



**ESTUDO DA INTEROPERABILIDADE ENTRE
REDES LOCAIS SEM FIO (WLAN) E O SISTEMA
MÓVEL CELULAR**

**GLEISON DE BARROS PINTO
OSÉIAS FONSECA DE AGUILAR**

**DISSERTAÇÃO DO PROJETO FINAL DE GRADUAÇÃO
EM ENGENHARIA ELÉTRICA**

**FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA**

**UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA**

**ESTUDO DA INTEROPERABILIDADE
ENTRE REDES LOCAIS SEM FIO (WLAN) E
O SISTEMA MÓVEL CELULAR**

**GLEISON DE BARROS PINTO
OSÉIAS FONSECA DE AGUILAR**

**ORIENTADOR: LEONARDO R. A. X. DE
MENEZES**

**DISSERTAÇÃO DO PROJETO FINAL DE
GRADUAÇÃO EM ENGENHARIA ELÉTRICA**

BRASÍLIA / DF FEVEREIRO / 2003

Agradecimentos

Agradeço primeiramente a Deus pelo dom da vida e aos meu Pais, familiares e amigos por sempre estarem ao meu lado nesta jornada. Agradeço também a todos professores e funcionários do ENE e da UnB, por terem contribuído de alguma forma na minha formação, profissional e humana. Em particular ao nosso orientador Prof. Leonardo, acima de tudo pela maneira como nos motivou a confiar em nós mesmos.

À todos agradecer sempre será pouco, retribuir quase impossível.

Gleison

RESUMO

Neste trabalho é desenvolvido um estudo que tem como tema central a interoperabilidade entre as redes locais sem fio (WLANs) e o sistema móvel celular. Inicialmente faz-se o estudo das WLANs mostrando suas principais características e o principal padrão atualmente, o 802.11. Em seguida, descreve-se o sistema móvel celular dentro do contexto da evolução das gerações deste sistema: da primeira geração às redes mais recentes de 2,5G. Ao descrever cada tipo de sistema e a geração da qual faz parte, procura-se dar uma visão geral onde os objetivos estão voltados para as principais características, suas vantagens, desvantagens e limitações. Também é apresentado o protocolo chamado IP Móvel, que é considerado a peça chave para a solução da interoperabilidade entre os sistemas. Finalmente, é apresentada e analisada a proposta da interoperabilidade mostrando o exemplo e os componentes necessários para a composição deste novo tipo de complementação das redes do sistema móvel celular.

ABSTRACT

In this work a study is developed that has as central subject the interoperability between the Wireless Local Area Network (WLANs) and the cellular mobile system. Initially, is developed the study of the WLANs showing its main characteristics and the main standard currently, the 802.11. After that, the cellular mobile system is described in context of the evolution of the generations of this system: of the first generation to the most recent 2,5G networks. When describing each type of system and the generation of which is part, is done a general vision where the objectives are come back toward the main characteristics, its advantages, disadvantages and limitations. The Mobile IP, that is considered the key for the solution of the interoperability between the systems, is also described. Finally, it is presented and analyzed the proposal of the interoperabilidade showing an example and the necessary components for the composition of this new type of complementation of the networks of the cellular mobile system.

ÍNDICE

CAPÍTULO	PÁGINA
UNIVERSIDADE DE BRASÍLIA.....	I
1 INTRODUÇÃO.....	1
2 WLAN	3
2.1 INTRODUÇÃO.....	3
2.2 O DESENVOLVIMENTO DAS WLANS.....	4
2.3 O PADRÃO IEEE 802.11.....	5
2.3.1 Topologia.....	6
2.3.1.1 Infra-estruturada.....	6
2.3.1.2 Ad hoc.....	7
2.3.2 Subcamada de Controle de Acesso ao Meio (MAC).....	7
2.3.3 Camada física.....	8
2.4 CONCLUSÕES.....	11
3 SISTEMA MÓVEL CELULAR.....	12
3.1 INTRODUÇÃO.....	12
3.2 REDES DE SEGUNDA GERAÇÃO (2G).....	13
3.2.1 TDMA / IS-136.....	13
3.2.2 CDMA/IS-95.....	17
3.2.3 GSM.....	19
3.3 REDES DA GERAÇÃO 2,5G.....	22
3.3.1 CDMA 1XRTT	23
3.3.2 GPRS.....	24
3.3.2.1 EDGE.....	27
3.4 CONCLUSÕES.....	28
4 IP MÓVEL.....	29
4.1 INTRODUÇÃO.....	29
4.2 EXEMPLO DA NECESSIDADE DO IP MÓVEL	29
4.3 O IPV6	31
4.3.1 Comparação entre IPv4 e IPv6.....	32
4.4 O IP MÓVEL.....	33
4.4.1 Entidades envolvidas com o IP Móvel.....	33
4.4.2 O problema do roteamento IP frente à mobilidade.....	34
4.4.3 A solução apresentada pelo IP Móvel.....	36
4.4.3.1 Descobrir o care-of-address.....	38
4.4.3.1.1 Descoberta automática do home agent.....	38
4.4.3.2 Registrar o care-of-address.....	39
4.4.3.2.1 Autenticação	40
4.4.3.2.2 Em serviço.....	41

4.4.3.2.3 Anular o registro.....	41
4.4.3.3 Estabelecer um túnel até ao care-of-address.....	42
4.5 CONCLUSÕES.....	43
5 INTEROPERABILIDADE: CELULAR & WLAN.....	44
5.1 INTRODUÇÃO.....	44
5.2 A SOLUÇÃO PARA INTEROPERABILIDADE	46
5.3 EXEMPLO DE SISTEMA IMPLEMENTADO.....	46
5.3.1 A Arquitetura do sistema com interoperabilidade.....	47
5.4 CONCLUSÕES.....	49
6 CONCLUSÃO.....	51
REFERÊNCIAS BIBLIOGRÁFICAS.....	53
A - TÉCNICAS DE ESPALHAMENTO ESPECTRAL.....	54
A.1 – DSSS (Direct Sequence Spread Spectrum): Espalhamento Espectral de Sequência Direta.....	54
A.2 – FHSS (Frequency Hopping Spread Spectrum): Espalhamento Espectral por Saltos em Frequência.....	56
6.1.1.1.1 A.3 - Comparação entre as técnicas de espalhamento.....	57
B –IPV6: PRINCIPAIS CARACTERÍSTICAS.....	58
6.1.1.1.1 B.1 - Estrutura do datagrama IPv6.....	58
B.1.1 - Autoconfiguração de endereço.....	59
B.1.2 - Segurança no datagrama IPv6.....	59
B.1.3 - Qualidade de serviço.....	60
B.1.4 - Mobilidade.....	60
B.1.5 - Transição do IPv4 atual para o IPv6.....	60

ÍNDICE DE TABELAS

Tabela 4.1 – Comparação entre IPv4 e IPv6.....	32
Tabela A.1 – Comparação entre métodos de espalhamento de espectro.....	56

ÍNDICE DE FIGURAS

Figura	Página
FIGURA 2.1 - CONEXÃO DE UMA REDE SEM FIO COM UMA CONVENCIONAL COM FIO 3	
FIGURA 3.2. TDMA: FREQUÊNCIA X TEMPO.....	14
FIGURA 3.3 BANDAS SEPARADAS PARA O UPLINK E O DOWNLINK.....	14
FIGURA 3.4 – ARQUITETURA DO SISTEMA TDMA/IS-136.....	15
FIGURA 4.5 MOVIMENTO DO NÓ.....	30
TABELA 4.6 COMPARAÇÃO ENTRE IPV4 E IPV6.....	33
FIGURA 5.7 INTEROPERABILIDADE: WLAN (HOT-SPOT) E CELULAR (2,5G OU 3G).....	45
FIGURA -5.8 - ARQUITETURA DE UM SISTEMA COM INTEROPERABILIDADE.....	47
Figura A.1 – Sinal resultante da multiplicação dos sinais.....	54
Figura A.2 – Diagrama de blocos do DSSS.....	54
Figura A.3 – Diagrama de bloco do FHSS.....	55
Figura B.1 – Estrutura do datagrama do IPv6.....	57
Figura B 2 – Estrutura de rede com VPNs.....	58

SÍMBOLOS, NOMENCLATURAS E ABREVIACÕES

3GPP	<i>3rd Generation Partnership Project</i>	Organização para o Projeto da 3ª Geração
AAA	<i>Authentication, Authorization and Accounting</i>	Autenticação, Autorização e Contabilidade
CDMA	<i>Code Division Multiple Access</i>	Acesso Múltiplo por Divisão de Código
CSD	<i>Circuit-Switched Data</i>	Dados de circuito chaveado
DHCP	<i>Dynamic Host Configuration Protocol</i>	Protocolo de configuração do terminal dinâmico
EDGE	<i>Enhanced Data Rates for Global Evolution</i>	Aperfeiçoamento de Taxa de Dados numa Evolução Global
ETSI	<i>European Telecommunication Standards Institute</i>	Instituto de Padrões para Telecomunicações Europeu
FA	<i>Foreign Agent</i>	Agente Estrangeiro
GPRS	<i>General Packet Data Radio</i>	Serviço Geral de Rádio de Pacotes
GSM	<i>Global System for Mobile Communications</i>	Sistema Global para Comunicações Móveis
HÁ	<i>Home Agent</i>	Agente Local
IEEE	<i>Institute of Electrical and Electronics Engineering</i>	Instituto de Engenharia Elétrica e Eletrônica
IETF	<i>Internet Engineering Task Force</i>	Força Tarefa de Engenharia para Internet
IP	<i>Internet Protocol</i>	Protocolo da Internet
IPv4	<i>Internet Protocol version 4</i>	Protocolo da Internet Versão 4
IPv6	<i>Internet Protocol version 6</i>	Protocolo da Internet Versão 6
ISP	<i>Internet Service Provider</i>	Provedor de Serviços de Internet
ISO	<i>International Standards Organizations</i>	Organização Internacional de Padrões
LAN	<i>Local Area Network</i>	Rede de Área Local ou Rede Local
MIP	<i>Mobile IP</i>	IP Móvel
OSI	<i>Open System Interconnection</i>	Interconexão de Sistemas Abertos
PCS	<i>Personal Communication Service</i>	Serviço Pessoal de Comunicação de Dados
RF		Radio Frequência
RTPC		Rede de Telefonia Pública Comutada
SIM	<i>Subscriber Identity Module</i>	Módulo de Identificação do Assinante
SMS	<i>Short Message Service</i>	Serviço de Mensagens Curtas
TCP	<i>Transmission Control Protocol</i>	Protocolo de Controle de Transmissão
TDMA	<i>Time Division Multiple Access</i>	Acesso Múltiplo por Divisão de Código
UMTS	<i>Universal Mobile Telecommunications System</i>	Sistema de Telecomunicações Móveis Universal
VPN	<i>Virtual Private Network</i>	Rede Privada Virtual
WAN	<i>Wide Area Network</i>	Rede de Área Dispersa
WLAN	<i>Wireless Local Area Network</i>	Rede Local sem Fio

1 INTRODUÇÃO

Este trabalho tem por objetivo expor um estudo teórico sobre a interoperabilidade entre dois sistemas sem fio (wireless) diferentes: WLAN (*Wireless Local Area Network*) e Celular. Vários fatores serão expostos também em cada capítulo a fim de justificar a complementação, e não a substituição, das redes móveis celulares com as redes locais sem fio (WLANs) como por exemplo o crescimento da demanda por serviços de dados e o atraso dos serviços de terceira geração (3G).

Inicialmente, no capítulo 2, serão abordadas as WLANs, o seu desenvolvimento até os dias de hoje, sua principal padronização (o IEEE 802.11) e as camadas de controle e física que definem este tipo de padrão.

No capítulo 3, é apresentado o sistema móvel celular, dando-se enfoque aos principais sistemas dentro do contexto das gerações da telefonia móvel. O objetivo deste capítulo é expor uma visão não muito detalhada do sistemas, mas sim mostrar as principais características quanto às suas capacidades, arquiteturas (componentes que os compõem) e principalmente as vantagens e desvantagens frente aos serviços de dados e a intenção de serem complementados com as WLANs.

No capítulo 4 é abordado àquele que posteriormente será chamado de a chave para a interoperabilidade entre diferentes redes baseadas em IP: o IP Móvel. Serão abordadas teoricamente as entidades que compõem a proposta do IP Móvel, bem como ações e casos específicos de mobilidade de uma estação móvel, por exemplo um *laptop*.

Dentro da realidade da demanda de serviços de dados, é exposto neste capítulo 5 a proposta da interoperabilidade WLAN e Celular, utilizando cada peça para a proposta da solução que são os componentes vistos em cada capítulo anteriormente: as WLANs, as redes móveis de telefonia celular mais recentes (2,5G e 3G) e o IP Móvel.

Por fim no capítulo 6 é feita a conclusão de todo o trabalho desenvolvido sobre a interoperabilidade e também apresentam-se propostas para trabalhos futuros nesta área.

No apêndice A serão abordadas em maiores detalhes as principais técnicas de transmissão comentadas dentro do contexto tanto das WLANs como dos sistemas celulares: são as técnicas de espalhamento espectral DSSS e FHSS. Já o apêndice B visa apresentar de uma maneira mais detalhada também o padrão mencionado no capítulo 4, o IPv6, levando em conta as suas principais características e contribuições em relação ao IP Móvel.

2 WLAN

2.1 INTRODUÇÃO

Os avanços nas comunicações nos últimos anos possibilitaram o surgimento de várias tecnologias, que desde então procuram atender a real necessidade de seus usuários, com a melhor qualidade possível. Nos últimos anos a comunicação sem fio ganhou um espaço considerável nas tecnologias de transmissão de dados, deixando de existir apenas nas comunicações de longa distância (feitas através de satélite), para fazer parte de ambientes locais. Essa tendência foi fortalecida pelo investimento de instituições e empresas no sentido de aplicar a transmissão sem fio em redes de computadores.

Uma rede sem fio (*Wireless*) é tipicamente uma extensão ou uma alternativa de uma rede local (*Local Area Network - LAN*) convencional com fio, criando-se o conceito de rede local sem fio (*Wireless Local Area Network - WLAN*). Uma WLAN converte pacotes de dados em onda de rádio ou infravermelho e os envia para outros dispositivos sem fio ou para um ponto de acesso que serve como uma conexão para uma LAN com fio.

De uma outra maneira, uma rede sem fio é um sistema que interliga vários equipamentos fixos ou móveis utilizando o ar como meio de transmissão.

A Figura 2.1 ilustra uma rede sem fio conectada por um ponto de acesso (*Access Point - AP*) a uma rede convencional com fio. Esses Pontos de Acesso também podem estar conectados a outros pontos de acesso ou também diretamente a um meio de acesso de banda larga como um modem DSL ou um *cable modem*.

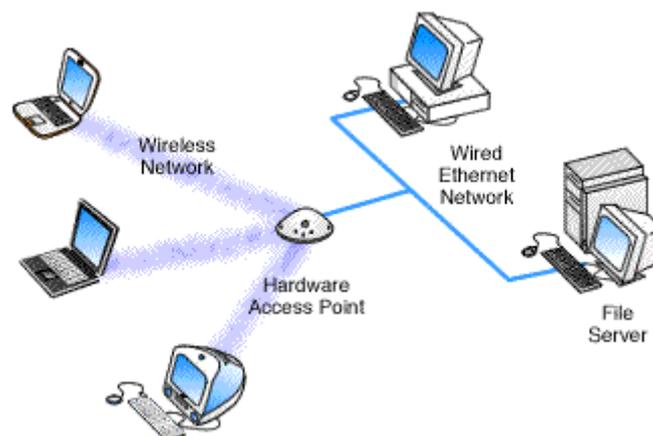


Figura 2.1 - Conexão de uma rede sem fio com uma convencional com fio

2.2 O DESENVOLVIMENTO DAS WLANs

O primeiro sistema de computadores que empregou as técnicas de radiodifusão ao invés de cabos ponto a ponto foi o sistema ALOHA. Na década dos 70, quando o projeto foi implantado, as linhas telefônicas disponíveis na ocasião eram caras e pouco confiáveis. Havia a necessidade da interligação de subredes espalhadas ao centro de processamento de dados em uma Universidade. No sistema, a comunicação foi realizada através da instalação, em cada estação, de um pequeno transmissor/receptor de rádio FM, com um alcance suficiente para se comunicar com o transmissor/receptor do Centro de Computação, foram usadas duas faixas de frequência e a transmissão foi feita a 9600 bps.

A largura de banda e a tecnologia de transmissão utilizadas no sistema ALOHA foram as limitações que não permitiram a comercialização do primeiro sistema sem fio. Entretanto, com a miniaturização dos componentes eletrônicos nas últimas décadas, bem como o grande interesse nas comunicações pessoais sem fio, fizeram com as redes locais sem fio despertassem grande interesse em termos de pesquisa e desenvolvimento, que resultou nas primeiras redes wireless comerciais no início dos anos 90.

A partir desse momento os fabricantes desenvolveram suas redes conforme a critérios próprios, pelo qual era possível encontrar redes com vazões e alcances diferentes, empregando diversos critérios de segurança e definindo os algoritmos das camadas com abordagens particulares, ou seja, não havia interoperabilidade entre equipamentos de fabricantes diferentes.

Em maio de 1991, foi pedido ao IEEE a elaboração de padrões adotados em redes locais e metropolitanas, formando-se o Grupo de Trabalho 802.11, cujo objetivo era definir uma especificação para conectividade sem fio entre estações de uma área local. A elaboração do padrão teve atrasos, o Grupo de Trabalho 802.11 publicou o padrão no segundo semestre de 1997.

Atualmente o foco das redes de computadores sem fio (*Wireless*) se encontra no contexto das redes locais de computadores, as WLANs, tanto em soluções proprietárias como no padrão do IEEE. Porém a maioria das empresas hoje baseiam seus produtos no padrão do IEEE, devido às inúmeras vantagens que o padrão aberto oferece: interoperabilidade, baixo custo, demanda de mercado, confiabilidade de projeto, entre outras.

2.3 O PADRÃO IEEE 802.11

O padrão IEEE 802.11 define basicamente uma arquitetura para as WLANs que abrange os níveis físico e de enlace., como aparece na figura 2.2. Da mesma forma, a subcamada LLC (*Logic Link Control*) e os níveis superiores não percebem as particularidades da subcamada MAC e de seus possíveis níveis físicos.

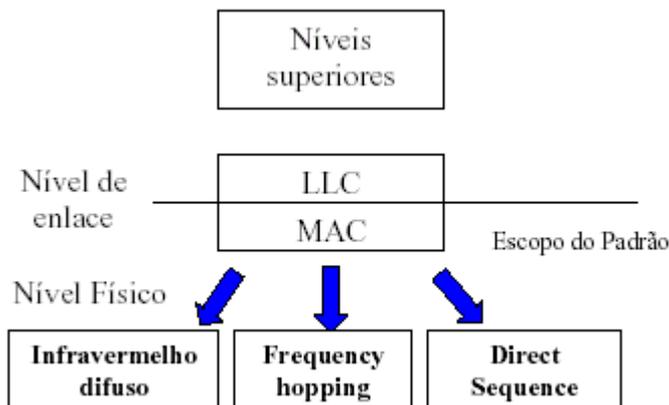


Figura 2.2 Escopo do Padrão IEEE 802.11

A Figura 2.3 ilustra o padrão IEEE 802.11, comparando com o modelo padrão de redes de computadores, o RM-OSI da ISO (*Reference Model – Open Systems Interconnection of the International Standardization Organization*).

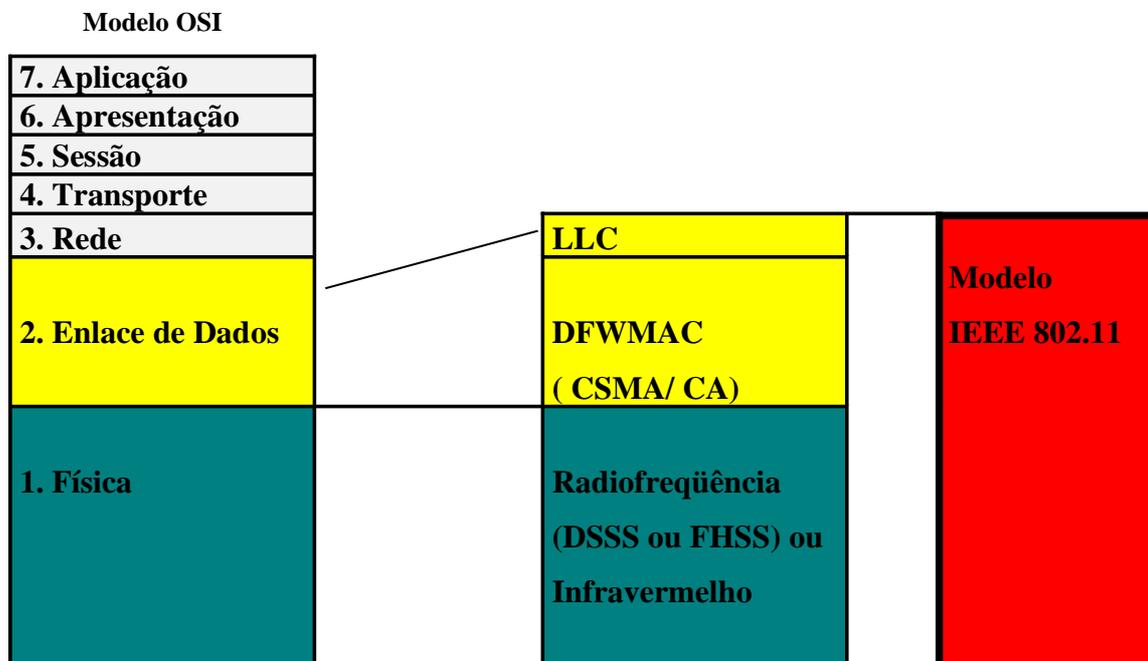


Figura 2.3 Comparação do padrão 802.11 com o RM-OSI

Esse padrão tem, entre outras, as seguintes premissas: suportar diversos canais; sobrepor diversas redes na mesma área de canal; apresentar robustez com relação a

interferência; possuir mecanismos para evitar nós escondidos; oferecer privacidade e controle de acesso ao meio.

A maioria das redes sem fio é baseada nos padrões IEEE 802.11 e 802.11b (sendo este último evolução do primeiro), para comunicação sem fio entre um dispositivo e uma rede LAN. Esses padrões permitem transmissão de dados de 1 a 2Mbps, para o padrão IEEE 802.11, e de 5 a 11Mbps, para o padrão IEEE 802.11b, e especificam uma arquitetura comum, métodos de transmissão, e outros aspectos de transferência de dados sem fio, permitindo a interoperabilidade entre os produtos.

Quanto à segurança, o padrão possibilita autenticação e criptografia do quadro MAC. Para isso, define um algoritmo denominado WEP (*Wired Equivalent Privacy*). O WEP utiliza o algoritmo RC4PRNG da *RSA Data Security*.

2.3.1 Topologia

As redes sem fio 802.11 podem apresentar-se fisicamente de dois modos: redes de infra-estrutura e redes ad hoc.

2.3.1.1 Infra-estruturada

As redes de infra-estrutura (Cliente/Servidor) caracterizam-se por possuir dois tipos de elementos: Estações Móveis (*Laptops*, *PADs*, outros) e Pontos de Acesso. Cada ponto de acesso é responsável pela conexão das estações móveis de uma área de cobertura com a rede local com fio. O ponto de acesso 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 controlado por outro ponto de acesso.

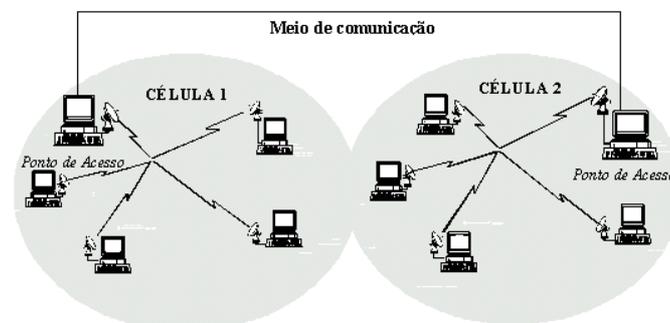


Figura 2.4 Rede sem fio infra-estruturada

2.3.1.2 Ad hoc

As redes *Ad Hoc* caracterizam-se por não possuírem qualquer infra-estrutura de apoio à comunicação. São diversos equipamentos móveis confinados em uma pequena área que estabelecem comunicação aos pares (*peer-to-peer*) por certo período de tempo.

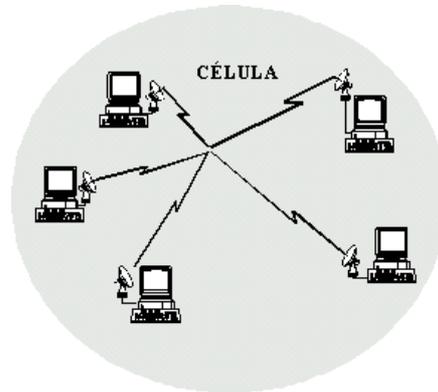


Figura 2.5 - Rede sem fio Ad Hoc

2.3.2 Subcamada de Controle de Acesso ao Meio (MAC)

Para o padrão 802.11, o IEEE definiu um protocolo de acesso ao meio (subcamada MAC do nível de enlace de dados), denominado de DFWMAC (*Distributed Foundation Wireless Medium Access Control*), que suporta dois métodos de acesso: um método distribuído básico, que é obrigatório; e um método centralizado, que é opcional, podendo esses dois métodos coexistir (IEEE802.11a). O protocolo de acesso ao meio das redes 802.11 também trata de problemas relacionados com estações que se deslocam para outra células (*roaming*) e com estações perdidas (*hidden node*).

O método de acesso distribuído forma a base sobre a qual é construído o método centralizado. Os dois métodos, que também podem ser chamados de funções de coordenação (*Coordination Functions*), são usados para dar suporte à transmissão de tráfego assíncrono ou tráfego com retardo limitado (*time bounded*).

Uma função de coordenação é usada para decidir quando uma estação tem permissão para transmitir. Na função de coordenação distribuída (*Distributed Coordination Functions - DCF*), essa decisão é realizada individualmente pelos pontos da rede, podendo, dessa forma, ocorrer colisões. Na função de coordenação centralizada, também chamada de função pontual (*Point Coordination Function - PCF*), a decisão de quando transmitir é centralizada em um ponto especial, que determina qual

estação deve transmitir em que momento, evitando teoricamente a ocorrência de colisões.

A função de coordenação distribuída representa o método de acesso básico do protocolo DFWMAC. É uma função conhecida como CSMA/CA (*Carrier Sense Multiple Access / Collision Avoidance*) com reconhecimento. A DFC trabalha semelhantemente a função CSMA/CD da tecnologia de rede local cabeada (Padrão Ethernet 802.3), apenas com uma diferença: o protocolo CSMA/CD do Ethernet controla as colisões quando elas ocorrem, enquanto que o protocolo CSMA/CA do padrão sem fio apenas tenta evitar as colisões.

2.3.3 Camada física

Dentro do padrão IEEE 802.11, as WLANs basicamente utilizam radiofrequência para a transmissão de dados, através de duas técnicas conhecidas como DSSS (*Direct Sequence Spread Spectrum*) e FHSS (*Frequency Hopping Spread Spectrum*), codificando dados e modulando sinais de modos diferentes para equilibrar velocidade, distância e capacidade de transmissão. A escolha da técnica DSSS ou FHSS dependerá de vários fatores relacionados com a aplicação dos usuários e o ambiente onde a rede operará.

Outras formas de transmissão também podem ser usadas em redes locais sem fio, como a transmissão em infravermelho, por exemplo. Mas transmissões com infravermelho não atravessam certos tipos de materiais, apesar de poder enviar mais dados do que a transmissão com radiofrequência. Com isso, a transmissão através de radiofrequência acaba sendo o padrão adotado nas transmissões WLAN.

As técnicas DSSS e FHSS transmitem os quadros de dados enviando-os por vários canais disponíveis dentro de uma frequência, ao invés de usar um único canal, possibilitando, dessa forma, a transmissão simultânea de vários quadros.

A técnica DSSS distribui o sinal em cima de uma gama extensiva da faixa de frequência e reorganiza os pacotes no receptor. Já técnica FHSS envia segmentos curtos de dados que são transmitidos através de frequências específicas, controlando o fluxo com o receptor, que negocia velocidades menores comparadas às velocidades oferecidas pela técnica DSSS, mas menos suscetíveis a interferências.

As WLANs baseadas em radiofrequência usam as faixas de frequência ISM (*Industrial - Scientific - Medical*), que assumem frequências de 900MHz, 2.4GHz e 5GHz e na maioria dos países são livres de licença dos órgãos reguladores, como por exemplo o Brasil. Quanto maior a frequência maior é a quantidade de informação que um dispositivo pode enviar num canal. As primeiras WLANs operavam na frequência de 900MHz, atingindo uma taxa de 256Kbps. O padrão IEEE 802.11 aumentou a taxa de transmissão para 1Mbps, usando a técnica FHSS, e posteriormente para 2Mbps, usando a técnica DSSS, trabalhando na frequência de 2.4GHz.

O padrão mais popular atualmente, o IEEE 802.11b, especifica a técnica básica de transmissão na camada física usando a técnica DSSS, passando a taxa de transmissão real de 2Mbps para 5Mbps (com a possibilidade de se chegar a 11Mbps), tornando as redes locais sem fio mais atrativas. As duas técnicas de transmissão aqui mencionadas são apresentadas detalhadamente no apêndice A. A figura 2.6 mostra a relação entre velocidade e mobilidade das redes WLAN em relação as redes LAN e os sistemas móveis celulares 2G, 2,5G e 3G, que serão abordados posteriormente no capítulo 3 deste trabalho.

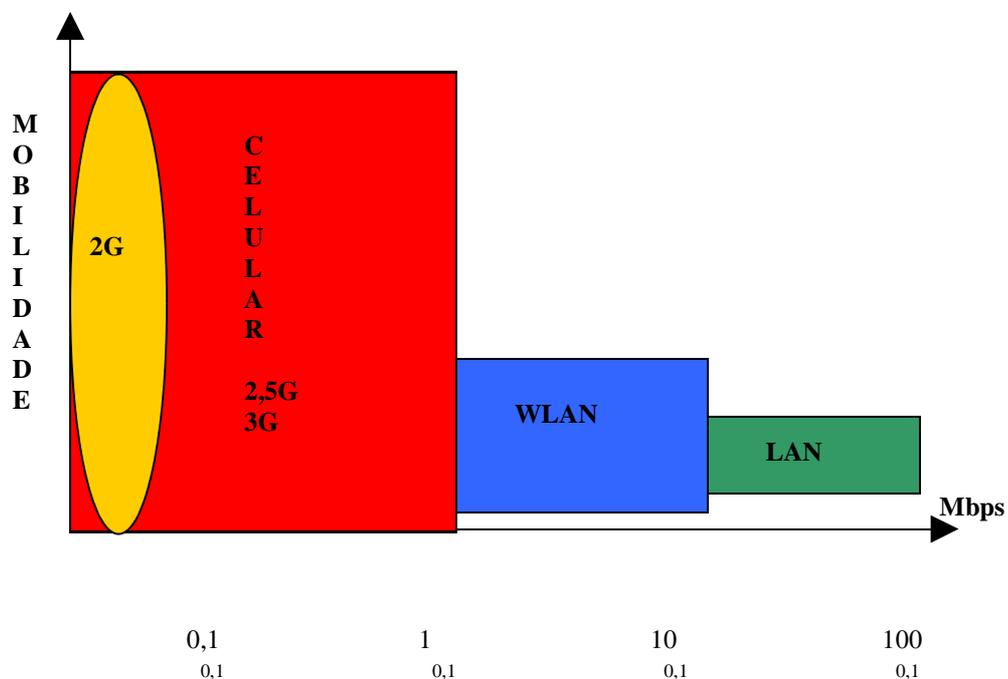


Figura 2.6 WLAN e outras tecnologias : Mobilidade X Velocidade (Mbps)

2.4 CONCLUSÕES

A adoção de sistema sem fio vem crescendo significativamente, em que muitas soluções WLAN estão ou já foram implantadas em empresas, universidades e outras instituições do mundo inteiro. Isso indica, sem dúvida, que as redes de computadores sem fio são uma realidade e, provavelmente, nos próximos anos, serão complementares aos sistemas sem fio já existentes como por exemplo as redes de telefonia celular.

A tecnologia sem fio não é recente, mas seus produtos caros e sua baixa taxa transferência de dados, inviabilizaram seu uso. Duas razões contribuíram bastante para que a tecnologia sem fio avançasse: a aprovação do padrão IEEE 802.11, em 1997, o que ajudou a tornar as WLAN uma realidade; e o barateamento dos equipamentos para WLAN, que fizeram com que as redes sem fio ficassem mais acessíveis para algumas empresas, aumentando consideravelmente a comercialização de produtos para computadores móveis, como o cartão PCMCIA para *Laptops* e o cartão ISA/PCI para PCs. Em muitos países, as WLANs vem sendo muito usadas por exemplo na medicina no atendimento aos pacientes, em construções antigas ou tombadas pelo patrimônio histórico, enfim, em lugares onde há a necessidade de mobilidade e flexibilidade nas estações de trabalho. Porém no Brasil, esta ainda não é uma realidade.

3 SISTEMA MÓVEL CELULAR

3.1 INTRODUÇÃO

A Primeira Geração de Redes de Telefones Celulares comerciais iniciou a sua operação foi em 1978 em New Jersey. Essas redes utilizavam a modulação analógica para que o sinal de voz fosse transmitido pelo espaço livre. A recepção e a transmissão do sinal de voz era feita pela mesma frequência portadora. Esse sistema era chamado de AMPS (*Advanced Mobile Phone Service*). O espectro de frequência era limitado, como foi determinado pelas agências reguladoras. Somente uma faixa finita do espectro era disponível para o sistema celular funcionar. Uma das dificuldades encontradas pelo sistema neste momento, além do aumento da demanda por parte dos usuários, foi a de se otimizar o sistema, codificar e comprimir o sinal de voz. Portanto era necessária a digitalização do sinal de voz.

A Segunda Geração de Redes de Telefones Celulares comerciais foi desenvolvida em quatro padrões diferentes. Um primeiro foi desenvolvido a partir da evolução do sistema AMPS, que foi chamado de DAMPS ou TDMA/IS-54. Esse novo sistema foi desenvolvido para ser totalmente compatível com o sistema AMPS.

Já um segundo padrão totalmente incompatível com o sistema analógico foi desenvolvido na Europa durante a década de 80. Ele foi criado a partir das necessidades do *roaming* entre as regiões próximas de operadoras diferentes, de uma padronização para um sistema único e da capacidade de suportar a crescente demanda. A esse novo sistema deu-se o nome de GSM (*Global System for Mobile Communications*). O GSM rapidamente tornou-se um padrão dominante e com grandes quantidades de serviços extras como o popular serviço de mensagens, o SMS (*Short Message Service*).

Em meados dos anos 90, surgiu outro sistema chamado de CDMA (IS-95) desenvolvido pela Qualcomm. Esse sistema utiliza a codificação do sinal de voz para fazer o espalhamento desse sinal por todo o espectro de frequência, método chamado de *Spread Spectrum*. No Japão foi desenvolvido outro padrão chamado de PDC (*Personal Digital Celular*), que colocou o Japão em uma posição de isolamento com um sistema velho e incompatível com os outros padrões.

Na atualidade é comum ouvirmos também falar de sistemas 2,5G. Esse termo se refere aos sistemas celulares com serviços e taxas adicionais àquelas oferecidas pelos

sistemas 2G, porém ainda não caracterizados como sistemas de terceira geração ou simplesmente 3G. Os PCSs (*Personal Communication Services*) se enquadram nessa categoria. Esses serviços são oferecidos principalmente através de versões melhoradas dos atuais sistemas 2G operando nas bandas destinadas aos serviços PCS, bandas essas que diferem de país para país. No Brasil a banda escolhida para os serviços PCS está na faixa de 1,8 GHz. Pode-se então interpretar PCS como uma extensão dos sistemas 2G, em bandas distintas e oferecendo serviços de maior valor agregado que os sistemas 2G.

A comunicação sem fio capaz de permitir a troca de informações a altas taxas e com alta qualidade entre terminais pequenos e portáteis, localizados em qualquer parte do mundo, representa a fronteira a ser alcançada pelos sistemas de terceira geração. O início dos estudos sobre os sistemas de terceira geração foi marcado por uma indecisão mantida por duas correntes: uma defendia a criação de um único padrão mundial; a outra defendia a evolução das redes e sistemas atuais de forma a atender aos requisitos definidos a partir da visão 3G.

Atualmente, as empresas prestadoras de serviço de telefonia móvel no Brasil que tem a permissão de funcionar nas Bandas A e B oferecem seus serviços nas tecnologias TDMA/IS-136 e CDMA/IS-95. As empresas que estão em processo de inclusão no mercado brasileiro, que estão operando nas Bandas C e D, oferecem seus serviços na tecnologia GSM/GPRS. Sabendo disso iremos descrever cada uma dessas tecnologias, suas arquiteturas, bem como suas vantagens, desvantagens e os possíveis caminhos de evolução de alguns desses sistemas dentro do contexto da geração a qual pertencem.

3.2 REDES DE SEGUNDA GERAÇÃO (2G)

3.2.1 TDMA / IS-136

O TDMA é uma tecnologia de transmissão digital que permite o acesso de 3 usuários em um único canal de rádio frequência sem interferência, usando a mesma frequência portadora, através da alocação de um par único time slot para cada usuário, como pode ser visto na figura 3.1.

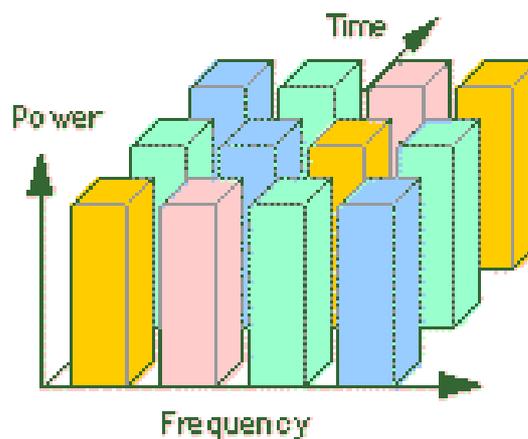


Figura 3.2. TDMA: Frequência X Tempo

O *dowlink* e o *uplink* são separados em frequências diferentes, conforme figura abaixo. No Brasil, a última versão dessa tecnologia disponível é o TDMA/IS-136 que é uma evolução do TDMA/IS-54.

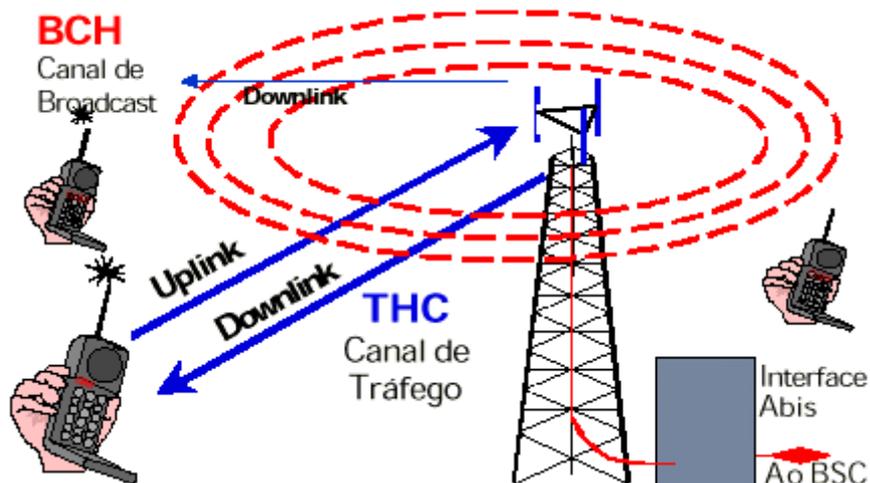


Figura 3.3 Bandas separadas para o uplink e o downlink

A vantagem do TDMA/IS-136 é a qualidade de voz superior as outras versões dessa tecnologia. O TDMA/IS-136 se diferencia do TDMA/IS-54 no tipo de modulação utilizada nos canais de controle: a modulação $\pi/4$ DQPSK. Ela eleva a taxa de transmissão nesses canais e provê serviços adicionais, tais como *paging* e o envio de mensagens curtas (SMS). A arquitetura do TDMA/IS-136 tanto para as frequências de 800MHz e 1900MHz consiste em quatro módulos principais, conforme a figura 3-2:

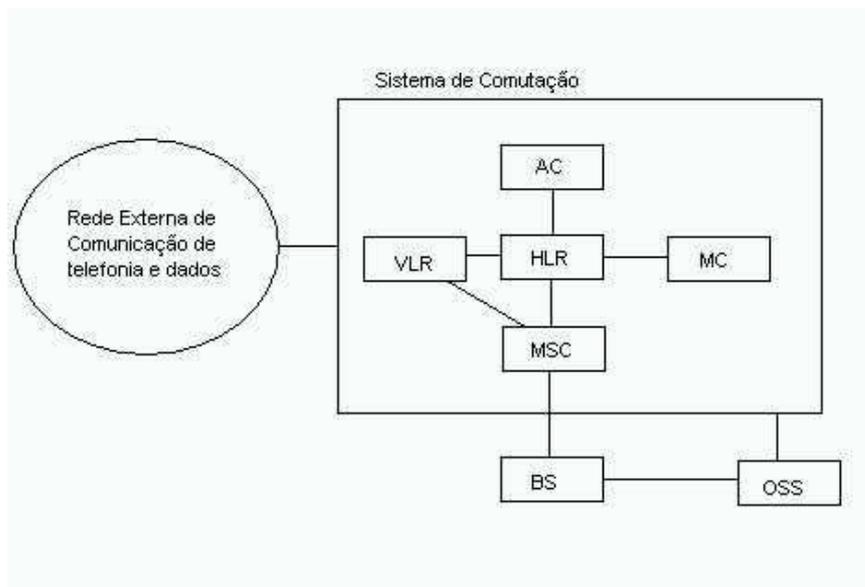


Figura 3.4 – Arquitetura do sistema TDMA/IS-136

Os módulos principais são: o sistema de comutação (CCC), a estação rádio base (ERB), o sistema de operação e suporte (OSS) e a estação móvel (Aparelho).

O sistema de comutação é quem controla o processamento de chamadas e as funções relacionadas aos assinantes, contém cinco sub-módulos:

- MSC (Mobile Switching Center) - Geralmente chamada de CCC, é o módulo que realiza as funções de roteamento do telefone para a rede, fazendo o controle das chamadas para outras redes de comunicações de telefone e dados como a PSTN (*Public Switched Telephone Networks*), a ISDN (*Integrated Services Digital Networks*) e várias redes privadas.
- VLR (Visitor Location Register) - Módulo que armazena todos os dados dos assinantes temporários necessários para que os assinantes visitantes utilizem os serviços do MSC.
- HLR (Home Location Register) - Banco de dados que armazena e gerencia todos os dados dos assinantes permanentes incluindo o perfil de serviços oferecidos aos assinantes, informação de localização e *status* de atividades, sendo considerado o módulo mais importante do sistemas de comutação.
- AC (Authentication Center) - Módulo que provê os parâmetros de autenticação e encriptação que verificam a identidade dos usuários e assegura a segurança de cada ligação e do sistema. Esta funcionalidade protege as operadoras de rede de fraude como clonagens de usuários.

- MC (Message Center) - Módulo que suporta vários serviços de mensagem, por exemplo, o voice mail e o SMS.
- ERB (Estação Rádio Base): é o módulo que conecta o usuário ao sistema de comutação, fazendo toda a comunicação de radiofrequência com o sistema de comutação e suporte (OSS). Ela é composta basicamente de equipamentos de rádios. O OSS auxilia na operação e na manutenção das atividades da rede permitindo a otimização dos serviços oferecidos.

No sistema TDMA/IS-136 contem 4 tipos de canais, o canal de controle analógico (ACCH), o canal de controle digital (DCCH), o canal de voz analógico (AVCH) e o canal de tráfico digital (DTC).

O TDMA/IS-136 traz como principal aprimoramento o canal de controle digital (DCCH) que substitui o canal de controle analógico (ACCH). O DCCH, que forma o centro das especificações do TDMA/IS-136, possibilita as operadoras serviços como o *short message* e *sleep mode*, que aumenta muito a funcionalidade como a carga da bateria dos celulares, além disso aumenta a capacidade do sistema.

Algumas outras das características importantes do TDMA/IS-136 são os serviços de pacotes de dados, o *handoff* móvel assistido, o SMS aperfeiçoado e o roaming inteligente. O *handoff* móvel assistido é usado para diminuir o número de ligações não completadas e garantir a qualidade do sistema móvel.

Para a comunicação de dados o TDMA/IS-136 é limitado, o que o ele oferece é a preparação do canal DCCH para aplicações de SMS que necessariamente requer uma plataforma externa e uma taxa de 9,6 Kbps fazendo o uso da tecnologia CSD (*Circuit Switch Data*) por canal de 30kHz.

3.2.2 CDMA/IS-95

O padrão CDMA/IS-95 é fundamentado em tecnologia com espalhamento espectral e foi projetado com o objetivo de possibilitar a transição suave da tecnologia analógica para a digital. O CDMA/IS-95 tem tido grande aceitação internacional entre os outros sistemas de telefonia móvel por melhorar alguns aspectos relevantes das outras tecnologias como a interferência, sinais refletidos, baixa potência e planejamento de frequências. Os usuários compartilham a mesma faixa de frequência, mesmo aqueles em células adjacentes onde o canal no CDMA/IS-95 ocupa 1,25MHz.

O uso da tecnologia CDMA foi liberado para a utilização para aplicações civis de telefonia móvel somente em 1989, mas foi proposto teoricamente na década de 40. Era usado nas aplicações militares, por exemplo, para esconder o sinal transmitido de espões e vencer os efeitos de forte interferência.

Além de basear-se no espalhamento espectral, otimiza a largura de banda por meio da equalização do SNR (*Signal to Noise Ratio*) entre todos os usuários, dividindo com maior precisão os recursos de potência do sistema em relação às tecnologias TDMA e GSM. Assim os usuários que estão perto da estação rádio base transmitem com menor potência, mantendo a mesma SNR que usuários mais distantes, por meio de uma menor potência a interferência entre canais é controlada. O IS-95, como o AMPS e o TDMA/IS-136 também usa o padrão IS-41 para gerenciar a mobilidade e protocolo de roaming.

A arquitetura do CDMA/IS-95 é muito parecida com a arquitetura do TDMA/IS-136, diferenciando-se somente na inclusão da BSC (*Base Station Controller*) e da BSS (*Base Station Support*). Tanto para as frequências de 800MHz e 1900MHz a arquitetura é composta por seis módulos principais, como podemos ver na figura 3.3:

- Sistema de comutação (CCC) - Controla as funções de interconexão e relacionadas aos assinantes;
- BSC - Controla o estabelecimento e processamento de chamadas;
- BSS - Auxilia as atividades de operação e manutenção das estações rádio base;
- BS ou ERB - Realiza a conexão do usuário ao BSC e as funções relacionadas a rádio comunicação;
- OSS - O Sistema de operação e suporte auxilia as atividades de operação e manutenção necessárias da central de comutação;
- Estação Móvel - Dispositivo de comunicação de voz e dados do usuário final.

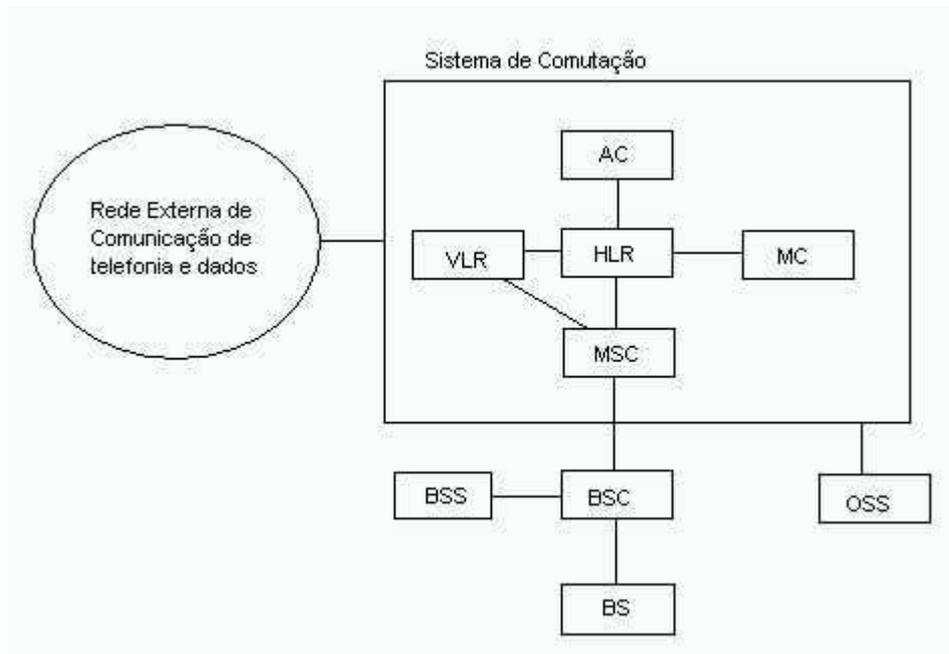


Figura 3.4 Arquitetura do sistema CDMA

As características técnicas principais do padrão CDMA/IS-95 são:

- Uso da mesma faixa espectral de operação do AMPS e IS-136 (800MHz);
- Largura de faixa de transmissão igual a 1.25MHz;
- No *downlink* (ERB para celular) são utilizados 64 códigos de Walsh-Hadamard combinados para ortogonalidade entre os sinais dos usuários, utilização de uma seqüência PN do tipo m para um espalhamento efetivo e robustez contra os efeitos dos multipercursos;
- No *uplink* (celular para ERB) são utilizados seqüências PN tipo m que apresentam melhores propriedades para sincronismo;
- Codificação de canal convolucional com taxa de 1/2 no *downlink* e taxa 1/3 no *uplink*;
- Uso da portadora piloto para sincronismo e detecção coerente nos terminais móveis;
- *Soft handoff* (mesma portadora para todo o sistema) - tem como principal objetivo melhorar o processo de *handoff*.

O CDMA/IS-95 ainda apresenta alguns recursos que podem ser considerados como vantagens frente aos outros sistemas:

- *Vocoder* variável: melhora a qualidade de voz , pois são introduzidas maiores redundâncias na codificação de voz, ficando menos susceptível ao ruído;
- Apresenta nas suas especificações telefones móveis duais (AMPS/IS-95). Quando usado como CDMA pode operar com um *vocoder* de 8kbps ou 13kbps.
- *Rake receiver*: é um receptor de rádio capaz de diferenciar multipercursos com uma resolução de até 0.81 μ s. O *rake receiver* é um dispositivo de diversidade que gera um ganho de recepção melhorando a qualidade e o desempenho do sistema.
- *Soft capacity* – degradação suave da qualidade do *uplink* quando há sobrecarga de usuários do sistemas.

Como o TDMA/IS-136, o CDMA/IS-95 se apresenta como uma tecnologia limitada à comunicação de dados com taxas de transmissão de 14.4kbps fazendo o necessário emprego do CSD. Também requer uma plataforma externa adicional para prover o SMS.

3.2.3 GSM

O sistema GSM teve suas especificações publicadas em 1990 pela ETSI (*European Telecommunication Standards Institute*). Ele foi introduzido na Europa em 1991 e rapidamente adotado em vários países do mundo.

Esse sistema, assim como o TDMA/IS-136, combina tanto o TDMA como o FDMA (*Frequency Division Multiple Access*). Nele a portadora de frequência é dividida em 8 *times slots*, sendo que a taxa de codificação de voz é de 13 kbps, e é modulada usando GSMK (*Gaussian Minimum Shift Keyed*) em uma portadora de 200kHz.

O controle de erro e equalização contribuem para a robustez do sinal de rádio contra interferência e atenuação na transmissão. Este sistema usa um codificador de voz para definir um modelo de geração de tons e ruídos na garganta humana e a filtragem acústica feita pela boca e língua. Estas características são usadas para produzir coeficientes, que são enviados pelo TCH.

O codificador de conversação é baseado em um codificador preditivo linear com excitação residual (RELTP); este codificador é aperfeiçoado com a inclusão de um dispositivo preditivo de longo prazo (LTP). O LTP melhora a qualidade da conversação removendo a estrutura dos sons das vogais antes de codificar os dados residuais. A saída

do codificador fornece 260 bits para cada bloco de conversação de 20 ms. Isto resulta em uma taxa de 13 kbps. Os bits da saída são ordenados, conforme a sua importância, em grupos de 182 e 78 bits. Os 182 bits mais importantes são subdivididos, com a separação dos 50 bits muito importantes. A taxa de dados de 13 kbps é consideravelmente menor que a digitalização direta da conversação, como a feita no PCM. No futuro, codificadores de voz mais avançados reduzirão esta taxa a até 6,5 kbps (codificação em meia taxa).

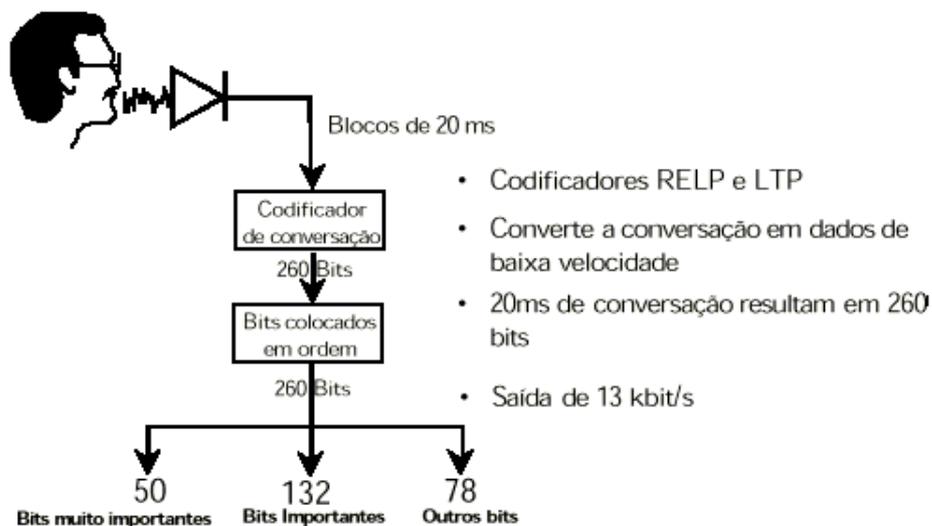


Figura 3.5 - Codificação da voz no GSM

A arquitetura do sistema GSM é similar a dos sistemas descritos anteriormente, exceto pela estação móvel (celular) que contém o elemento SIM (*Subscriber Identity Module*). A rede GSM é subdividida em dois subsistemas, cada qual com suas respectivas unidades funcionais. O primeiro módulo é o sistema de comutação, composto pela CCC, bases de VLR, HLR, MSC, AUC e EIR. O segundo módulo é denominado de Estação Base que é composta pela BSC e BTS que têm a mesma função dos sistemas explicados anteriormente.

Os três módulos que compõem a arquitetura do GSM e não existem nos demais descrito acima são:

- **AUC** - Base de dados conectada ao HLR que é denominado centro de autenticação, cuja função é autenticar os assinantes que tentam utilizar uma rede, por meio de perfis de autenticação e chaves de cifragem. Este recurso permite a proteção das operadoras do serviços contra fraude.

- **EIR** - Base de dados denominada registradora de identidade de equipamento, inclusive o número de série eletrônico de cada aparelho (ESN), e tem como finalidade bloquear as chamadas não autorizadas, “clonadas” ou com defeito.
- **MSC** - *Gateway* que permite a conexão para efeito de roteamento ou conexão de chamada entre o sistema de comutação GSM e outras redes, como por exemplo a rede fixa comutada.

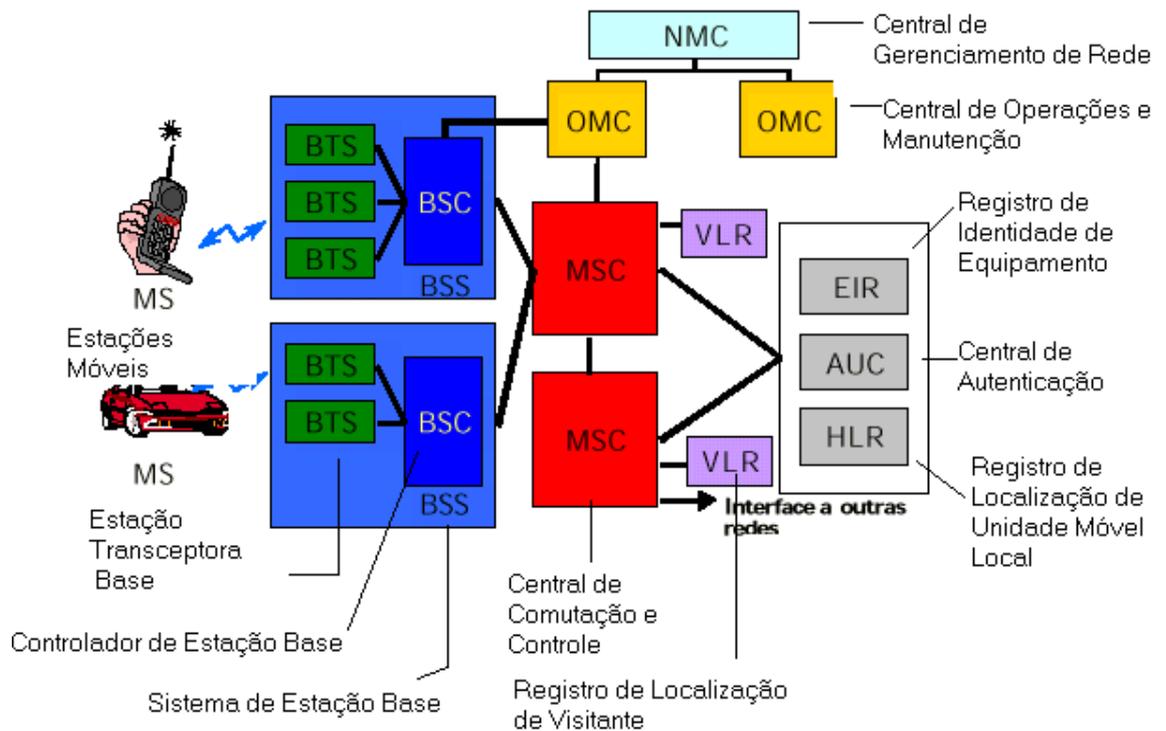


Figura 3.6 Arquitetura do sistema GSM

O terminal móvel opera em várias frequências (900,1800 e 1900MHz) e modos compatibilizando com o sistema GSM. Esse sistema separa o *uplink* e o *downlink* em bandas de frequência distintas, da mesma forma que o TDMA/IS-136. Dentro de cada banda, o esquema de numeração de canais usado é o mesmo. Na verdade, um canal do GSM é formado por um *uplink* e um *downlink*.

É interessante observar que, enquanto o TCH usa um canal de frequência no *uplink* e no *downlink*, o BCH somente ocupa um canal no *downlink*. O canal correspondente no *uplink* é na verdade deixado desocupado. Este canal pode ser usado pela unidade móvel para canais não programados ou canais de acesso aleatório (RACH). Quando a unidade móvel quiser chamar a atenção da estação base, para fazer uma chamada, por exemplo ela poderá fazê-lo usando este canal de frequência desocupado para enviar um RACH. Como mais de uma unidade móvel pode querer

chamar a atenção da estação ao mesmo tempo, é possível que haja uma colisão de canais RACH, e talvez seja necessário que as unidades móveis façam diversas tentativas para serem ouvidas.

Os terminais móveis são compostos por duas partes principais, a primeira composta pelo equipamento em si e a segunda o “*Subscriber Identity Module*”, o SIM Card. Ele contém as informações de identificação e dados usados pelo assinante, por exemplo:

- Seu número exclusivo de assinante ou IMSI (Identificação Internacional de Assinante Móvel);
- As redes e países em que o assinante pode receber o serviço (MCC e MNC);
- Quaisquer outras informações específicas do usuário, como números de discagem rápida e memórias.

O SIM *Card* trouxe mobilidade pessoal e mobilidade para o terminal, sendo uma das vantagens do GSM.

O SMS é o atual padrão de comunicação de textos identificado pelos serviços das redes GSM e permite ao usuário consultar a base de informações da operadora em formato “texto”, sem estar conectado em banda larga e sem usar o padrão de mensagem da Internet. A velocidade dessa comunicação está entre 9.6kbps e 14kbps.

O sinal TDMA do GSM por ser de natureza digital permite a utilização de vários processos para melhorar a qualidade de transmissão, o tempo de vida útil da bateria, e a eficiência espectral em relação ao sistema AMPS. Outra vantagem do GSM é o controle de potência que permite minimizar a potência de transmissão das estações móveis e da BS, reduzindo assim a interferência gerada nos canais e o consumo.

Como o TDMA/IS-136 e o CDMA/IS-95, o GSM é excelente para comunicação de voz, mas se apresenta uma tecnologia limitada à comunicação de dados com taxas de transmissão de 9.6kbps fazendo o necessário emprego do CSD, ainda requerendo uma plataforma externa adicional para prover o SMS.

3.3 REDES DA GERAÇÃO 2,5G

3.3.1 CDMA 1XRTT

A tecnologia CDMA 1XRTT é o primeiro passo na evolução do padrão CDMA/IS-95 para a terceira geração (3G), nas frequências de 800MHz e 1.9GHz. Essa versão também é conhecida como CDMA2000-1X.

As especificações atuais do CDMA são às vezes referenciadas como IS-95C e correspondem à fase 1 de implementação do CDMA2000, também conhecida por CDMA 1XRTT. As atuais implementações do padrão têm como principais características:

- Melhorias nos quesitos capacidade, cobertura e eficiência espectral;
- Maiores taxas de dados (64 a 144 kbps), incluindo transmissão de dados por comutação de pacotes;
- Maior tempo de duração da bateria no modo *stand-by*;
- Processos de *handoff* mais eficientes.
- Internet móvel, acesso à Intranet e à Internet, vídeo conferência;
- Para acesso fixo sem fio usa-se Walsh 128 *versus* o 64, usado no CDMA;

As principais alterações de hardware de forma a atender as características anteriormente citadas são: no *downlink*

- Controle de potência mais rápido e preciso;
- Substituição da modulação BPSK por QPSK, com 128 funções Walsh;
- Redução no *overhead* por *soft-handoff*.

E no *uplink*:

- Redução de retardo no processo de controle de potência;
- Uso de modulação BPSK com detecção coerente auxiliada por código piloto;
- Uso de codificação de canal com taxa 1/4 ao invés de 1/2 e 1/3.

O CDMA2000-1XEV-DO(DATA ONLY) é o primeiro passo de evolução da tecnologia CDMA2000-1X suportando a comutação de voz por pacotes e dados a altas velocidades também comutadas em portadoras separadas, sendo que necessariamente uma portadora deve ser dedicada para dados. O canal de dados possibilita o roteamento flexível e as vantagens de transmissões de baixo custo de uma rede baseada na transmissão de pacotes. O CDMA2000-1X EV-DO fornecerá velocidades de dados de até 2,4Mbps na mesma portadora.

A promessa da tecnologia CDMA 1X-EV é de fornecer 2,4Mbps em picos de dados, média de 600kbps com alta qualidade de voz e dados em tempo real com a mesma alocação de espectro de 1,25MHz.

3.3.2 GPRS

O **GPRS** é um novo serviço de valor agregado, não baseado em voz, que permite o envio e recepção de informações através de uma rede telefônica móvel.

Esse padrão de rede é uma evolução das redes GSM existentes que introduzem transmissão de dados por pacotes, permitindo que os terminais móveis operem em modo sempre conectados (*always on*). Essa estrutura de comunicação permite que os usuários possam sempre receber e-mail, manter-se acessando aplicações pela Internet e outros serviços.

O GPRS é considerado um meio de caminho do GSM até a terceira geração de redes de serviços móveis, que terá comutação de pacotes em conexão virtual permanente junto com as conexões de circuitos de circuito. O ETSI homologou esse sistema como a segunda fase da rede GSM. O modelo de roteamento e transporte de pacotes viabiliza a cobrança mensal por serviços e/ou volume de dados trafegados em vez de cobrança por tempo e distância geodésica.

Esse padrão viabiliza várias aplicações novas que não eram possíveis em redes GSM devido às limitadas velocidades na comunicações de dados, baseadas em comutação por circuito e modems, que permitiam atingir taxas de apenas 9,6kbps e suportavam apenas a troca de mensagens de pequenos cumprimentos.

Com o GPRS, os pacotes podem ser enviados e recebidos em taxas de até 115kbps. A máxima taxa teórica permitida no GPRS é de até 171,2kbps. É realizável com o uso de todos os oitos time slots do rádio canal ao mesmo tempo, sem qualquer proteção de erro no quadro GSM, para um único canal físico para transporte de diversos canais lógicos IP. Evoluindo para o sistema EDGE (*Enhanced Data for GSM Evolution*), que será abordado no item 3.3.2.1, essas taxas de dados poderão aumentar para até 384kbps.

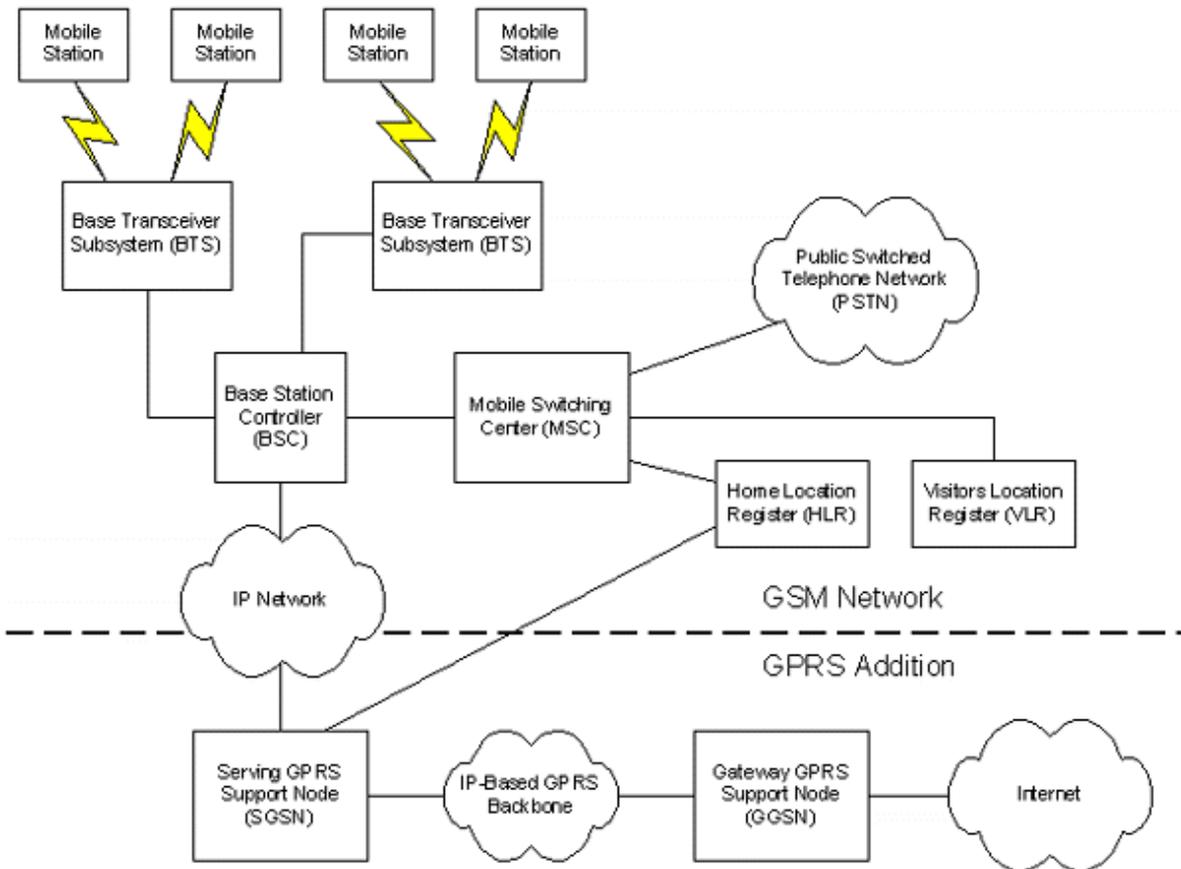


Figura 3.7. Arquitetura do sistema GSM/GPRS

A estrutura GPRS, figura 3.6, é implementada acrescentando nós de pacotes à rede GSM por meio de “gateways”, que permitem a interconexão dos roteadores GPRS com os comutadores CCC/GSM. O acesso via “gateway” permeia o *interworking* com acesso a aplicações Internet e Intranets. As características do sistema são:

- Prover acesso à Internet por meio de protocolos TCP/IP;
- Utilizar roteamento IP com rotas fixas ou dinâmicas;
- IP móvel utiliza pacotes de dados CDMA como padrão;

Como os protocolos em uso são os mesmos, as redes GPRS podem ser encaradas como sub-redes da Internet e os telefones GPRS compatíveis podem ser vistos como nós móveis dessa rede. Isso significa que cada terminal GPRS pode potencialmente ter seu próprio endereço IP e ser endereçável, provendo o acesso à Internet de várias maneiras como é descrito na figura 3.8 abaixo.

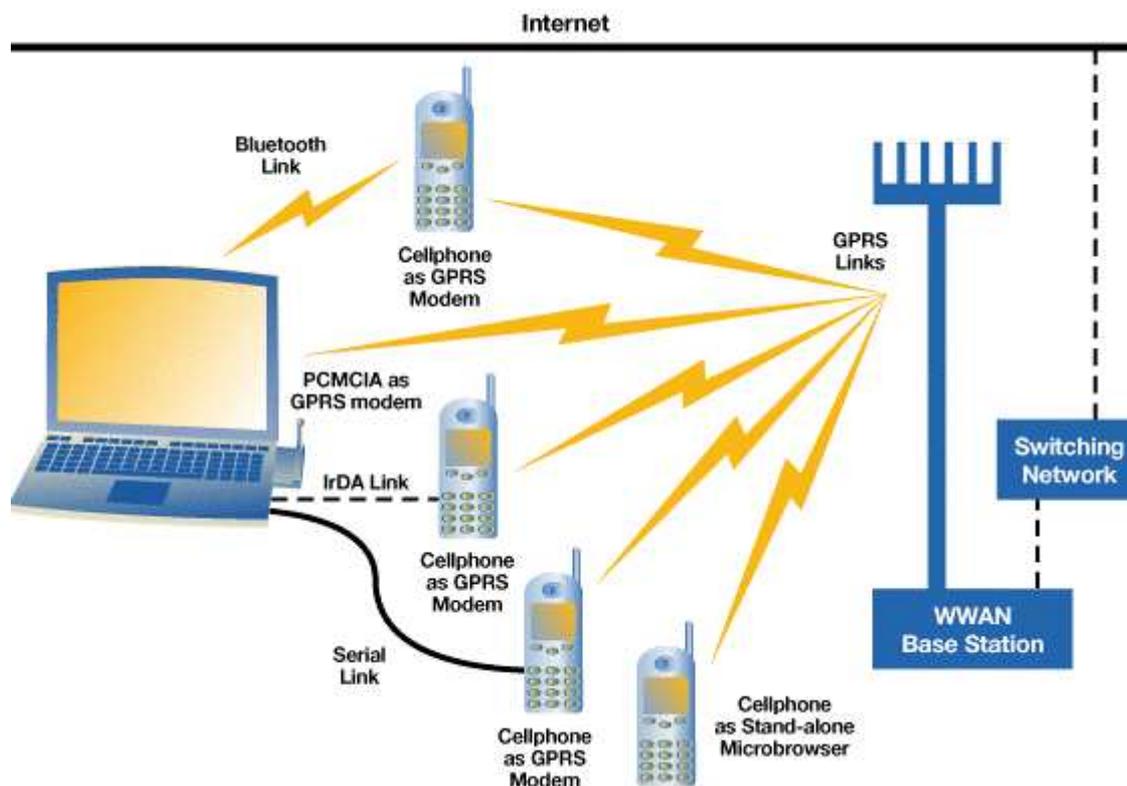


Figura 3.8 – Configurações diferentes da utilização do GPRS para o acesso à Internet.

O GPRS mantém a largura de faixa de canais GSM com os 200kHz atuais, 8 *timeslots* por quadro e taxa de símbolos de 270,833kHz. No caso da utilização da taxa de dados mais altas (permite uma taxa de bit bruta de 22,8kbps por *timeslot*), os dados são transportados em diversos canais, usando diversos *timeslots* com uma taxa final agregada. A taxa máxima teórica do GPRS é de 171,2kbps, usando todos os oito *timeslots* simultaneamente, sendo aproximadamente dez vezes mais rápida que os serviços atuais do CSD nas redes GSM.

Apesar dos melhoramentos na eficiência espectral, na capacidade e na funcionalidade se comparada com os serviços de dados oferecidos atualmente é importante notar algumas limitações como a limitação na capacidade da célula em prover serviço para todos os usuários por causa do compartilhamento dos rádios entre o sistema de dados GPRS e de voz GSM, a taxa de transmissão na prática é muito menor.

A primeira rede GSM/GPRS no Brasil foi ativada pela operadora Oi/Telemar em junho de 2002. A tecnologia inicialmente disponibilizada permite a transmissão de voz e dados a uma velocidade de até 64kbps. O assinante da telefonia móvel celular baseada

na tecnologia GSM/GPRS poderá escolher o seu provedor de telefonia de longa distância, diferente do que ocorre hoje no serviço móvel celular tradicional.

3.3.2.1 EDGE

O EDGE (*Enhanced Data for GSM Evolution*) representa a evolução final de comunicações de dados dentro do padrão de GSM. Esse esquema utiliza uma nova modulação disponível nas redes GSM, de forma a ampliar a taxa de transmissão para até 384kbps (teoricamente até 473kbps), praticamente aproveitando muito da infra-estrutura GSM atualmente existente.

O GPRS prevê a implementação de um novo Sistema de Estação Base (BSS), o que facilitaria a migração para o EDGE. Desta forma, para o EDGE será necessário a substituição da Unidade Transceptora EDGE (TRU), acrescida de atualizações de software. A adição de hardware de transceptores é comum ao ampliar a rede. A necessidade adicional será a instalação do TRU EDGE, em vez do TRU GSM no BSS, ao implementar o EDGE. As unidades transceptoras EDGE podem controlar simultaneamente voz comutada em circuitos e roteamento de pacotes GPRS.

O EDGE mantém o espaçamento de canais GSM de 200kHz existentes, 8 timeslots por quadro e taxa de símbolos de 270,833kHz. O que muda é a modulação no enlace de rádio comunicação, no modo GSMK a 8PSK. Essa modulação permite uma taxa bruta de bits de até 69,2kbps por timeslot.

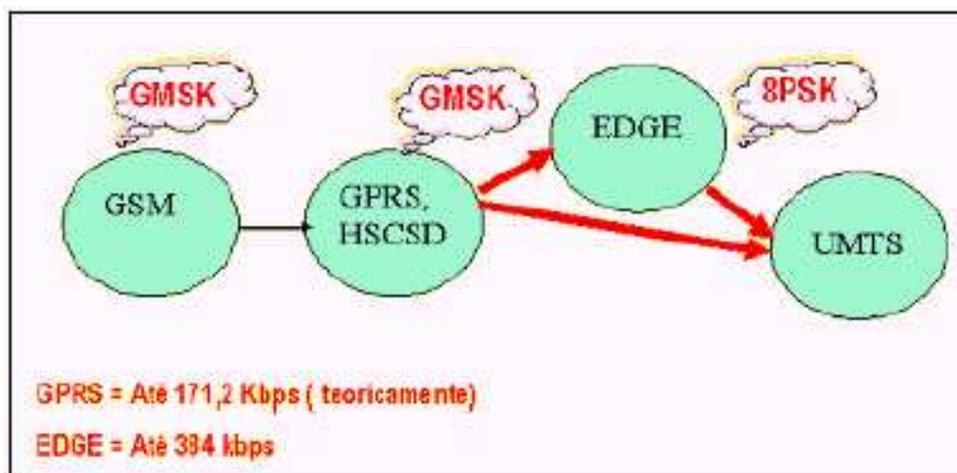


Figura 3.9 Caminhos para evolução de uma rede GSM

O 8PSK é usado para uma rotação de $3\pi/8$ entre símbolos (constelação 16PSK) com 3 bits por símbolo. Entre as suas desvantagens está uma redução na imunidade ao ruído, o que requer maiores níveis de potência.

Os provedores de serviços precisarão bloquear canais específicos para entrar no EDGE que não encaixa diretamente no sistema existente, mas exige uma reutilização das bandas na rede, níveis de potência e um novo cálculo do sistema de *link budget*.

O EDGE está baseado em um esquema de modulação na interface aérea usando o 8PSK que também é usado para o 3GSM (3ª geração do GSM). As operadoras de rede que incorporassem este sistema estariam a meio caminho para a transição definitiva para a terceira geração de sistemas móveis. Com EDGE a taxa de sinalização de dados na interface aérea poderia chegar a 59,2kbps.

3.4 CONCLUSÕES

Para aumentar a capacidade de tráfego dos sistemas de primeira geração, que havia atingido o limite de suas capacidades nos grandes centros urbanos, foram desenvolvidos os sistemas de segunda geração que continham várias funcionalidades que atendiam completamente às necessidades de comunicação de serviços de voz. Mas viu-se uma crescente necessidade de comunicações de dados por parte dos usuários, característica não detectada inicialmente quando estava se propondo os sistemas de segunda geração.

O esforço para suprir essa demanda de comunicação de dados é grande, esforço que originou várias tecnologias que dão sobrevivência aos sistemas de segunda geração e fez com que fossem propostos sistemas de terceira geração que tenham altas taxas de transmissão, segurança, acesso a Internet entre outros serviços demandados pelos usuários.

4 IP MÓVEL

4.1 INTRODUÇÃO

As Redes IP não são orientadas à conexão, ou seja não é estabelecido um caminho ou reserva de caminho entre origem e destino. As redes IP são redes baseadas em datagramas, cuja identificação é baseada em endereços de origem e destino.

As principais características das redes IP são:

- Baseadas em datagramas;
- Não oferecem segurança;
- Não garantem entrega dos datagramas e nem com a ordem em que esses datagramas serão entregues;
- Utilizam endereços para identificar origem e destino do datagrama.

O protocolo utilizado nessas redes é o protocolo IP que após os estudos que resultaram nas especificações do IPv6 passou a ser denominado IPv4.

O crescimento da população utilizando a Internet que vem crescendo a passos largos nos últimos anos fez a capacidade de endereçamento do IP chegar ao seu limite, as novas aplicações para Internet que necessitavam de novos serviços que o IPv4 não pode fornecer. Um exemplo é a transmissão de vídeo em tempo real é o comércio eletrônico que dentre as novas aplicações desenvolvidas para a Internet podemos destacar, necessita ter bons mecanismo de segurança e privacidade.

Atualmente essas necessidades estão se tornaram mais essenciais, assim como um novo mercado está se abrindo : a transmissão de dados via comunicação móvel celular a partir da Terceira Geração de Telefonia Móvel Celular.

4.2 EXEMPLO DA NECESSIDADE DO IP MÓVEL

Servidores e roteadores baseiam-se em informações contidas dentro do cabeçalho do pacote IP para decidir sobre o direcionamento de pacotes. Especificamente, decisões de roteamento são feitas baseadas no prefixo de rede do endereço IP de destino. Isto implica que todos os nós com interfaces em um dado enlace têm que ter o prefixo de rede idêntico aos de todos os endereços IP daquela interface. Para ilustrar esta necessidade, examinemos o que acontece se um nó, no qual seu prefixo de rede foi designado a um determinado link, for retirado deste link e ligado a

um novo, ao qual foi atribuído um prefixo de rede diferente. Esta situação é ilustrada na figura 4.1.

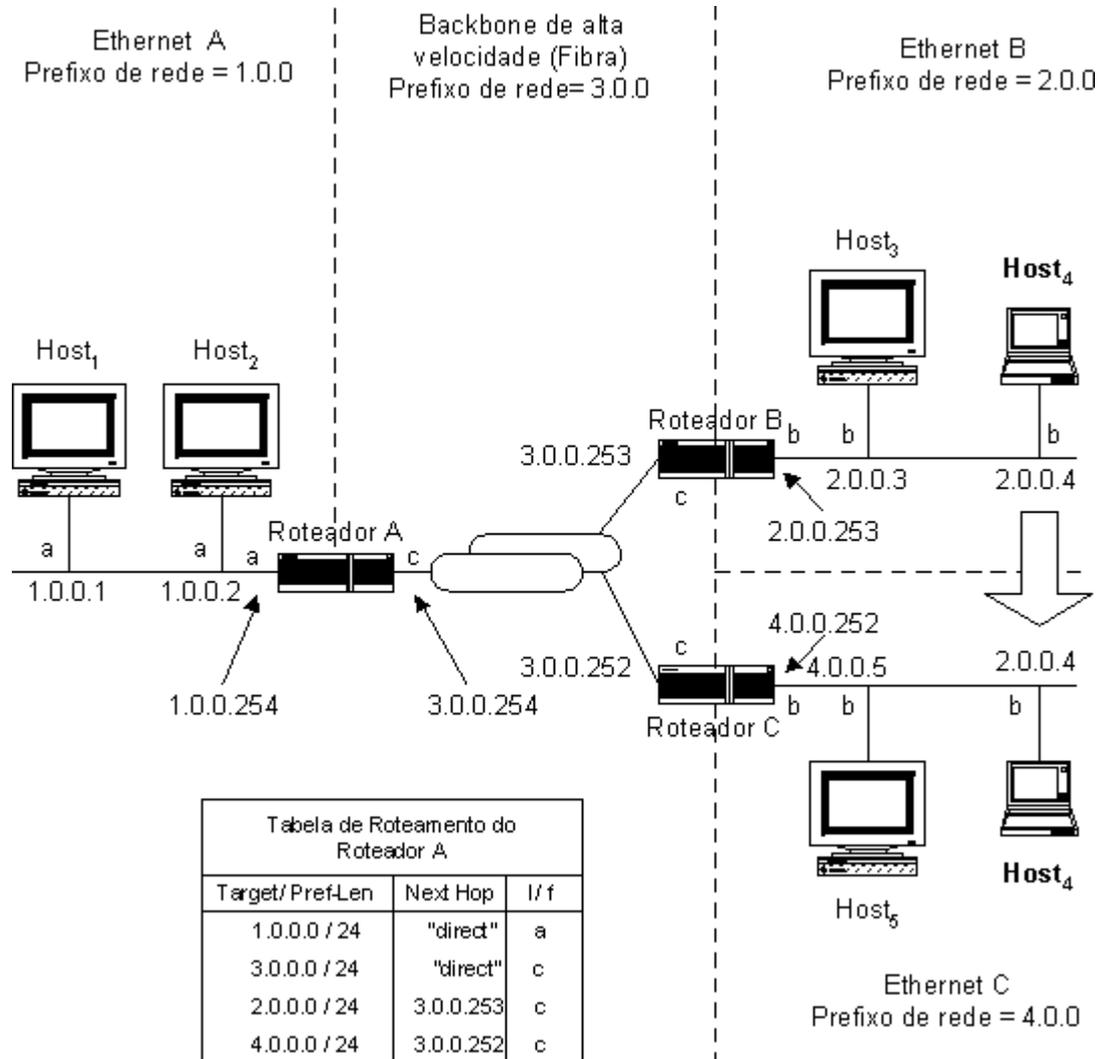


Figura 4.5 Movimento do Nó

Na figura 4.1, o endereço IP do Host₄ tem um prefixo de rede 2.0.0, mas o Host₄ é mostrado conectado num link no qual o prefixo de rede é 4.0.0. Também são mostradas na figura as entradas na tabela de roteamento do Roteador A. As duas primeiras entradas na tabela do Roteador A são para links nos quais o Roteador A está diretamente conectado. As duas últimas entradas são rotas para o prefixo de rede 2.0.0 (via Roteador B) e 4.0.0 (via Roteador C). Examinemos o que ocorre quando Host₁ tentar enviar pacotes para o Host₄:

- **Primeiro Passo-** O Host₁ gera um pacote IP no qual o endereço IP fonte é 1.0.0.1 e o endereço IP de destino é 2.0.0.4. A única compatibilidade na tabela de roteamento

do Host₁ para este destino é o Roteador padrão, o qual especifica o próximo salto para o Roteador A (1.0.0.254), via interface a. Portanto, o Host₁ direciona o pacote para o Roteador A.

- **Segundo Passo** - O Roteador A encontra uma entrada para alvos com prefixo de rede 2.0.0 na terceira coluna de sua tabela de roteamento, a qual especifica um próximo salto para o Roteador B (3.0.0.253), via interface c. Portanto, o Roteador A direciona o pacote para o Roteador B.
- **Terceiro Passo** - O Roteador B tem uma rota direta em sua tabela de roteamento para alvos com prefixo de rede igual a 2.0.0, então o Roteador B transmite o pacote via interface b no link Ethernet B. Entretanto, o pacote não poderá ser entregue, porque o Host₄ não está conectado na Ethernet B (onde supostamente ele deveria estar, baseado no seu prefixo de rede). O Roteador B então envia uma mensagem "ICMP Host Unreachable Error" para o host que originou o pacote (Host₁).

Neste exemplo, assumimos que as entradas da tabela de roteamento dos vários roteadores foram criadas por algum tipo de protocolo de roteamento dinâmico e o Roteador B deve ser necessariamente informado da acessibilidade do prefixo de rede 2.0.0. Note que o pacote do exemplo foi roteado em direção ao Roteador B simplesmente pelo fato dele ter sido informado pelo prefixo de rede (*Advertising Reachability*) do endereço IP do Host₄. Isto é uma importante regra do roteamento IP, pacotes IP destinados a um endereço específico serão roteados em direção ao Roteador ou Roteadores que possuem acessibilidade para os prefixos de rede destes endereços. Além do mais, se um nó não está localizado no link onde seu prefixo de rede diz que ele supostamente deveria estar localizado, pacotes enviados para este nó não poderão ser entregues ao mesmos. Como resultado, um nó não deve mover-se de um link para outro que ele deseja comunicar-se, sem no mínimo alterar o prefixo de rede de seu endereço IP para refletir seu novo ponto de conexão na rede.

4.3 O IPV6

O IPv6 tem como principal característica o espaço de endereçamento que é muito maior que o IPv4. Além disso, foram acrescentadas outras características para suprir as necessidades descritas anteriormente, da mesma forma que foi lhe dado robustez para atender as novas tendências de mercado. Conforme será mostrado adiante, uma nova necessidade surgiu quando o IPv6 já estava definido, fazendo com que um

novo protocolo fosse concebido: o IP Móvel. Esta mobilidade não está simplesmente relacionada com a mobilidade física do equipamento portador de um endereço IP.

O IPv6 trouxe consigo uma série de vantagens sobre o protocolo IP original, também chamado por IPv4:

- Espaço de endereçamento de 128 bits – estima-se que seja suficiente para os próximos 30 anos;
- Propõe uma redução na tabela de roteamento e por consequência uma maior rapidez na rede;
- Mecanismo para encapsulamento próprio e de outros protocolos;
- Simplificação do cabeçalho;
- Distinção de tipo de dado;
- Segurança de dados, incluindo criptografia de dados;
- Suporte para roteamento multicast de maneira mais eficiente e ainda a implementação do modelo anycast;
- Métodos de transição e compatibilidade com o IPv4;
- Mecanismo de autoconfiguração;
- Suporte para hosts móveis, incluindo comunicação via rádio;
- Permite que dados multimídia em tempo real trafeguem com mais eficiência.

4.3.1 Comparação entre IPv4 e IPv6

As diferenças entre o IPv4 e o IPv6 podem ser visualizadas a partir da composição dos seus datagramas na figura 4.2 abaixo.

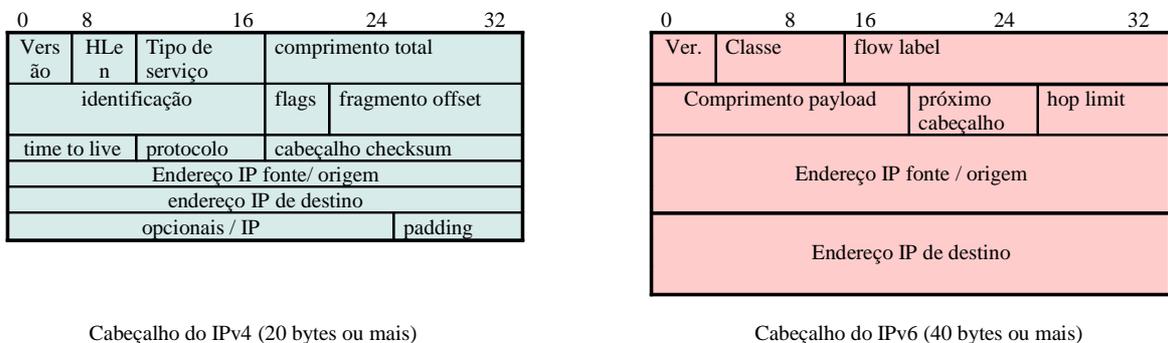


Figura 4.2 Comparação dos Cabeçalhos dos Ipv4 e Ipv6

Tabela 4.6 Comparação entre IPv4 e IPv6

	IPv6	IPv4
Espaço de endereçamento	128 bits	32 bits
Suporte para IP Móvel	Bom suporte para o IP Móvel	Suporte precário
Segurança	Oferece cabeçalhos para inserir segurança	Nenhuma Segurança
Autoconfiguração	Padrão da versão	Não existe

4.4 O IP MÓVEL

O principal objetivo do IP Móvel é fazer com que um host possa mudar de sub-rede sem que o usuário perceba essa mudança, conservando seu endereço IP original. Essas sub-redes podem não ser homogêneas, fazendo com que o protocolo tenha processos de reconhecimento de tecnologias diferentes. A transparência da transição de uma sub-rede para uma outra também se aplica às camadas superiores da camada do protocolo IP Móvel.

A base do funcionamento do protocolo IP Móvel vem de definição do IPv6 – em algumas referências das quais este trabalho foi extraído o IP Móvel é chamado por IPv6 Móvel – onde o endereço IP original do host é acessível através de um host intermediário denominado carrier-host. O IP Móvel deve fornecer meios para que o host móvel possa se comunicar com hosts que não suportam essa tecnologia.

A idéia de mobilidade também se aplica em hosts em movimento – como um laptop conectado a um celular – onde a comunicação é via ondas de rádio e que por consequência tem alta probabilidade de ocorrer erros na transmissão. Um outro fator a ser considerado é que equipamentos de comunicação móvel são movidos a bateria e, portanto o consumo de energia. Esse consumo de energia não é um problema a ser resolvido exclusivamente pelos fabricantes de equipamentos de comunicação móvel, mas também pelos desenvolvedores do protocolo.

4.4.1 Entidades envolvidas com o IP Móvel

A mobilidade no IP Móvel introduziu sete entidades:

- **Mobile Node (Nó Móvel)**– um nó ou host que faz parte de uma rede, mas que pode mudar de rede, mas continuar a pertencer a rede original;
- **Home Agent (Agente Local)**– um nó que representa a rede original do Agente Móvel. Este agente redireciona todos os datagramas endereçados ao Agente Móvel.
- **Foreign Agent (Agente Estrangeiro)**– um nó ou host que representa a rede onde o Agente Móvel está temporariamente alocado. Ele é o intermediador entre o Agente Móvel e o Agente de Origem.
- **Home Address** – é o seu endereço original e permanente que o identifica junto a sua rede de origem.
- **Local-link Address** – é um endereço com o qual os hosts da rede de origem podem se comunicar com o Agente Móvel sem o intermédio de roteadores.
- **Care-of Address** – é o endereço que é associado ao Nó Móvel, quando ele não se encontra em sua rede de origem.
- **Túnel** – é um caminho, o qual os pacotes endereçados ao host móvel deve ser encapsulado

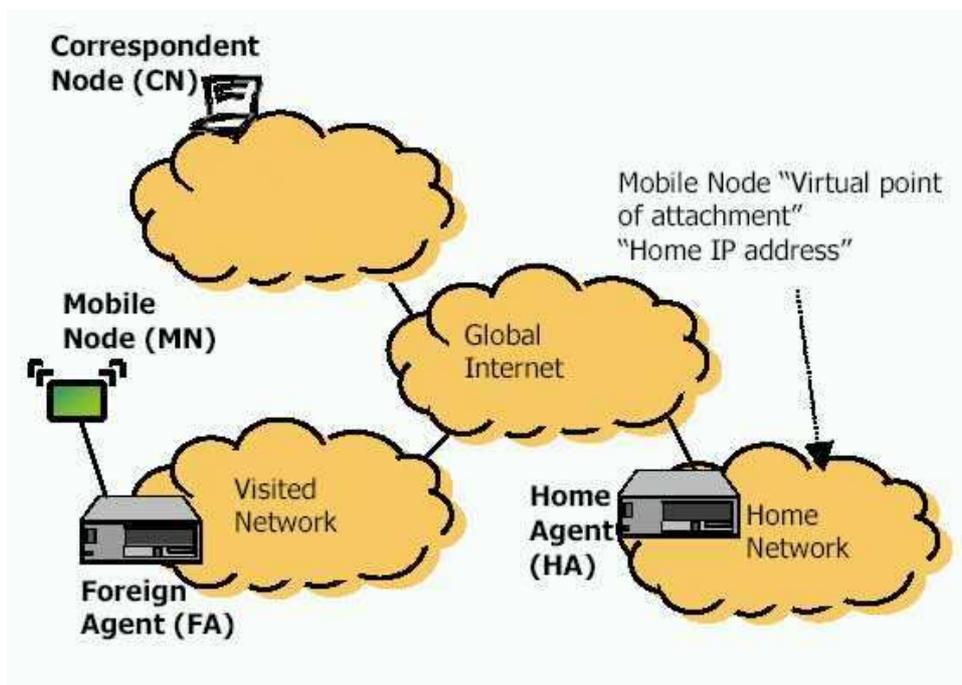


Figura 4.3 - Entidades envolvidas com o IP Móvel

4.4.2 O problema do roteamento IP frente à mobilidade

O roteamento de datagramas IP baseia-se em endereços de rede. Os dispositivos que realizam o encaminhamento são conhecidos por roteadores, ou na terminologia da Internet, por *gateways*. Um roteador IP não é mais do que um *host* que possui um endereço IP em mais do que uma rede. Com o software adequado pode assegurar a transferência de datagramas entre as várias redes nas quais possui endereço.

Geralmente um roteador possui mais do que uma interface física, assegurando a transferência de datagramas entre diferentes tecnologias de enlace. Também pode ligar duas redes baseadas em IP. Neste caso um roteador de ligação destas redes IP sobrepostas pode assegurar a sua interligação como uma única interface física possuidora de dois endereços IP.

Uma tabela de encaminhamento é um conjunto de associações (rede, caminho 1, caminho 2, ...). Cada associação regista várias rotas possíveis para atingir a rede indicada. Cada caminho é da forma (próximo *gateway*, métrica), indica qual o *gateway* seguinte para onde deve ser enviado o datagrama e qual a métrica associada a esse caminho. A métrica é uma medição da eficiência do caminho até ao destino, pode ser definida com base em vários critérios tais como:

- Atraso na Transmissão;
- Número de *Hosts* (nós intermédios);
- Capacidade das linhas;
- Preço da ligação

Tanto os *hosts* como os *gateways* implementam geralmente tabelas de encaminhamento. Estas tabelas de encaminhamento podem ser estáticas ou dinâmicas. Uma tabela estática é definida pelo administrador da rede, e sempre que se produzem alterações na topologia da rede as tabelas devem ser atualizadas manualmente.

As informações de encaminhamento podem ser trocadas entre *gateways* de modo a atualizar dinamicamente as tabelas. Para o efeito usam-se protocolos de roteamento. Os protocolos de roteamento usados nas redes terminais são conhecidos por IGP (*Interior Gateway Protocols*), sendo o mais comum o RIP (*Routing Information Protocol*). Os protocolos usados nas redes de trânsito são conhecidos por EGP (*Exterior Gateway Protocols*).

O IP faz o roteamento de pacotes de um ponto final fonte a um destino, permitindo que os roteadores façam seguir os pacotes de entrada para interfaces de rede de saída de acordo com as tabelas de roteamento. Estas tabelas tipicamente mantêm a

interface de saída para cada endereço IP destino, de acordo com o número de redes às quais o endereço IP está ligado. O número de rede é derivado a partir do endereço IP definindo os quatro últimos bits iguais a zero. Assim, o endereço IP leva consigo informação que especifica o nó IP de conexão.

Para manter as atuais conexões da camada de transporte à medida que o nó móvel viaja de um ponto para outro, ele tem de manter o seu endereço IP. No TCP (o protocolo usado na maioria das conexões à Internet), as conexões são indexadas pelo conjunto (IP Fonte; Porta Fonte; IP Destino; Porta Destino). Alterando qualquer um destes quatro números fará com a que a conexão seja interrompida e perdida. Por outro lado, a entrega correta de pacotes ao ponto atual de conexão do nó móvel depende do número da rede contido no endereço IP do nó móvel, que se altera em cada novo ponto de conexão. Para mudar o roteamento é necessário um novo endereço IP associado ao novo ponto de conexão.

4.4.3 A solução apresentada pelo IP Móvel

O IP Móvel foi desenvolvido para resolver o problema do roteamento IP permitindo que o nó móvel tenha dois endereços. No IP Móvel, o *home address* (endereço local) é estático e é usado, por exemplo, para identificar conexões TCP. O *care-of-address* muda a cada novo ponto de conexão e pode ser visto como o endereço topológico do nó móvel; ele indica o número de rede e assim indica o ponto de conexão do nó móvel com respeito à topologia de rede.

O *home address* faz parecer que o nó móvel está continuamente disponível para receber dados na sua rede local, onde o IP Móvel requer a existência de um nó de rede conhecido como *home agent* (agente local). Sempre que o nó móvel não está ligado à sua rede local (estando portanto ligado ao que se designa por *foreign network*), o *home agent* recebe todos os pacotes destinados ao nó móvel e encontra uma maneira de os entregar no ponto atual de conexão do nó móvel.

Sempre que o nó móvel se muda para outra localização, registra o seu novo *care-of-address* no seu *home agent*. Para entregar um pacote a um nó móvel da sua rede local, o *home agent* envia o pacote da sua rede local para o *care-of-address*. Esta entrega requer que o pacote seja modificado para que o *care-of-address* apareça como o endereço IP destino. Esta modificação pode ser entendida como um redirecionamento.

Quando o pacote chega ao *care-of-address*, a transformação inversa é efetuada para que o pacote, uma vez mais, apareça com o endereço local como endereço IP destino. Quando o pacote chega ao nó móvel, endereçado ao endereço local, é processado corretamente pelo TCP ou outro qualquer protocolo de transporte, que o receba da camada IP do nó móvel.

No IP Móvel o *home agent* redireciona os pacotes da rede local para o *care-of-address* construindo um novo cabeçalho IP que contém o *care-of-address* do nó móvel como endereço IP destino, como vemos na figura 4.4. O novo cabeçalho encapsula o pacote original, fazendo com que o endereço local do nó móvel não tenha qualquer efeito no direcionamento do pacote encapsulado até ele chegar ao *care-of-address*. Tal encapsulamento também é designado por tunelamento, o que sugere que o pacote viaja pela Internet, passando por cima dos efeitos normais do roteamento IP.

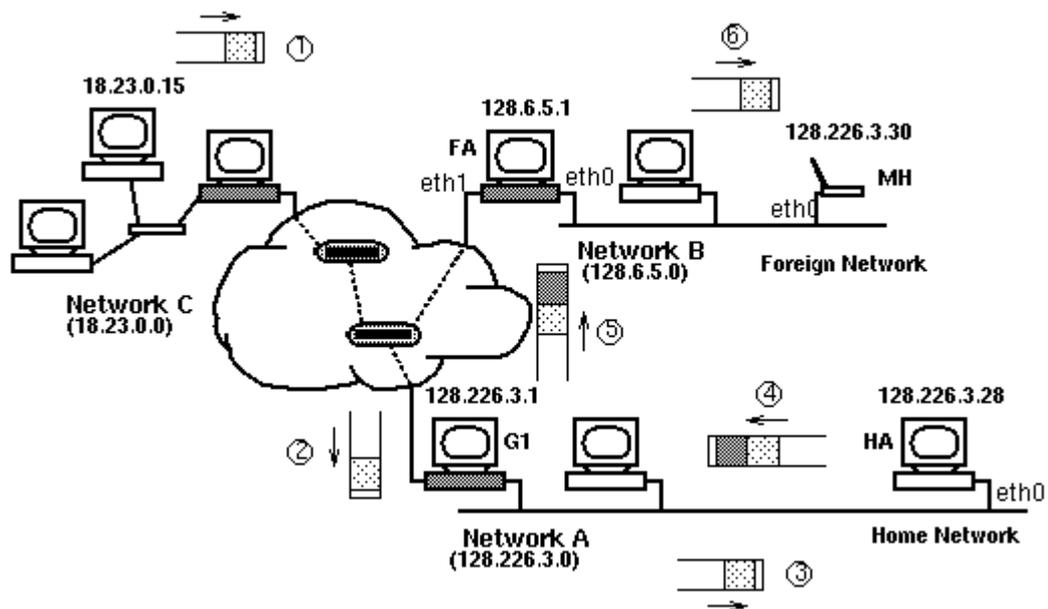


Figura 4.4 – Roteamento no IP Móvel

O IP Móvel é portanto a cooperação de três mecanismos separados:

- Descobrir o *care-of-address*;
- Registrar o *care-of-address*;
- Estabelecer um túnel até ao *care-of-address*.

4.4.3.1 Descobrir o *care-of-address*

Os *home agents* e *foreign agents* emitem em *broadcast* anúncios de agentes (anúncios que contêm *care-of-addresses*) a intervalos regulares (por exemplo uma vez por segundo ou uma vez cada três segundos). Se, no entanto, um nó móvel precisa de obter um *care-of-address* e não quer esperar por um destes anúncios periódicos, pode então emitir em *broadcast* ou *multicast* uma solicitação que será respondida por algum *foreign agent* ou *home agent* que a receber.

Os *home agents* usam anúncios de agentes para se tornarem conhecidos, mesmo que não ofereçam nenhum *care-of-address*. Assim, um anúncio de agente efetua as seguintes funções:

- Permite a detecção de agentes móveis;
- Lista um ou mais *care-of-addresses* disponíveis;
- Informa o nó móvel sobre capacidades especiais disponibilizadas por *foreign agents*, por exemplo, técnicas alternativas de encapsulamento;
- Permite aos nós móveis determinar o endereço de rede e estado das suas ligações à Internet;
- Permite aos nós móveis saber se o agente é uma *home agent*, *foreign agent* ou ambos e se portanto está na sua rede local ou numa exterior.

Os nós móveis usam as solicitações do roteador para detectar alguma alteração no conjunto de agentes móveis disponíveis no ponto atual de conexão. (No IP Móvel isto é designado por *agent solicitation* – solicitação de agentes). Se os anúncios não são mais detectados por um *foreign agent* que previamente tinha oferecido um θ ao nó móvel, o nó móvel deve presumir que o *foreign agent* não se encontra mais no raio de ação da interface de rede do nó móvel. Nesta situação, o nó móvel deve começar a procurar um novo *care-of-address*, ou possivelmente usar um *care-of-address* conhecido pelos anúncios que ainda esteja a receber. O nó móvel pode escolher ficar à espera de um outro anúncio se não recebeu recentemente nenhum *care-of-address* anunciado, ou enviar uma solicitação de agentes.

4.4.3.1.1 Descoberta automática do *home agent*

Quando o nó móvel não consegue contactar o seu *home agent* o IP Móvel tem um mecanismo que deixa o nó móvel tentar registrar-se com outro *home agent* desconhecido na sua rede local. Este método de descoberta automática do *home agent* é

conseguido usando um endereço IP de *broadcast* em vez do endereço IP do *home agent* como destino do pedido de registro. Quando o pacote de *broadcast* chega à rede local, outros *home agents* da rede irão enviar uma mensagem de rejeição ao nó móvel. No entanto, os seus avisos de rejeição contêm os seus endereços para o nó móvel os usar numa nova tentativa de registro. Note-se que este *broadcast* não é um *broadcast* na Internet, mas um *broadcast* direcionado que chega apenas a nós IP da rede local.

4.4.3.2 Registrar o *care-of-address*

O nó móvel registra o seu *care-of-address* no seu *home agent* de forma a obter serviços. O processo de registo pode ser processado diretamente pelo nó móvel ou facultado pelo *foreign agent* até ao *home agent*, dependendo se o *care-of-address* foi dinamicamente atribuído ou associado ao seu *foreign agent*. Note-se que registos simultâneos com múltiplos *care-of-addresses* são possíveis, como visto na figura 4.5 abaixo.

Uma vez que um nó móvel tenha o seu *care-of-address* o seu *home agent* deve ser informado. O processo de registo começa quando o nó móvel, possivelmente com a ajuda de um *foreign agent*, envia um pedido de registro com a informação do *care-of-address*. Quando o *home agent* recebe este pedido, ele, geralmente, adiciona a informação necessária à sua tabela de roteamento, aprova o pedido e envia uma resposta a este pedido ao nó móvel. Apesar de no protocolo IP Móvel, não ser necessário que o *home agent* trate os pedidos de registro atualizando as entradas na sua tabela de roteamento, ao fazê-lo oferece uma natural estratégia de implementação.

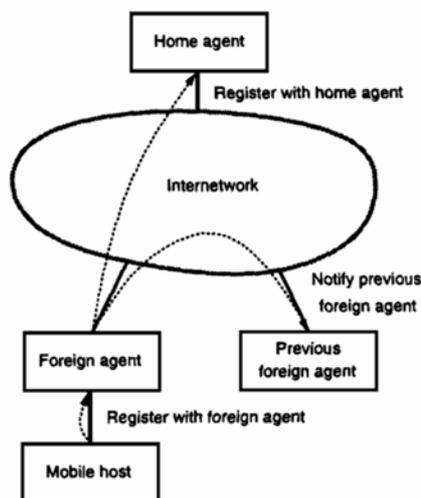


Figura 4.5 – Registros: Agentes Local e Estrangeiro

4.4.3.2.1 Autenticação

A necessidade de autenticar a informação do registra desempenhou um papel fundamental na especificação do IP Móvel. Cada nó móvel e o *home agent* têm de partilhar uma associação de segurança e serem capazes de usar Message Digest 5 (RFC 1321) com chaves de 128 bits para criar assinaturas digitais impossíveis de falsificar nos pedidos de registo. A assinatura é calculada aplicando o algoritmo hash do MD5 a todos os dados do cabeçalho da mensagem e às extensões que precedem a assinatura.

Para assegurar o pedido de registo, cada pedido deve conter informação unívoca para que na prática dois diferentes pedidos de registo não tenham o mesmo hash MD5. Se assim não fosse, o protocolo estaria sujeito a ataques por resposta, nos quais nós maliciosos poderiam guardar registos válidos para respostas posteriores, destruindo a possibilidade do *home agent* estabelecer posteriormente um túnel com o *care-of-address* do nó móvel. Para assegurar que isto não acontece o IP Móvel inclui na mensagem de registo um campo especial de identificação que muda em cada novo registo. A semântica exata do campo de identificação depende de vários parâmetros, que estão descritos com grande detalhe na especificação do protocolo. Grosso modo, existem duas formas principais de tornar o campo de identificação único:

- Usar um selo temporal: Assim cada novo registo terá um selo temporal posterior diferindo assim de registos anteriores.
- Usar um número pseudo aleatório: Usando bits suficientes é muito improvável que dois valores independentes escolhidos para o campo de identificação sejam iguais. Quando este método é usado, o IP Móvel define um método que protege tanto o pedido de registo como a resposta de se repetirem e usa 32 bits aleatórios no campo de identificação.

Se o nó móvel e o *home agent* se afastarem demasiadamente na sincronização no uso de selos temporais ou se perderem o rastro aos números aleatórios esperados, o *home agent* rejeita os o pedido de registo e inclui informação que permita uma nova sincronização dentro da resposta.

O campo de identificação também é usado pelo *foreign agent* para fazer corresponder pedidos de registo pendentes às respostas aos registos quando estes chegam ao *home agent* e para subsequente ser capaz de fazer chegar a resposta ao nó móvel. O *foreign agent* também guarda outra informação para os pedidos pendentes, incluindo o *home address* do nó móvel, o endereço MAC do nó móvel, o número do

porto fonte para o pedido de registro do nó móvel, o tempo de vida do registro proposto pelo nó móvel e o endereço do *home agent*.

O *foreign agent* pode limitar os tempos de vida dos registros a um valor configurável que ele põe nos seus anúncios de agente. O *home agent* pode reduzir o tempo de vida do registro, que ele inclui como uma parte da resposta ao pedido, mas nunca o pode aumentar.

No IP Móvel os *foreign agents* são sobretudo passivos, entregando pedidos de registro e respostas para a frente e para trás entre o *home agent* e o nó móvel, fazendo essencialmente o que lhe dizem para fazer. O *foreign agent* também desencapsula o tráfego vindo do *home agent* e envia-o ao nó móvel. Note-se que os *foreign agents* não têm de se autenticar perante o nó móvel ou o *home agent*. Um *foreign agent* fictício pode-se fazer passar por um *foreign agent* verdadeiro simplesmente seguindo o protocolo e oferecendo anúncios de agente ao nó móvel. O agente fictício pode, por exemplo, então recusar-se a fazer seguir os pacotes desencapsulados para o nó móvel quando os recebe. No entanto, o resultado não é pior do que se algum nó fosse levado a usar o roteador errado, o que é possível usando anúncios de roteamento não autenticados.

4.4.3.2 Em serviço

Este é o período depois do processo de registro e antes do tempo de vida do serviço expirar, desde que o nó móvel permaneça na área de serviço. Durante este tempo de serviço o nó móvel recebe os pacotes enviados pelo *foreign agent* que foram originalmente enviados pelo *home agent* do nó móvel. O tunelamento é o método usado para fazer seguir a mensagem do *home agent* para o *foreign agent* e finalmente para o nó móvel.

4.4.3.2.3 Anular o registro

Depois do nó móvel retornar à sua rede local, ele anula o registro no seu *home agent* para libertar o seu *care-of-address* registrado. Em outras palavras, ele configura o seu *care-of-address* de volta ao seu *home address*. O nó móvel consegue efetuar esta operação enviando um pedido de registro diretamente ao seu *home agent* com o tempo de vida definido a zero. Não existe a necessidade de anular o registro no *foreign agent* porque o serviço expira automaticamente quando o tempo de vida do serviço terminar.

4.4.3.3 Estabelecer um túnel até ao care-of-address

O mecanismo de encapsulamento por defeito que tem de ser suportado por todos os agentes móveis que usam IP Móvel é o *IP-within-IP*. Ao usar *IP-within-IP* o *home agent*, o início do túnel, insere um novo cabeçalho IP à frente do cabeçalho IP de qualquer datagrama endereçado ao *home address* do nó móvel. O novo cabeçalho do túnel usa o *care-of-address* do nó móvel como endereço IP destino, ou destino do túnel. O endereço IP do início do túnel é o *home agent* e o cabeçalho do túnel usa o número do nível mais alto do protocolo (número 4), indicando que o próximo cabeçalho é novamente um cabeçalho IP. No *IP-within-IP* o cabeçalho original IP é preservado como a primeira parte dos dados a ler do cabeçalho do túnel. Portanto, para recuperar o pacote original o *foreign agent* apenas tem de eliminar o cabeçalho do túnel e entregar o resto ao nó móvel.

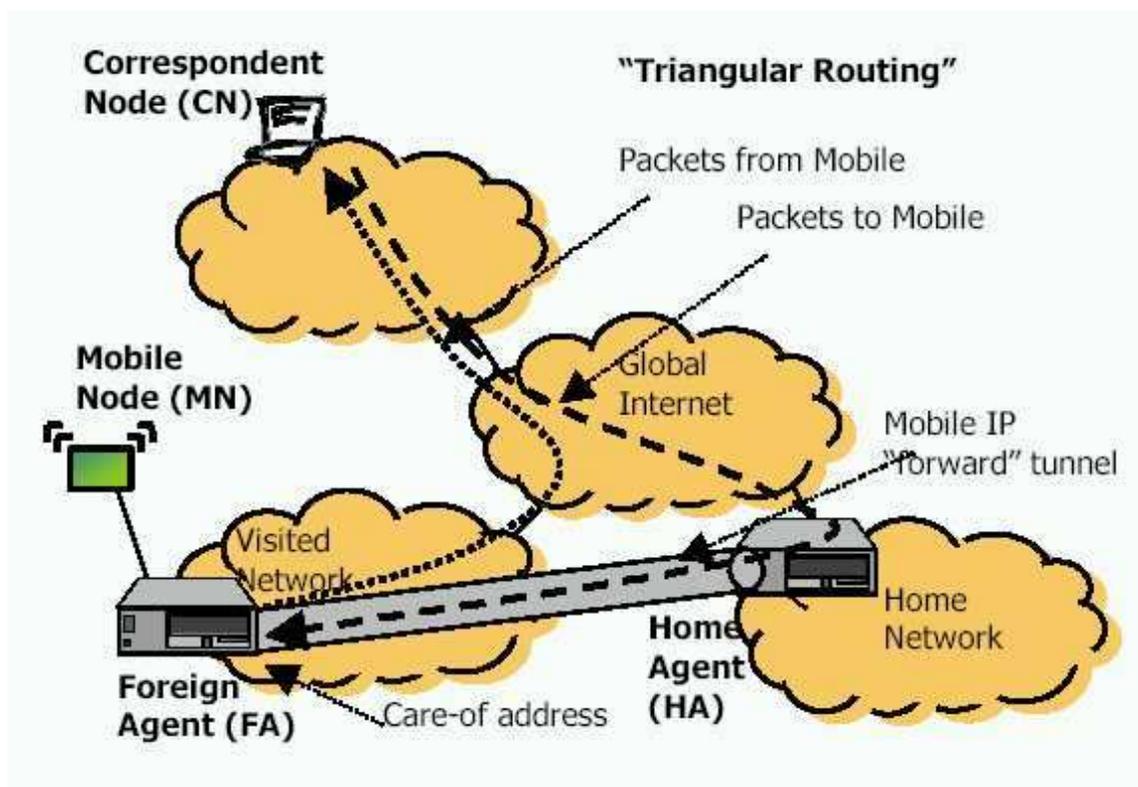


Figura 4.6 – Estabelecendo um túnel até o *care-of-address*

Por vezes o cabeçalho do túnel usa o número 55 no cabeçalho interior. Isto acontece quando o *home agent* usa encapsulamento mínimo em vez do *IP-within-IP*. O processamento no cabeçalho do encapsulamento mínimo é ligeiramente mais complicado do que o processamento no *IP-within-IP*, porque alguma da informação do

cabeçalho do túnel está combinada com informação no cabeçalho de encapsulamento mínimo para reconstituir o cabeçalho IP original. Por outro lado, o *overhead* no cabeçalho é reduzido.

4.5 CONCLUSÕES

Desenvolvido para suprir as necessidades que surgiram como maior capacidade de endereçamento e mobilidade, o IP Móvel ainda não está consolidado. Ainda existem algumas questões abertas que ainda necessitam de pesquisas para se obter eficiência deste protocolo.

Uma das questões é a segurança. Os *firewalls*, em particular, causam dificuldades ao IP Móvel porque bloqueiam todos os tipos de pacotes de entrada que não estejam de acordo com determinados critérios. Os *firewalls* estão tipicamente configurados para bloquear pacotes de entrar via Internet que parecem provir de computadores internos. Apesar disto permitir a gestão de nós internos com acesso à Internet sem grandes atenções com a segurança, apresenta dificuldades aos nós móveis que pretendam comunicar com outros nós dentro das suas redes locais. Tais comunicações, originárias do nó móvel, levam o *home address* do nó móvel, sendo assim bloqueados pelo *firewall*.

Como vimos anteriormente, a forma de encapsular datagramas consiste em pôr o datagrama original (= cabeçalho IP + dados) dentro de outro envelope IP, obtendo assim o pacote a enviar (= cabeçalho IP exterior (*care-of-address*) + datagrama original). Os campos do cabeçalho IP exterior adicionam muito *overhead* ao datagrama final – vários campos são duplicados do cabeçalho IP interior. Este desperdício de espaço não é desejável. Apesar de um modelo com um único *home agent* ser simples e de fácil configuração, tem a desvantagem da fragilidade. O nó móvel some quando o *home agent* falhar.

Enfim, mesmo com todos problemas apontados estarem sendo resolvidos ainda, o IP Móvel já foi capaz de dar suporte para que propostas como a interoperabilidade entre WLANs e o Sistema Móvel Celular, obtivessem êxito em seus testes, ou seja, neste tipo de solução o IP Móvel tornou-se a peça chave para o sucesso.

5 INTEROPERABILIDADE: CELULAR & WLAN

5.1 INTRODUÇÃO

Os novos sistemas de comunicações móveis que passaram a ser conhecidos como de terceira geração, ou simplesmente “3G”, prometem oferecer aos usuários serviços avançados de multimídia e acesso à Internet em alta velocidade.

Os sistemas 3G visam a evolução em direção aos serviços de telecomunicações móveis universais, o chamado UMTS. O objetivo do UMTS é prover um padrão universal para as comunicações pessoais, provendo qualidade de serviços. Uma das premissas do UMTS é permitir o uso de diversos meios complementando-se mutuamente, de modo a permitir uma rede multimídia móvel mundial. Então teremos acessos via redes celulares terrestres e via satélites de baixa órbita. O UMTS deve suportar facilidades como as seguintes:

- Portadoras que podem ser alocadas novamente, banda atribuível sob demanda, como, por exemplo, 2Mbps para comunicações em ambientes internos e pelo menos 144kbps para ambientes externos.
- Variedade de tipo de tráfego compartilhando o mesmo meio.
- Tarifa cobrada por serviços e/ou volumes, que é uma forma mais adequada para aplicações do tipo multimídia.
- Serviços pessoais.
- Facilidade de implementação de novos serviços devido ao uso de ferramentas padronizadas para o desenvolvimento de aplicações, e pelo uso de software na rede e sinalização e estruturas de rede inteligente.

Com o atraso da chegada da terceira geração de telefonia celular (3G), as WLANs tornam-se uma solução atraente para as empresas que desejam satisfazer os usuários que desejam acesso móvel e rápido à Internet. Entretanto, é um erro enxergar essas duas tecnologias como rivais ou ameaça à outra. Na verdade, elas são vistas cada vez mais como complementares.

A WLAN é ideal para pequenos ambientes. Sua velocidade de até 11 Mbps (*Wi-Fi* / 802.11b) é muito maior que os cerca de 2 Mbps prometidos para a 3G. Todavia, nunca as redes WLAN terão uma cobertura similar àquela das operadoras celulares,

tipicamente nacional na maioria dos países. Desta forma, a proposta da interoperabilidade entre as duas tecnologias é unir o melhor de cada mundo.

A idéia é que os usuários de acesso móvel à Internet possam usar cartões PCMCIA híbridos. Quando estiverem com seus *laptops* na rua, a conexão será feita via rede celular. Ao adentrarem um ambiente coberto por um ponto de acesso, a conexão automaticamente passará a ser feita via WLAN. Desta forma, os usuários poderiam estar conectados da melhor maneira ao moverem-se de um lugar para outro, como por exemplo da sua casa para o trabalho ou um lugar público que tenha uma *hot-spot*.

Por exemplo, um empresário poderia estar trabalhando em seu *laptop* em um centro para conferências onde a cobertura é feita por uma WLAN. Quando estivesse em um táxi a caminho do aeroporto poderia ainda permanecer com a sua conexão de dados, enviando ou recebendo *e-mails*, saindo da cobertura da WLAN para a cobertura da rede celular. Ao chegar ao aeroporto, poderia retornar à cobertura de uma outra WLAN e fazer uso do serviço com velocidade de conexão maior.

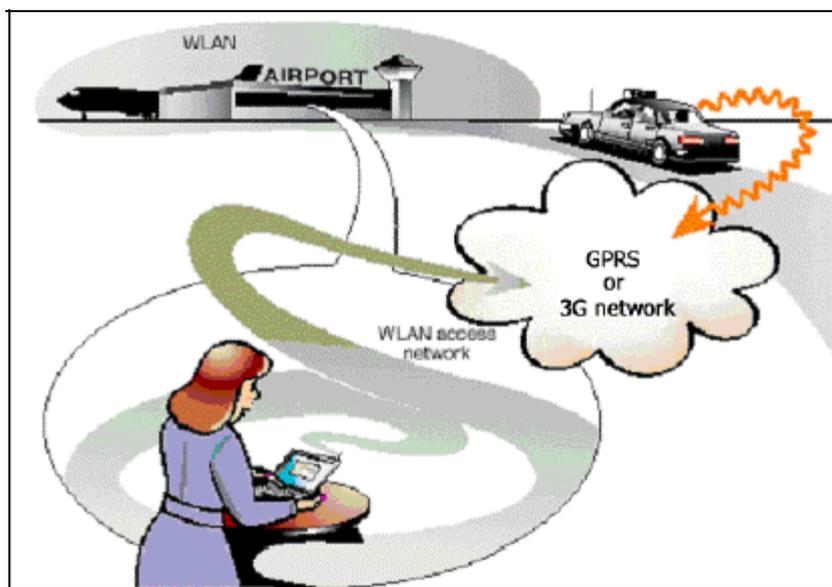


Figura 5.7 Interoperabilidade: WLAN (Hot-spot) e Celular (2,5G ou 3G)

A soma dessa nova capacidade na prestação de serviços de dados é maior do que as tecnologias isoladas. Com a mobilidade e interoperabilidade entre os sistemas, muitos usuários passariam a se acostumar mais a utilizar os serviços de acesso de dados e o tráfego iria ter um aumento considerável em ambos os sistemas.

Desta forma, acredita-se que as WLAN seriam um complemento das futuras redes móveis celular como a tão esperada 3G, e não uma ameaça. A rede celular é

imensamente maior que qualquer rede WLAN, mas a velocidade de transmissão é muito menor.

Portanto, o objetivo da interoperabilidade é permitir que os usuários de dados que utilizam o serviço móvel celular usem a rede celular nas ruas e a WLANs quando entrarem em um *hot spot* sem perder a conectividade. Desta forma poderiam mover-se livremente de uma rede para outra sem ter que reconectar e mudar todas as configurações antes estabelecidas.

5.2 A SOLUÇÃO PARA INTEROPERABILIDADE

Redes como a GPRS, o CDMA1X e as WLANs são redes sem fio de serviço de dados que estão começando a serem implementadas por todo mundo, bem como no Brasil. Os *Laptops* e os PDAs com múltiplas interfaces de acesso estão tomando cada vez mais espaço no mercado, permitindo que as pessoas têm acesso a todas essas redes. Os usuários, todavia, ainda têm que reconectar e mudar todas as suas configurações manualmente quando movem-se de uma rede de um tipo para outra, freqüentemente resultando reinicialização de seus terminais móveis.

O sucesso da proposta da interoperabilidade das WLANs e as redes celulares está intimamente relacionado a um padrão chave chamado IP Móvel, abordado anteriormente neste trabalho.

O IP Móvel é um padrão aberto, definido pelo IETF, que permite que os usuários de dados permanecerem com o mesmo endereço IP, não percam a conexão e mantenham as suas configurações antes estabelecidas automaticamente, enquanto estão fazendo roaming entre duas redes baseadas em IP, como exemplo entre redes celulares 2,5G/ 3G e as WLANs.

5.3 EXEMPLO DE SISTEMA IMPLEMENTADO

A implementação desse tipo de interoperabilidade entre redes celulares 2,5G/3G e WLANs estão sendo desenvolvidas e testadas por laboratórios e fabricantes interessadas nesse novo mercado. Alguns testes estão unindo grandes e pequenos fornecedores de equipamentos e software em todo mundo. Algumas dessas propostas

obtiveram sucesso e foram disponibilizadas e publicadas em artigos da área. Descreveremos uma solução a fim de exemplificar tipos desses sistemas.

5.3.1 A Arquitetura do sistema com interoperabilidade

Será descrito a solução proposta pela ipUnplugged que é uma empresa que fornece os componentes necessários para a solução. Neste caso, a solução para a interoperabilidade consiste em três componentes que juntos formam a solução adequada baseada no IP Móvel. São eles:

- *Roaming Gateway;*
- *Roaming Server;*
- *Roaming Client software.*

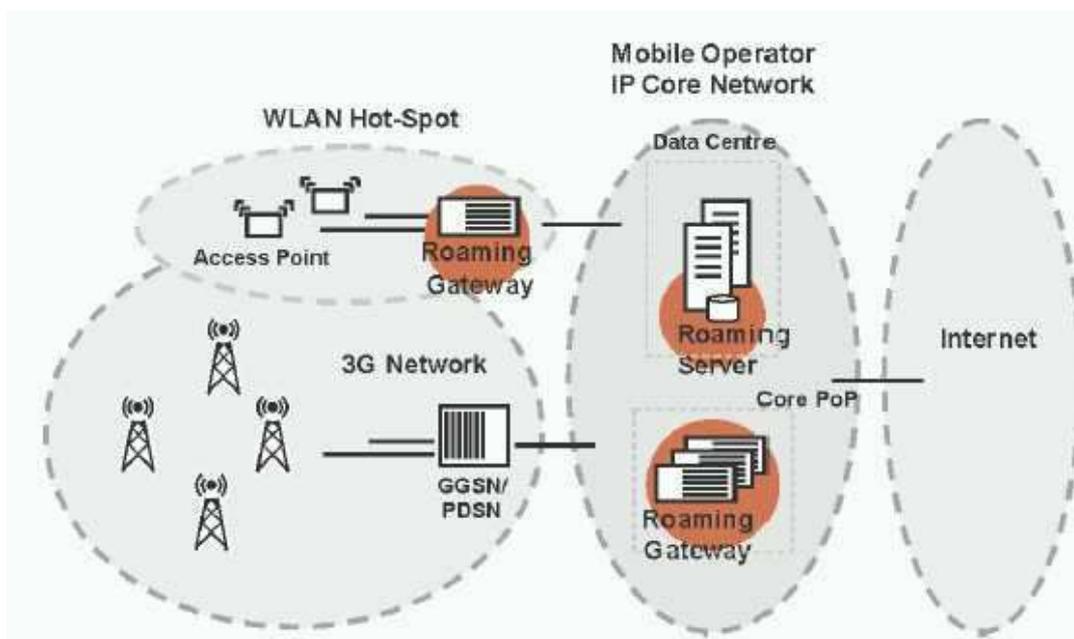


Figura -5.8 - Arquitetura de um sistema com interoperabilidade

- *Roaming Gateway*

Esse componente é um hardware (gateway) preparado para possibilitar o acesso dos usuários a Internet, conectando os *access points* a Internet, controlando-os e lidando com aplicações de acessos restritos. Ele dá suporte a mobilidade dos usuários, contendo funcionalidades capazes de lidar com mobilidade através de vários pontos de acessos e de vários meios de acessos. Ele tem especialidades seguras para prover conectividade

VPN entre sites e filtrar os pedidos de serviços por usuários individualmente baseado em arquivos de serviço. O Roaming Gateway ainda pode suportar conexões de servidores de AAA (Cobrança, Autenticação e Autorização). Ele também provê as configurações básicas do IP para o acesso do usuário, via DHCP.

- Roaming Server

Este componente é um servidor configurado para controlar o sistema com as funcionalidades completas de AAA para prover o roaming em acessos múltiplos das redes. Ele pode mapear facilmente o usuário pelos arquivos de serviços pelas complexas regras dos *firewall* e distribuir estas requisições pelas entidades de redes. Ele foi projetado para proporcionar uma ferramenta robusta e poderosa e de manuseio amigável para configuração de redes, controle de segurança. A arquitetura do Roaming Server reflete a necessidade para cumprir os requisitos de robustez, confiabilidade e custo benefício.

- Roaming Client

Este componente é um software controlador (*device driver*) que faz com que o terminal, por exemplo um *laptop*, esteja informado quanto às suas possibilidades em relação à mobilidade através das redes celular e WLAN. Por isso tem por finalidade ajudar no provimento do roaming transparente sem a intervenção do usuário entre uma rede celular e uma WLAN.

Este software também tem por objetivo livrar o usuário das configurações embaraçosas caso tivesse que reconectar em caso de perda de conexão no roaming através das redes. Ele faz o download dos dados de configuração num formato criptografado do Roaming Server.

O Roaming Client em ação:

Supomos duas situações diferentes:

- **Primeira situação:** O usuário está em sua rede de origem (*home network*), não necessitando o uso de um *care-of-address*, ele está utilizando somente o seu IP próprio e todas as suas facilidades. Após algum tempo ele começa a se mover de forma a passar para outra rede (*foreign network*), fazendo-se necessário agora o uso de um *care-of-address* para que ele possa continuar a receber seus dados sem perda

e continuar fazendo uso de suas facilidades. Para isso é necessário que seu Agente local (*home agent*) saiba qual rede esse usuário está localizado, saiba para onde direcionar os pacotes de dados endereçados a ele e o agente estrangeiro (*foreign agent*) saiba que esse usuário esteja em sua rede. Tudo isso se dá quando é definido o *care-of-address* do nó móvel.

- **Segunda situação:** usuário está em uma rede estrangeira (*foreign network*) e passa para uma outra rede (*foreign network*), necessita-se da mesma forma que seu Agente Local esteja informado de seu novo *care-of-address*.

Nos dois processos, os papéis de descobrir o *care-of-address*, registrar o *care-of-address*, autenticar é feito pelo *software Roaming Client*, que efetua esse processo de forma suave e transparente em relação aos usuários. O Mobile IP fornece todas as ferramentas que a mobilidade requisita e garante que não haja perda nenhuma nesse processo. O *Home Gateway* atua tanto como agente local como agente estrangeiro. Toda a autenticação, autorização e cobrança é feita pelo *Home Server*.

Notamos que neste caso o meio de acesso ao provedor de serviço independe do software. De fato o usuário poderia estar acessando o provedor por meio das ERBs dos sistema celular com taxas de transmissão mais baixas mas distantes dos pontos de acessos, e ao se mover para perto de um ponto de acesso de um WLAN passasse a utilizar as melhores taxas de transmissão dessas redes.

Foi baseado nesta solução da IpUnplugged que a Lucent obteve sucesso no testes feitos em sua rede 3G UMTS em setembro de 2002 e garantiu o roaming com uma WLAN sem a perda da conexão, tudo isso baseado no padrão do IP Móvel.

5.4 CONCLUSÕES

Mesmo ainda em desenvolvimento, notamos que o IP Móvel irá ser peça fundamental para o desenvolvimento dos futuros sistemas de comunicações, as chamadas tecnologia de terceira geração.

O funcionamento simultâneo dos sistemas de telefonia móvel 2,5G e 3G e das Wireless LAN só pode ser concebido com o desenvolvimento do IP Móvel e poderá ser uma ótima opção para as empresas de telefonia móvel como opção de serviço de dados melhores que as disponíveis atualmente.

A solução que garante a interoperabilidade entre as redes WLAN e Celular será capaz de permitir que as operadoras de telefonia celular e os provedores de Internet ofereçam o melhor do dois mundos, onde será possível combinar a extensa cobertura de redes celular, como a GPRS por exemplo, com as alta taxas de acesso da WLAN. Esse tipo de solução será capaz de garantir a mobilidade sem costuras entre as redes sem perdas de conexão.

Um dos grandes benefícios para algumas redes 2,5G, como por exemplo as redes GSM/ GPRS, serão as facilidades de cobrança (*billing*) e autenticação. As operadoras poderiam integrar a administração, autenticação e funções de cada usuário fazendo uso da estrutura dessas redes. Os usuários, por sua vez, poderiam receber uma única cobrança e estar apto a usar os serviços independente do sistema. A solução também seria capaz de integrar as redes privadas (VPNs) das grandes empresas, alcançando um número ainda maior de usuários.

As operadoras que proverem a interoperabilidade entre a redes celular e WLAN poderiam fazer crescer rapidamente a adoção dos usuário por novas formas de acesso de serviços dados, como os *hot-spots* onde estariam as WLANs. Além disso, a implementação desses *hotspots* em áreas de bastante concentração de pessoas que necessitam de serviços de acesso de dados (aeroportos, centros de convenção, hotéis) são um complemento da rede celular com custo eficiente capazes de aumentar a capacidade e velocidade dos acessos.

A capacidade de interoperabilidade Celular-WLAN não visa somente que as operadoras de telefonia móvel possam fazer uso da sua infra-estrutura já instalada para o provimento do acesso em altas taxas com as WLANs, mas visa aumentar a competitividade das empresas, aumentar as suas receitas e ainda estarão retendo os clientes desejosos de dados em altas taxas. A operadoras poderiam escolher em investir em ambas as redes, WLAN e Celular, ou também o que seria mais viável, seria dividir os investimentos das WLANs com as outras partes interessadas como os aeroportos, redes de hotéis, centros de conferências e feiras, ou também grandes redes de cafés e lanchonetes.

6 CONCLUSÃO

Neste trabalho foram expostos dados sobre as WLANs, sobre as diversas tecnologias de telefonia móvel, possíveis evoluções e finalmente sobre a interoperabilidade entre esses sistemas tendo o protocolo IP Móvel como a chave desse tipo de solução. Foram trabalhadas as características, vantagens e desvantagens de cada uma das tecnologias.

Observamos que a partir do crescimento da demanda de dados transmitidos em altas taxas e a necessidade de mobilidade dos terminais, houve a necessidade do desenvolvimento de um novo protocolo de Internet que garantisse a mobilidade, além do aumento da capacidade de endereçamento e a segurança dos dados transmitidos foi proposto pelo EITF o IP Móvel, que como foi descrito ainda não está totalmente concluído. O IP Móvel irá possibilitar a mobilidade de um nó em uma rede de forma a ser transparente para os usuários e não causando perdas de dados ou interrupções na transmissão.

A partir do desenvolvimento do IP Móvel foi possível a interação de dois sistemas baseados em IP compartilhando agora os usuários de forma a oferecer “o melhor dos dois mundos”.

No caso descrito a interação dos sistemas comunicações móveis de 2,5G e 3G com as WLANs, o usuário passa a poder utilizar da ampla cobertura das redes celulares mesmo tendo relativamente baixas taxas de transmissão de dados e próximo de pontos de acessos das Wireless LAN usufruir das altas taxas de dados, podendo estar em movimento pelas redes sem ter que reinicializar ou reconfigurar as propriedades de seu terminal.

Já para as operadoras de telefonia móvel, esse tipo de implementação poderá oferecer aos usuários um serviço de dados de melhor qualidade se comparado aos atuais serviços de dados. Isso possibilitará o aumento da receita da empresa e a retenção dos usuários que necessitam de dados e de mobilidade. Os altos investimentos propostos pelas implementações de redes móveis de 2,5G e até 3G poderiam ser diminuídos com os baixos custos da solução de interoperabilidade, quando comparado às redes de última geração.

Como resultado de todo trabalho feito chegou-se a um estudo desse novo tipo de solução para as comunicações móveis no mundo: a interoperabilidade entre o sistema

celular e as WLANs. Foram apresentadas visões gerais dessas tecnologias de forma simples, fácil e de rápida compreensão, como era o objetivo inicial. Este trabalho também poderá servir de referência e base para trabalhos futuros a serem realizados nesta mesma área.

REFERÊNCIAS BIBLIOGRÁFICAS

- [1] IETF – *Internet Engineering Task Force – Mobile IP Working Group IP Routing for Wireless/Mobile Hosts* – 2002. www.ietf.org
- [2] IEEE - *IEEE Standard 802.11.-* 1997. www.ieee.org
- [3] IEEE Standards Department. - *IEEE Draft Standard for Wireless LAN – Medium Access Control (MAC) and Physical Layer (PHY) Specification* - Documento P802.11D6.1, 1997. www.ieee.org
- [4] ANDERSSON, Christoffer - *GPRS and 3G Wireless Applications: Professional Developer's Guide Series* - John Wiley & Sons, Inc., 2001.
- [5] *Plataforma CDMA2000 (1XRTT)* - Lucent Technologies, Junho, 2002 (Apresentação para TCO Centro Oeste Celular).
- [6] *A 3G Introduction to Technology, 3G Standards and 3G Spectrum* - Junho/2002 - <http://andrew100.tripod.com/3g.html>.
- [7] BERNAL, Paulo Sérgio M. - *Comunicações Móveis – Tecnologias e Aplicações* - São Paulo, Editora Érica, 2002.
- [8] CHEN, Yi-an - *A Survey Paper on Mobile IP* - <http://www.securitytechnet.com/hot-topic/mip.html>
- [9] *Mobility and Mobile IP, Introduction* – IPUnplugged, 2002. www.ipunplugged.com
- [10] *IPUnplugged Solution Brief Seamless Roaming – 3G / Wireless LAN* – 2002 – www.ipUnplugged.com
- [11] *3GPP2 PR001 v1.0.0/ Wireless IP Network Architecture based on IETF protocols* – Julho, 2000 – www.3gpp2.org/docs
- [12] KELLER, Ralf; GOLDBECK, Tomas e BOSTROM, Tomas - *Ericsson Mobile Operator WLAN Solution* – www.ericsson.com
- [13] RAMASWAMY, Kumar - *Issues in Inter-working Models for 3G and Wireless Local Area Networks* – THOMSON Multimedia, 2002.
- [14] GEIER, Jim - *Wireless Networking Handbook* – Macmillan, 2002. <http://news.dcn-asu.ru/BOOKS/Wireless/ewtoc.html>
- [15] SOARES, L. F. G. Et al. – *Redes de Computadores - Das LANs, MANs e WANs às redes ATM* - Ed. Campus – 1995.
- [16] HAYKIN, Simon – *Communication Systems* – 4ª Edição - Wiley & Sons, Inc., 2002.

A - TÉCNICAS DE ESPALHAMENTO ESPECTRAL

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

A.1 – DSSS (DIRECT SEQUENCE SPREAD SPECTRUM): ESPALHAMENTO ESPECTRAL DE SEQUÊNCIA DIRETA

Na técnica de Espalhamento Espectral de Sequência Direta define-se uma sequência de dados que contém a informação $b(t)$, a qual é usada para modular uma sequência pseudo-aleatória $c(t)$ de faixa larga através da multiplicação dos dois sinais. Como o sinal $c(t)$ é de faixa larga, o sinal $m(t)$ resultante da multiplicação dos dois sinais também será de faixa larga. O sinal $c(t)$ neste caso então age como um código de espalhamento. O sinal $m(t)$ pode ser expresso como:

$$m(t) = c(t)b(t) \quad (\text{A.1})$$

Após o espalhamento o sinal é modulado novamente (na frequência central de faixa) e transmitido. Uma representação gráfica é mostrado na figura A.1. Quando é recebido e demodulado, o sinal pode ser expresso da seguinte forma:

$$r(t) = c(t)b(t) + i(t) \quad (\text{A.2})$$

Onde $i(t)$ é uma interferência aditiva presente no canal, a decodificação é realizada multiplicando o sinal $r(t)$ novamente pelo código de espalhamento em perfeito sincronismo com o transmissor, resultando:

$$z(t) = r(t)c(t) = c^2(t)b(t) + c(t)i(t) \quad (\text{A.3})$$

Como o código de espalhamento alterna entre +1 e -1, quando ele é multiplicado consigo mesmo essa alternância é destruída, ou seja:

$$c^2(t) = 1, \text{ para todo } t \quad (\text{A.4})$$

aplicando-se o resultado acima, a equação A.4 se torna:

$$z(t) = b(t) + c(t)i(t) \quad (\text{A.5})$$

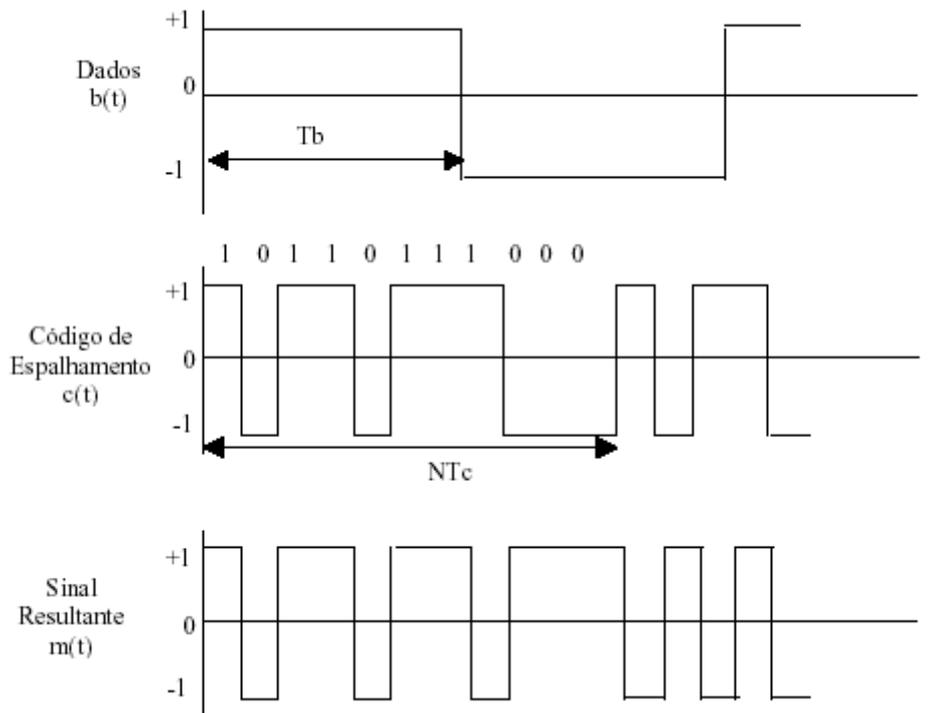


Figura A.1 Sinal resultante da multiplicação dos sinais.

A supressão da interferência é realizada através da passagem do sinal por um filtro passa-baixa, já que o sinal $b(t)$ é de faixa-estreita e o componente $c(t)i(t)$ é de faixa-larga, recupera-se, desta maneira, a informação que foi transmitida.

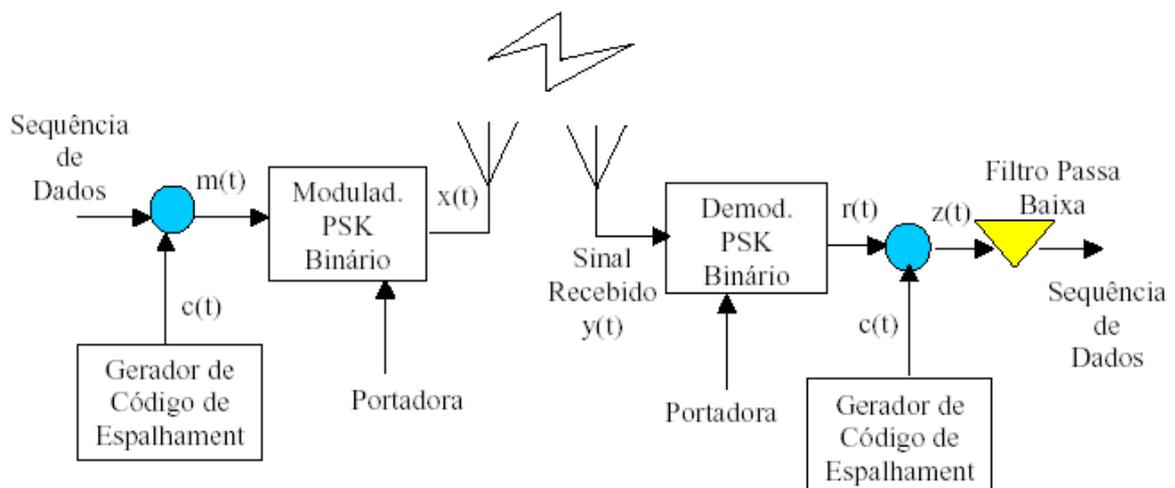


Figura A.2 - Diagrama de blocos do DSSS

A figura A.2 mostra o diagrama de blocos para um sistema DSSS simples. No diagrama, o sinal $b(t)$ (seqüência de bits) é multiplicado pelo sinal $c(t)$ (código de espalhamento) dando origem ao sinal $m(t)$, que é em seguida modulado por uma portadora senoidal, na freqüência central da banda utilizada, usando BPSK (*Binary Phase Key Shiting*).

A.2 – FHSS (FREQUENCY HOPPING SPREAD SPECTRUM): ESPALHAMENTO ESPECTRAL POR SALTOS EM FREQUÊNCIA

No sistema DSSS, o uso de uma seqüência de espalhamento provoca um espalhamento instantâneo da faixa de transmissão. Um método alternativo é cobrir todo o espectro simplesmente fazendo o sinal modulado "saltar" aleatoriamente de uma freqüência para outra, de acordo com um código de espalhamento. Neste caso, o espectro do sinal transmitido é espalhado seqüencialmente, e não instantaneamente como no caso do DSSS. Este método é denominado Espalhamento Espectral por Saltos em Freqüência (*Frequency Hopping Spread Spectrum - FHSS*).

A figura A.3, mostra o diagrama de blocos de um sistema FHSS utilizando modulação FSK (*Frequency Shift Key*). Pode-se observar que o código de espalhamento altera a freqüência da portadora com a qual é modulado o sinal de informação.

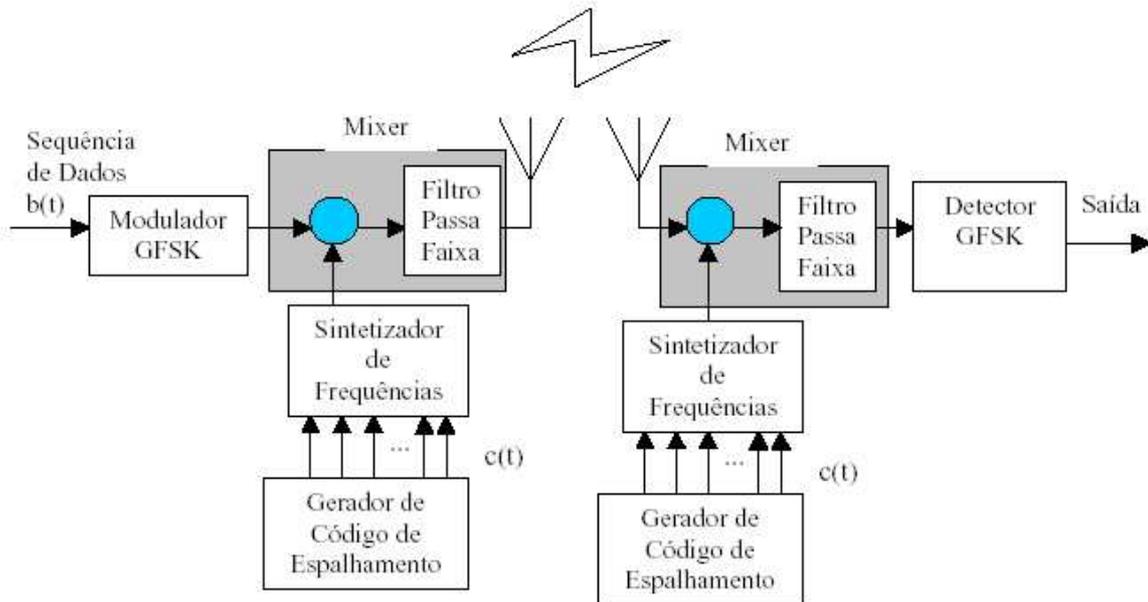


Figura A.3 - Diagrama de blocos do FHSS

Existem dois tipos de Espalhamento de Freqüência (FH): Slow (SFH), no qual vários símbolos do sinal são transmitidos em um único salto e Fast FH (FFH), onde a freqüência da portadora saltará várias vezes durante a transmissão de um símbolo.

Em sistemas de redes sem fio, FFH não é usado por ser cara e consumir muita energia. Também, tanto o receptor como o transmissor tem que saltar em sincronismo, SFH é melhor por possuir melhor tolerância em relação ao grau de sincronismo usado.

6.1.1.1.1 A.3 - Comparação entre as técnicas de espalhamento

Nos sistemas DSSS comerciais, a taxa típica entre a seqüência de espalhamento e o sinal situa-se entre 10 e 100. Esse número é conhecido como o fator de espalhamento. Sistemas DS, de acordo com regulamentos da FCC, precisam manter um fator de espalhamento de pelo menos 10. Se a eficiência espectral da sinalização é 1 (um) e a faixa alocada é W , então a taxa de dados por usuário não pode exceder $W/10$. A taxa de dados por usuário depende ainda da distribuição geográfica dos usuários e portanto pode ser muito menor.

Os sistemas FH que operam nas bandas ISM são limitadas quanto à sua largura de faixa instantânea a 0,5 MHz (faixa de 915 MHz) ou 1,00 MHz (faixas de 2,4 e 5,8 GHz). Em sistemas FH não sincronizados (exigência da FCC), no pior caso, a taxa de dados agregada chega a $W/4$ e este valor não depende da distribuição geográfica dos usuários.

Sistemas FH possuem um potencial maior para rejeição de interferência que sistemas DS, já que podem administrar seu espectro com mais facilidade. Desta forma possuem uma capacidade maior de evitar interferência com usuários de maior prioridade, como operadores de rádio amador.

Devido à forma como os sistemas FH e DS ocupam a faixa, é necessário que compartilhem a mesma entre seus usuários. Alguns sistemas DS são projetados para usarem menos que a faixa disponível, que é dividida em canais. Assim, cada usuário trabalha em um canal, não havendo então, interferência. Em sistemas FH, a mesma largura de faixa total é usada por diferentes redes, mas cada rede usa canais estreitos de 0,5 ou 1 MHz e seguem seu próprio padrão de saltos em frequência. Na tabela A.1 se faz uma comparação entre os diferentes métodos DSSS e FHSS.

Tabela A.1 - Comparação entre os métodos de Espalhamento do Espectro

	DSS	FHSS
Necessita de licença	Não	Não
Capacidade no pior caso	$< W/10$	$W/4$
Capacidade de evitar interferência	Baixa	Alta
Capacidade de evitar usuário prioritário	Baixa	Alta
Redes simultâneas	Poucas	Muitas

B –IPv6: PRINCIPAIS CARACTERÍSTICAS

6.1.1.1.1 B.1 - Estrutura do datagrama IPv6

O datagrama do IPv6 tem um cabeçalho de tamanho variado, esta característica lhe dá flexibilidade para adaptação em futuras tecnologias. O IPv6 foi projetado para determinar o tamanho de pacote máximo permitido no link, dessa maneira os roteadores ficam livres da tarefa de fragmentar os pacotes.

Com um cabeçalho base mais simples e opcionalmente um cabeçalho adicional, algumas informações contidas no cabeçalho do IPv4 (versão atual do IP) se tornaram opcionais para um melhor rendimento do roteamento. A figura 4.2 mostra a estrutura do datagrama IPv6.



Figura B.1 - Estrutura do datagrama IPv6

- *Version* – função idêntica a do IPv4;
- *Priority* – campo que identifica a prioridade do datagrama. Os valores de 0 a 7 são destinados a protocolos capazes de diminuir o fluxo de envio caso ocorra o congestionamento. Para pacotes de aplicações em tempo real que são enviados a taxa constante, valores de 8 a 15 dizem quais datagramas podem ser descartados com prioridade maior para valores mais altos;
- *Flow label* – identifica se um datagrama precisa de um tratamento especial nos roteadores como datagramas de aplicações de vídeo em tempo real;
- *Payload Length* – tamanho do datagrama sem o cabeçalho;
- *Next Header* – identifica se há cabeçalho de extensão após o cabeçalho base, se houver identifica que cabeçalho é. Este campo tem dois propósitos: generalização e eficiência. A generalização é conseguida com a inclusão de funções adicionais, como fragmentação, roteamento na origem e autenticação. A eficiência é conseguida a partir do momento que se não forem preciso estas características os seus campos não necessitam estar presentes.

Como a maioria dos valores são provenientes do IPv4. Os cabeçalhos de extensão são classificados da seguinte maneira:

- *Routing* - roteamento estendido (IPv4 possui roteamento livre).
- *Fragmentation* - Fragmentação e Remontagem.
- *Authentication* - Integridade e Autenticação. Segurança.
- *Encapsulation* - Confidencialidade.
- *Hop-by-Hop Option* - Opção especial que requer processamento de hop para hop.
- *Destination Options* - Informação opcional a ser examinada pelo destino.

- Hop Limit – número máximo de hops para um datagrama. Ele é decrementado a cada hop até chegar ao destino ou se igualar a zero e então é descartado;
- Source Address – endereço origem do datagrama de tamanho 128;
- Destination Address – endereço destino do datagrama;

B.1.1 - Autoconfiguração de endereço

A autoconfiguração é um mecanismo que permite que a máquina obtenha um endereço IP assim que ela é ligada. Haverá dois métodos:

- Configuração *Statefull* – onde há um servidor de configuração, como os servidores DHCP com o qual a interface se comunica para obter seu endereço, é claro que esse fator acarreta em um aumento de operações e um gerenciamento bem eficiente;
- Configuração *Stateless* – o endereço de interface é a base para a confecção do endereço IP, o mecanismo a interface identifica o primeiro roteador através de um endereço local de enlace que é identificado manualmente pelo usuário.

B.1.2 - Segurança no datagrama IPv6

O protocolo IPv4 não garantia integridade e segurança de dados. O IPv6 foi desenvolvido para oferecer características de segurança aos datagramas.

Uma dessas características é a adição do Cabeçalho de Encapsulamento do *Payload* que fornece integridade e confiabilidade para os datagramas ou o Cabeçalho de Autenticação que fornece integridade sem confiabilidade através de algoritmos de criptografia. Esquemas de Segurança em datagramas são fundamentais, por exemplo, quando se trabalha com Redes Virtuais Privadas como ilustrado na figura abaixo:

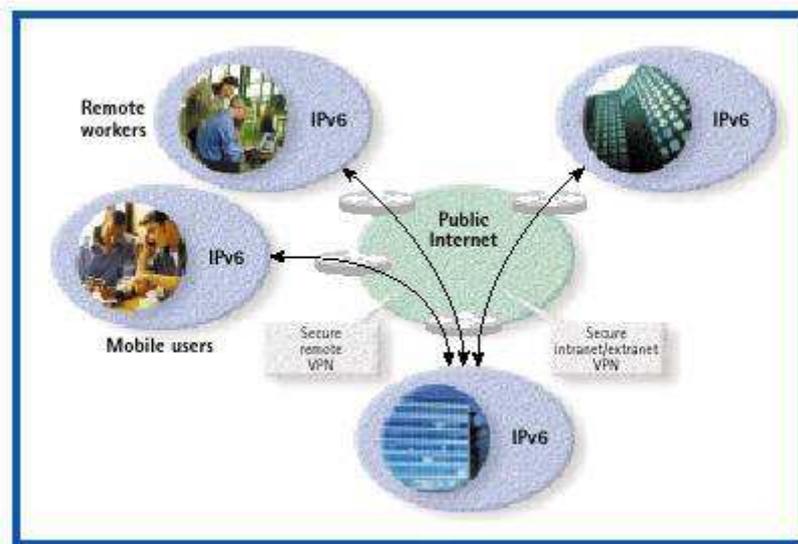


Figura B.2 – Estrutura de rede com VPNs

B.1.3 - Qualidade de serviço

A qualidade de serviço é um fator de extrema importância no desenvolvimento do IPv6, para atender essa necessidade foi acrescentado os campos *Priority* e *Flow Label*:

- *Flow Label* identifica o fluxo requerido para o datagrama: fluxo orientado ou fluxo não orientado, onde o fluxo orientado estabelecerá uma rota, ou conjunto de rotas a serem seguidas, enquanto que o fluxo não orientado continuará o tratamento já conhecido.
- *Priority* identifica a prioridade do datagrama em relação à outros datagramas ao chegar a um *host*. Datagramas de mesmo fluxo devem ter prioridades iguais para evitar que datagramas cheguem ao destino em desordem.

Os dois campos mencionados se preocupam basicamente com a velocidade de transmissão dos datagramas. É claro que o fato do IPv6 prover uma maior segurança de dados, como foi mencionado anteriormente, também é um fator de melhoria de qualidade de serviço.

B.1.4 - Mobilidade

Como mencionado anteriormente, o projeto IPv6 previa suporte a novos serviços, e um desses novos serviços é a mobilidade do terminal conectado a uma rede. Cada nó móvel é identificado como um endereço independente na rede, quando ele se move é considerado ausente de sua rede. Então ele é associado com um endereço de tratamento que fornece informações da atual situação do nó. A rede a qual pertence o nó e o próprio nó ficam periodicamente recebendo informações sobre a mobilidade do nó.

Quando o nó móvel se encontra fora da sua rede, para enviar um pacote ele utiliza o endereço provisório como fonte. O endereço original é utilizado quando a rede deve enviar um pacote ao nó móvel para informar que o pacote foi recebido corretamente, pois quando o nó móvel recebe o pacote verifica este endereço. É claro que o endereço provisório é utilizado para roteamento, porém isso é transparente.

B.1.5 - Transição do IPv4 atual para o IPv6

A transição do IPv4 para o IPv6 deve ser gradual. Uma vez que o IPv6 é introduzido, é possível que ele continue a acessar os serviços disponíveis em IPv4, pois eles não serão substituídos rapidamente, assim como também é interessante que aplicações IPv4 possam acessar serviços disponíveis em IPv6. Existem três formas de fazer esse processo:

- Dispositivos IPv6/IPv4 – uso de dispositivos IPv6/IPv4 é o principal mecanismo de transição. Num lado da rede, um dispositivo GPRS é vital para a comunicação entre IPv6 e IPv4. As extremidades do roteador também possuem esses dispositivos, assim como terminais móveis.
- Tunelamento – consiste em encapsular o datagrama IPv6 em datagramas IPv4;
- Tradutores – também pode ser utilizado protocolos tradutores, porém deve ser analisado que eles causam uma demora nos terminais, assim como estão mais aptos a falhas.