WAP permite um modelo com uma infra-estrutura que implementa mecanismos de segurança durante uma conexão WAP.

O protocolo WAP pode fornecer uma segurança fim-a-fim entre os terminais que se comunicam. Se um browser ou servidor WAP desejar uma segurança deste tipo, deve-se comunicar diretamente, através de diretivas específicas do modelo de segurança

do protocolo WAP [WTLS 99].

6.5 Componentes da Arquitetura WAP

6.5.1 Componentes para ambiente wireless

Os componentes da arquitetura de WAP criam um ambiente escalonável e extensível para o desenvolvimento de aplicações voltadas para o ambiente de comunicação *wireless* [WAE 99]. Cada camada da arquitetura é acessada pelas camadas imediatamente superiores, ver figura 3.4, assim como por outros serviços e aplicações.

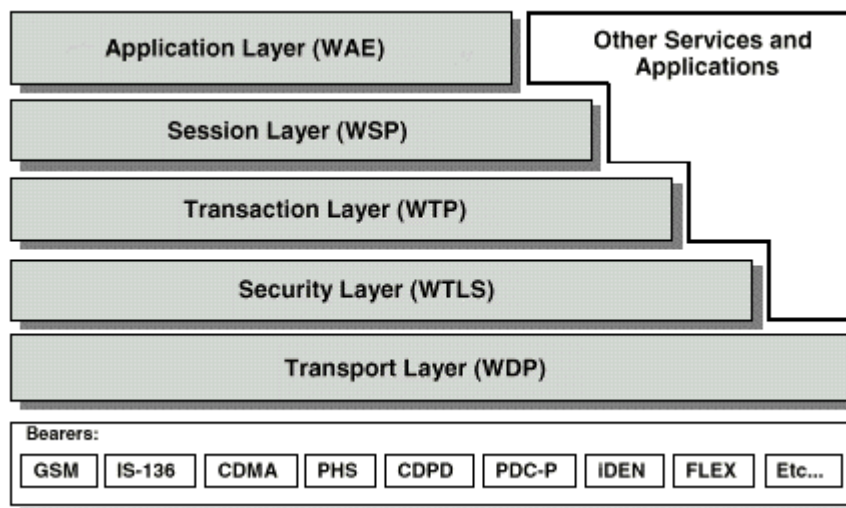


Figura 3.4 - Camadas do protocolo WAP

Utilizando-se de princípios de interoperabilidade entre camadas, já consagrados por outros modelos recomendados, a arquitetura oferece às aplicações externas, os mecanismos necessários para o estabelecimento de uma sessão, transação, política de segurança e de transporte.

As camadas da arquitetura WAP são :

- Camada de Aplicação

- Camada de Sessão
- Camada de Transação
- Camada de Segurança
- Camada de Transporte
- Bearers (Serviços de Entrega)

6.5.2 Camada de Aplicação WAE (Wireless Application Environment)

Esta camada fornece estrutura para o ambiente de interação entre o modelo WWW e as tecnologias dos dispositivos móveis, conforme a Figura 3.5.

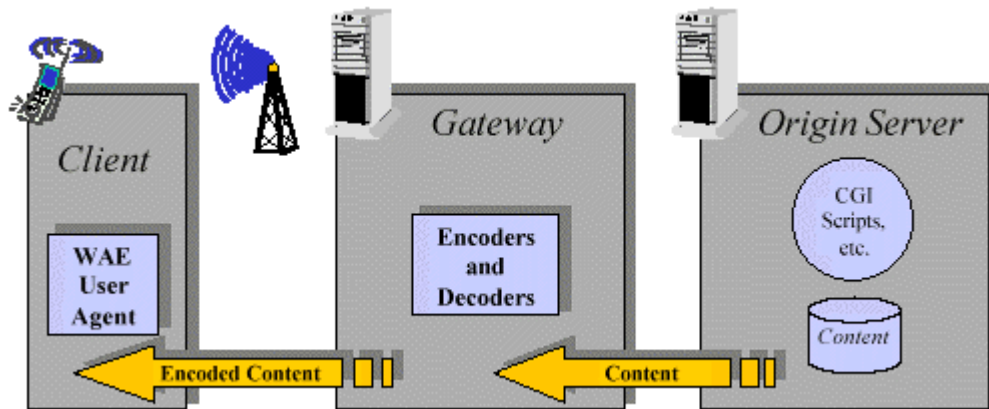


Figura 3.5 - Ambiente de Interação do WAE.

O objetivo da WAE é estabelecer um ambiente que permita aos operadores e aos fornecedores de serviços construir aplicações que possam alcançar uma gama de plataformas diferentes de redes *wireless*, de maneira eficiente e útil [WAE 99]. Para tanto, o WAE permite o uso das seguintes funcionalidades :

- A Linguagem WML - uma linguagem leve e clara, semelhante ao HTML, otimizada para uso em dispositivos móveis, permitindo visualização das imagens, armazenamento de dados e informações [WML 99];
- WMLScript - uma linguagem script, similar a JavaScript [WMLScript 99, JavaScript 97];

- Serviços WTA (*Wireless Telephony Application*) - permitem a execução de serviços de telefonia e interfaces de programação [WAE 99].

6.5.3 Camada de Sessão WSP (Wireless Session Protocol)

A camada de sessão (WSP) fornece o protocolo responsável pela garantia de estabelecimento, conexão e desconexão de uma sessão entre dois agentes (servidor e terminal) [WSP 99], através de dois tipos de serviços:

- Orientado a conexão, que opera acima da camada WDP;
- Sem conexão (Confiável ou não) que funciona na camada WDP.

O protocolo permite o funcionamento dos seguinte serviços :

- Compatibilidade com o protocolo HTTP, possibilitando a comunicação através do proxy WAP;
- Suspensão, encerramento e garantia das conexões estabelecidas; e,
- Garantia de protocolos de confiança para conexões seguras.

6.5.4 Camada de Transação WTP (Wireless Transaction Protocol)

O WTP opera sobre os serviços de datagrama, nas redes *wireless* seguras ou não, fornecendo as seguintes características [WTP 99]:

- Modos de operação simples, half-duplex e full-duplex;
- Envio de mensagens opcionais de confirmação de pedidos ou conexões, através de triggers;
- Junção de datagramas, para economia de processamento;
- Transações assíncronas.

6.5.5 Camada de Segurança WTLS (Wireless Transport Layer Security)

O WTLS é um protocolo implementado com recomendações semelhantes ao SSL (Secure Sockets Layer), e tem sido utilizado para as comunicações de canais de banda estreita. O WTLS possui as seguintes características [WTLS 99]:

- **Integridade dos dados** - Garante a veracidade das informações transmitidas, assegurando que não haja alteração ou corrupção dos dados entre o servidor e terminal.
- **Privacidade** - Transmite os dados de maneira codificada, tornando-os ilegíveis a um possível programa ou usuário interceptador.
- **Autenticação** - Possibilita mecanismos de autenticação no estabelecimento de conexão entre o terminal e uma aplicação do servidor.
- **Negação de conexões** - possui mecanismos para rejeição ou detecção de pedidos de conexão, quando determinados requisitos implementados não foram aceitos.

As aplicações *wireless* podem habilitar ou desabilitar, seletivamente, o protocolo WTLS, dependendo das exigências de segurança e das características da rede, caso esta já tenha oferecido o serviço de segurança.

6.5.6 Camada de Transporte WDP (Wireless Datagram Protocol)

O protocolo de transporte do WAP é um serviço de datagrama através da camada WDP, que opera acima dos serviços de transporte suportados pelas redes de comunicação de dados [WDP 98]. Como qualquer camada de transporte, em geral, o WDP oferece um serviço consistente aos protocolos das camadas superiores do WAP e comunica-se de forma transparente sobre os diferentes portadores de serviços das redes

wireless, como GSM, CDMA e PHS.

6.5.7 Bearers (Serviços de Entrega)

O protocolo WAP foi projetado para interagir com uma variedade de serviços diferentes, incluindo os de mensagem curta, GSM, PDC, CDPD, CDMA, TDMA, PHS e DECT. Estes serviços apresentam diferentes requisitos quanto à qualidade, taxa de erros e retardos. A intenção do WAP é compensar ou tolerar estas variações da maneira mais eficiente e clara possível [WAP 98]. Na especificação da camada WDP, existe uma lista dos portadores que são suportados e as técnicas necessárias ao funcionamento de cada portador, sendo a volatilidade a principal característica desta lista, dada a evolução da tecnologia das redes *wireless* [WDP 98].

6.5.8 Outros Serviços e Aplicações

A arquitetura WAP permite que aplicações externas possam acessar diretamente as camadas de sessão, transação, segurança e transporte. Isto habilita o WAP para o uso de futuras aplicações que ainda não foram especificadas pelo fórum WAP, mas que podem ser importantes no ambiente *wireless*. Atualmente, temos o correio eletrônico, agendas, lista telefônicas e comércio eletrônico que estão sendo implementados e testados [WAP 98].

6.5.9 Configurações da Tecnologia WAP

Um exemplo da configuração da tecnologia WAP pode ser vista na figura 3.6, onde se descreve uma possível conexão com as demais tecnologias do ambiente *wireless* [WAP 98]. No exemplo, o agente (dispositivo móvel) opera diretamente com a camada WAE, trocando primitivas de serviços para o início de uma conexão e no segmento transações tem-se os dados que estão sendo pretendidos pela camada de transporte. No terceiro bloco, os datagramas serão transportados conforme o tipo de segurança escolhida pela aplicação.

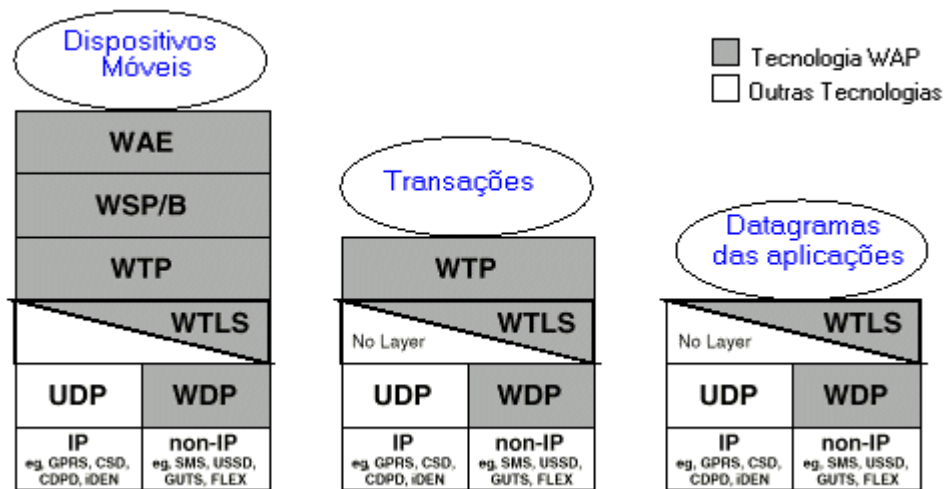


Figura 3.6 - WAP e outras tecnologias wireless.

6.6 Conclusão do capítulo

A inserção do protocolo WAP trará um novo enfoque para a Internet sem fio. O uso desta tecnologia nas áreas financeiras, comunicativas, entretenimentos e comercial são infinitas. A aliança entre o poder da Internet, que permite o acesso global e rápido a qualquer tipo de informação, e as redes digitais sem fio, que permitem a mobilidade total dos equipamentos de acesso, representa um passo importante para uma nova era da tecnologia da informação.

Entretanto, ainda há o que se definir para o aperfeiçoamento do protocolo WAP. O fórum WAP, apresenta uma coletânea dos artigos para futuras recomendações citadas, que não são fixas e não há prioridades, podendo ser adicionados novos artigos ou removidos a qualquer tempo. Atualmente, a coletânea apresenta os seguinte artigos [WAP 98]:

1. Comutação de pacotes com conexão orientada.
2. Integração com o toolkit da SIM e o smartcard.
3. Integração com o ExE (ETSI).
4. Integração com os serviços de telefonia.
5. Download de biblioteca dinâmicas do WMLScript.

6. Compressão da camada de segurança (WTLS).
7. Aprimoramento da arquitetura da segurança, incluindo os certificados de autenticação e autoridade.
8. Suporte para objetos de multimídia, como GPRS.
9. Suporte para multicast.
10. Download de aplicações.
11. Aceitação de API's.
12. Definições de entidade de gerência para cada camada e através de todas as camadas do protocolo WAP.
13. Definições de Qualidade do serviço conforme a interface do usuário (SMS, Smartcad, Flex, etc).
14. Interface de programação para as camada do protocolo WAP.
15. Testes de interoperabilidade entre dispositivos móveis.

Capítulo 7 - WLANS em ação

7.1 BreezeNET no Super Bowl

Estava um dia quente tanto dentro quanto fora do campo em San Diego para o Super Bowl XXXIII, mas foi o que ocorreu fora do campo aquilo que teve o maior significado sobre como as notícias serão coletadas e distribuídas ao público no futuro.

Por anos, gigantes da mídia tais como a Associated Press, usaram estafetas (runners) e, mais recentemente, fibras óticas para transportar fotografias e outras informações importantes do campo para seus assinantes ao redor do mundo durante grandes eventos como o Super Bowl. Este método provou ser extremamente caro e requeria a instalação permanente de fibras óticas em vários locais.

A Associated Press, a preeminente organização mundial de coleta de notícias, identificou o problema e começou a procurar uma maneira de melhorar o antigo método de transmissão de fotografias do local de um evento para os jornais de todo o mundo. Durante a série mundial (World Series), a Associated Press decidiu experimentar as WLANs como uma solução. Eles compraram produtos wireless de cinco fornecedores diferentes e os testaram no que diz respeito ao alcance, velocidade e facilidade de uso durante a série mundial. Como resultado destes testes, a Associated Press decidiu usar uma solução totalmente wireless no Super Bowl XXXII, em San Diego. Para o Super Bowl, a Associated Press decidiu usar os produtos de rede wireless BreezeNET PRO, da BreezeCom, para transmitir, eficientemente, fotografias do jogo para todo o mundo, gastando substancialmente menos dinheiro que através dos meios convencionais, tais como a instalação de fibras óticas em todo o estádio.

Os técnicos da Associated Press usaram a BreezeNET para interligar, sem fio, seis câmeras fixas e vários fotógrafos móveis com câmeras digitais a computadores Powerbooks Macintosh. Conforme as câmeras capturavam a ação do jogo, as fotografias digitais eram armazenadas em discos rígidos padrão PCMCIA. Assim que os discos estavam cheios, eles eram inseridos em um dos seis Powerbooks G-3 Macintosh instalados no campo. Cada Powerbook estava equipado com um Adaptador de Estação (Station Adapter) BreezeNET SA-10, conectado à sua porta Ethernet.

As imagens digitais capturadas e armazenadas nos Powerbooks eram remotamente acessadas pelo AP instalado na sala de notícias móvel localizada em um trailer estacionado fora do estádio a uma distância de cerca de 500 metros. Estas imagens eram transmitidas para a sala de notícias móvel através de pontos de acesso BreezeNet, modelo “D”, usando antenas destacáveis. As antenas dos pontos de acesso foram direcionadas para seis repetidores instalados nos postes de luz do estádio e daí para os seis Powerbooks do campo. No AP da sala de notícias, as imagens eram processadas e transferidas como arquivos, via FTP, para um servidor AIX instalado em Nova Iorque, através de um roteador localizado no AP do Centro Técnico em Cranbury, NJ. As milhares de fotografias capturadas durante o Super Bowl foram arquivadas em uma localização central, permitindo que os assinantes da Associated Press tivessem acesso à vasta quantidade de fotografias a partir de qualquer parte do mundo.

“Esta tecnologia nos permite cobrir um evento de um dia com prazos apertados para as fotografias sem a necessidade da instalação de fibras óticas nem manutenção,” afirmou Howard Gros, gerente de projetos da Associated Press. “O sistema da BreezeCom é também reusável, o que nos permite utilizá-lo em eventos similares no futuro sem nenhum custo adicional”.

A incorporação do método sem fio da BreezeCom para a transmissão de fotografias provou ser um grande sucesso para a Associated Press. Aumentando a eficiência como um todo, o gigante da mídia foi capaz de remeter as fotografias das câmeras para o trailer fora do estádio em 25 segundos. O AP também transmitiu a fotografia da primeira jogada do jogo, para os assinantes fora do estádio, via satélite, em somente cinco minutos após o chute inicial. O método de transferência de dados sem fio da BreezeCom teve tanto sucesso que a Associated Press imediatamente transportou o sistema para Nagano, no Japão, para facilitar a organização da cobertura dos Jogos Olímpicos de Inverno.

Capítulo 8 - Uma proposta para um centro cultural

Está sendo conduzido um estudo para a implementação de uma solução de rede sem fio (wireless lan) com o intuito de cobrir todo o espaço de um centro cultural, o qual já utiliza tecnologia de redes com fio. Esta cobertura deverá atender tanto a rede interna como disponibilizar acesso externo.

O centro cultural em questão ocupa uma área de 500 metros quadrados contendo escritórios, livraria, sala de treinamento, salão de jogos, auditório, sala de leitura e café. A rede original possuía 75 (setenta e cinco) pontos de rede instalados totalizando 4 quilômetros de cabos. Havia a necessidade de expansão dessa quantidade de pontos de atendimento o que, afinal, se configuraria como extremamente caro e trabalhoso caso se optasse por manter a estrutura de rede com fios. Daí o surgimento da rede sem fio como uma alternativa viável e madura para a solução do problema.

8.1 Objetivos da WLAN

O objetivo primário é usar a tecnologia WLAN para fornecer acesso às bases de dados locais e às bases de dados externas independentemente da localização do usuário dentro do centro cultural. A configuração de um sistema WLAN irá prover conectividade de rede enquanto permite mobilidade, desta forma oferecendo agilidade e rapidez na prestação de serviços aos usuários do centro. Dentre a gama de serviços a serem disponibilizados em função da adoção da nova tecnologia estão, entre outros:

- Informações sobre programação, promoções e ofertas para os usuários que, usando a tecnologia e equipamentos Bluetooth, estejam nas proximidades do centro cultural.
- Acesso instantâneo, pelos funcionários do centro, às informações sobre os clientes e suas preferências, produtos em oferta, condições de pagamento, descontos especiais, etc., usando-se para isso de palmtops com acesso sem fio às bases de dados integradas do centro e à Internet.

- Disponibilizar informações gerais sobre o centro cultural para todo e qualquer usuário habilitado usando, para isso, recursos de SMS (Short Message Service - Serviço de Mensagens Curtas) em conjunto com, por exemplo, as empresas fornecedoras de telefonia celular.
- Possibilidade de efetuar pagamentos eletrônicos usando dispositivos sem fio como celulares e smartcards.
- Acesso ao site do centro cultural, através da Internet, para dispositivos sem fio usando-se WAP.

8.2 Áreas envolvidas

Existirão vários núcleos envolvidos em todo o projeto. Dentre eles citam-se: o próprio centro cultural; o provedor de acesso à Internet; empresas prestadoras de serviço de telefonia celular; empresas prestadoras de serviço de TV; e, bancos.

8.3 Solução proposta

No centro cultural será adotada uma solução com a instalação de uma célula (BSS) para atendimento de todos os ambientes que compõem o centro (escritórios, sala de treinamento, sala de leitura, etc.). Existirão antenas direcionais que farão a interface das redes com fio existentes à célula instalada. Além disso, haverá a instalação de uma rede de computadores totalmente sem fio a qual permitirá que se façam treinamentos e experiências tanto para o público externo como para o pessoal interno. Adicionalmente, serão instalados antenas direcionais que farão conexão com as outras empresas envolvidas no projeto.

Entre o centro cultural e a prestadora de serviço de TV será instalado um conjunto de redes direcionais que permitirão uma alta taxa de transferência (11 Mbps) compatível com o tipo de serviço a ser prestado.

Capítulo 9 - CONCLUSÃO

Com a disseminação e o crescimento irreversível das redes de comunicação multimídia, torna-se cada vez mais preocupante o problema relativo à infra-estrutura necessária à implementação e manutenção dessas redes.

A base física na qual se apoiam todas as redes de comunicação tende a chegar a um limite, a partir do qual qualquer modificação se tornará proibitiva tanto no que diz respeito a custos quanto no que diz respeito às tecnologias de comunicação que permitam maiores bandas ou, por outro lado, que possibilitem maiores fatores de compressão de dados. Por outro lado, a cada dia que passa, os requisitos de qualidade, rapidez e confiabilidade das redes de comunicação vêm aumentando de uma forma exponencial. Estes requisitos derivam do fato de que os usuários querem mais informação, com mais rapidez e com maior frequência. Além disso, com a globalização das informações não é mais aceitável que o usuário tenha que ficar restrito à necessidade da existência de um ponto de acesso físico para prover acesso às informações. Um exemplo dessas novas exigências é a expansão dos serviços de telefonia celular, no qual o usuário, em qualquer parte do mundo e a qualquer hora, tem acesso à rede telefônica mundial, em detrimento dos serviços de telefonia convencionais.

Estas limitações ficam ainda mais evidentes naquelas regiões onde, por diversos motivos, a infra-estrutura existente não atende às especificações mínimas necessárias para a disponibilização de tais serviços.

Em função disso, se torna necessária a avaliação da implementação de redes de comunicação alternativas, nomeadamente, as redes de comunicação sem fio. Esta é uma solução aplicável em locais onde o cabeamento não é viável, é muito difícil ou de custo muito elevado. Tais redes de comunicação permitem a disponibilização de todos os serviços atualmente em uso e de outros que, porventura, venham a surgir.

Capítulo 10 - Glossário

802.11	- Uma norma da IEEE para a banda de 2.4 GHz usada pelas WLANs
ADSL	- Asynchronous Digital Subscriber Line, serviço de conexão à Internet em alta velocidade. É oferecido pelas companhias telefônicas.
API	- Interfaces com programas de aplicações disponibilizadas pelos softwares.
Área de serviço estendida	- A sobreposição, pelo AP, da área de cobertura de rádio em células contíguas
Associação	- O serviço usado para estabelecer o mapeamento entre as estações e os pontos de acesso e habilitar a invocação, pela estação, dos serviços do sistema de distribuição.
Autenticação	- O serviço usado para estabelecer a identidade de uma estação como membro do conjunto de estações autorizadas a se associar com outra estação.
Back Off Exponencial	- Quando uma colisão ocorre, é o método de cálculo do tempo para uma nova tentativa.
Banda de 2.4 GHz	- O espectro de frequência, destinado pela FCC, para os sistemas de rede sem fios.
Banda larga	- Diz-se dos meios de acesso à Internet de alta velocidade. Os mais populares são a TV a cabo e a linha ADSL.
bps (bits por segundo)	- Medida da velocidade da transmissão de dados. A velocidade dos modems vendidos atualmente é de 56000 bps. O número também pode ser escrito como Kbps (milhares de bits por segundo). No caso, 56000 bps equivalem a 56 Kbps.
Browser	- Programa que permite navegar na Internet. Os mais utilizados, como o Microsoft Internet Explorer e o Netscape Navigator, vêm acompanhados de outros programas, como o leitor de correio eletrônico.
Camada MAC	- A segunda camada na pilha do protocolo.
Célula	- Nas WLANs, a área local na qual um transmissor/receptor particular opera.
Celular 3G	- Diz-se do celular de terceira geração, um sistema baseado em aparelhos pessoais multimídia capazes de acessar todo tipo de informação digital - música, fotos, vídeo e TV - de qualquer lugar. Também servirá para envio e recebimento de mensagens multimídia e pagamentos eletrônicos.
Células acopladas (linked cells)	- Células contíguas inter-conectadas para prover interoperabilidade transparente.
Células autônomas	- Uma célula sem fio com um único AP.
Configuração ponto-a-	- A configuração ponto-a-multiponto, de uma bridge

multiponto	(ponte) sem fio, é usada quando conectando nós remotos de uma rede, ou até mesmo redes remotas, a um hub central da rede.
Configuração ponto-a-ponto	- A configuração ponto-a-ponto, de uma bridge (ponte) sem fio, é usada para conectar dois nós ou redes remotas entre si.
Conjunto de serviços básicos	- Um conjunto de estações controladas por uma Função de Coordenação de Sinal (Signal Coordination Function).
Criptografar	- Embaralhar os dados de um arquivo para torná-lo inacessível a quem não tiver uma chave (senha). O recurso também é usado para garantir o sigilo em comunicações seguras via Internet.
CSMA/CA	- Um protocolo usado para evitar conflitos de tráfego em um sistema de rádio compartilhado.
Direct Sequence Spread Spectrum (DSSS)	- Uma abordagem alternativa de difusão de espectro na qual o transmissor substitui um sinal de banda-base por blocos calculados de código com tamanho fixo.
Distributed Coordination Function (DCF – Função de Coordenação Distribuída)	- Uma classe de funções de coordenação onde a mesma função de coordenação lógica está ativa em cada estação no conjunto básico de serviços (BSS) sempre que a rede estiver em operação.
Distribution Service (DS – Serviço de Distribuição)	- A rede 802 conectada é chamada de Serviço de Distribuição (DS).
Diversidade de antenas	- Um arranjo de antenas permite que múltiplas antenas transmitam e recebam sinais modulados em amplitude ou em frequência (phase).
Downstream	- Nas conexões de alta velocidade, refere-se ao fluxo de dados que vem do provedor de acesso rumo ao micro do usuário.
DSP	- Processador digital de sinais. Tipo especial de chip capaz de processar sinais de voz, som e dados. É peça-chave em celulares digitais e aparelhos de som de última geração.
EIFS – Espacejamento Inter-Frames Estendido	- Este é o tempo que uma estação deve esperar se não entendeu uma mensagem de definição de tempo, antes de mandar qualquer outra coisa através do PIFS.
Encriptação	- Aplicação de um algoritmo específico a um dado de forma a alterar sua aparência e evitar que outros dispositivos consigam ler a informação. A desencriptação aplica o algoritmo de forma reversa para recuperar o dado à sua forma original.
Endereço de camada MAC (Media Access Control Layer Address)	- Também chamada do endereço de hardware ou endereço físico. Um endereço da camada de conexão de dados associado com um dispositivo da rede particular. Contrasta com o endereço de rede ou do protocolo, o qual é um endereço da camada de rede.
Escalável	- Um termo implicando que uma tecnologia referenciada

	particular possa ser expandida em termos de capacidade e desempenho.
Espectro eletromagnético	- A banda total de frequências usadas nas emissões eletromagnéticas desde a luz visível até às ondas de rádio.
Ethernet	- Designação do padrão de rede de computadores mais popular do mercado. Refere-se à parte física da rede (cabos e conectores).
Federal Communications Commission - FCC	- Órgão regulador dos Estados Unidos.
Firewall	- Software que filtra os dados provenientes da Internet. Dessa forma, evita acesso não autorizado, sabotagem e roubo de informações no computador do usuário.
Fragmentação	- O processo de quebrar um pacote em unidades menores quando transmitindo em uma mídia de rede que não suporte o tamanho original do pacote.
Frequency Hopping Spread Spectrum (FHSS)	- Um sistema operacional de rádio que usa um grande número de canais de frequência, no qual o transmissor envia um sinal de “burst” em um determinado canal e então “salta” para outro canal.
FSK	- Modulação de sinal que envolve a alternância do valor de uma frequência delta a partir da frequência portadora em função do bit a ser representado. Para V23, 0 = 400 MHz e 1 = -400MHz.
Gigahertz (GHz)	- Medida de velocidade dos novos processadores fabricados pelas concorrentes Intel e AMD. Um gigahertz equivale a 1 bilhão de hertz, ou 1000 megahertz.
GPS	- Sigla de Global Positioning System, um sistema de coordenadas que se baseia nos sinais de 24 satélites ao redor da Terra para fornecer a posição exata do usuário.
GSM	- Sigla de Global System for Mobile Communications, um sistema de comunicação digital sem fio. Versões avançadas dessa tecnologia permitem o acesso rápido à Internet por meio de aparelhos celulares. É um dos sistemas conhecidos como celular de terceira geração (3G).
Handheld	- Computador de dimensões reduzidas o bastante para caber no bolso da camisa ou do paletó.
Hardware	- Parte física dos computadores: CPU, monitor, teclado e circuitos. Também inclui periféricos como as impressoras.
Interoperabilidade	- Um termo que implica que produtos da mesma tecnologia e de diferentes fornecedores possam operar com sucesso entre si.
ISDN (RDSI)	- Sigla para Integrated Services Digital Network (Rede Digital de Serviços Integrados). Linha telefônica

	digital para o tráfego de dados.
ITU-T	- International Telecommunication Union - Órgão regulador internacional.
Kb	- Abreviatura de quilobit, medida equivalente a 1024 bits, em geral usada para indicar velocidade de transferência de dados, como na unidade Kbps (quilobits por segundo).
Link	- (1) Denominação da conexão de banda larga entre empresas e provedores de acesso, ou entre esses provedores e as grandes prestadoras de serviços de comunicação. Um link é compartilhado, via rede local, entre todos os usuários da empresa que o solicitou. (2) Palavras-chave em páginas de sites Web que, quando clicadas, remetem a outros documentos na Web. Também chamado de hiperlink.
m-commerce	- Termo que designa o Mobile Commerce, ou comércio móvel - a oferta de bens e serviços acessíveis pela Internet por meio de computadores portáteis tipo handheld e celulares WAP e 3G.
Megabit (Mb)	- O bit é a menor unidade de informação possível. Um megabit equivale a 1 milhão de bits. É usado na indicação da velocidade de transferência de dados, como em 100 Mbps (megabits por segundo).
Método de Acesso Básico	- O método usado pelas estações sem fio para acessar o ponto de acesso.
MIB	- Management Information Base - Base de informação de gerenciamento
Multi-células	- Um conjunto de células sem fio que sobrepõem a mesma área.
Network Allocation Vector (NAV – Vetor de Alocação de Rede)	- Uma parte do protocolo WLAN indicando que a estação percebeu o uso da portadora virtual.
Point Coordination Inter Frame Spacing (PIFS)	- O tempo usado pelo AP para garantir acesso ao meio antes de qualquer outra estação.
Ponte (bridge)	- Um dispositivo que conecta e passa pacotes entre dois segmentos de rede. As bridges operam na camada 2 do modelo de referência OSI (a camada de link de dados – data-link layer) e são insensíveis ao protocolo das camadas superiores. A bridge irá examinar todos os frames (quadros) que chegam em suas portas e irá encaminhá-los ou não dependendo do endereço de destino da camada 2 de cada quadro.
Ponto de Acesso (Access Point – AP)	- Ponto central em uma célula sem fio, o qual age como uma ponte (bridge) de e para as estações sem fio da célula.
Portal	- O AP que conecta com outra rede 802 (como em uma Ethernet).
Propagação por caminhos	- Quando o sinal transmitido chega ao receptor vindo de

múltiplos	diferentes direções e com distâncias diferentes, os sinais são atenuados e retardados diferentemente.
PUSH	- Técnica na qual as informações são remetidas para os usuários periodicamente.
Rádio-frequência Rede empresarial	- A faixa na qual os sinais de rádio são transmitidos. - Uma rede completa do negócio consistindo de funções, divisões e outros componentes usados para alcançar objetivos específicos e metas definidas.
Redes infravermelhas	- Redes sem fio baseadas em transmissões de raios infravermelhos difusos ou diretos, de um único feixe ou de múltiplos feixes.
Redes ISM (Industrial, Scientific e Medical)	- Redes médicas, científicas e industriais que operam localmente em bandas não licenciadas.
Roaming	- (1) A capacidade de estações portáteis se mover livremente entre células de rádio que se sobreponham. (2) A função de mover uma estação de uma célula para outra.
RS-232	-
Scaneamento Ativo (Active Scanning)	- A estação envia um Quadro de Requisição de Sonda (Probe Request Frame), o qual é uma solicitação para que o AP reconheça sua existência.
Scaneamento passivo	- A estação espera por uma mensagem de quadro BEACON periódica, vinda do AP.
Short Inter Frame Spacing (SIFP – Espacejamento Inter-Frames Curto)	- O tempo máximo que o transmissor tem que respeitar ao esperar uma resposta.
SOHO	- Termo usado para pequenos escritórios ou para operações efetuadas em casa.
SPREAD SPECTRUM (Difusão de Espectro)	Um sistema de transmissão de rádio que usa frequências múltiplas, dentro da faixa atribuída, para incrementar a imunidade a ruídos em qualquer frequência específica.
Wired Equivalent Privacy (WEP - Proteção Equivalente ao Fio)	- O algoritmo de criptografia opcional, definido pela IEEE 802.11, usado para fornecer a confidencialidade subjetivamente equivalente àquela de uma rede com fio que não usa, normalmente, técnicas de criptografia para realçar a proteção.
WLAN	- Rede, sem fio, com abrangência local.
WMAN	- Rede, sem fio, com abrangência metropolitana.
WWAN	- Rede, sem fio, de longo alcance, por exemplo, telefonia celular.

Capítulo 11 – Bibliografia

- [BAU95] BAUCHOT, F. J; LANNE, F. IBM Wireless RF LAN Design and Architecture. **IBM Systems Journal**, Armonk, EUA, v.34, n.3, pp.390-408, Março de 1995
- [BHA94] BHARGHAVAN, Vaduvur; DEMERS, Alan; SHENKER, Scott; ZHANG, Lixia. **MACAW: A Media Access Protocol for Wireless LAN's**. Proceedings SIGCOMM'94 Conference, ACM, pp.212-225, 1994.
- [CHA96] CHAYAT, Naftali. **3 Mbit/sec FH PHY format definition**. Documento P802.11-96/52, disponível por FTP anônimo em atg.apple.com no diretório /pub/802.11/ibmpc/1996_docs, Março de 1996.
- [CHE94] CHEN, Kwang-Cheng. **Medium Access Control of Wireless LANs for Mobile Computing**. IEEE Network. New York, Estados Unidos, v.8, n.5, Set./Out. 1994.
- [DAY97] DAYEN, Rifaat. **Mobile Data and Wireless LAN Technologies**. New Jersey, Estados Unidos: Prentice-Hall, 1997, 294p.
- [GEI96] GEIER, Jim. **Wireless Networking Handbook**. Indianapolis, Estados Unidos: New Riders Publishing, 1996, 413p.
- [HAY96] HAYES, Vic. **Tutorial on 802.11 to 802**. Documento IEEE P802.11-96/49A, disponível por FTP anônimo em atg.apple.com no diretório /pub/802.11/ibmpc/1996_docs, Março de 1996.
- [IEE97] IEEE Standards Department. **IEEE Draft Standard for Wireless LAN – Medium Access Control (MAC) and Physical Layer (PHY) Specification**. Documento P802.11D6.1, Piscataway, Estados Unidos, Maio de 1997.
- [LAW91] LAW, Averill M.; KELTON, W. David. **Simulation, Modeling and Analysis**. New York, Estados Unidos: Editora McGraw-Hill, 1991.
- [MOU86] MOURA, José Antônio Beltrão; SAUVÉ, Jacques Philippe; GIOZZA, William Ferreira; DE ARAÚJO, José Fábio Marinho. **Redes de Computadores**. São Paulo: Editora McGraw-Hill, 1986
- [PIT96] PITTS, J. M.; SCHORMANS, J. A. **Introduction to ATM Design and Performance: with applications analysis software**. Londres, Reino Unido: Editora John Wiley and Sons Ltd, 1996, 190p.
- [SOU97] SOUZA, Adriano A. de; CUNHA, Paulo R. F. **Uma Extensão da Plataforma ANSAware para Suportar a Comunicação Móvel**. XV Simpósio Brasileiro de Redes de Computadores, Maio de 1997.
- [TAN96] TANENBAUM, Andrew S. **Computer Networks**. 3ª ed. New Jersey: Prentice-Hall, 1996, 814p.
- [ECMAScript 97] Standard ECMA-262: "ECMAScript Language Specification", ECMA, June 1997.
- [JAVASCRIPT 97] "JavaScript: The Definitive Guide", David Flanagan. O'Reilly & Associates, Inc. 1997.
- [ISO10646 93] "Information Technology - Universal Multiple-Octet Coded Character Set (UCS) - Part 1: Architecture and Basic Multilingual Plane", ISO/IEC 10646-1:1993.
- [HDML2 97] "Handheld Device Markup Language Specification", P. King, et al., April 11, 1997.

- [HTML4 97] "HTML 4.0 Specification, W3C Recommendation 18-December-1997, REC-HTML40-971218", D. Raggett, et al., September 17, 1997. URL: <http://www.w3.org/TR/REC-html40>
- [ISO8879 86] "Information Processing - Text and Office Systems - Standard Generalised Markup Language (SGML)", ISO 8879:1986.
- [RFC 1766 95] "Tags for the Identification of Languages", H. Alvestrand, March 1995. URL: <http://www.ietf.org/rfc/rfc1766.txt>
- [RFC1738 94] "Uniform Resource Locators (URL)", T. Berners-Lee, et al., December 1994. URL: <ftp://ftp.isi.edu/in-notes/rfc1738.txt>
- [RFC1808 95] "Relative Uniform Resource Locators", R. Fielding, June 1995. URL: <ftp://ftp.isi.edu/in-notes/rfc1808.txt>
- [RFC2045 96] "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", N. Freed, et al., November 1996. URL : <http://www.ietf.org/rfc/rfc2045.txt>
- [RFC 2047 96] "MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text", K. Moore, November 1996. URL: <http://www.ietf.org/rfc/rfc2047.txt>
- [RFC 2048 96] "Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures", N. Freed, et al., November 1996. URL: <http://www.ietf.org/rfc/rfc2048.txt>
- [RFC 2068 97] "Hypertext Transfer Protocol - HTTP/1.1", R. Fielding, et al., January 1997. URL:<http://www.ietf.org/rfc/rfc2068.txt>
- [RFC 2119 97] "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1 1997.URL: <http://www.ietf.org/rfc/rfc2119.txt>
- [RFC 2396 98] "Uniform Resource Identifier (URI): Generic Syntax", T. Berners-Lee, et al., August 1998. URL:<http://www.ietf.org/rfc/rfc2396.txt>
- [UNICODE 96] "The Unicode Standard: Version 2.0", The Unicode Consortium, Addison-Wesley Developers Press, 1996. URL: <http://www.unicode.org/>
- [VCARD 96] vCard - The Electronic Business Card; version 2.1; The Internet Mail Consortium (IMC),September 18, 1996, <http://www.imc.org/pdi/vcard-21.doc>
- [VCAL 96] vCalendar - the Electronic Calendaring and Scheduling Format; version 1.0; The Internet Mail Consortium (IMC), September 18, 1996, <http://www.imc.org/pdi/vcal-10.doc>
- [VITERBI] A . J. Viterbi, Principles of Digital Communication and Coding.
- [WAE 99] "Wireless Application Environment Specification", WAP Forum, 04-November-1999 . URL: <http://www.wapforum.org/>
- [WAP 98] "Wireless Application Protocol Architecture Specification", Wireless Application WAP Forum, April 30, 1998. URL: <http://www.wapforum.org/>
- [WBXML 99] "Binary XML Content Format Specification", WAP Forum, 04-November-1999 . URL: <http://www.wapforum.org/>
- [WDP 98] "Wireless Datagram Protocol Specification", WAP Forum, April 30, 1998. URL: <http://www.wapforum.org/>
- [WML 99] "Wireless Markup Language Specification", WAP Forum, 04-November-1999 . URL: <http://www.wapforum.org/>
- [WMLScript 99] "WMLScript Language Specification", WAP Forum, 04-November-1999 . URL: <http://www.wapforum.org/>
- [WMLStdLib 99] "WMLScript Standard Libraries Specification", WAP Forum, 04-November-1999 . URL: <http://www.wapforum.org/>

- [WSP 99] "Wireless Session Protocol", WAP Forum, 05-November-1999. URL: <http://www.wapforum.org/>
- [WTA 99] "Wireless Telephony Application", WAP Forum, 08-November-1999. URL : <http://www.wapforum.org/>
- [WTAI 99] "Wireless Telephony Application Interface Specification", WAP Forum, 08-November-1999. URL: <http://www.wapforum.org/>
- [WTLS 99] "Wireless Transport Layer Security", WAP Forum, 05-November-1999. URL: <http://www.wapforum.org/>
- [WTP 99] "Wireless Transaction Protocol", WAP Forum, 11-June-1999. URL: <http://www.wapforum.org/>
- [XML 97] "Extensible Markup Language (XML), W3C Proposed Recommendation 8-December-1997, PR-xml-971208", T. Bray, et al, December 8, 1997. URL: <http://www.w3.org/TR/PR-xml>

11.1 Referências Bibliográficas

11.1.1 Livros

Soares, Luiz F., Lemos Guido, Colcher Sérgio . Rede de computadores: das LANs, MANs e WANs às redes ATM. 6ª edição, Editora Campus, 1999.

Fórum WAP, Wireless Markup Language Specification 1.2 1999 .

Fórum WAP, Wireless Application Protocol Specification Version ,1999 .

Fórum WAP, Wireless Application Environment Specification Version ,1999 .

Fórum WAP, Wireless Session Protocol Overview Version , 1998 .

Fórum WAP, Wireless Transaction Protocol, 1999 .

Fórum WAP, Wireless Transport Layer Security Version , 2000 .

Fórum WAP, Wireless Datagram Protocol, 1999 .

11.1.2 Internet

Anywhere you go, <http://www.anywhereyougo.com>

WAP Fórum, <http://www.wapforum.org>

WAP Net, <http://www.wapnet.com>