Universidade da Região da Campanha - URCAMP
Centro de Ciências da Economia e Informática - CCEI

# Segurança em Transações e Aplicações WAP

Universidade da Região da Campanha - URCAMP
Centro de Ciências da Economia e Informática - CCEI

# Segurança em Transações e Aplicações WAP

Jorge Luis Morales Cabral
jlmcinfo@bol.com.br
Leonardo Mascarenhas Leite
leoleite@matrix.com.br

Orientador
Sandro Silva Camargo
scamargo@urcamp.tche.br

# Agradecimentos

Existem pessoas que cruzam nossas vidas e que, por um gesto ou palavra, ficam guardadas em nossas lembranças.

Para aqueles que compartilharam nossos ideais, alimentando-os e incentivando-nos a seguir em frente.

Para aquelas pessoas especiais, cujo apoio, amizade, amor e compreensão foram essenciais para atingirmos nossa meta.

Para os professores, que sempre estiveram presentes ao longo de nossa jornada, especialmente ao nosso orientador, professor Sandro Camargo, por estar sempre disposto a apontar novos horizontes, visando apenas o sucesso desta empreitada.

E também a Deus, pela vida, pela oportunidade, pela sociedade que com ele fazemos e pela consciência de que em tudo Dele dependemos para a realização de nossos melhores sonhos.

A vocês dedicamos nossa conquista, com a mais profunda admiração e respeito.

***Muito Obrigado!***

## Resumo

O objetivo deste trabalho, é realizar um estudo sobre os aspectos de segurança envolvidos na utilização da tecnologia WAP, tratando de assuntos como a arquitetura WAP, padrões utilizados na telefonia celular para transporte e roteamento de dados, o modo que o protocolo WAP trata a segurança frente a outros protocolos já utilizados na *WWW*, e também frente ao modelo de referência OSI. Fornecendo ao final uma fonte de referência bastante atualizada em Língua Portuguesa, disponível na Internet para todos aqueles que buscam informações sobre esta nova tecnologia.

## Abstract

The goal of this doc, is to accomplish a study on safety's aspects involved in the use of the WAP technology, dealing with matters as the WAP architecture, standards used in the cellular telephony for data transport and routing, the way that the WAP protocol already treats the safety front the other protocols used in WWW, and also front to the RM-OSI. Supplying at the end a reference source quite modernized in Portuguese Language, available in the Internet for all those that look for information on this new technology.

# Siglas e Abreviaturas

**AP** - Access Points
**API** - Application Program Interface
**ASP** - Application Service Provider
**AuC** - Autentication Center
**BSC** - Base Station Controller
**BSS** - Basic Service Set
**BTS** - Basic Transceiver Station
**CD** - Collision Detect
**CEPT** - Conference of European Posts and Telegraphs
**CGI** - Common Gateway Interface
**CPU** - Central Processing Unit
**CSD** - Circuit-Switched Data
**CSMA** - Carrier Sequence Multiple Access CTS - Clear To Send
**CTIA** - Cellular Telecommunications Industry Association
**CTS** - Clear To Send
**Db** - Decibéis
**DES** - Data Encryption Standard
**DNS** - Domain Named System
**DS** - Distribution System
**DSS** - Distribution System Services
**DTD** - Document Type Definition - Define a sintaxe do documento.
**EIR** - Equipment Identity Register
**ESS** - Extended Service Sets
**ETSI** - European Telecommunications Standards Institute
**FC** - Frame Check
**FCS** - Frame Check Sequence
**FTP** - File Transfer Protocol
**GSM** - Group Special Mobile
**GSMK** - Gaussian Minimum Shift Keying
**GUI** - Guide User Interface
**HDML** - Handheld Device Markup Language
**HDTP** - Handheld Device Transport Protocol
**HTML** - Hyper Text Markup Language
**HTTP** - Hyper Text Transfer Protocol
**IBSS** - Independent Basic Service Set
**ID** - Identification
**IEEE** - Internet of Electrical and Electronics Engineers
**IETF** - Internet Engineering Task Force
**IMEI** - International Mobil Equipment Identity
**IMSI** - International Mobile Subscriber Identity
**IP** - Internet Protocol
**IPSec** - IP Secure - O mesmo que Ipv6
**IPv4** - IP Versão 4

**IPv6** - IP Versão 6
**ISDN** - Integrated Services Digital Network
**ISO** - International Organization for Standardization
**ISP** - Internet Service Provider
**ITTP** - Intelligent Terminal Transfer Protocol
**LLC** - Logical Link Control
**MAC** - Medium Access Control
**MD5** - Message Digest 5
**MDI** - Mobile Data Initiative
**ME** - Mobile Equipment
**MexE** - Mobile Execution Environment
**MSC** - Mobile Services Switching Center
**MSDU** - MAC Service Data Unit
**PCI** - Protocol Control Information
**PDA** - Personal Digital Assistant.
**PDU** - Protocol Data Unit
**PHY** - Physical Layer
**PKI** - Public Key Interface
**PSTN** - Public Switched Telephone Network
**RAM** - Random Access Memory
**RC4** - Algoritmo de Criptografia
**RC5** - Algoritmo de Criptografia
**RM-OSI** - Reference Model for Open Systems Interconection
**ROM** - Read-Only Memory
**RSA** - Rivest, Shamir and Adleman
**RTS** - Ready To Send
**SAP** - Service Access Point
**SDU** - Service Data Unit
**SGML** - Standardised Generalised Markup Language
**SHA** - Secure Hash Algorithm
**SIM** - Subscriber Identity Module
**SMS** - Short Message System
**SMTP** - Simple Mail Transfer Protocol
**SS** - Station Services
**SSH** - Secure Shell
**SSL** - Secure Socket Layer
**TCP** - Transfer Control Protocol
**TDMA** - Time Division Multiple Access
**TIA** - Telecommunications Industry Association
**TLS** - Transport Layer Security
**TSAP** - Transport Service Access Point
**TTML** - Tagged Text Markup Language
**UA** - User Agent
**UDP** - User Datagram Protocol
**UMTS** - Universal Mobile Telecommunication System
**URI** - Uniform Resource Identifier
**URL** - Unit Resource Locator

**VLR** - Visitor Location Register
**XML** - Extensible Markup Language
**W3C** - World Wide Web consortium
**WAE** - Wireless Application Protocol
**WAP** - Wireless Application Protocol
**WDP** - Wireless Datagram Protocol
**WEP** - Wireless Equivalent Privacy
**WML** - Wireless Markup Language
**WMLS** - Wireless Markup Language Script
**WSP** - Wireless Session Protocol
**WSPB** - Wireless Session Protocol Browsing
**WTA** - Wireless Telephony Application
**WTAI** - Wireless Telephony Application Interface
**WTLS** - Wireless Transport Layer Security
**WTP** - Wireless Transaction Protocol
**WWW** - World Wide Web

# Lista de Figuras

# LISTA DE TABELAS

# SUMÁRIO

# 1 Introdução

## 1.1 Motivação

A computação móvel é um novo paradigma computacional que tem como objetivo permitir que usuários tenham acesso permanente à rede, independente de sua localização física. Nas redes wireless, a tecnologia que está emergindo, como padrão para acesso à Internet, é o WAP (Wireless Aplication Protocol). O WAP está posicionado na convergência de duas tecnologias de rede que estão evoluindo muito rapidamente - a transmissão de dados sem fio e a Internet. Embora muito esteja sendo falado sobre as limitações do WAP, esta nova tecnologia possui um enorme potencial, que ainda não está sendo explorado.

Fato semelhante ocorreu com a Internet, e hoje ela tornou-se uma ferramenta indispensável nas mais diversas atividades, sendo utilizada para realizar pesquisas, comunicar-se e efetuar transações de comércio eletrônico. Espera-se que o mesmo ocorra brevemente com a tecnologia WAP. Embora possua várias limitações e até mesmo falhas, este cenário deve ser modificado rapidamente, visto que existem várias ações no sentido de aperfeiçoa-lo, e o modelo que se apresenta atualmente tende a ser apenas um esboço do que realmente virá a ser a computação móvel dentro de pouco tempo, pois a sociedade encontra-se ainda no início da curva de absorção desta nova tecnologia, a fase do aprendizado, mas se for possível diminuir a margem de risco e erros, com certeza os resultados serão mais positivos.

A segurança na realização de transações e na utilização de aplicações WAP deve ser considerada objeto de estudos de alta prioridade, pois atualmente, com a crescente quantidade de informações relevantes e confidenciais que trafegam através da Internet, a segurança deve ser considerada uma questão de vital importância para o sucesso de operações deste tipo. Muitos usuários ainda receiam enviar dados como números de cartões de crédito pela Internet, utilizando o acesso convencional, podem se sentir ainda mais receosos de realizarem o mesmo através de dispositivos móveis.

Para que ocorra o aperfeiçoamento da tecnologia WAP, e sua conseqüente utilização em transações de comércio eletrônico e outros, é preciso mais do que apenas criticar, é preciso buscar soluções para as falhas e inconveniências atualmente existentes.

Diante disto, será apresentado a seguir um estudo sobre a tecnologia WAP, abordando vários aspectos, como sua arquitetura, a utilização da telefonia celular, dando ênfase à segurança, objetivo deste trabalho, onde serão apontados os elementos utilizados para oferecer segurança, suas falhas e soluções possíveis de serem implementadas, na tentativa de tornar o WAP um modo de acesso a Internet realmente seguro.

## 1.2 Objetivos

Os objetivos propostos no projeto estão descritos a seguir:

### 1.2.1 Objetivo Geral

O objetivo geral deste trabalho consiste na identificação dos aspectos de segurança da Tecnologia *WAP*.

### 1.2.2 Objetivos Específicos

- definir o que é WAP;
- mostrar o funcionamento do WAP;
- apresentar as características da arquitetura WAP;
- analisar os aspectos de segurança do protocolo;
- realizar um comparativo com outros Protocolos (Modelo OSI, TCP/IP);
- realizar experiências "in loco" em ambiente *Wireless*;
- criar uma *home-page*, em html contendo informações sobre o protocolo e aplicações WAP como exemplo.

Nos capítulos 2 e 3 foram apresentadas a definição de WAP, e também seu funcionamento. As características da arquitetura WAP estão descritas no capítulo 4, no capítulo 5 foi demonstrado o funcionamento de telefonia celular, para situar o leitor no contexto em que está situado o funcionamento da tecnologia WAP. No capítulo 6 foi realizado o comparativo de arquitetura WAP com o modelo OSI e a arquitetura utilizada na *WWW*, que está baseada no protocolo TCP/IP, apresentando detalhadamente o modelo OSI, por tratar-se de referência na construção de qualquer outro protocolo. Os aspectos relativos a segurança, estão detalhados no capítulo 7, apesar de outros capítulos também apresentarem enfoque em segurança, por tratar-se do objetivo geral deste projeto. As experiências realizadas estão descritas em Anexo (anexo 1), por ser este um objetivo suplementar ao projeto. Uma *home-page* foi criada e está sobre constante atualização na URL www.ccei.urcamp.tche.br/~wap, contendo várias informações sobre o tema.

## 1.3 Metodologia

A realização deste projeto baseou-se em pesquisas bibliográficas através de revistas, livros, jornais, participação em seminários e *Internet*, onde foi realizado interação com grupos de usuários e desenvolvedores WAP para que fossem obtidas as conclusões necessárias à realização do mesmo.

# 2 A criação do protocolo WAP

## 2.1 Histórico

Em Junho de 1997, quatro empresas uniram-se para desenvolver um protocolo de aplicações sem fio em comum. Esse protocolo foi inicialmente chamado de MDI (*Mobile Data Initiative*). A iniciativa teve o objetivo de unir os esforços das companhias para portar aplicações avançadas e conteúdo de *Internet* para telefones móveis digitais. O Protocolo de Aplicação Sem fios herdou as características principais e a funcionalidade do HDML (*Handheld Device Markup Language*) e HDTP (*Handheld Device Transport Protocol*) desenvolvido através da *Unwired Planet* (agora *Phone.com*), a especificação TTML (*Tagged Text Markup Language*) desenvolvido através da *Nokia*; e o ITTP (*Intelligent Terminal Transfer Protocol*) especificação desenvolvida através da *Ericsson*. Desta união surgiu o *WAP Forum*, um órgão independente com a finalidade de desenvolver este protocolo e padronizar seu conteúdo.

Através do *WAP Forum*, em 15 de Setembro de 1997 foi publicada a versão 1.0 do WAP. Desde então o número de sócios do *WAP Forum* cresceu muito, reunindo provedores de serviço *wireless*, fabricantes de equipamento portáteis, provedores de infra-estrutura e pesquisadores de *software*, já possuindo mais de duzentos sócios [PHO99].

## 2.2 A busca pela padronização do protocolo WAP

O *Wireless Application Protocol* (WAP) é o padrão mundial de fato para a apresentação e entrega de informação *wireless* e serviços de telefonia em telefones móveis e outros terminais *wireless*. Fabricantes de dispositivos portáteis, que representam 90 por cento do mercado mundial, entraram em acordo para entregar dispositivos WAP. Operadoras de telefonia representando mais de 100 milhões de assinantes no mundo todo uniram-se no *WAP Forum*. Este compromisso disponibilizará 10 milhões de produtos com WAP *browser* habilitados para consumidores até o final de 2000 [PHO99]. O WAP permite as operadoras fortalecer os serviços oferecidos, disponibilizando aos assinantes a informação desejada, onde quer que estejam. A Infra-estrutura dos fabricantes dará o suporte aos equipamentos de rede necessários na implantação. Os pesquisadores de aplicações e provedores de conteúdo que entregam os serviços de valor adicional estão contribuindo para a especificação do WAP. Habilitar o acesso de Informações em dispositivos portáteis requer um profundo conhecimento sobre a parte técnica e de mercado, fatores determinantes no ambiente *wireless*. A especificação WAP foi desenvolvida por alguns dos melhores pesquisadores da indústria.

Redes *wireless* são limitadas pela pequena largura de banda, alta latência, imprevisível disponibilidade e estabilidade. Porém, o mais importante de tudo, é que assinantes *wireless* possuem um perfil diferente de necessidades dos usuários de *desktop* ou até mesmo os usuários de *Internet* em *laptop*s. Nos dispositivos WAP serão disponibilizadas informações oportunas, validação de transações e procura.

Os provedores de serviços WAP podem ter o acesso ao dispositivo e entregar informações enquanto o ambiente de tela não está cheio. A especificação do WAP envia estes conteúdos utilizando os melhores padrões existentes, e está desenvolvendo novas extensões onde é necessário, permitindo que os participantes da indústria desenvolvam soluções como interfaces aéreas independentes, dispositivos independentes e completamente interoperáveis.

O protocolo WAP necessitou de um grande investimento em novos servidores, ferramentas, programadores e aplicações no ambiente *WWW*, enquanto se estava resolvendo o problema associado ao domínio *wireless*.

A especificação assegura que esta solução será rápida, confiável e segura. Permitindo aos pesquisadores utilizar ferramentas existentes para produzir aplicações sofisticadas com uma interface de usuário amigável. Com isto, assinantes *wireless* serão beneficiados com o ganho de poder de acesso de informação onde quer que estejam.

O *WAP Forum* criou uma especificação *wireless* global, baseada em padrões *internet* existentes como o XML e IP, para todas as redes *wireless*. A especificação WAP é desenvolvida e apoiada pela comunidade de telecomunicação *wireless*, de forma que toda a indústria e mais importante, seus assinantes, possam se beneficiar de uma especificação única e aberta.

Provedores de serviço *wireless* podem oferecer uma dimensão nova de serviços que complementa as características existentes das suas redes, estendendo o acesso do assinante para o ilimitado mundo da *WWW*.

Fabricantes de dispositivos móveis podem integrar a funcionalidade de um *micro-browser* a custo mínimo, porque a especificação WAP está aberta ao público. Profissionais que desenvolvem aplicações ganham acesso a um mercado novo de informação, influenciando os investimentos atuais em suas tecnologias *WWW*. Assinantes ganham acesso a informações a qualquer hora, e em qualquer lugar com uma interface de usuário simples e efetiva, disponível em uma variedade de redes e dispositivos.

Enquanto a especificação WAP resolve os problemas de transporte e satisfação nas limitações do ambiente *wireless* de hoje, o *WAP Forum* está trabalhando constantemente para aperfeiçoar o estado do acesso *wireless* para informação, juntamente com várias entidades como ETSI, TIA e W3C, para assegurar que um padrão único e aberto esteja disponível para acessar informações *wireless* necessárias aos assinantes e participantes da indústria em todo mundo. O *WAP Forum* trabalha com estes padrões para uma meta de convergência com o HTML e padrões como o HTTP para aperfeiçoar o ambiente *wireless*.

### 2.2.1 As Metas do *WAP Forum*

O *WAP Forum* possui as seguintes metas [WAP98]:

- Trazer conteúdo de *Internet* e serviços de dados avançados a telefones e outros terminais *wireless*
- Criar uma especificação de protocolo *wireless* global que trabalhe com todas as tecnologias de rede *wireless*
- Habilitar a criação de conteúdo e aplicações que buscam por uma gama extensiva de redes portadoras *wireless* e tipos de dispositivo
- Estender os padrões e tecnologia existentes, onde quer que seja possível e apropriado

O *WAP Forum* não desenvolve produtos, cria padrões de licenças livres, para toda a indústria desenvolver produtos. A linha de produto de cada companhia pode oferecer, então, suas próprias características, mantendo a conformidade com a especificação WAP. O WAP Forum não é um fabricante de equipamentos portáteis, vendedor de serviços, ou provedor de infra-estrutura. Todas as companhias na indústria de telecomunicações estão seguras que eles não estão competindo com WAP, porque WAP não promove qualquer produto particular ou linha de produto. Pelo contrário, o *WAP Forum* promove e apoia todas as companhias que possuem produtos em desenvolvimento fundamentadas na especificação WAP.

### 2.2.2 Utilizando Padrões Existentes

O *WAP Forum* busca utilizar padrões existentes na indústria como a base para sua própria arquitetura e projeto. Por exemplo, é exigido um WAP *gateway* para se comunicar com outros nós da *Internet*, que utilizam o protocolo HTTP 1.1. Além disso, a especificação de chamada para dispositivos *wireless* utiliza o padrão URL de endereçamento de requisição de serviço.

Também é muito importante para os padrões do *WAP Forum* serem desenvolvidos do mesmo modo que os padrões existentes. Por exemplo, a especificação WAP não deve estabelecer como devem ser transmitidos os dados sobre a interface aérea. Na especificação WAP procura-se utilizar o topo dos padrões do canal de portador existente de forma que qualquer padrão portador seja usado com os protocolos WAP para implementar soluções completas.

Quando o *WAP Forum* identifica uma área nova de tecnologia onde um padrão não existe, ou existe mas precisa de modificação para *wireless*, trabalha para submeter suas especificações para outros grupos de padrões da indústria. O *WAP Forum* possui várias relações com outros padrões [PHO99]:

- O *WAP Forum* está submetendo suas especificações ao ETSI (*European Telecommunications Standards Institute*). Além de existir uma ligação formal entre os dois grupos, o MExE (*Mobile Execution Environment*) subgrupo dentro do ETSI Grupo 4 móvel Especial, está cruzando as referências na especificação WAP para definir uma conformidade no perfil GSM e UMTS.

- A CTIA (*Cellular Telecommunications Industry Association*) possui um funcionário de ligação para o *WAP Forum*.

- O *WAP Forum* estabeleceu uma relação de ligação formal com o W3C (*World Wide Web consortium*) e a TIA (*Telecommunications Industry Association*), colaborando com estas organizações na área de tecnologia *WWW* dentro do setor *wireless*. O W3C, TIA e o *WAP Forum* pretendem continuar trabalhando juntos nas áreas técnicas selecionadas para criar juntamente e promover especificações técnicas de interesse para todas as três organizações.

- O *WAP Forum* está buscando formar uma relação de ligação com a IETF (*Internet Engineering Task Force*).

# 3 O que é WAP (Wireless Application Protocol)

O WAP (*Wireless Application Protocol*, ou Protocolo para Aplicações Sem Fio) é o resultado dos esforços do *WAP Forum*, visando promover uma série de especificações a serem utilizadas pela indústria no desenvolvimento de aplicações e serviços para ambientes móveis. O WAP especifica um ambiente de aplicação e uma pilha de protocolos para dispositivos sem fio, como telefones celulares, pagers e PDA's (*Personal Digital Assistants*, ou Assistentes Pessoais Digitais), também especifica uma integração API computador-telefone, chamado WTAI (*Wireless Telephony Application Interface*), entre dados e voz. Isto permite as aplicações tirarem proveito do fato de que freqüentemente o usuário de *Internet* possui um dispositivo de telefonia móvel. O WAP está posicionado na convergência de duas tecnologias de rede que estão evoluindo muito rapidamente: a transmissão de dados sem fio e a *Internet* [WAP00]. A grande maioria das tecnologias desenvolvidas para a *Internet*, entretanto, são destinadas a computadores de mesa, com alto poder de processamento, grande quantidade de memória, com média para alta largura de banda, em redes geralmente confiáveis, por este motivo à utilização em dispositivos sem fio obrigou a criação de um padrão que pudesse manter a independência dos dispositivos e assegurar a interoperabilidade conforme demonstrado na figura 3.1.

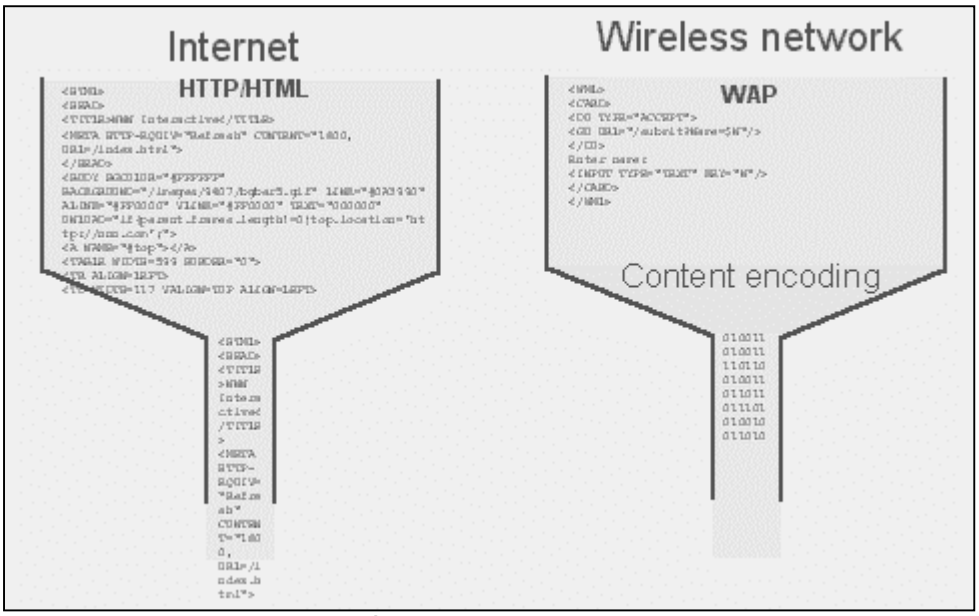


FIGURA 3.1 - CODIFICAÇÃO DO CONTEÚDO VIA WAP

## 3.1 Independência dos Dispositivos

A especificação WAP é uma interface aérea independente e também independe de qualquer dispositivo particular. Especifica a funcionalidade mínima que um dispositivo deve ter e foi projetado para aceitar funcionalidade extra sobre este mínimo.

A independência do dispositivo oferece benefícios semelhantes à independência de portador:

- aplicações desenvolvidas para um padrão podem operar em uma variedade ampla de dispositivos que implementam a especificação;
- pesquisadores de aplicação não necessitam escrever versões separadas de código para dispositivos diferentes;
- os provedores de serviço podem escolher qualquer dispositivo compatível ao padrão que se encontra com suas próprias exigências de mercado.

## 3.2 Assegurar a Interoperabilidade

Os Provedores de serviços necessitam ter a confiança que seus investimentos renderão benefícios no futuro.

A especificação WAP foi projetada para promover a fácil e aberta interoperabilidade entre seus componentes fundamentais. Qualquer componente construído para ser compatível com a especificação WAP pode interoperar com qualquer outro componente WAP compatível.

Provedores de serviços podem escolher equipamento e *software* de múltiplos vendedores compatíveis com o padrão WAP, selecionando cada parte da solução apropriada para o serviço, a cada necessidade dos provedores.

O portador e a independência de dispositivo, ajudam na adoção da interoperabilidade. Mas esta vai além destes dois princípios, para requerer que cada componente WAP compatível se comunique com todos os outros componentes na rede devem ser utilizados os métodos e protocolos padrões definidos na especificação.

A interoperabilidade provê benefícios claros para os fabricantes de dispositivos portáteis e infra-estrutura de provedores. Os fabricantes estão seguros de que se os dispositivos estiverem de acordo com a especificação WAP, poderão conectar-se com qualquer servidor WAP compatível, indiferentemente do fabricante. Igualmente, os fabricantes de servidores WAP compatíveis estão seguros que qualquer dispositivo WAP conectará corretamente com os seus servidores.

## 3.3 A Diferença da Rede

As Redes de dados *wireless* apresentam um ambiente de comunicação mais limitado, comparado com as redes comuns. Por causa de limitações fundamentais de potência, espectro disponível e mobilidade. Redes de dados *wireless* tendem a ter [WAP98]:

- ♦ menor largura de banda;
- ♦ mais latência;
- ♦ menos estabilidade de conexão;
- ♦ disponibilidade imprevisível;

Além disso, com aumentos de largura de banda, o consumo de potência do dispositivo portátil, também impõe um aumento de consumo na já limitada carga da bateria, de um dispositivo móvel. Então, até mesmo com as melhorias das redes *wireless* com a habilidade de entregar largura de banda mais alta, a disponibilidade de potência ao dispositivo portátil ainda limitará o processamento efetivo de dados para o dispositivo. Uma solução de dados *wireless* deve poder superar estas limitações de rede e ainda disponibilizar uma experiência satisfatória ao usuário, conforme Figura 3.2.

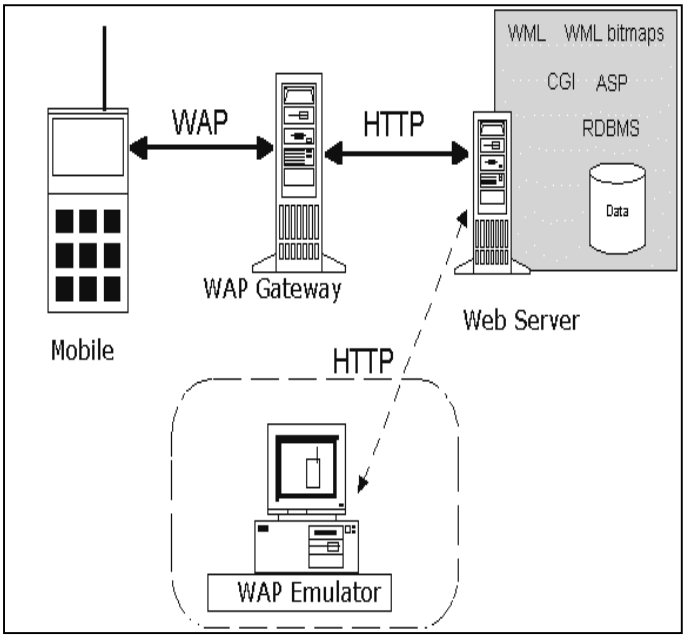


FIGURA 3.2 – REDE WAP

## 3.4 Diferenças do Dispositivo WAP

Os dispositivos *wireless* apresentam várias limitações quando comparados a computadores *desktop*. Devido a estas limitações fundamentais de bateria e ergonomia, estes dispositivos tendem a ter [WAP98]:

- CPU's menos poderosas;
- menos memória (ROM e RAM);
- consumo de potência restringido;
- telas menores;
- dispositivos de contribuição diferentes (por exemplo, um teclado telefônico complementar, contribuição de voz, etc.).

Por causa destas limitações, a interface de usuário de um dispositivo *wireless* é diferente da de um computador *desktop*. O tamanho de tela limitado e a falta de um mouse requerem uma metáfora de interface de usuário diferente que o *desktop* GUI (*Guide User Interface*) tradicional.

Não é provável que estas condições mudem dramaticamente no futuro próximo. Os dispositivos portáteis *wireless* mais populares foram projetados para serem leves e adequarem-se ao formato da mão. Além disso, consumidores desejam dispositivos portáteis com bateria de duração mais longa, o que sempre vai limitar a largura de banda disponível, e o consumo de potência da CPU, memória e exibição.

## 3.5 Modificação dos modelos da *WWW* para utilização em WAP

O modelo WAP é bastante similar ao modelo *internet*, os desenvolvedores do WAP basearam o projeto sobre idéias e padrões existentes. Isto deu mais razões para desenvolvedores de conteúdo implementarem serviços e produtos visando transferência de dados. Esta tentativa de produzir um ambiente coerente com a estrutura já existente, não está apenas no nível de transferência de dados, mas também no modo como os desenvolvedores poderiam comunicar estas informações através de uma linguagem comum. Muitas das características descritas abaixo [WAP00a] demonstram este modelo e mostram como implementações existentes tem sido modificadas para serem utilizadas no modelo WAP.

### 3.5.1 HDML (Handheld Device Markup Language) e WML (Wireless Markup Language)

O HDML é a linguagem que oferece ao programador ferramentas para produzir conteúdo para um dispositivo WAP. O WML é também uma linguagem de *markup* (marcadores) utilizada como interface para o WAP *browser*, mas permite que um programador

desenvolva simultaneamente aplicações *WWW* que podem ser vistas dentro de um *browser* tradicional e dentro de um dispositivo WAP.

### 3.5.2 Otimização de Transferência de Dados

É importante lembrar que a comunicação entre dispositivos sem fio é bastante lenta (por volta de 9.600 kbps). Por esta razão, os desenvolvedores WAP concentraram-se em otimizar os protocolos existentes tais como o HTTP (*Hyper Text Transfer Protocol*) e o TCP (*Transmission Control Protocol*) para maximizar a transferência de dados e utilizar pouca taxa de transmissão em conta.

### 3.5.3 Independência de Sistema Operacional

O WAP pode ser usado em qualquer sistema operacional, incluindo plataformas populares de *handhelds* como *Palm OS*, *Windows CE* e *Java OS*. Ele também é compatível com *Windows 95/98/NT*, *Linux*, *Solaris*, etc. Isto é devido ao fato do protocolo ser dependente de padrões de comunicação ao invés de estarem baseados nas plataformas. Qualquer plataforma capaz de implementar os padrões de comunicação é compatível com WAP.

# 4 Arquitetura WAP

A principal característica do padrão WAP é a utilização de vários protocolos já existentes na *internet*, como os de comunicação TCP/IP e UDP/IP, os de "conversão" de linguagem XML e HTML, os de programação como CGI, Perl e ASP, os de comunicação HTTP, e protocolos de segurança SSL [WAP98].

A arquitetura WAP obedece à estrutura demonstrada na figura 4.1.

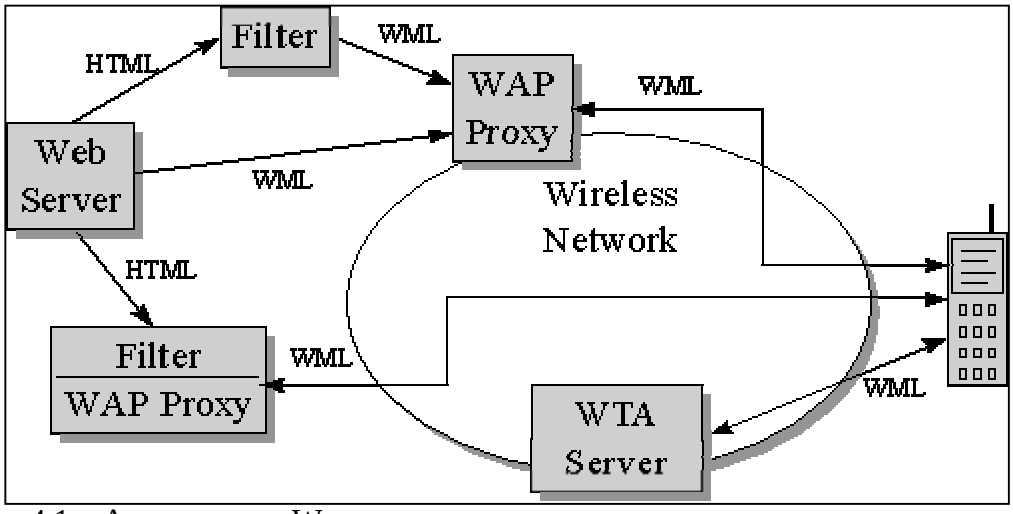


FIGURA 4.1 - ARQUITETURA WAP

O modelo de programação do WAP é similar ao modelo *WWW*, como visto anteriormente. Isto provê vários benefícios à comunidade de desenvolvimento, incluindo a familiarização com o modelo existente, a confiabilidade de uma arquitetura testada e a possibilidade de utilização de ferramentas existentes (como servidores *Web*, editores XML, etc).

Entretanto, otimizações e extensões foram realizadas de forma a adaptar este modelo a realidade de ambientes móveis. Sempre que possível os padrões existentes foram adotados ou utilizados como base para desenvolvimento da tecnologia WAP.

O conteúdo e as aplicações WAP foram especificadas através de um conjunto de formatos bem conhecido, baseado nos conteúdos utilizados na *WWW* tradicional. Os dados são transportados utilizando um conjunto de protocolos de comunicação baseados nos protocolos utilizados na *internet* e o *micro-browser* de um dispositivo móvel foi especificado de forma análoga ao *browser WWW*.

O *browser* interpreta e exibe conteúdo desenvolvido para o ambiente WAP. Esse conteúdo é criado através da linguagem WML (*Wireless Markup Language* ou Linguagem de Marcação *Wireless*). A WML é semelhante a HTML que é usada na criação de páginas da *WWW*. Mas, ao contrário da linguagem HTML, a linguagem WML foi criada para atender às necessidades dos dispositivos e redes *wireless*.

Para acrescentar recursos dinâmicos às aplicações WML, utiliza-se a linguagem WMLScript, uma linguagem semelhante a JavaScript. Tanto WML como WMLScript são adaptadas e otimizadas para utilização em ambiente *wireless*.

Na *WWW*, os ***sites*** (locais) são constituídos de páginas. Páginas são arquivos com extensão .html. A primeira página de um *site* é a *Home page*. Na rede *wireless* o *mini-site* é chamado de *deck* (maço, grupo ou conjunto) e a *mini-page* é chamada de *card*. *Deck*, um arquivo com extensão .wml. *Card* é o conteúdo de uma única mini- tela. Um *site* é um conjunto de pages. Um *deck* é um conjunto de *cards*. Mas as telas dos celulares estão crescendo, já podem ser roladas, os PDA's têm mini-telas "gigantes" e o jargão que vai se firmando já era esperado: *mini-sites* ou "WAP *sites*", *mini-pages* ou "WAP pages", "WAP *phones*" (celulares WAP), WAP *browsers*, etc. No entanto, no código da linguagem WML os textos das WAP pages estão contidos entre as *tags* <*card*> e </*card*> e isto não vai mudar.

O WAP definiu um conjunto de componentes padronizados que permitem a comunicação entre terminais móveis e servidores de rede, incluindo [WAP98]:

- ♦ modelo de Nomenclatura Padrão - O padrão WWW de URLs foi utilizado para identificar o conteúdo WAP nos servidores de origem. Outro padrão WWW, o URI, foi utilizado para identificar recursos locais num dispositivo, como funções de controle de chamadas;
- ♦ tipagem de Conteúdo - Todos os conteúdos WAP possuem um tipo de conteúdo específico, consistente com o modelo WWW;
- ♦ formato de Conteúdo Padrão - O formato de conteúdo WAP é baseado na tecnologia WWW e inclui marcações de visualização, informação de agenda, cartões de visita, imagens e linguagem de *script*;
- ♦ protocolos de Comunicação Padrão - Os protocolos WAP permitem a transmissão de pedidos do *browser* para o servidor de rede *WWW*.

## 4.1 WAP *gateway*

O *WAP gateway* (também conhecido por *WAP Proxy*) é um *software* que basicamente realiza uma conexão entre o cliente (dispositivo móvel) e o servidor (HTTP *Server*, HTTP *Proxy* etc.).

O WAP gateway possui as seguintes funcionalidades [PHO99]:

♦ *gateway* de protocolo - o *gateway* de protocolo traduz pedidos do protocolo WAP ao protocolo *WWW* (HTTP e TCP/IP);

♦ codificadores e Decodificadores de conteúdo - o codificador de conteúdo traduz o conteúdo da Wap para um formato de código compactado (*bytecode*), com a intenção de reduzir o tamanho e o número de pacotes que trafegam na rede de dados *wireless*;

A infra-estrutura criada, certifica que os usuários de terminais móveis possam navegar por uma grande variedade de aplicações e conteúdo WAP, certifica também que o

autor da aplicação tenha condições de criar serviços de conteúdo que sirvam a uma grande base de terminais.

Devido ao WAP *gateway*, os conteúdos e aplicações são hospedados em servidores *WWW* e podem ser desenvolvidos utilizando aplicações *WWW* como CGI *scripts*, conforme figura 4.2.

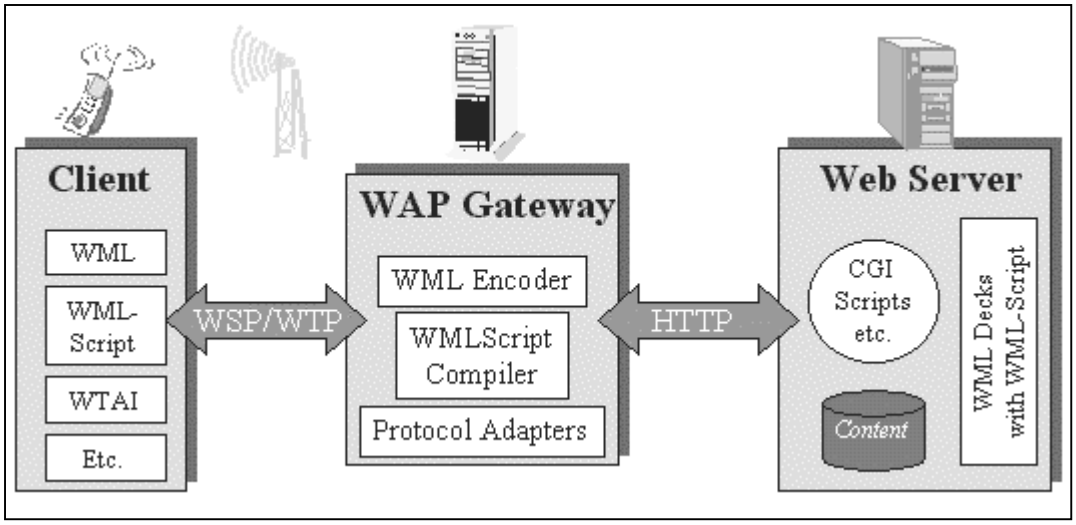


FIGURA 4.2 - FUNCIONALIDADE DO WAP *GATEWAY*

O WAP *gateway* diminui o tempo de resposta do dispositivo portátil, agregando dados de diferentes servidores na *WWW* e guardando informações freqüentemente acessadas. O WAP *gateway* também pode se conectar a bancos de dados de assinantes e utilizar informações da rede *wireless*, tais como informação de localização, para personalizar as páginas WML de acordo com o usuário. Tal servidor pode ser utilizado para facilitar soluções *end-to-end* de segurança ou aplicações que requerem um melhor controle de acesso ou resposta, como o WTA.

### 4.1.1 Influência da Tecnologia *Proxy*

A especificação WAP utiliza o padrão de tecnologia *proxy*, existente na *WWW* para conectar o domínio *wireless* com a *WWW* [PHO99]. Utilizando os recursos de computação no WAP *gateway* , a arquitetura WAP permite que os dispositivos portáteis sejam simples e baratos. Por exemplo, um WAP *gateway* vai tipicamente acessar todos os servidores DNS para resolver os nomes de domínios usados nas URLs, assim assumindo, esta tarefa computacional dos dispositivos portáteis, conforme demonstrado na figura 4.3.

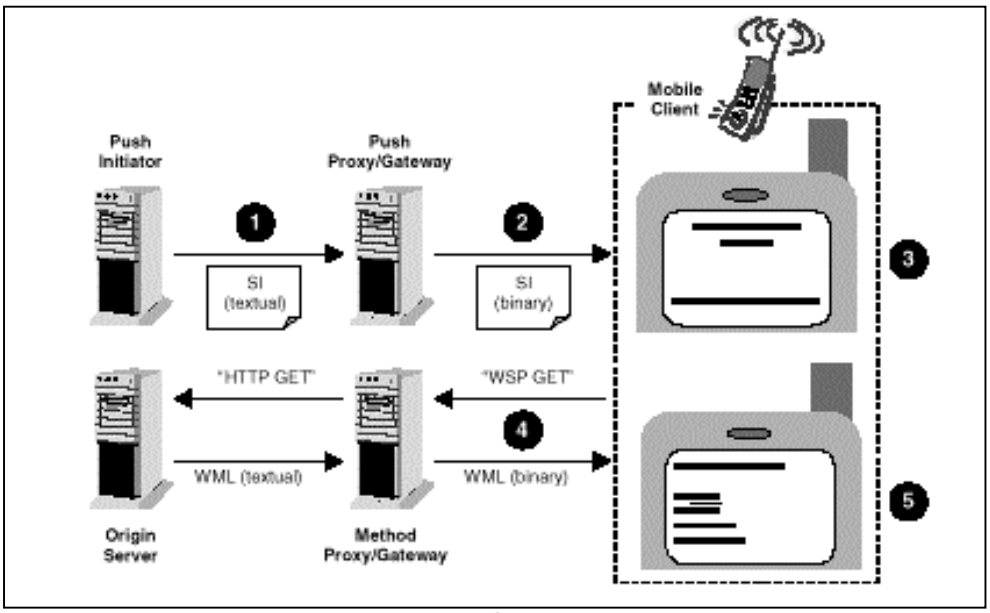


FIGURA 4.3 - ACESSO AOS SERVIDORES ATRAVÉS DO WAP *PROXY*

O WAP *gateway* também pode ser utilizado para disponibilizar serviços aos assinantes e proporcionar ao operador de rede um ponto de controle para administrar as fraudes e a utilização dos serviços, conforme Figura 4.4.

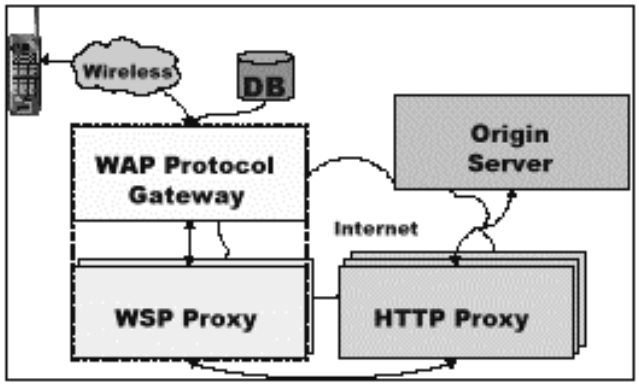


FIGURA 4.4 - ARQUITETURA WAP *PROXY*

### 4.1.2 A transmissão de Dados

O padrão WAP define um ambiente de aplicações e protocolos de aplicações. Ele também define a tecnologia conhecida como WTA (*Wireless Telephony Application* ou Aplicações em Telefonia *Wireless*).

A finalidade de WTA é fornecer meios para criar serviços de telefonia (voz) utilizando WAP. A interface entre as funções relacionadas à telefonia no dispositivo WAP

é chamada de WTAI (*Wireless Telephony Application Interface* ou Interface para Aplicações de Telefonia *Wireless*).

Quando o WAP *browser* é utilizado para solicitar informação, o pedido da URL é enviado utilizando os protocolos WAP. Esse pedido é enviado através da rede *wireless* para o WAP *gateway* . O *gateway* permite aos usuários da rede *wireless* conectarem-se à *Internet*.

Quando a solicitação recebida é decodificada, o *gateway* executa algumas tarefas, então a solicitação decodificada é convertida do protocolo WSP (no padrão WAP) para o protocolo da *internet* HTTP. A seguir, o que acontece é o envio dessa requisição para o *Web Server* através da *Internet*. O *Web Server* recebe, lê a requisição e retorna uma resposta com conteúdo WML para o WAP *gateway* .

O WAP *gateway* recebe o conteúdo WML do Servidor *Web* e o converte para o padrão *bytecode* do WAP, codificando a informação para um formato binário de forma que possa ser utilizada menor largura de banda.

O conteúdo codificado é criptografado e enviado através da rede *wireless* para o WAP *browser*. O *browser* recebe a resposta do WAP *gateway* e a exibe na tela do dispositivo WAP conforme figura 4.4.

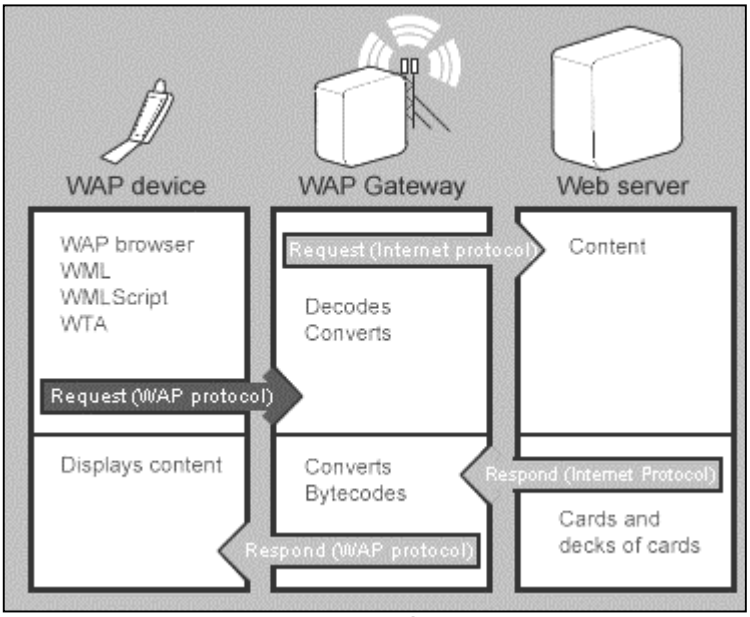


FIGURA 4.4 - REQUISIÇÃO E RESPOSTA DE CONTEÚDO WAP

## 4.2 Pilha de Protocolos

Apesar de ser visto como um protocolo, na verdade o WAP é uma pilha composta por cinco (05) protocolos independentes, organizados em um ambiente escalável e extensível para o desenvolvimento de aplicações direcionadas a utilização em dispositivos

móveis. Isto foi alcançado através da construção de uma pilha de protocolos dividida em camadas, conforme figura 4.5.

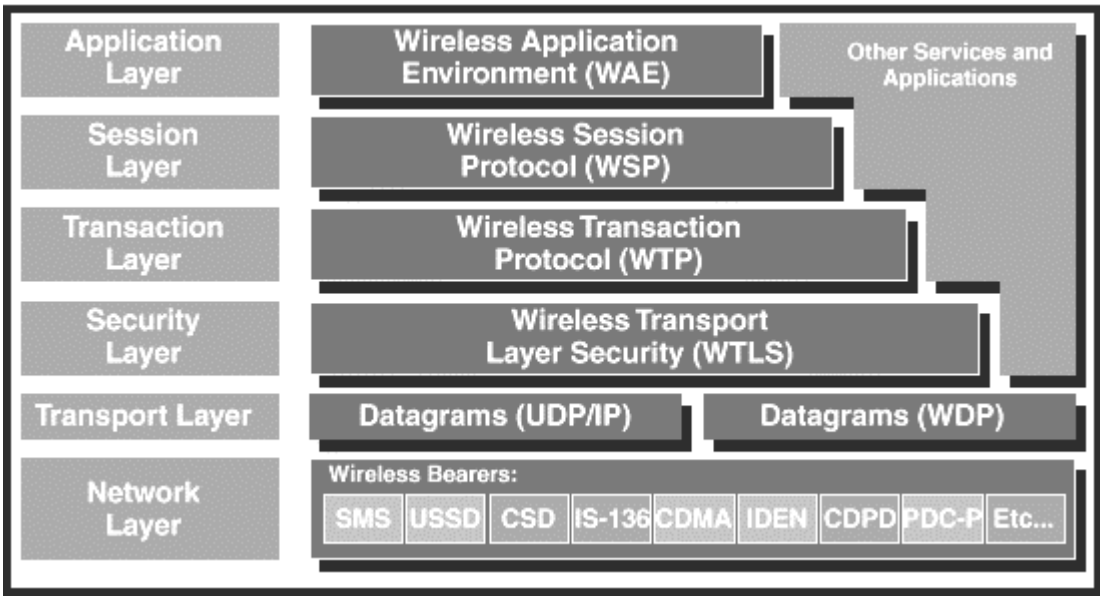


FIGURA 4.5 – PILHA DE PROTOCOLOS WAP

A divisão em camadas permite que outros serviços e aplicações utilizem as características da pilha WAP através de um conjunto de interfaces bem definidas. Aplicações externas podem, desta forma, acessar as camadas *Session*, *Transaction*, *Security* e *Transport* diretamente [WAP98].

A pilha de protocolos isola a aplicação das operadoras. Isto torna possível que as aplicações sejam executadas, independentemente do serviço de transporte utilizado.

### 4.2.1 Camada de Aplicação – Wireless Application Environment (WAE)

O WAE é a camada responsável por estabelecer um ambiente interativo onde operadoras e prestadores de serviços poderão construir aplicações que alcançarão um grande número de plataformas sem fio de uma maneira eficiente. O WAE inclui um ambiente de *micro-browser* contendo as seguintes funcionalidades:

- *Wireless Markup Language* (WML), uma linguagem de marcação leve, similar ao HTML, mas otimizada para utilização em dispositivos móveis;
- WMLScript, uma linguagem de *script* leve, similar ao JavaScript;
- serviços de telefonia e interfaces de programação: *Wireless Telephony Application* (WTA, WTAI);

- um conjunto de formatos de dados bem definidos, incluindo imagens, registros de agenda de telefones e de compromissos.

O WAE assume a existência de funcionalidades de *gateway* responsáveis pela codificação dos dados transferidos para o cliente móvel. O objetivo da codificação dos dados é minimizar o tamanho desses dados enviados por ar, e a utilização de recursos necessário para o cliente processar esses dados. A funcionalidade do *gateway* pode ser adicionada a servidores já existentes ou colocada em *gateways* dedicados, como mostra a figura 4.6.

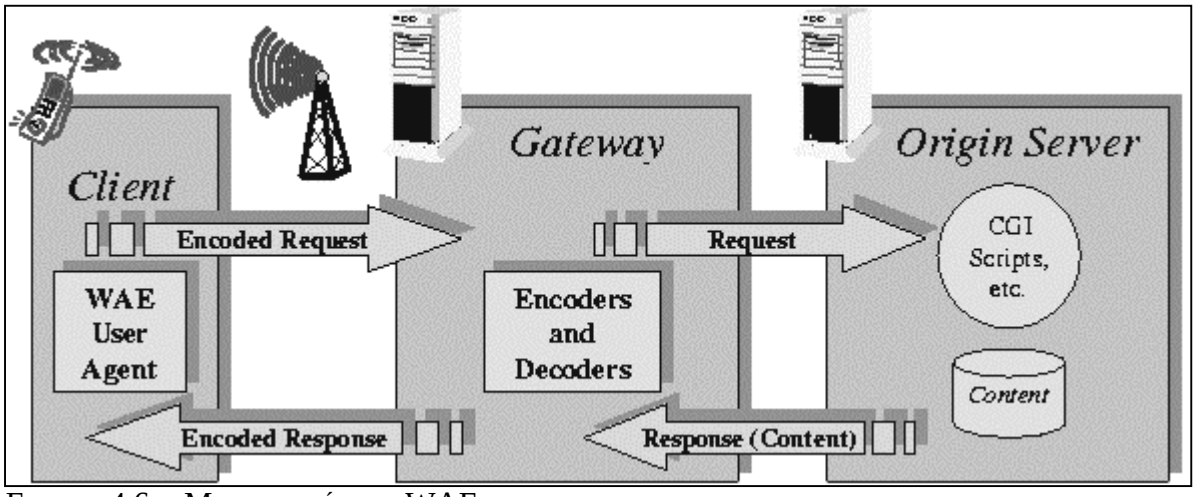


FIGURA 4.6 - MODELO LÓGICO WAE

O resultado da arquitetura WAE, será um modelo que oferece as seguintes vantagens:

- tira vantagem dos padrões, tecnologia e infra-estrutura desenvolvidas para a *internet;*
- disponibiliza Serviços de Rede Móvel avançados ao usuário, através de serviços de telefonia controlados pelo operador da rede;
- fornece uma área de trabalho extensa para a construção de serviços *wireless*.

### 4.2.2 Camada de Sessão – Wireless Session Protocol (WSP)

O WSP disponibiliza para a camada de aplicação do WAP com uma interface consistente para dois serviços de sessão. O primeiro é o serviço orientado a conexão, que opera sobre o protocolo de transação WTP. O segundo é o serviço não orientado a conexão, que opera sobre o serviço de datagrama seguro ou não (WDP).

O WSP atualmente consiste em serviços adequados para aplicações de *browsing* (WSP/B) que oferece as seguintes funcionalidades:

- funcionalidades e semântica do HTTP/1.1 através de uma codificação compacta;
- estado de sessão de longa vida;
- suspensão e retomada de sessões;
- facilidades na utilização de tecnologia push;
- protocolo para negociação de capacidades.

Os protocolos da família WSP são otimizados para uma banda de conexão baixa, com latência relativamente longa. WSP/B foi projetado para permitir que um *proxy* WAP conecte um cliente WSP/B a um servidor HTTP comum.

### 4.2.3 Camada de Transação – *Wireless Transaction Protocol* (WTP)

O WTP é executado no topo de um serviço de datagramas, provendo um protocolo orientado a conexão leve, utilizado em dispositivos móveis, como telefones celulares. O WTP opera eficientemente sobre datagramas, disponibilizando os seguintes serviços:

- três classes de serviços de transação;

  Requisições *one-way* (pedidos) não confiáveis

  Requisições *one-way* (pedidos) confiáveis

  Requisições *two-way* (pedidos e respostas) confiáveis.

- confiabilidade opcional *user-to-user* - O usuário ativa a confirmação a cada mensagem recebida;
- concatenação de PDU e reconhecimento do atraso para reduzir o número de mensagens enviadas;
- transações Assíncronas.

### 4.2.4 Camada de Segurança – *Wireless Transport Layer Security* (WTLS)

O WTLS é um protocolo de segurança baseado no protocolo TLS (*Transport Layer Security*), também conhecido como *Security Sockets Layer* (SSL).

O WTLS disponibiliza os seguintes serviços:

- integridade de Dados - O WTLS contém dispositivos que asseguram que os dados transmitidos entre o terminal e um servidor de aplicações não foram modificados ou corrompidos;
- privacidade - WTLS contém dispositivos que asseguram que os dados transmitidos entre o terminal e o servidor de aplicações não podem ser compreendidos por ninguém que tenha interceptado o fluxo de dados;
- autenticação - permite facilidades que estabeleçam a autenticidade do terminal e do servidor de aplicações;
- detecção e rejeição de dados incorretamente enviados.

### 4.2.5 Camada de Transporte – *Wireless Datagram Protocol* (WDP)

O WDP opera sobre os serviços dos portadores de dados disponíveis nos diferentes tipos de redes. Como um serviço geral de transporte de dados, o WDP oferece uma forma consistente de transmissão de pacotes das camadas superiores da pilha WAP. Desta forma, as camadas de Segurança, Sessão e Aplicação podem funcionar independentemente da rede sem fio utilizada, como está demonstrado na figura 4.7.

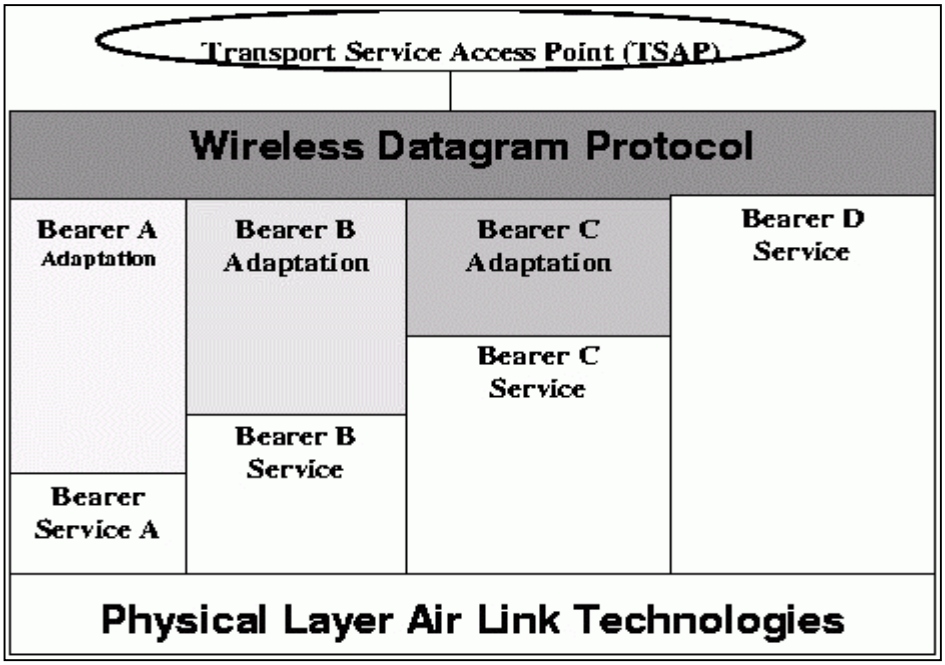


FIGURA 4.7 - CAMADA WDP

O WDP oferece um serviço consistente no Ponto de acesso ao Serviço de Transporte (TSAP) ao protocolo de nível superior do WAP. Esta consistência de serviços permite às aplicações trabalharem de forma transparente sobre os diferentes serviços portadores (*bearer services*) disponíveis. A variação de níveis entre cada um dos serviços portadores ilustra a diferença nas funções fornecidas através dos portadores e

conseqüentemente a diferença no protocolo WDP necessária para operar sobre esses portadores para poder manter a mesma oferta de serviço no Ponto de acesso ao Serviço de Transporte. Isto é conseguido através da adaptação ao portador. O WDP pode ser mapeado para diferentes portadores, com características diferentes. Para otimizar o protocolo com respeito à utilização de memória e eficiência da transmissão de rádio, o desempenho do protocolo sobre cada portador pode variar. Contudo, as primitivas de serviço do protocolo WDP permanecerão as mesmas, mantendo uma interface consistente para as camadas superiores.

## 4.3 Camada de Rede – Portadoras

A camada de protocolos WAP foi projetada para operar sobre uma variedade de serviços de portadoras, incluindo *short message* (SMS), *circuit-switched data* (CSD) e pacotes de dados. Cada uma das portadoras oferece um nível de qualidade de serviço diferente em relação à velocidade de transmissão, taxa de erros e atrasos. A rede portadora é responsável pelo encaminhamento de datagramas até ao dispositivo destino. O endereçamento varia conforme o tipo de rede portadora (endereços IP ou números de telefone). Algumas redes utilizam alocação dinâmica de endereços, e é necessário utilizar um servidor para encontrar o endereço atual de um certo dispositivo. Os endereços de rede dentro da pilha WAP podem incluir o tipo de portadora e o endereço (ex.: IP; 123.456.789.123). Os protocolos WAP foram projetados de forma a compensar ou tolerar estas diferenças.

### 4.3.1 Independência do Portador

Para o melhor endereçamento das necessidades da possível população de usuários final, o protocolo de aplicação *wireless* é projetado para otimizar o trabalho com todas as interfaces aéreas. Este princípio permite que um número maior de provedores de serviço, pesquisadores de *software* e fabricantes de dispositivos portáteis se beneficiem com uma única especificação.

Provedores de Serviços podem implementar uma solução comum através das próprias redes, de forma que todo assinante tenha a melhor satisfação possível dos usuários em cada rede. Aplicações podem ser desenvolvidas utilizando um padrão que trabalhará sobre uma variedade de redes. Fabricantes de dispositivos portáteis podem utilizar o mesmo *software* em todas as linhas de produto, reduzindo o tempo de desenvolvimento e simplificando o suporte.

A Interface aérea sendo independente também torna mais fácil a extensão da especificação. Como interfaces aéreas ficam mais sofisticadas, os serviços, que eles disponibilizarem poderá ser projetado para obedecer à especificação WAP, encorajando a utilização de um padrão para todas as redes.

Apesar do WAP ser independente do ambiente portador, o ambiente mais utilizado é o GSM, devido a sua grande aceitação. Por este motivo será realizada uma breve descrição sobre seu funcionamento no capítulo que trata de telefonia celular.

# 5 Telefonia Celular

## 5.1 Group Special Mobile (GSM)

Na década de 80, sistemas de telefones celulares analógicos, foram desenvolvidos na Europa, especialmente na Escandinávia, Reino Unido, França e Alemanha. Foram desenvolvidos diversos sistemas, o que levou a incompatibilidades entre eles, devido à forma de envio de dados, protocolos e freqüência de comunicação. Em 1982 foi realizada a "*Conference of European Posts and Telegraphs* (CEPT)" onde se formou um grupo denominado "Group Special Mobile (GSM)", com o objetivo de estudar e desenvolver um sistema móvel que obedecesse alguns padrões [GSM99]:

- boa qualidade de voz;
- eficiência espectral;
- terminais pequenos e baixos custos;
- suporte para "*roaming*" internacional;
- capacidade para suportar terminais "*handheld"*;
- suportar uma larga área de novos serviços e utilidades;
- compatibilidade ISDN.

Em 1989 a responsabilidade passou para o "*European Telecomunication Standards Institute* (ETSI)" onde em 1990 foram publicadas as especificações do GSM. Tal padrão generalizou-se então pelo resto do mundo.

### 5.1.1 Descrição do sistema

Uma rede GSM é composta por várias entidades com funções e interfaces específicas. A rede GSM pode ser dividida em três partes: a estação móvel, a estação de subsistema base, e o subsistema de rede, conforme demonstrado na figura 5.1.

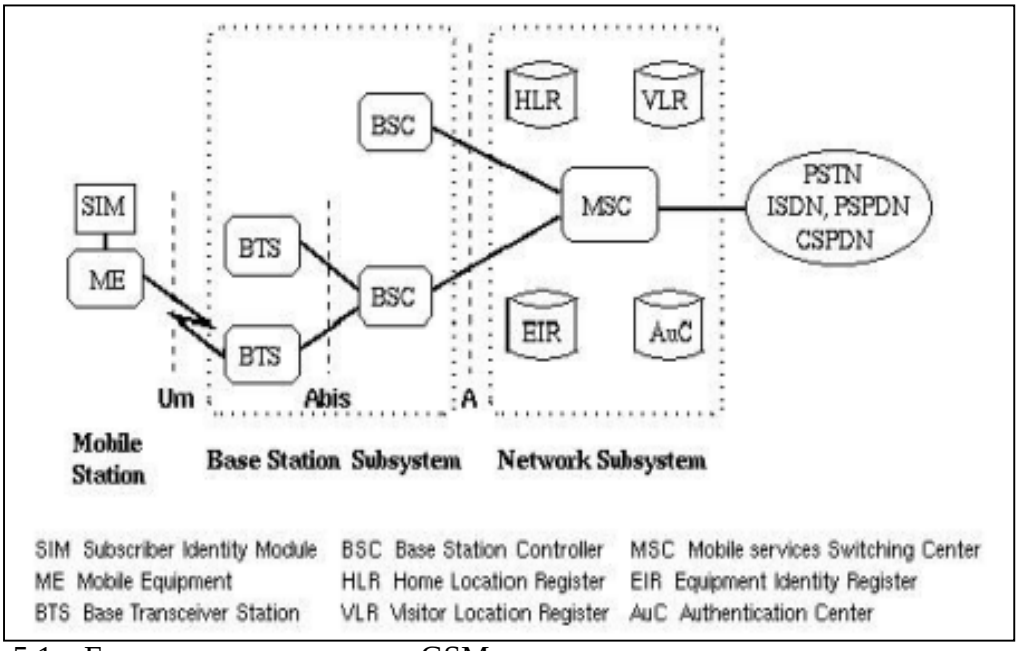


FIGURA 5.1 - ESTRUTURA DE UMA REDE GSM

A Estação móvel (terminal) é um cartão inteligente designado de SIM. O cartão providencia mobilidade pessoal, de tal forma que o assinante consegue ter acesso aos serviços subscritos independentemente do terminal utilizado, isto é, ao inserir o cartão SIM num terminal diferente, o assinante pode usufruir os serviços a partir desse terminal. O cartão SIM tem uma identificação única mundial (IMSI), assim como o terminal (IMEI). Estes códigos são independentes permitindo uma maior mobilidade e uma segurança pessoal contra o uso não autorizado.

O subsistema rádio base encarrega-se do controle de ligação rádio com a estação móvel. É dividido em duas partes: a estação rádio base de transmissão (BTS) e a estação rádio base de controle (BSC). A comunicação entre estas duas estações é realizada através de uma interface que permite (como no resto do sistema) a operação entre componentes realizada por diferentes fornecedores. A BTS aloja os receptores-transmissores de rádio que definem a célula e suportam os protocolos de ligação rádio com a estação móvel. Numa grande área urbana a quantidade de BTS's deverá existir em maior número. A BSC gerência os recursos para uma ou mais BTS's, tais como, configuração dos canais rádio, saltos de freqüência e transição entre células *(hand-off*). A BSC realiza a conexão entre as estações móveis (celulares) e o centro de comutação móvel (MSC).

O principal componente do subsistema rede é o MSC, que se encarrega de fazer a comutação de chamadas entre estações móveis ou entre uma estação móvel e um terminal fixo. Comporta-se como um nó de comutação de PSTN ou ISDN, e adicionalmente providencia toda a funcionalidade necessária para o tratamento de um assinante móvel, realizando o registro, autenticação, atualização da localização, transição entre células (*Hand-off*) e gerenciamento de um assinante em *roaming*. Estes serviços são

providenciados em conjunto com várias entidades funcionais que juntas formam o subsistema rede: MSC, HLR, VLR, EIR, AuC. O HLR, o VLR e o MSC, em conjunto providenciam as capacidades de *roaming* do GSM.

O HLR (*Home Location Register*) contém toda a informação administrativa de todo assinante registrado na correspondente rede de GSM, juntamente com a localização da estação móvel. A localização da estação móvel está geralmente na forma do endereçamento do VLR (*Visitor Location Register*). As informações fornecidas pelo VLR, são necessárias para controlar a chamada e providenciar os serviços de cada assinante, situada dentro de uma determinada área de controle. Outros dois registros são usados para segurança e autenticação. O EIR é uma base de dados que contém listagens de todos os equipamentos móveis válidos na rede, onde todas as estações móveis são identificadas pelo IMEI. Um IMEI é considerado como inválido se declarado como roubado ou incompatível com a rede. O AuC é uma base de dados protegida que guarda uma cópia do código de cada SIM, que é usado para autenticar e criptografar através do canal de rádio.

### 5.1.2 Codificação de canal e voz

A voz em GSM é codificada digitalmente a uma taxa de 13 Kbps (260 *bits* transmitidos a cada 20ms.). Com a adição posterior de código para a correção de erros, passa-se a ter uma taxa de 22.8 Kbps (456 *bits* cada 20ms). Estes 456 *bits* são divididos em 8 blocos de 57 *bits*, e o resultado é o envio de 8 *slots* de tempo sucessivo, para proteção contra erros de transmissão. Cada envio tem 156.25 *bits* e contém 2 blocos de 57 *bits*, e uma seqüência de treinamento de 26 *bits* usada para equalização. Cada envio é transmitido em 0.577ms. para uma taxa total de 270.8 Kbps, e é modulada utilizando GMSK numa portadora de 200 kHz. O controle de erro e equalização contribuem para a robustez do sinal rádio contra interferência e atenuação na transmissão. A natureza digital do sinal TDMA permite a utilização de vários processos para melhorar a qualidade de transmissão, o tempo de vida útil da bateria, e a eficiência espectral.

Outra característica do GSM é o controle de potência, que minimiza a potência de transmissão das estações móveis e da BTS, e assim minimiza a interferência gerada nos canais e o consumo.

## 5.2 Roteamento da Transmissão

Conforme descrito em [LAD00], para a implantação da telefonia móvel celular, subdivide-se a área geográfica em pequenas células hexagonais, cada uma dispondo de uma estação de rádio-base e de conjuntos de antenas direcionais para supervisão e controle das suas radiofreqüências disponíveis. Estações rádio-base são conectadas ao "Terminal de Controle", estes são conectados entre si e com a "Rede Nacional e Internacional de Telefonia". Terminais de Controle são centros de comutação de rádio-freqüência e interligação com o sistema telefônico convencional.

O telefone celular, em trânsito por determinada área, quando deseja realizar uma chamada, envia uma mensagem ao rádio-base. Essa mensagem, após ser processada e aceita pelo Terminal de Controle, implica a conexão do telefone celular à estação telefônica

celular através da concessão de uma rádio-freqüência disponível. Todas as transmissões são "*full duplex*", com um canal de transmissão e outro de recepção.

A passagem do assinante de um setor para outro, dentro da mesma célula, fica a cargo dos equipamentos de controle internos à célula. Quando o assinante move-se de uma célula para outra, o procedimento é diferente. Ao verificar a apresentação de um nível mínimo de recepção do sinal na célula de origem, o Terminal de Controle comuta o assinante para uma rádio-freqüência disponível em uma célula vizinha. A rádio-freqüência utilizada na célula de origem é desalocada e torna-se disponível para nova alocação. Muitos sistemas celulares esperam em torno de 100 milisegundos, após a liberação da radiofreqüência de origem, antes de alocar nova rádio-freqüência na célula vizinha. Este atraso não ocasiona descontinuidade na comunicação de voz, mas causa problemas na transmissão de dados. Dentro do setor, as células são projetadas de forma a garantir que a razão entre o sinal recebido e o ruído na transmissão nas fronteiras da célula seja, no mínimo, 18dB. Este valor é significantemente menor do que em um sistema telefônico convencional que, no pior caso, apresenta razão de 26dB, para canal de voz. Para compensar esse fato, são instaladas de 3 a 4 antenas direcionais em cada célula, dividindo-a em setores. Quando uma estação é ligada ou entra na área de cobertura de um ponto de acesso, inicia-se o processo de associação. Ao deslocar-se de uma região coberta por um ponto de acesso para outro ponto de acesso, o processo realizado é de reassociação. Uma única célula pode cobrir a área de 5000 metros quadrados.

### 5.2.1 Estrutura da Célula

O tamanho de cada célula hexagonal é definido através da potência dos transmissores do telefone celular e pela atenuação do sinal, sendo que este pode ser escutado na sua célula e, no máximo, nas células vizinhas. Cada célula possui um grupo específico de radiofreqüências. Como existe um número limitado de radiofreqüências disponíveis para comunicação, elas são utilizadas mais de uma vez, mas células vizinhas têm que possuir grupos diferentes de rádio-freqüência para evitar que haja interferência entre elas. O padrão de reutilização de freqüências conhecido como 1-em-7 é comumente utilizado em telefonia celular e está representado na figura 5.2.

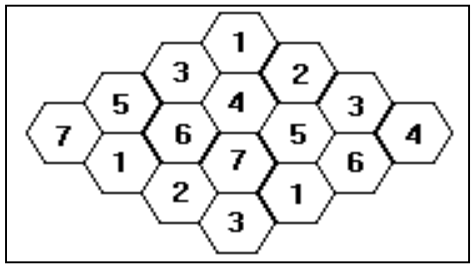


FIGURA 5.2 - PADRÃO 1-EM-7

## 5.3 A norma IEEE 802.11

Com a crescente utilização de redes com *Wireless*, o IEEE formou um grupo para desenvolver a norma da camada de acesso ao meio (*Medium Access Control* - MAC) e a norma da camada Física (*Physical Layer* - PHY). Esse grupo dá origem ao IEEE 802.11 que é o padrão para transmissões *Wireless*.

Na norma IEEE 802.11 cada computador, móvel, portátil ou fixo é definido como sendo uma estação. A diferença entre estação portátil e estação móvel verifica-se pelo fato de uma estação portátil mover-se de ponto a ponto embora apenas seja usado num ponto fixo, enquanto que a estação móvel não se restringe a limitações físicas durante o movimento [IEEE99]. Quando duas ou mais estações se juntam, para comunicar-se, formam um conjunto de serviços básicos (*Basic Service Set* - BSS). O mínimo BSS consiste em duas estações. A norma 802.11 utiliza o BSS como fundamento para a comunicação.

Um BSS que não está ligado a uma base é visto como um BSS independente (IBSS) ou como uma rede *Ad-Hoc*, que é uma rede onde as estações comunicam-se apenas utilizando *peer-to-peer*. Não existe uma base e não é dado, por ninguém, a permissão para falar, a maioria destas redes são espontâneas e podem ser criadas rapidamente. As redes IBSS têm como características o fato de serem limitadas tanto em tempo como em espaço.

Uma vez ligado um BSS a uma rede, esta une-se à infra-estrutura da rede. A infra-estrutura da norma 802.11 tem vários elementos: dois ou mais BSS são ligados utilizando um sistema de distribuição (*Distribution System* - DS). Este conceito de DS aumenta a cobertura da rede permitindo a cada BSS passar a ser um componente de uma rede mais ampla. Acessos ao Ds é concretizado através de pontos de acesso (*Access Points* - AP), que é uma estação, o que permite que possa ser endereçada. Os dados movimentam-se através de BSS e DS utilizando estes pontos de acesso.

Criar redes maiores e mais complexas utilizando BSS e DS, obriga a seguir para o próximo nível da hierarquia, ou seja, para o conjunto de serviços estendidos (*Extended Service Sets* - ESS). Para o ESS, a rede apresenta-se como um conjunto de serviços básicos (BSS) para a camada *Logical Link Control* (LLC), o que indica que estações podem comunicar-se ou até mover-se através de BSS, dentro do ESS, com total transparência na camada LLC, permitindo um controle independente das camadas inferiores.

Um dos requisitos da norma 802.11 é que é possível utilizar-se em redes convencionais (ligados com cabos) já existentes, o que se torna viável através do uso de um Portal. Um Portal é uma integração lógica entre redes convencionais e redes *Wireless*, utilizando a norma 802.11. Podem também servir como pontos de acesso para o DS. Os dados partindo de uma rede 802.11 para uma rede 802.x deverão passar por um portal, funcionando assim como uma ponte entre *Wireless* e rede convencional.

A independência de DS não é especificada na norma 802.11, por isso o sistema de distribuição pode ser criado a partir de tecnologias rivais ou já existentes. Uma *Bridge*

ponto-a-ponto, ligando dois edifícios, poderá ser um DS. Enquanto que a implementação de DS não seja especificada, a norma 802.11 especifica o que o DS deve suportar. Os serviços estão divididos em duas seções, Serviços de Estações (*Station Services* - SS) e Serviço do Sistema de Distribuição (*Distribution System Services* - DSS).

Existem 5 serviços fornecidos pelo DSS: Associação, Re-associação, Desassociação, Distribuição e Integração. Os três primeiros serviços focam a mobilidade da estação. Se a estação está movendo-se dentro do próprio BSS ou não, se estiver deslocando a mobilidade da estação e defini-la como intransitória. Se uma estação move-se entre BSS no mesmo ESS, então a mobilidade da estação é BSS - transição. Se a estação se desloca entre BSS de diferentes ESS, então pertence à categoria ESS - transição.

Uma estação deve-se associar a uma infra-estrutura BSS, quando deseja utilizar a rede. Este efeito é conseguido associando-se a estação a um ponto de acesso. Associações são dinâmicas por natureza porque as estações movem-se, desligam-se e ligam-se. As estações só podem estar associadas a um único ponto de acesso, o que permite ao DS saber onde essa estação está localizada. Associação suporta mobilidade não transitória mas não consegue processar BSS - transição. Para esse efeito é utilizada a re-associação, o que permite à estação, alterar a sua ligação de um AP para outro AP, ambos os serviços, Associação e Re-associação são efetuados pela estação, Desassociação permite quebrar a ligação entre o AP e a estação, e pode ser originada por qualquer uma das partes intervenientes. Uma estação Desassociada não pode receber ou transmitir dados.

A ESS - transição, não é suportada, a estação ao mudar para outro ESS terá obrigatoriamente de reiniciar as ligações. Distribuição é o serviço que permite entregar a informação do transmissor para o receptor respectivo. A mensagem é enviada para o AP local e distribuído para o DS que encaminha para o AP final, ao qual o destinatário está associado.

Caso o destinatário e a origem estejam no mesmo BSS, o AP local e o AP final serão o mesmo, sendo o serviço de distribuição acionado logicamente, independentemente de os dados passarem por um DS ou não.

O Serviço de integração verifica-se quando o AP final é um portal, sendo necessário integrar a rede 802.x em um DS do 802.11.

Os serviços das estações são: Autenticação, Falta de Autenticação, Privacidade e Serviço de Entrega de Unidade de Dados MAC (MAC *Service Data Unit* - MSDU). Com um sistema *Wireless* o meio não é exatamente definido como num sistema convencional. De maneira a controlar o acesso à rede, as estações deverão primeiro estabelecer a sua identidade, o que utiliza o serviço de autenticação. Uma vez uma estação esteja autenticada, esta pode associar-se. A autenticação pode ser efetuada através de duas estações dentro de um IBSS ou através de um AP pertencente ao BSS. Autenticação fora do BSS não é aceita.

Existem dois tipos de autenticação fornecidos pela norma 802.11: Autenticação Aberta do Sistema, o que permite dar autenticação a quem requisitar; e Autenticação de

Chave (*Shared Key*), que apenas permite autenticar quem fornece a chave secreta, tornando assim o serviço restrito.

A chave secreta é implementada utilizando o algoritmo da privacidade equivalente ao *Wireless* (*Wireless Equivalent Privacy* - WEP).

A falta de autenticação ocorre quando a estação ou o AP decide terminar a autenticação, o que faz com que a estação seja automaticamente desassociada.

O serviço Privacidade consiste na criptografia, através de um algoritmo para que outros utilizadores do 802.11 não consigam entender a transmissão efetuada. O algoritmo WEP é especificado pela norma 802.11 como um algoritmo opcional para a privacidade. Quando o WEP não é usado, as estações estão em modo "claro", o que significa que as transmissões não estão criptografadas. Dados transmitidos no modo "claro" são denominados como texto simples (*plaintext*) enquanto que dados criptografados são chamados de texto cifrado (*ciphertext*). As estações ao iniciar, estão todas em modo "claro" até serem autenticadas.

A entrega MSDU certifica-se que a informação percorra o meio através de AP de Serviços de Controle.

O algoritmo WEP permite a mudança da chave para prevenir utilização anormal das transmissões. O método WEP pode ser implementado através de *software* ou *hardware*. A razão para a qual o WEP é opcional é que a criptografia não pode ser exportada para fora dos Estados Unidos, desta maneira a norma 802.11 pode ser um padrão no resto do mundo sem conflitos de regras.

### 5.3.1 *Frames*

O formato dos *frames* para redes *Wireless*, foi definido na norma 802.11 [IEEE99]. Cada *frame* consiste de um cabeçalho MAC, do corpo do *frame* (*frame body*) e da seqüência de verificação do quadro (*Frame Check Sequence* - FCS). O *frame* básico é descrito na figura 5.3.

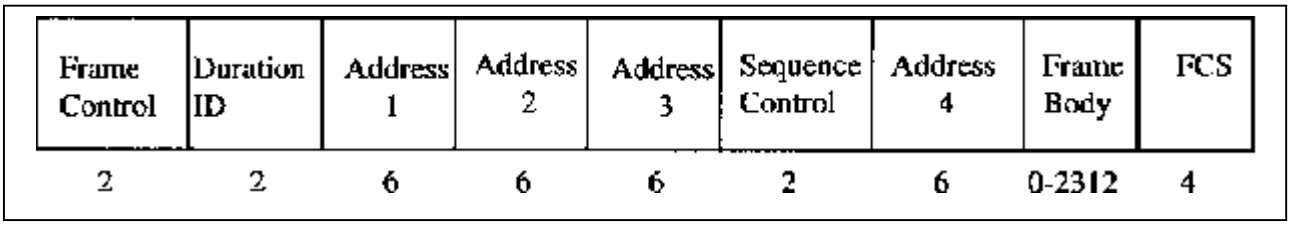


FIGURA 5.3 - *FRAME* 802.11

O cabeçalho MAC consiste em 7 campos com um tamanho de 30 *bytes*. Os campos são: controle do *frame* (*Frame Control*), tempo *(Duration* ID), endereço 1, endereço 2, endereço 3, controle da seqüência (*Sequence Control*) e endereço 4. O campo controle do

*frame* ocupa 2 *bytes* e é composto por 11 sub-campos, como pode ser observado na figura 5.4.

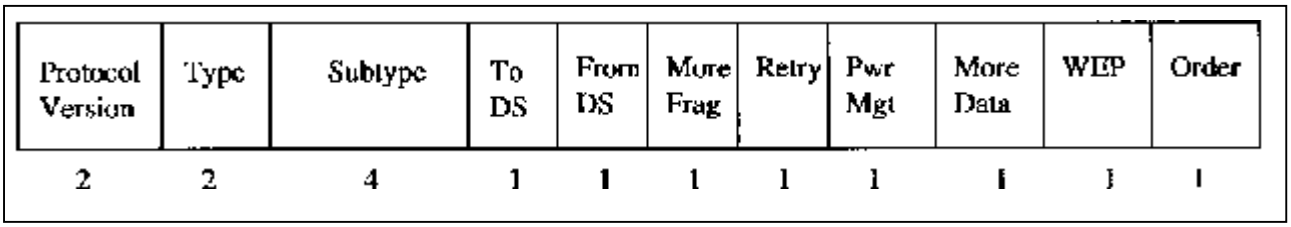


FIGURA 5.4 - CAMPO DE CONTROLE DO *FRAME* 802.11

O campo "versão do protocolo" ocupa 2 *bits* e armazena a versão utilizada na norma 802.11. O valor inicial do 802.11 é zero, sendo os outros valores (1,2,3) reservados. Os campos tipo e sub-tipo correspondem 2 e 4 *bits* respectivamente e operam hierarquicamente para determinar a função do *frame*. Os 8 campos restantes possuem tamanho de 1 *bit*. O campo "*To* DS" possui valor 1 quando o *frame* destina-se ao Sistema de Distribuição (*Distribution System* - DS). O seguinte campo "*From* DS" possui valor 1 quando o *frame* parte do DS. Quando os *frames* ficam no Serviço Básico, ambos os campos possuem valor 0, porque não necessitam do DS. O campo "*More Frag*" (mais fragmentação) será ativado se existir um próximo fragmento do MSDU atual. No campo "*Retry*" (voltar a tentar) será definido se o presente *frame* é a repetição de uma transmissão. Quando a estação estiver em modo "*power save*" o campo "*power management*" receberá o valor 1. Se existirem mais MSDU destinados a essa estação, o campo "*More Data*" (mais dados) é ativado.

No *bit* WEP será determinado se o corpo do campo foi processado utilizando o algoritmo WEP. No campo "*order*" indica-se que os *frames* devem ser exclusivamente ordenados.

No *frame*, o campo "tempo/ID" (identificação) possui 2 *bytes* e armazena o valor do tempo de duração (validade) para cada campo e para os *frames* de controle que contêm a mesma identificação da estação transmissora. Os campos de endereços identificam o conjunto de serviços básicos, o endereço de destino, o endereço de origem e os endereços do receptor e do transmissor. Cada campo de endereço tem um tamanho de 6 *bytes*. O campo "Controle de Seqüência" contém dois *bytes* e é dividido em dois campos menores: o número de fragmentos e o número da seqüência, com tamanho respectivo de 4 *bits* e 12 *bits*. O número de fragmentos, indica em quantos fragmentos o MSDU é dividido, enquanto que o número de seqüência determina a localização do *frame* dentro da seqüência.

O corpo do *frame* contém um campo de tamanho variável de 0 a 2.312 *bytes*, onde está situada a informação concreta. A seqüência de verificação do *frame* (*Frame Check Sequence* - FCS) é composta por 32 *bits* redundantes, que servem para verificar a existência de possíveis erros no *frame* transmitido.

### 5.3.2 Protocolos de Controle de acesso ao Meio (MAC)

As redes convencionais utilizam o *Carrier Sequence Multiple Access* com detecção de colisões (*Collision Detect* - CD) ou CSMA-CD, como protocolo de MAC. Este protocolo estipula que a estação deve escutar o meio antes de transmitir, se já houver uma transmissão a ser efetuada, a estação espera um período de tempo para tentar transmitir novamente. Se não houverem transmissões a serem efetuadas então a estação tem a oportunidade para transmitir. Se duas estações chegarem à mesma conclusão simultaneamente e iniciarem a transmissão ao mesmo tempo, haverá uma colisão e os dados podem se perder. É neste ponto que a detecção de colisões se aplica. Se a colisão ocorrer, as estações esperam e tentam transmitir novamente. O tempo de espera da estação é determinado através do algoritmo utilizado. Esta técnica trabalha bem em redes convencionais mas para topologias *Wireless* surge um conflito no CSMA/CD, ou seja, o problema do nodo escondido, representado na figura 5.5.

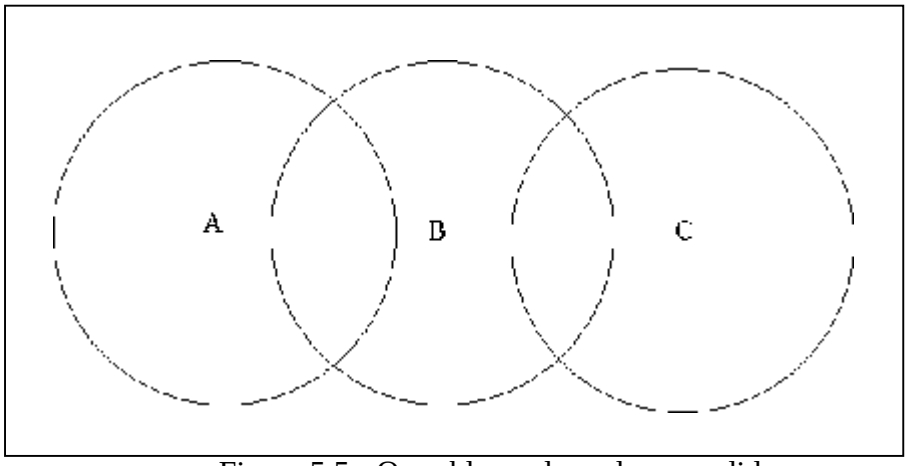


Figura 5.5 - O problema do nodo escondido

O problema do nodo escondido é descrito na figura anterior, da qual percebe-se que o Nodo C não detecta o Nodo A se o Nodo A transmitir, o Nodo C não reconhece esta transmissão, podendo iniciar a sua própria transmissão simultaneamente, o que dará origem a conflitos de colisão.

A solução para o problema é o CSMA com *Collision Avoidance* (CA) ou CSMA/CA. Antes de enviar, a estação escuta o meio, se este já estiver ocupado por outra transmissão, espera por um período de tempo e volta a repetir o processo inicial. Caso não haja nenhuma transmissão a ser concretizada, então a estação envia uma curta mensagem: "preparado para enviar" (*Ready To send* - RTS). Esta mensagem contém o endereço do destinatário e o tempo de duração da transmissão. As outras estações deverão então esperar esse período de tempo até que possam transmitir.

O destinatário envia como resposta uma mensagem : "livre para enviar" (*Clear To Send* - CTS), que avisa à origem que pode transmitir sem receios de colisão, evitando assim possíveis conflitos.

O recebimento de cada pacote (transmissão) é confirmado, se não é recebida uma confirmação, a camada MAC transmite novamente os dados perdidos. Esta seqüência é chamada de 4-*way hand shake* (4 sentidos), sendo tomado como protocolo padrão para a norma 802.11 de *Wireless*. A seqüência de 4-*way hand shake* é demonstrada na figura 5.6.

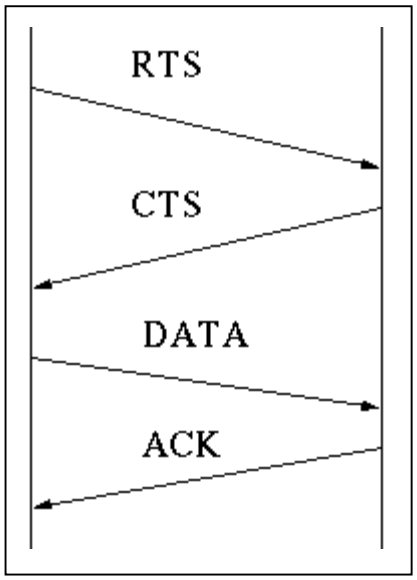


FIGURA 5.6 - THE 4-*WAY HANDSHAKE*

# 6 Protocolos

## 6.1 Modelo OSI

No final da década de 70 foi criado um modelo padrão para implementação de protocolos, a partir de então todos os protocolos deveriam buscar uma série de objetivos, pois a heterogeneidade de padrões existentes praticamente impossibilitava a interconexão entre sistemas de fabricantes distintos.

Alguns dos objetivos necessários para a implementação de um sistema aberto são [MOU86]:

- interoperabilidade: capacidade que os sistemas abertos possuem de troca de informações entre eles, mesmo que sejam fornecidos por fabricantes diversos;

- interconectividade: é a maneira através da qual se pode conectar computadores de fabricantes distintos;

- portabilidade da aplicação: é a capacidade de um *software* de rodar em várias plataformas diferentes;

- Ser escalável: capacidade de um *software* rodar com uma performance aceitável em computadores de capacidades diversas, desde computadores pessoais até supercomputadores.

Para se atingir estes objetivos, a ISO (*International Organization for Standardization*) passou a se ocupar em criar um padrão de arquitetura aberta e baseada em camadas. Foi então definido o Modelo de Referência para Interconexão de Sistemas Abertos (*Reference Model for Open Systems Interconection* - RM OSI) [ISO89].

A utilização de um ambiente de sistema aberto nos oferece algumas vantagens, como:

- liberdade de escolha entre soluções de diversos fabricantes;

- acesso mais rápido a novas tecnologias e a preços mais accessíveis, já que é mais barato e rápido fabricar produtos baseados em uma plataforma padrão;

- redução de investimentos em novas máquinas, já que os sistemas e os *software*s de aplicação são portáveis para os vários tipos de máquinas existentes.

A adoção de um modelo baseado em camadas também não é ar*bit*rária. Considerando que uma rede de computadores tem como objetivo o processamento de tarefas distribuídas pela rede de forma harmônica e cooperativa entre os vários processos de aplicação, o projeto desta deve levar em conta vários fatores, como:

- considerar todos os eventos possíveis de acontecer durante a comunicação;
- conhecer todos os efeitos e causas destes eventos;
- especificar em detalhes todos os aspectos técnico-operacionais dos meios físicos a serem utilizados como suporte à comunicação;
- detalhes das próprias aplicações a serem executadas.

Pode ser percebido, então, que o problema é extremamente complexo e abrangente. A fim de se lidar com esta complexidade (facilitando a implementação e manutenção), projeta-se a rede como um conjunto de camadas.

Este conjunto de camadas é hierárquico, ou seja, cada camada baseia-se na camada inferior [MOU86]. Reduzindo-se o projeto global da rede ao projeto de cada uma das camadas, simplifica-se consideravelmente o trabalho de desenvolvimento e de manutenção. O projeto de uma camada é restrito ao contexto dessa camada e supõe que os problemas fora deste contexto já estejam devidamente resolvidos.

Na realidade existem duas vantagens práticas na utilização de uma arquitetura em camadas. Em primeiro lugar, a complexidade do esforço global de desenvolvimento é reduzida através de abstrações (não interessa para uma determinada camada como as demais implementam o fornecimento de seus serviços, só o que elas oferecem). Na arquitetura hierárquica, a camada (N) sabe apenas que existem a camada (N-1), prestadora de determinados serviços e a camada (N+1), que lhe requisita os serviços. A camada (N) não toma conhecimento da existência das camadas (N±2), (N±3), etc.

O segundo aspecto é relacionado com a independência entre as camadas. A camada (N) preocupa-se apenas em utilizar os serviços da camada (N-1), independentemente do seu protocolo. É assim que uma camada pode ser alterada sem mudar as demais (facilidade de manutenção) - desde que os serviços que ela presta não sejam modificados. É assim também que novas aplicações podem ser implementadas, na camada apropriada, aproveitando os mesmos serviços já fornecidos pelas outras camadas (redução dos esforços para evoluções).

Porém a elaboração de um sistema aberto passa por algumas etapas obrigatórias que podem ser observadas claramente na definição do modelo OSI, da ISO:

- definição do modelo do sistema aberto (padrão para arquitetura do sistema aberto);
- definição dos padrões dos componentes que fazem parte do modelo (padrões de interoperabilidade e portabilidade), não só os relacionados à comunicação, mas também alguns não relacionados, como estrutura de armazenamento de dados, etc;
- seleção dos perfis funcionais.

Pode ser observado que o modelo OSI da ISO corresponde exatamente ao primeiro item citado acima. O modelo OSI é um modelo de referência e define apenas a arquitetura do sistema. O padrão criado para o modelo OSI, então, define exatamente o que cada camada deve fazer, mas não define como isto será feito, ou seja, define os serviços que cada camada deve prestar, mas não o protocolo que o realizará. Este primeiro passo já está bem definido pela ISO.

A definição dos protocolos de cada camada, então, fica por conta do segundo passo. Esta parte também está definida pela ISO, mas é realizado por grupos de estudo diversos. Este passo é uma tarefa muito dinâmica, pois novas tecnologias de transmissão surgem a todo instante. Portanto por um lado existem alguns padrões bem documentados, mas por outro, existem tecnologias emergentes que precisam ser adaptadas às condições do modelo OSI e ainda estão em processo de definição.

Já a terceira etapa não é uma fase de responsabilidade da ISO. Esta etapa de definição de perfis funcionais é realizada por cada país, que escolhe os padrões que lhe cabem baseados em condições tecnológicas, base instalada, visão futura, etc. Por exemplo, no Brasil existe o Perfil Funcional do Governo Brasileiro. A escolha do Perfil Funcional é uma etapa importante, pois apesar de dois sistemas seguirem o Modelo OSI, se eles adotarem perfis diferentes, eles nunca vão conseguir interoperar.

A arquitetura OSI foi desenvolvida a partir de três elementos básicos, conforme figura 6.1 [MOU86]:

- os processos de aplicação existentes no ambiente OSI;
- as conexões que ligam os processos de aplicação e que lhes permitem trocar informações;
- os sistemas.

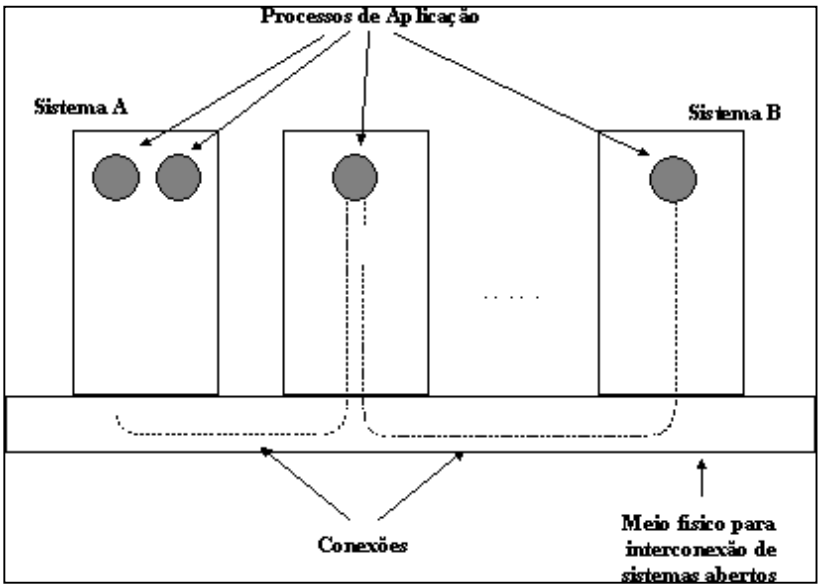


FIGURA 6.1 - PROCESSOS DE APLICAÇÃO, CONEXÕES E SISTEMAS

A figura 6.2 nos dá uma idéia da arquitetura de uma máquina pertencente a um sistema de comunicação.

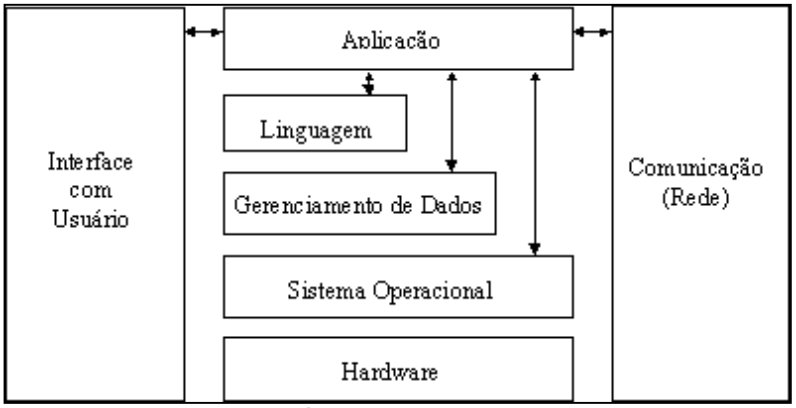


FIGURA 6.2 - ARQUITETURA DE UMA MÁQUINA DO SISTEMA

*Hardware*: provê a infra-estrutura necessária (no nível mais baixo) para o processamento da aplicação, como a manipulação de *bits*, acesso a disco, etc.

Sistema operacional: provê os serviços básicos de acesso a *hardware*, etc.

Gerenciamento de dados: cuida de tarefas como o acesso, manipulação e troca de vários tipos de dados. Uma consistência nesta tarefa é um grande passo rumo à portabilidade de aplicações.

Linguagem: tem sido feitos esforços em relação à criação de uma linguagem com independência da plataforma, de forma a prover a portabilidade de código.

Interface com o usuário: um dos principais fatores de portabilidade, já que provê a interface com o usuário da aplicação.

Comunicação: Proporciona a comunicação e interoperação entre máquinas e sistemas diferentes, cuidando de características como padrões de interoperação, endereçamento, etc.

O modelo OSI, então, se encaixa na figura 6.2 como um conjunto de funções que possibilitam que máquinas distintas possam se comunicar e trocar informações. Ele possui sete camadas, conforme figura 6.3, onde cada camada é responsável por uma determinada função específica. Os princípios utilizados para se chegar a estas camadas são [TAN94]:

- uma camada deve ser criada onde é necessário um nível de abstração diferente;
- cada camada deve desempenhar uma função bem definida;
- a função de cada camada deve ser definida tendo em vista a definição de protocolos padrões internacionais;
- as fronteiras entre as camadas devem ser escolhidas de forma a minimizar o fluxo de informações através das interfaces;
- o número de camadas deve ser grande o suficiente para que não seja preciso agrupar funções em uma mesma camada por necessidade, e pequeno o suficiente para que a arquitetura fique manejável.

Cada camada é usuária dos serviços prestados pela camada imediatamente inferior e presta serviços para a camada imediatamente superior. Esta troca de informações entre as camadas adjacentes ocorre por meio da troca de primitivas de serviços nas interfaces entre as camadas.

Apesar do modelo OSI estar dividido em sete níveis, pode-se considerar genericamente que as três camadas mais baixas cuidam dos aspectos relacionados à transmissão propriamente dita e a camada de transporte lida com a comunicação fim-a-fim, enquanto que as três camadas superiores se preocupam com os aspectos relacionados à aplicação, já a nível de usuário.

A comunicação entre sistemas ocorre a nível de camadas, ou seja, a camada de aplicação do sistema A se comunica com a camada de aplicação do sistema B e assim por diante até o nível físico, onde ocorre a comunicação física entre os sistemas.

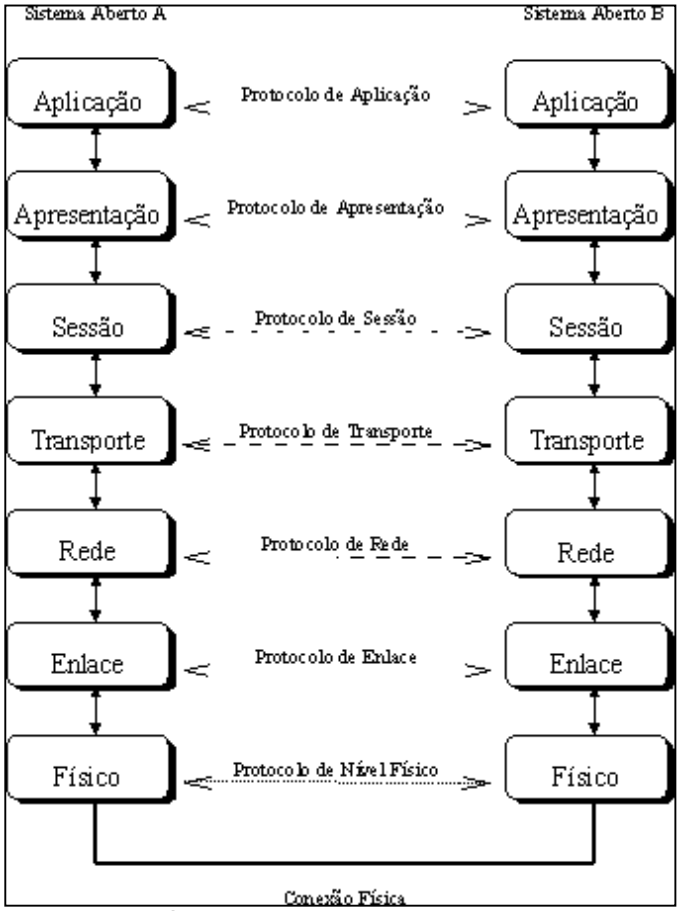


FIGURA 6.3 - MODELO DE REFERÊNCIA OSI

Uma maneira bastante fácil e simplificada de se enxergar a funcionalidade de um modelo em camadas, como o modelo OSI, é imaginar que cada camada tem como função adicionar um cabeçalho aos dados do usuário a serem transmitidos para outro sistema, conforme figura 6.4. Deste modo a função de cada camada do outro sistema é exatamente a inversa, ou seja, retirar os cabeçalhos dos dados que chegam e entregá-los ao usuário em sua forma original.

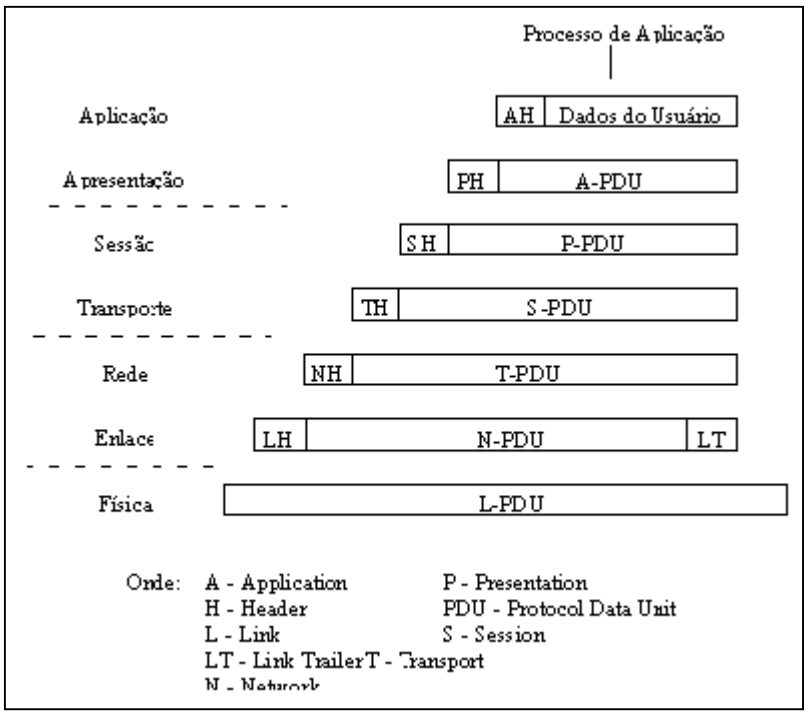


FIGURA 6.4 - TRANSFERÊNCIA DE DADOS ENTRE CAMADAS

Os dados entregues pelo usuário à camada de aplicação do sistema recebem a denominação de SDU (*Service Data Unit*). A camada de aplicação, então, junta à SDU (no caso, os dados do usuário) um cabeçalho chamado PCI *(Protocol Control Information*). O objeto resultante desta junção é chamado de PDU (*Protocol Data Unit*), que corresponde à unidade de dados especificada de um certo protocolo da camada em questão.

### 6.1.1 Primitivas de Serviços

As primitivas de serviços são informações trocadas entre duas camadas adjacentes de forma a realizar um serviço. No modelo OSI são definidas quatro tipos de primitivas:

- pedido (*Reques*t): utilizada para solicitar ou ativar um determinado serviço;
- indicação (*Indication*): informa a ocorrência de um determinado evento;
- resposta (*Response*): utilizada para responder a um determinado evento;
- confirmação (*Confirmation*): utilizada para confirmar a execução de um serviço solicitado.

As primitivas possuem parâmetros de entrada e saída. Por exemplo, em um pedido de conexão, os parâmetros podem especificar a máquina à qual se conectar, o tipo de serviço desejado e o tamanho máximo de mensagem a ser utilizada e os parâmetros em uma

indicação de conexão podem conter a identidade do solicitante, o tipo de serviço e o tamanho máximo de mensagem proposto. Quem cuida dos detalhes desta negociação é o protocolo. Por exemplo, caso duas propostas para o tamanho máximo das mensagens trocadas seja conflitante, o protocolo deve decidir qual das duas será aceita.

Os serviços prestados podem ser basicamente de dois tipos: confirmado e não confirmado. No serviço confirmado, há um pedido, uma indicação, uma resposta e uma confirmação. Já no serviço não confirmado, há apenas um pedido e uma indicação. Um exemplo de um serviço confirmado é o estabelecimento de uma conexão, enquanto que a desconexão é um serviço não confirmado. Será visto o exemplo de um serviço de conexão na figura 6.5.

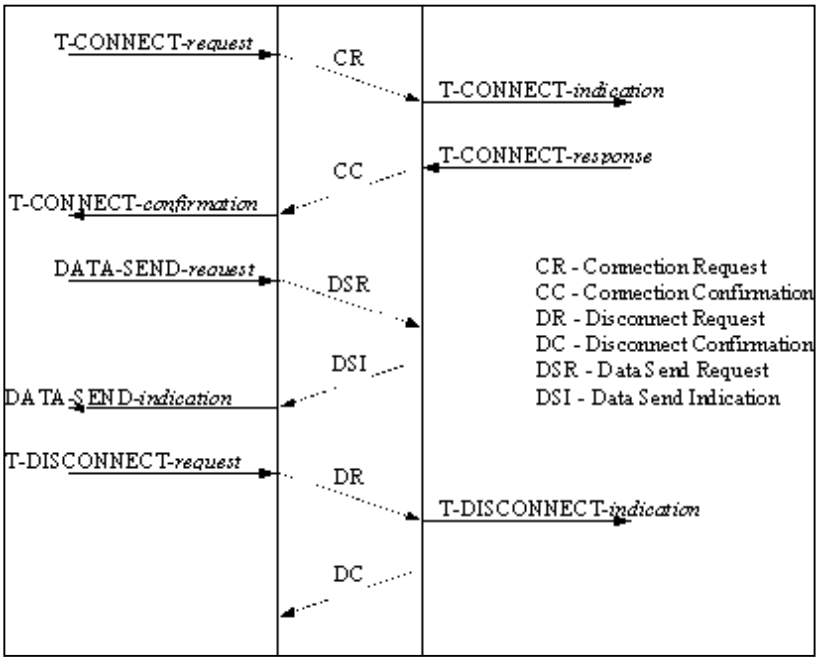


FIGURA 6.5 - DIAGRAMA DE TEMPO DE ESTABELECIMENTO DE CONEXÃO

Este serviço pode ser descrito da seguinte forma:

- *request*.CONEXÃO - solicita o estabelecimento de uma conexão;
- *indication*.CONEXÃO - informa à parte chamada;
- *response*.CONEXÃO - entidade chamada aceita ou rejeita chamadas;
- *confirmation*.CONEXÃO - indica ao solicitante se a chamada foi aceita;
- *request*.DADOS - solicita a transmissão de dados;
- *indication*.DADOS - avisa sobre a chegada de dados;

- *request*.DESCONEXÃO - solicita que a conexão seja liberada;

- *indication*.DESCONEXÃO - informa ao parceiro sobre o pedido.

### *6.1.2 Serviços e Protocolos*

Faz-se necessário deixar bem clara a distinção entre serviços e protocolos. Um serviço é um conjunto de primitivas que uma camada oferece à camada superior adjacente, ou seja, é uma interface entre duas camadas onde a inferior se comporta como provedora do serviço e a superior a usuária do serviço. O serviço define as operações que a camada está preparada para realizar em nome de seus usuários, mas não diz nada a respeito do modo como isso deve ser implementado [MOU86].

Já um protocolo é um conjunto de regras que governa o formato e o significado dos quadros, pacotes ou mensagens trocados entre entidades parceiras dentro de uma mesma camada. Os protocolos são utilizados para implementar os serviços, não sendo diretamente visíveis aos usuários, ou seja, o protocolo utilizado pode ser modificado, desde que o serviço oferecido ao usuário permaneça o mesmo.

Deve-se sempre lembrar que ao falar em serviços, fala-se em camadas adjacentes (níveis diferentes, no mesmo sistema), e ao falar em protocolo, fala-se de entidades pares (no mesmo nível, em sistemas diferentes), conforme figura 6.6.

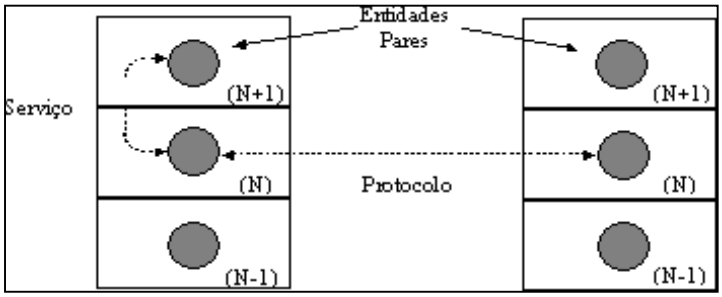


FIGURA 6.6 - SERVIÇOS E PROTOCOLOS NO MODELO OSI

Os serviços providos pela camada (N) são disponíveis para a entidade (N+1) através dos SAP´s (*Service Access Point*). Os SAP´s são interfaces lógicas entre as entidades (N) e (N+1). Portanto, quando a entidade (N+1) precisa utilizar o serviço provido pela camada (N), ela busca este no SAP(N).

As informações entre entidades (N+1) são trocadas através de uma associação chamada conexão (N) , estabelecida na camada (N) utilizando o protocolo (N). A figura 6.7 ilustra este conceito.

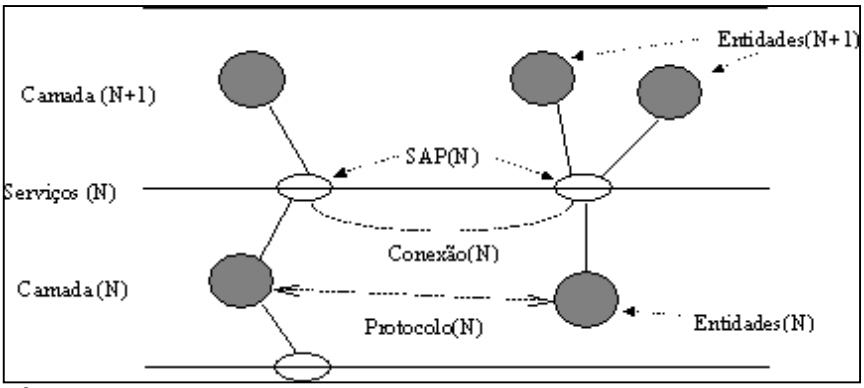


FIGURA 6.7 - SAP´S E CONEXÕES

## 6.2 Arquitetura *internet*

A arquitetura *internet* se baseia praticamente em um serviço de rede não orientado à conexão (datagrama não confiável), o *Internet Protocol* (IP) e em um serviço de transporte orientado à conexão, oferecido pelo *Transmission Control Protocol* (TCP). Juntos, estes protocolos se completam, oferecendo um serviço confiável de uma forma simples e eficiente.

A arquitetura *internet* se baseia em um modelo com quatro camadas [SOU99], demonstrado na figura 6.8, onde cada uma executa um conjunto bem definido de funções de comunicação. No modelo em camadas da *internet*, não existe uma estruturação formal para cada camada, conforme ocorre no modelo OSI. Ela procura definir um protocolo próprio para cada camada, assim como a interface de comunicação entre duas camadas adjacentes.

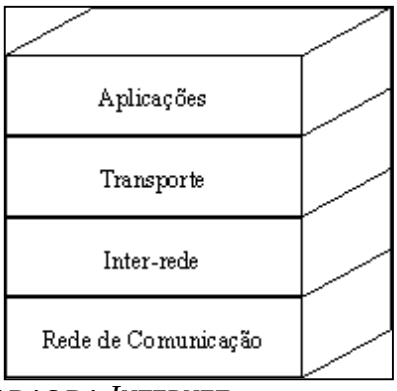


FIGURA 6.8 - MODELO EM CAMADAS DA *INTERNET*

Estas camadas trocam informações entre si de uma forma vertical e hierárquica, ou seja, a camada APLICAÇÕES passa informações para TRANSPORTE, que passa para REDE que passa para ACESSO A REDE. Cada camada trata das informações que correspondem a sua função.

Quando fala-se em comunicação entre dois *hosts*, a comunicação entre as camadas é vista então de uma maneira horizontal, ou seja, a Camada TRANSPORTE do *host* destino conversa somente com a Camada TRANSPORTE do *host* Origem, assim como a camada APLICAÇÕES só conversará com a camada APLICAÇÕES, e assim por diante.

### 6.2.1 Protocolo TCP

O protocolo TCP é utilizado na comunicação entre computadores de uma rede *internet*. Através dele, pode-se obter um serviço confiável, ou seja, que os dados sejam transmitidos integralmente para os destinos corretos.
Para que seja possível identificar a que serviço um determinado datagrama pertence, o TCP utiliza o conceito de "portas". Determinada a porta, toda a comunicação com a aplicação é realizada e endereçada através dela. Uma porta é a representação numérica de um serviço *internet*.

As principais funções do TCP são [TAN94]:

- transferência de dados - transmissão de dados em blocos (datagramas) e em modo *full-duplex* (envio e recebimento simultâneos);
- transferência de dados urgentes - transmite primeiro datagramas que contenham sinalização de urgência;
- estabelecimento e liberação de conexão;
- segmentação - O TCP pode dividir os dados a serem transmitidos em pequenos blocos (datagramas) que são identificados para, no *host* destino, serem agrupados novamente.
- controle de fluxo - o TCP é capaz de adaptar a transmissão dos datagramas às condições de transmissões (velocidade , tráfego ...) entre os sistemas envolvidos.
- controle de erros - como visto na segmentação, os datagramas são identificados antes de serem transmitidos. Além disso é adicionado o *checksum*, um número utilizado para verificar e corrigir erros na transmissão.

### 6.2.2 Protocolo IP

O IP é o protocolo responsável por definir o caminho que um pacote de dados deverá percorrer do *host* origem ao *host* destino, passando por uma ou várias redes. Ao contrário do TCP, o protocolo IP é chamado de Protocolo não-orientado a conexão, o que significa que não há nenhuma verificação de erro na transferência, ele apenas roteia os pacotes pela rede.

### 6.2.3 Limitações do Protocolo

Embora os protocolos do TCP/IP viabilizem a *Internet* e ofereçam valiosos serviços, existem algumas imperfeições, como por exemplo a questão da segurança. Quando uma empresa conecta sua rede na *Internet* sem as defesas, qualquer computador na rede interna com TCP/IP pode (teoricamente) ser acessado por qualquer usuário da *Internet*, o que representa um risco altíssimo para a segurança das informações e até mesmo para a continuidade dos serviços.

Muitos dos problemas atuais de segurança da transmissão de dados pela *Internet* estão relacionados com o fato de que o protocolo TCP/IP na sua forma atual (IPv4) não foi projetado para ser seguro, e é sujeito a uma série de ataques. Como conseqüência, vários serviços da *Internet* que são baseados no TCP/IP, como o TELNET, o FTP e o E-Mail (SMTP) também não são seguros, pois utilizam mensagens que são transportadas pelo TCP/IP em *cleartext* e portanto são vulneráveis a ataques passivos (como captura de tráfego através de *sniffers*) ou ataques ativos como "roubo" de sessões, *sequence guessing*, etc.
Além da questão da segurança, há um outro problema em relação à versão atual do TCP/IP. Com o campo de endereços dos pacotes limitados em 4 *bytes* (32 *bits*), espera-se que a *Internet* fique sem novos endereços dentro de alguns anos, o que poderá ter conseqüências extremamente sérias

### 6.2.4 A próxima versão do TCP/IP - IPv6

Para resolver as limitações do IPv4, está sendo desenvolvida uma nova versão do TCP/IP, o IPv6 (ou IPSec). Neste novo protocolo, a segurança é um pré-requisito. O IPSec oferecerá serviços de autenticação de usuários e garantia de confidencialidade e de integridade dos dados através de criptografia. O IPSec também está sendo projetado para resolver a questão dos endereços IP, pois o novo tamanho do campo de endereços passa para 16 *bytes* (128 *bits*), o que permitirá a expansão da *Internet* sem problemas. Devido à imensa base instalada de *hosts* e roteadores compatíveis com o IPv4, o IPv6 está sendo desenvolvido de forma que seja possível uma migração gradual para o novo protocolo. O novo endereço IP contará com 16 octetos [ROS99].

## 6.3 Comparação entre o modelo OSI e o protocolo WAP

Como pode ser observado na figura 6.9, a principal diferença entre as duas arquiteturas está no número de camadas, enquanto no modelo RM-OSI, são definidas 7 camadas, no protocolo WAP são definidas 5, além da camada portadora, que funciona independente das demais.

No modelo OSI são formalmente definidos os serviços de cada camada, a interface utilizada pelas camadas adjacentes para a troca de informações e o protocolo de comunicação que define as regras de comunicação para cada uma destas.

Alguns dos serviços definidos no RM-OSI são opcionais [SOA95], como exemplo, os níveis de enlace, rede e transporte podem oferecer serviços orientados a conexão

(circuito virtual) ou não orientados à conexão (datagrama). Estas características são conseqüência do tratamento dado pela ISO na criação do modelo o qual se propõem a tratar todos os aspectos da interconexão aberta de sistemas.

No protocolo WAP, os serviços de nível de rede OSI relativos à interconexão de redes distintas são implementados de forma independente, pois a camada de transporte WDP funciona independentemente da rede *wireless* utilizada. Acima da camada de transporte o protocolo WAP oferece as camadas de segurança, transação, sessão e aplicação.

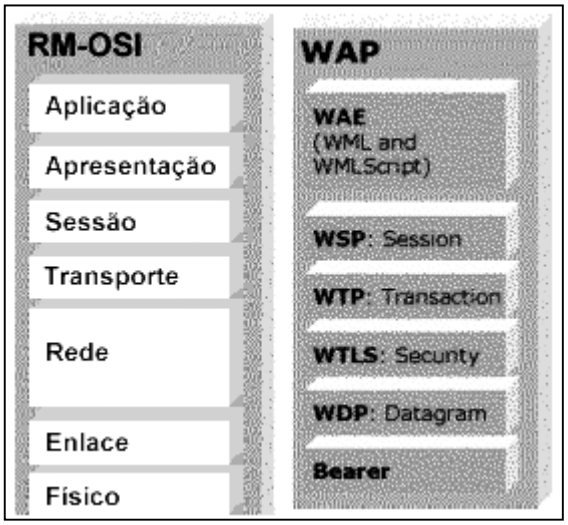


FIGURA 6.9 - COMPARAÇÃO ENTRE AS CAMADAS DO MODELO OSI E PROTOCOLO WAP

O nível de sessão descrito no modelo OSI fornece mecanismos que permitem estruturar os circuitos oferecidos pelo nível de transporte, no protocolo WAP este mecanismo é oferecido através de dois serviços, o primeiro orientado a conexão, que opera sobre o protocolo de transação e o segundo, não orientado a conexão que opera sobre a camada de datagramas.

No protocolo WAP, existe uma camada que trata especificamente de segurança, esta camada é opcional no modelo OSI, é utilizada para disponibilizar serviços de criptografia, necessários ao serviço de transporte seguro, requerido por muitas aplicações.

## 6.4 Protocolos utilizados na *WWW* x Protocolo WAP

A pilha de protocolos WAP consiste em cinco camadas, que possuem correspondência com os protocolos utilizados na *internet*, conforme demonstrado na figura 6.10.

Na pilha de protocolos WAP a aplicação é isolada das operadoras, tornando possível que as aplicações sejam executadas, independentemente do serviço de transporte utilizado.

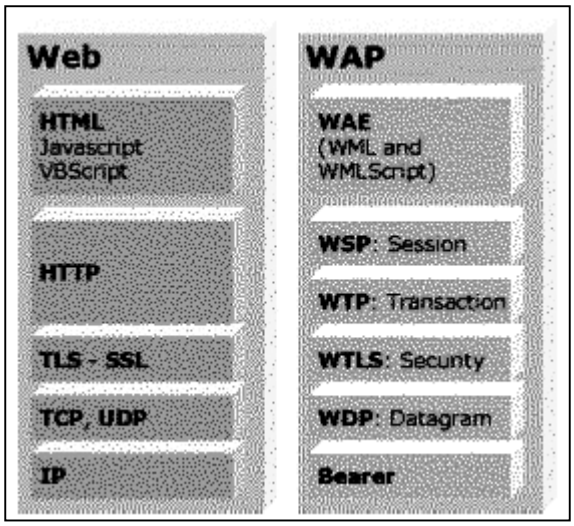


FIGURA 6.10 - COMPARAÇÃO DAS ARQUITETURAS *WWW* E WAP

A pilha de protocolo definida no WAP aperfeiçoa os padrões de protocolos *WWW*, como HTTP, para utilização de baixa largura de banda, condições de alta latência que freqüentemente são encontradas em redes *wireless*. Um número crescente de camadas de sessão, transação, segurança e transporte promovem uma melhor funcionalidade ao HTTP no ambiente de rede *wireless*.

Aqui estão alguns exemplos destas melhorias [WAP98]:

Os textos de cabeçalho do HTTP são traduzidos em código binário (*bytecode*) o que reduz significativamente a quantidade de dados que devem ser transmitidos na interface aérea.

Um protocolo leve de restabelecimento de sessão é definido para permitir que sessões possam ser suspensas e retomadas sem o *overhead* de estabelecimento inicial. Isto permite suspender uma sessão enquanto espera um recurso de rede, minimizando a utilização da bateria.

O WAP possui um Protocolo de Transação *wireless* (WTP) que disponibiliza um serviço de datagrama confiável, com muitas características úteis do protocolo TCP tradicional, mas sem o comportamento que o faz inadequado nas redes *wireless*. Por exemplo, TCP transmite uma grande quantidade de informação para cada transação de pedido e resposta, incluindo informações necessárias ao controle de entrega de pacote fora de ordem. No WAP só há uma rota possível entre o *proxy* WAP e o dispositivo portátil, então não há nenhuma necessidade de controle desta situação. O WTP elimina esta informação desnecessária e reduz a quantia de informação para cada transação de pedido e resposta. Este é um exemplo da otimização que o WTP promove.

A solução WTP do WAP também menciona que não é necessária uma pilha TCP no telefone, permitindo a redução significativa de processamento e memória no dispositivo portátil.

As melhorias feitas na pilha de protocolo WAP significaram uma economia na largura de banda *wireless*. A figura 6.11 demonstra a comparação entre o número de pacotes necessários em um processo utilizando um *browser* convencional HTTP 1.0 e um WAP *browser*. O protocolo WAP utiliza menos da metade do número de pacotes necessários para disponibilizar um conteúdo com protocolos HTTP/TCP/IP. Esta melhoria é essencial para melhor utilização da largura de banda que é limitada nas redes *wireless*

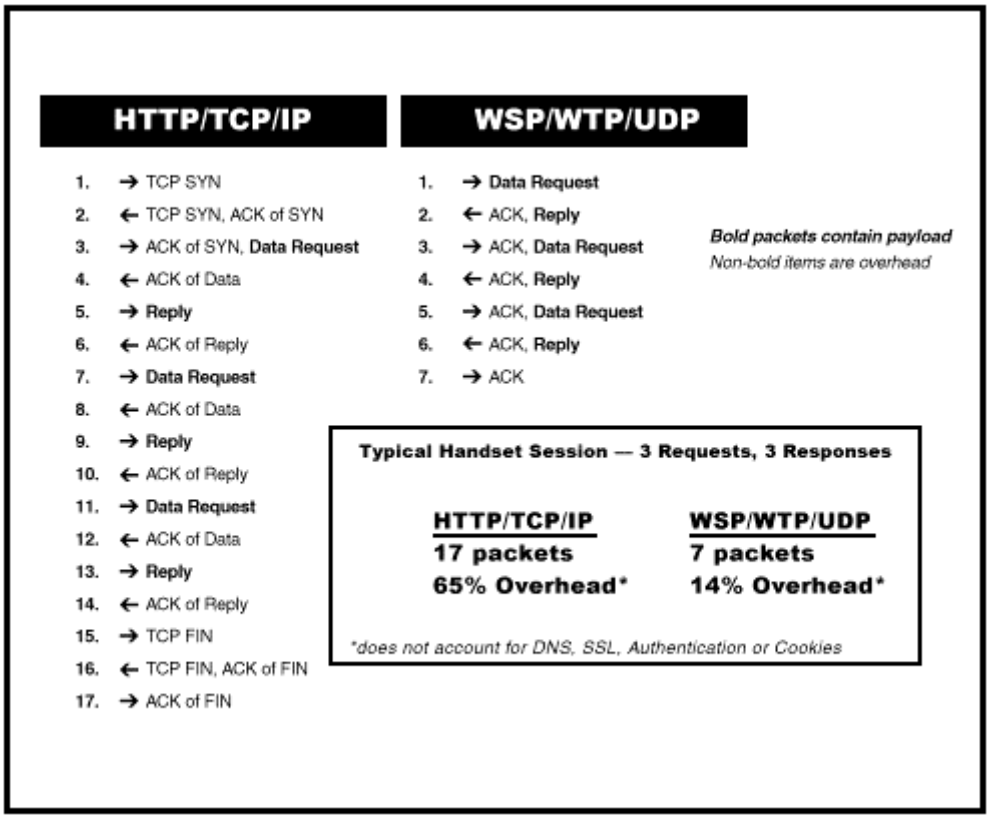


FIGURA 6.11 - CONSERVAÇÃO DE LARGURA DE BANDA NO PROTOCOLO WAP

### 6.4.1 Comparação do funcionamento WAP x *WWW*

Fornecer serviços de *Internet* em uma rede *wireless* representa novos desafios para todos os envolvidos nessa atividade. O mercado é diferente e os consumidores têm novas necessidades e expectativas. A rede *wireless* tem menor largura de banda e algumas dificuldades de comunicação. Os dispositivos utilizados também são diferentes, principalmente por terem menos memória, menor poder de processamento, uma tela menor e recursos de entrada de dados limitados.

Atualmente a *Internet* é amplamente utilizada. Muitas pessoas a utilizam para encontrar informação de todos os tipos. Exemplos de serviços disponíveis são acesso ao banco, compras e troca de informações com pessoas que têm os mesmos interesses.

Ainda que esses serviços e até algumas aplicações sejam diferentes, o processo é o mesmo.

Na *WWW* convencional encontram-se clientes e servidores, conforme demonstrado na figura 6.12. Clientes são os navegadores (*browsers*) e os servidores (*server*s) são os computadores dos provedores de serviços de *Internet* (ISP - "*Internet Service Providers*"). Estes servidores, entre outras atividades, hospedam páginas estáticas de HTML ou produzem páginas resultantes de aplicações dinâmicas construídas no momento em que são solicitadas ("*on the fly*").

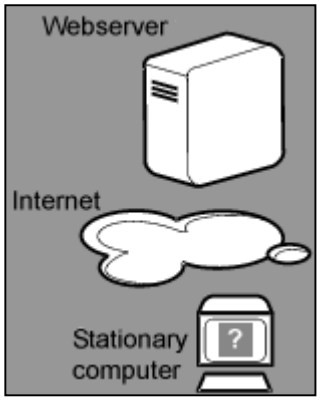


FIGURA 6.12 - MODELO DE COMUNICAÇÃO *WWW*

A comunicação entre clientes e servidores é constituída basicamente de troca de "solicitações". O WAP *gateway* pode ser visto como um "conversor de solicitações".

1. O usuário inicializará o *browser* e especificará uma URL (digitará um endereço no campo apropriado)

2. O *browser* analisará o endereço e enviará uma solicitação para o servidor utilizando o protocolo HTTP (protocolo para *internet*)

3. O servidor analisará a solicitação. Se for uma página comum, estática, ela será localizada; se for uma aplicação dinâmica (por exemplo, uma consulta a um banco de dados) o programa correspondente será disparado e uma página de resposta será gerada (isto poderá ocorrer no próprio servidor do provedor ou em qualquer outro da rede)

4. O servidor colocará um cabeçalho HTTP na página resposta e enviará de volta ao *browser*

5. O *browser* analisará e exibirá o resultado na tela do *micro*.

Ao utilizarmos WAP, haverá um cenário mais complexo, conforme figura 6.13.

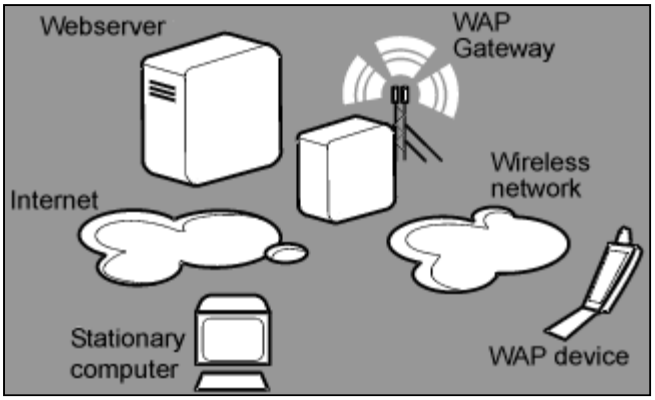


FIGURA 6.13 - MODELO DE COMUNICAÇÃO WAP

1. O usuário utilizará um aparelho WAP para solicitar o endereço (escolhendo um item em um menu, por exemplo).

2. O WAP *browser* do celular analisará e enviará a solicitação ao servidor WAP (WAP *gateway*). Neste trecho da transmissão será utilizado o protocolo WAP e não o HTTP.

3. O WAP *gateway* analisará e "converterá" o protocolo WAP em HTTP; a solicitação será então enviada a um Servidor *Web* comum, presente na rede.

4. O servidor do destino fará seu trabalho, como visto anteriormente e enviará a resposta (com protocolo HTTP) ao WAP *gateway* .

5. O servidor WAP analisará o que recebeu, validará o código WML, removerá o cabeçalho HTTP, acrescentará o cabeçalho WAP e enviará ao dispositivo WAP.

6. O WAP *browser* analisará e exibirá o resultado em sua tela.

### 6.4.2 Comparativo de Segurança *WWW* x WAP

Segurança é sempre uma questão importante, principalmente quando se pensa em utilizar WAP para aplicações e serviços como acesso a dados bancários ou mesmo transações comerciais, no chamado *m-commerce*. Os usuários precisam sentir-se seguros para começarem a acessar os serviços disponíveis.

Atualmente, na *WWW* uma conexão segura entre o cliente e o servidor de aplicações é necessária. A especificação WAP garante que um protocolo de segurança estará disponível para essas transações.

Uma das tarefas do WAP *gateway* é converter os protocolos WAP para protocolos *internet* e vice-versa.

Para ser extensível, flexível e escalável, os protocolos WAP foram criados sob uma arquitetura em camadas. Cada camada da pilha de protocolos especifica uma interface bem definida com a camada superior.

Após isso, a solicitação é convertida para protocolos da *internet*. Como pode ser observado na figura 6.14, a solicitação é segura desde o dispositivo WAP até o *gateway*. Entretanto, entre as camadas de segurança WAP e as camadas TLS-SSL da *Internet* a informação não é criptografada.

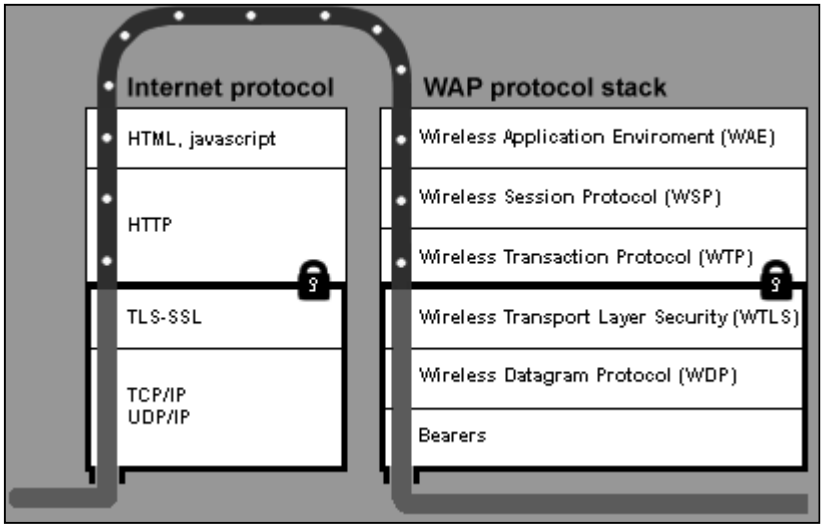


FIGURA 6.14 - MODELO DE CONVERSÃO DE PROTOCOLOS

Isso significa que a pessoa que administrar o WAP *gateway* poderá ter acesso às informações, o que torna ainda mais importante o controle do acesso físico ao WAP *gateway*. Mesmo assim, aplicações WAP são seguras, pois o protocolo WTLS implementa opções para autenticação e criptografia otimizados para o uso em ambientes *Wireless*.

# 7 Segurança

## 7.1 Introdução

*"Use dinheiro sempre que possível. Não forneça seu telefone, seu endereço e os números dos seus documentos, a não ser que seja absolutamente necessário. Não preencha questionários nem responda a serviços de telemarketing. Exija que o banco, a companhia de cartão de crédito e o governo lhe mostrem todos os dados que têm sobre você. Bloqueie identificadores de chamadas e mantenha seu número fora da lista telefônica. jamais deixe seu celular ligado enquanto viaja – ele pode ser rastreado. Se você tiver de utilizar a Internet, use e-mail criptografado, rejeite todos os cookies e nunca dê seu verdadeiro nome quando se registrar em sites. No trabalho, presuma que todos os telefonemas, mensagens de voz, e-mail e computadores sejam monitorados." [ECO99]*

A recomendação acima, foi divulgada recentemente na revista americana *"The Economist"* e resume o medo instalado em torno das questões relativas à segurança de informações nos dias de hoje.

Com o advento do comércio eletrônico e bancos *on-line*, a *Internet* mudou o modo de vida de muitas pessoas, que passaram a realizar compras e administrar finanças *on-line*. Estes serviços estão surgindo agora na *Internet* sem fios, permitindo aos usuários ter acesso a contas bancárias, ações de comércio e bens de consumo, na tela do seu telefone móvel. De acordo com departamentos de pesquisas e estatísticas, haverá mais de 525 milhões de dispositivos WAP habilitados no mercado no ano 2003 [OVU00], criando grande expectativa referente ao crescimento econômico gerado por este novo segmento de mercado, porém, a disseminação do acesso a *Internet*, seja ela móvel ou tradicional, acarreta os seguintes fatores:

- cada vez mais pessoas, com formação mais heterogênea, tem acesso à *Internet;*
- recursos valiosos são armazenados para uso sem intermediação humana; programas acessam programas;
- ampliadas facilidades de acesso e administração de sistemas remotamente facilitando a obtenção de controle total de um sistema conectado à *Internet;*
- literatura e conferências eletrônicas ensinam como quebrar a segurança de sistemas.

Portanto, é necessária uma grande preocupação quanto a segurança, por parte dos desenvolvedores de aplicações para *Internet*, para que os usuários não precisem se preocupar com isto, sentindo-se á vontade para fornecer informações confidencias através dela.

Segurança é um conceito utilizado freqüentemente com pouco rigor. Isto ocorre porque o conceito de segurança é polêmico e freqüentemente equivocado. Quando fala-se de segurança em tecnologias da informação, falam-se de várias coisas ao mesmo tempo: que ninguém roube ou modifique os dados, que nenhuma informação seja extraviada, etc.

Para focalizar a discussão, se deve utilizar os padrões ISO, onde, dentro do modelo de referencia OSI está definido uma arquitetura de segurança dentro da qual existe uma serie de serviços de segurança. Segundo esta especificação, para proteger as comunicações é necessário dotar as mesmas de alguns serviços, que são os seguintes [WAP99]:

- privacidade - Garante que só o remetente e o receptor de uma mensagem codificada possam ler os conteúdos daquela mensagem. Para garantir a privacidade, uma solução de segurança deverá assegurar que ninguém poderá visualizar, acessar ou utilizar informação privada, como endereços, informações de cartão de crédito e números de telefone transmitidos através de transações *wireless*.

- integridade - Garante a descoberta de qualquer mudança no conteúdo de uma mensagem entre o envio e a recepção. Por exemplo, quando um usuário instrui um banco para transferir determinada quantia de uma conta para outra, a integridade garante que os números da conta e valor da transação constem na mensagem do usuário e não possam ser alterados sem que o banco ou o usuário perceba. Se a mensagem for alterada de qualquer forma durante transmissão, o sistema de segurança deverá ter um modo de descobrir e informar esta alteração. Em muitos sistemas, se uma alteração é descoberta, o sistema receptor pede que a mensagem seja enviada novamente.

- autenticação - Garante que todas as partes envolvidas em uma comunicação são quem dizem ser. O Servidor de autenticação fornece um modo de verificar que os usuários realmente estão se comunicando com o ponto de rede desejado.

- não rejeição - Oferece uma garantia que ambas as partes participaram da transação, não podendo ser reivindicada posteriormente, a não participação nesta transação. Pode ocorrer de duas maneiras:

    - **Com prova de origem ou emissor**: o destinatário possui a garantia de quem é o emissor concreto dos dados.

    - **Com prova de entrega ou receptor**: o emissor possui a prova de que os dados da comunicação chegaram integralmente ao destinatário correto em um determinado momento.

O WAP permite a utilização de um modelo flexível de infra-estrutura de segurança que busca oferecer conexões seguras entre o cliente wap e o servidor. Se um *browser* e um servidor de origem desejarem, eles devem comunicar-se utilizando diretamente um protocolo WAP. O protocolo também poderá ser considerado seguro, se o WAP *gateway* for confiável, ou seja, estando localizado em um lugar fisicamente seguro, na mesma localização do servidor.

Para que o WAP consiga ser a tecnologia adotada na realização de *M-commerce*, será preciso vencer alguns desafios no que se refere à segurança. O principal deles é disponibilizar uma forma segura de processar as transações efetuadas.

Diante destes aspectos, serão apresentados no decorrer deste capítulo elementos de segurança utilizados na *Internet* e no ambiente WAP (SSL, WTLS, TLS), mostrando também as falhas de segurança e soluções já encontradas, demonstrando ao final a construção do modelo de um ambiente *wireless* seguro.

## 7.2 SSL (*Secure* Socket *Layer*)

Na *Internet*, normalmente é utilizado o protocolo SSL (*Secure Sockets Layer*, criado por *Netscape Commumications*) [FRE96], que dispõe de um nível seguro de transporte entre o serviço de transporte utilizado na *Internet* (TCP) e as aplicações que se comunicam através dele, como garantia de segurança no acesso a serviços que requerem maior preocupação com a confidencialidade dos dados transmitidos, como comercio eletrônico ou transações bancárias.

O modo de funcionamento do SSL é bastante simples, sendo composto de duas partes diferenciadas [FER00]:

- *Handshake Protocol* - Encarrega-se de estabelecer a conexão, verificando a identidade das partes (opcionalmente) e determinando os parâmetros que serão utilizados posteriormente (fundamentalmente se trata de um acordo sobre qual chave simétrica será utilizada para transmitir os dados durante esta conexão, para o qual se utiliza criptografia de chave pública).

- *Record Protocol* - Comprime, criptografa, descriptografa e verifica a informação que é transmitida desde o inicio da conexão (*handshake*).

O SSL, como protocolo de transporte seguro, proporciona somente alguns dos serviços de segurança necessários:

- confidencialidade - a informação que circula entre o cliente e o servidor que atua na frente do serviço de criptografia, utilizando criptografia de chave simétrica (com uma chave de sessão definida no *handshake*).

- autenticação - as partes que mantêm a comunicação se autenticam mediante certificados baseados em criptografia de chave pública. Isto não é sempre assim, O mais ha*bit*ual é que seja unicamente o servidor autenticado mediante um certificado digital.

- integridade - a integridade dos dados transmitidos é assegurada usando códigos de integridade (MAC) calculados mediante funções de *hash* (SHA ou MD5).

SSL além de ser bastante utilizado na WWW para codificar o fluxo de dados entre o *browser* e o Servidor *Web*, é também utilizado para o ambiente WAP. Porém, o SSL só é utilizado entre o Servidor *Web* e o WAP *gateway*. Entre o WAP *gateway* e o dispositivo WAP é utilizado um sistema semelhante chamado WTLS ou *Wireless Transport Layer Security*. O WTLS foi especialmente desenvolvido para ser utilizado em ambiente *wireless*.

## 7.3 TLS (Transport *Layer Security*)

O protocolo TLS 1.0 [DIE99] se baseia na especificação do protocolo SSL 3.0, as diferenças entre ambos são pouco significativas, permitindo a comunicação entre TLS e SSL, seu principal objetivo é oferecer privacidade e integridade dos dados, na comunicação entre duas aplicações. O protocolo é composto de duas camadas: o protocolo de gravação TLS e o protocolo TLS *Handshake*. No nível mais baixo da pilha de protocolos, acima do protocolo de transporte (por exemplo, TCP), é o protocolo de gravação TLS. O protocolo de gravação oferece uma conexão segura, com as seguintes propriedades básicas:

- conexão privada - Criptografia simétrica é utilizada para criptografar os dados (por exemplo, DES, RC4, etc.) As chaves para esta criptografia simétrica são geradas exclusivamente para cada conexão e são baseadas em um código secreto gerado por outro protocolo (como o TLS *handshake*). O Protocolo de gravação também pode ser utilizado sem criptografia.

- conexão confiável - O transporte da mensagem inclui uma mensagem de integridade que utiliza uma chave MAC. Funções de *hash* (por exemplo, SHA, MD5, etc.) são utilizados em cálculos MAC. O protocolo de gravação pode operar sem um MAC, mas geralmente só é utilizado este modo enquanto outro protocolo está usando o Protocolo de gravação como um transporte par negociar os parâmetros de segurança.

O protocolo de gravação TLS é utilizado para encapsulamento de vários protocolos situados nos níveis mais altos da pilha. A partir de seu encapsulamento, o protocolo TLS *handshake*, permite ao servidor e ao cliente autenticar um ao outro e negociar um algoritmo e uma chave de criptografia antes que o protocolo de aplicação transmita ou receba seu primeiro *byte* de dados.

O protocolo TLS *handshake* também é utilizado para fornecer segurança na conexão através de três propriedades básicas:

- a identificação do usuário pode ser autenticada utilizando cálculo assimétrico, chave pública ou criptografia (por exemplo, RSA, DSS, etc.). esta autenticação pode ser opcional, mas geralmente é requerida para pelo menos uma das partes;

- a negociação de um código compartilhado é segura: os códigos de criptografia negociados não estarão disponíveis, e em qualquer conexão autenticada o código não poderá ser obtido, até mesmo por um invasor que possa acessar a conexão;

- a negociação é confiável: nenhum invasor poderá modificar a comunicação da negociação sem ser descoberto por uma das partes envolvidas na comunicação.

### 7.3.1 Objetivos

Os objetivos propostos através da criação do Protocolo TLS são [DIE99]:

- segurança na criptografia - TLS deverá ser utilizado para estabelecer uma conexão segura entre as partes;

- interoperabilidade - Programadores independentes deverão ser capazes de desenvolver aplicações que utilizem parâmetros de troca de criptografia, sem ter conhecimento de outros códigos;

- flexibilidade - TLS procura oferecer uma estrutura que permita a incorporação de uma nova chave pública e métodos de criptografia conforme necessário. Isto previne contra a necessidade de criar um novo protocolo (arriscando a introdução de novas falhas) e evitando a necessidade de implementar uma nova biblioteca de segurança;

- relativa eficiência - Operações de Criptografia tendem a utilizar muitos recursos de CPU. Por esta razão, o protocolo TLS incorporou uma sessão opcional de *caching* para reduzir o número de novas conexões a serem estabelecidas. Este cuidado foi tomado de forma a reduzir a atividade da rede.

### 7.3.2 Segurança na Camada de Transporte

Existem dois enfoques fundamentalmente diferentes a respeito da segurança dos dados em trânsito [BEL98]. No enfoque da camada de rede, a criptografia e a autenticação são agregadas diretamente na implementação dos protocolos de rede, de modo que o tráfico seja protegido sem requerer que a aplicação incorpore alguns conceitos. O tráfico a alcançar o sistema remoto é descriptografado automaticamente e verificado pelo conjunto de protocolos de rede (por exemplo TCP/IP) antes que o sistema operacional o transfira para a aplicação no servidor. A principal desvantagem de segurança na camada de rede é que o endereço IP deve ser modificado, e estas trocas são realmente necessárias. A longo prazo as redes de alta velocidade poderiam também sofrer problemas de performance. A partir destas desvantagens foram propostos enfoques alternativos como *Secure Shell* (SSH), SSL e TLS, que funcionam na camada de transporte.

No enfoque a nível de aplicação, a própria aplicação é modificada de modo que o tráfico seja criptografado antes de ser enviado ao sistema operacional e à camada de rede, para depois ser descriptografado pela aplicação contida no servidor que o receber.

Ambos os enfoques possuem vantagens e desvantagens. Para a WWW, por exemplo, a segurança a nível de aplicações é uma opção melhor porque torna mais fácil a definição de limites de confiabilidade entre dois agentes que se encontrem realizando transações.

### 7.3.3 Diferenças entre SSL e TLS

A tabela 7.1 apresenta as principais diferenças entre as camadas SSL e TLS [BEL98].

| | **SSL** | **TLS** |
|---|---|---|
| Alerta de Erros | Durante a execução do protocolo *Handshake* o servidor deverá esperar pela resposta do cliente. Se o servidor enviar uma mensagem de requisição do certificado, o cliente deverá enviar a mensagem com o certificado ou um alerta **no_certificate**, descrito a seguir:<br><br>no_certificate: Uma mensagem de alerta no_certificate pode ser enviada em resposta a requisição do certificado se o certificado disponível não for apropriado. | Uma vez que o servidor envie uma mensagem solicitando o certificado, a resposta deverá ser enviada pelo cliente contendo o certificado. |
| Algoritmos para troca de Chaves | No SSL os algoritmos de troca de chaves existentes são RSA, Diffie Hellman e Fortezza Kea.<br><br>A nível de protocolo, o FORTEZZA é similar ao Diffie-Hellman, com valores públicos fixos, contidos nos certificados. | TLS não suporta o algoritmo de troca de chaves Fortezza Kea |
| Cálculo MAC | No SSL, no cálculo do MAC não se insere o tipo de conteúdo nem a versão do protocolo, portanto estes campos não estão protegidos de ataques contra sua integridade. | Os campos tipo de conteúdo e versão do protocolo, são protegidos, estando incluídos no cálculo MAC. |

Tabela 7.1 - Diferenças entre SSL e TLS

## 7.4 WTLS (Wireless Transport Layer Security)

O objetivo primário da camada WTLS [WAP99] (também chamada protocolo WTLS) é oferecer privacidade, integridade dos dados e autenticação entre duas aplicações enquanto estas se comunicam. A camada WTLS possui características similares ao TLS 1.0, foi desenvolvida para trabalhar com pacotes de dados em uma rede de alta latência e banda curta, além das outras limitações do protocolo WAP, como baixo poder de processamento, pouca memória e economia de bateria. O WTLS trabalha em uma camada acima do protocolo de transporte de pacotes entre o cliente e o servidor WAP.

Para trabalhar nesse ambiente o WTLS oferece, além das características do TLS, um "*handshake*" (um protocolo que é iniciado a cada conexão) otimizado e um gerenciamento de conexão mais detalhado. Com estes recursos, transações comercias como vendas *on-line* e I*nternet* banking possuem um nível de segurança confiável, porém é importante salientar que, sendo o wap um protocolo aberto, pode-se esperar novas ferramentas de segurança, assim como novos tipos de ataques e invasões.

O WTLS possui as seguintes características:

integridade de dados - O WTLS possui facilidades para assegurar que os dados enviados entre o terminal e o servidor de aplicação continuem inalterados e não sofram alterações;

privacidade - O WTLS possui facilidades para assegurar que a informação transmitida através do terminal a um servidor de aplicação seja privada e não possa ser entendida por qualquer pessoa que possa ter interceptado o fluxo de dados;

autenticação - O WTLS facilita o estabelecimento da autenticidade do terminal e do servidor;
proteção contra *Denial-of-service* – O WTLS consegue detectar e rejeitar dados que foram duplicados ou não foram verificados com sucesso. WTLS faz com que muitos ataques típicos de *denial-of-service* sejam mais difíceis de serem executados e protege as camadas de protocolos acima dele;

O protocolo WTLS é divido em dois sub-protocolos, que são o Protocolo de *Handshake* e o Protocolo de Gravação (*Record Protocol*). O acompanhamento da comunicação entre estes protocolos é realizado através de primitivas de serviços. Estas primitivas representam, de maneira abstrata, a troca de informação e controle entre a camada de segurança e as camadas adjacentes. Consistem em comandos e suas respectivas respostas, associadas com os serviços requeridos pelo outro protocolo.

### 7.4.1 Protocolo *Handshake*

O protocolo *handshake* é utilizado por WTLS para permitir que uma das partes envolvidas na conexão concorde com os parâmetros de segurança definidos, autenticar-se, iniciar estes parâmetros de segurança e informar aos outros participantes sobre as condições em que serão emitidos alertas de erro [WAP99]. A utilização de chaves dinâmicas recuperáveis permite a atualização de chaves criptográficas, verificação de parâmetros e protocolos em uma sessão, o que possibilita a detecção de um acesso externo e o fechamento da conexão.

O protocolo *handshake* também é responsável pela negociação da conexão segura, que consiste nos itens especificados na tabela 7.2.

| Item | Descrição |
|---|---|
| Identificador de Sessão | Uma seqüência de *bytes* definida pelo servidor para identificar uma sessão Segura. |
| Versão do Protocolo | Numero da versão do protocolo WTLS. |
| Ponto Certificado | Certificado do ponto. Este elemento poderá ser nulo. |
| Método de Compressão | O algoritmo utilizado para compressão dos dados a serem criptografados. |
| Especificação da Criptografia | Especifica o algoritmo de criptografia (RC5, DES, etc.) e o algoritmo MAC. Também define os atributos criptográficos. |
| Código Mestre | Código de 20 *bytes* compartilhado entre o cliente e o servidor. |
| Modo do Número de Seqüência | O esquema da seqüência numérica a ser utilizado. (chave criptográfica, cálculo de MAC). |
| Atualização de Chave | Define como será realizada a atualização dos cálculos de alguns valores de estado de conexão (Código MAC, Chave Criptográfica). |
| Resumo | Um *flag* indicando onde a sessão segura pode ser utilizada para iniciar novas conexões seguras. |

Tabela 7.2 - Itens de uma negociação segura

Estes itens serão utilizados na criação dos parâmetros de segurança da camada de gravação (Record Protocol).

Quando ocorre qualquer tipo de erro, a camada de *handshake* sinaliza a ocorrência deste erro, e envia este sinal para alertar a camada de gravação do WTLS. Estes alertas podem indicar o encerramento da conexão segura, ou um erro nesta conexão. A sinalização de erros no protocolo *handshake* é muito simples, quando um erro é detectado, à parte que o detectar envia uma mensagem para outra parte. Após a transmissão ou recepção desta mensagem que contém um alerta de erro fatal, ambas as partes imediatamente encerram a conexão segura. Os servidores e clientes envolvidos na conexão apagam qualquer identificador de sessão, chaves e códigos de criptografia associados com a conexão segura que tenha falhado. Após a transmissão ou recepção de uma mensagem de alerta crítico, ambas as partes imediatamente encerram a conexão segura, porém podem preservar os

identificadores de sessão e usa-los para estabelecer uma nova conexão segura. Na tabela 7.3 serão descritos alguns alertas de erro

| Alerta | Descrição |
|---|---|
| No_connection | Uma mensagem foi recebida enquanto não havia uma conexão segura com o emissor, esta mensagem pode ser fatal ou critica. |
| *Handshake*_failure | A recepção deste alerta indica que o emissor não pode negociar ou aceitar o conjunto de parâmetros de segurança propostos. Este é um erro fatal. |
| Session_not_ready | Ocorre quando a sessão segura não está pronta para receber novas conexões por razões administrativas, como por exemplo, a manutenção do servidor. Geralmente este é um alerta crítico. |

Tabela 7.3 – Alertas de erro

### 7.4.2 Protocolo de Gravação (*Record Protocol*)

O protocolo de Gravação WTLS recebe as mensagens a serem transmitidas, comprime os dados (opcional), aplica o código MAC, criptografa e transmite o resultado. Os dados recebidos são descriptografados, verificados e descomprimidos, passando então para o nível de apresentação do cliente [WAP99].

Vários registros podem ser concatenados em um SDU (*Service Data Unit*) de transporte. Por exemplo, várias mensagens de *handshake* podem ser transmitidas em um SDU. Isto é muito utilizado em transporte orientado à conexão, como o serviço de mensagens curtas do sistema GSM.

### 7.4.3 Gerenciamento de Conexões WTLS

O gerenciamento de conexões WTLS permite ao cliente conectar-se ao servidor e verificar as opções de protocolo a serem utilizadas. O estabelecimento de conexões seguras consiste em vários passos e tanto o cliente como o servidor podem interromper a negociação quando desejarem (ex.: se os parâmetros propostos por um dos participantes da comunicação não puderem ser aceitos). A negociação pode incluir os parâmetros de segurança (ex: algoritmos de criptografia e tamanho das chaves), troca de chaves e autenticação. Tanto o utilizador do serviço cliente ou servidor podem terminar a conexão a qualquer momento. Uma seqüência de passos deve ser seguida para estabelecer uma conexão com segurança, como mostra a figura 7.1 [WAP99].

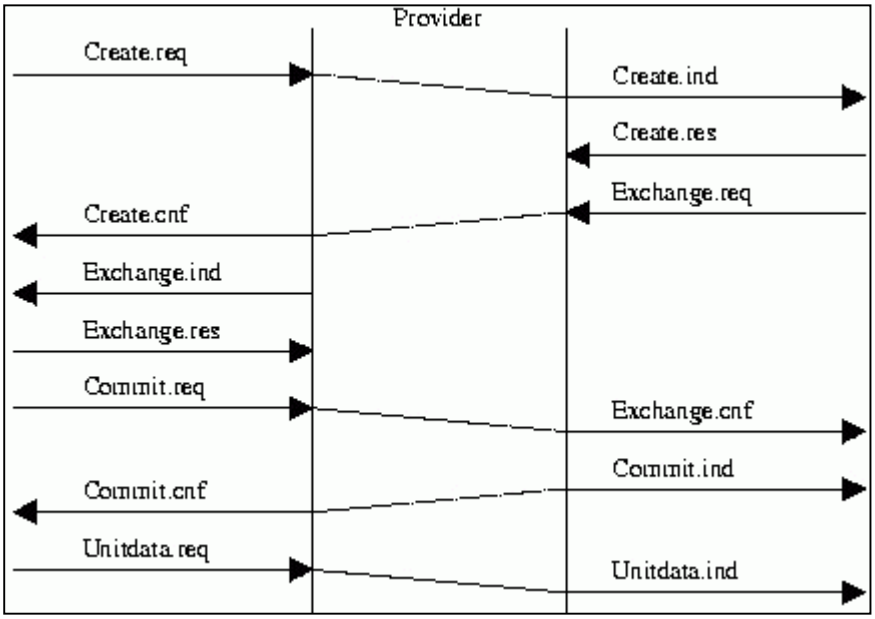


FIGURA 7.1 - *HANDSHAKE* COMPLETO

A seqüência de passos para estabelecer uma sessão segura pode ser otimizada ou abreviada, conforme demonstra a figura 7.2, embora a não execução de todos os passos necessários possa comprometer a segurança da conexão.

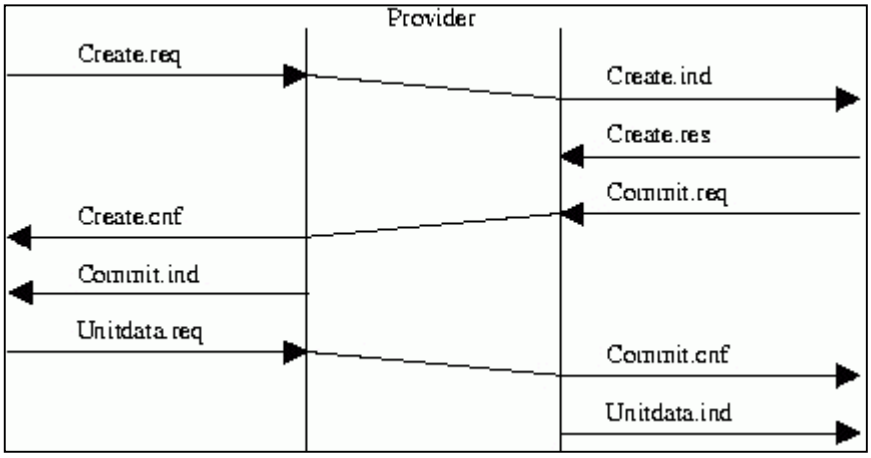


FIGURA 7.2 - *HANDSHAKE* OTIMIZADO OU ABREVIADO

## 7.5 Falhas de Segurança

Ao falar em falhas de segurança em transações e aplicações WAP, deve ser levado em consideração, que a tecnologia WAP utiliza não somente o ambiente *wireless*, mas também a troca de informações através do meio físico utilizado na WWW, portanto, além

das falhas de segurança que podem ocorrer no ambiente WAP, devem-se estar atentos para as já conhecidas falhas da WWW, tais como:

- vírus;
- *worms;*
- cavalos de tróia;
- *hackers.*

Estas falhas podem ocasionar vários danos à suas informações, como:

- destruição de informação ou de outros recursos;
- modificação ou deturpação da informação;
- roubo, remoção ou perda da informação ou de outros recursos;
- revelação de informações;
- interrupção de Serviços.

Serão apresentadas a seguir as falhas que podem ocorrer no ambiente WAP, e também, as possíveis soluções para estas falhas.

### 7.5.1 Falha de Segurança no WAP *Gateway*

Os protocolos SSL e WTLS em seus próprios domínios oferecem segurança adequada para a maioria das aplicações. Porém, há um problema de segurança em potencial onde os dois protocolos se encontram, ou seja, no WAP *gateway*.

O protocolo SSL não é diretamente compatível com WTLS, assim o WAP *gateway* deve descriptografar o fluxo de dados provenientes do servidor, que se encontram protegidos por SSL e então criptografar novamente estes dados, utilizando WTLS antes de passar os dados para o dispositivo WAP. Dentro da memória do WAP *gateway*, os dados não estarão protegidos durante um breve período de tempo conhecido como *White spoot*. O modelo atual é descrito na figura 7.3

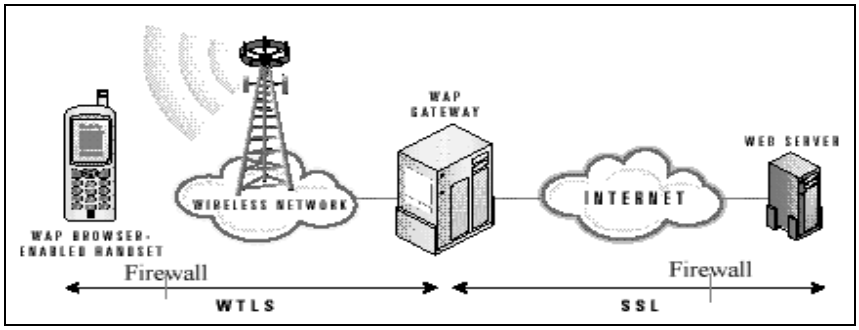


FIGURA 7.3 - MODELO UTILIZANDO CONVERSÃO DO PROTOCOLO WTLS PARA SSL

Imagine que um banco ou outra instituição que trabalhe com dados confidenciais disponibilize um serviço WAP. Quando os dados deixam a segurança de seu sistema de rede eles estão protegidos. Então, quando eles entram no WAP *gateway* que geralmente é operado por um terceiro elemento, como uma operadora de telefonia celular, os dados são

descriptografados. Neste momento, suas informações estariam disponíveis para a operadora, e se a rede da operadora for vulnerável a ataques, seus dados também estarão desprotegidos.

Todos os principais desenvolvedores WAP estão desenvolvendo soluções para este problema, porém estas soluções criam outros problemas. Desenvolvedores dos chamados "servidores WAP", ou servidores WWW com implementação de WAP *gateway* oferecem segurança de um extremo a outro da conexão, porque o fluxo de dados deixa o servidor de conteúdo (o "servidor" WAP) já codificado em WTLS. O modelo então ficaria conforme descrito na figura 7.4

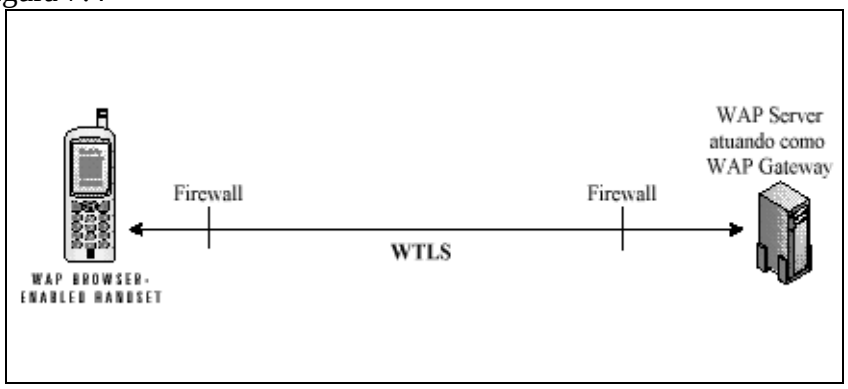


FIGURA 7.4 - MODELO UTILIZANDO APENAS O PROTOCOLO WTLS

Porém, o WAP *gateway* da operadora não poderá participar deste processo, e o usuário terá que configurar novamente o dispositivo WAP para enxergar o "servidor WAP" que se tornará o WAP *gateway* para esta sessão. Mas, este WAP *gateway* só disponibilizará acesso para o servidor configurado, porém, quando o usuário for acessar outro *site* WAP, ele terá que configurar novamente seu telefone.

Somando a este problema o fato que muitos operadores móveis oferecem o serviço ponto-a-ponto, onde o dispositivo móvel efetua a conexão, e o WAP *gateway* no mesmo IP privado percorre a rede, normalmente atrás de um *firewall*. Este *firewall* normalmente só é configurado para permitir a utilização do protocolo HTTP na porta 80 [FIE97] que é padrão para este protocolo. O WAP *gateway* utiliza esta porta para receber dados de servidores de conteúdo na *Internet*, e tudo que for necessário. Quando o dispositivo WAP tenta acessar outro WAP *gateway* na *Internet*, o *firewall* não permitirá, porque o *firewall* diz que o endereço IP do dispositivo WAP não está configurado para realizar o roteamento dos dados na *Internet*, ou que não pode abrir as portas necessárias. Isto efetivamente faz com que o usuário deixe de utilizar outros *gateways* que não sejam o oferecido pela operadora.

Outra forma de compensar a brecha de segurança apresentada pelo WAP *gateway*, é a utilização da linguagem WMLScript criptografada, que fornece segurança a partir da camada de aplicação WAE, assim a segurança dos dados não ficará restrita a segurança oferecida pela camada WTLS, pois será criptografada diretamente em sua linguagem, e também durante o transporte dos dados.

### 7.5.2 Autenticação do usuário

A ausência de criptografia de um extremo a outro da conexão não é a única falha de segurança encontrada no modelo WAP. Se perderá também a autenticação entre as partes. A existência de dois domínios tecnológicos provoca o surgimento de duas autenticações diferentes, pois o dispositivo móvel é autenticado junto ao WAP *gateway* e não ao servidor de conteúdo e o WAP *gateway* apenas eventualmente oferece autenticação ao servidor, embora seja de extrema importância a utilização de certificação digital para WAP *Gateway*/*Server*.

A principio, a autenticação dos usuários deve ser similar a utilizada na *internet*. A maneira mais simples é utilizar um conjunto de chaves integradas com a própria autenticação do Servidor *Web*, porém a tecnologia WAP pode utilizar os elementos de autenticação próprios da rede GSM. A partir do momento que o dispositivo WAP estiver autenticado na rede GSM, o operador telefônico poderá enviar o número de telefone ao servidor de conteúdos em forma de um cabeçalho HTTP, desde que este número esteja criptografado, para que somente a aplicação que possuir a chave para descriptografar este número possa obtê-lo.

Outra solução, que tende a se tornar padrão para a realização da autenticação do usuário, é a utilização de uma PKI (*Public Key Infrastructure*) ou seja, um sistema de chave pública compatível com SSL, através do qual será possível transmitir dados criptografados de forma segura, pois somente será necessário saber a chave pública utilizada pelo destinatário da transmissão. Não existe portanto uma troca das chaves secretas entre os participantes da transmissão, o que normalmente torna a mesma menos segura, sendo que cada participante da conexão possui uma chave secreta que não necessita ser revelada.

## 7.6 Modelo de Ambiente WAP Seguro

Conforme visto nos capítulos anteriores, para que uma transação realizada em WAP possa ser considerada segura, deverão ser utilizados:

- criptografia de 128 *Bits*, a nível de aplicação e transporte;
- *gateway* com implementação de segurança;
- autenticação digital através de PKI;
- certificação digital;
- *firewall*.

A utilização dos itens acima citados, está representada na figura 7.5.

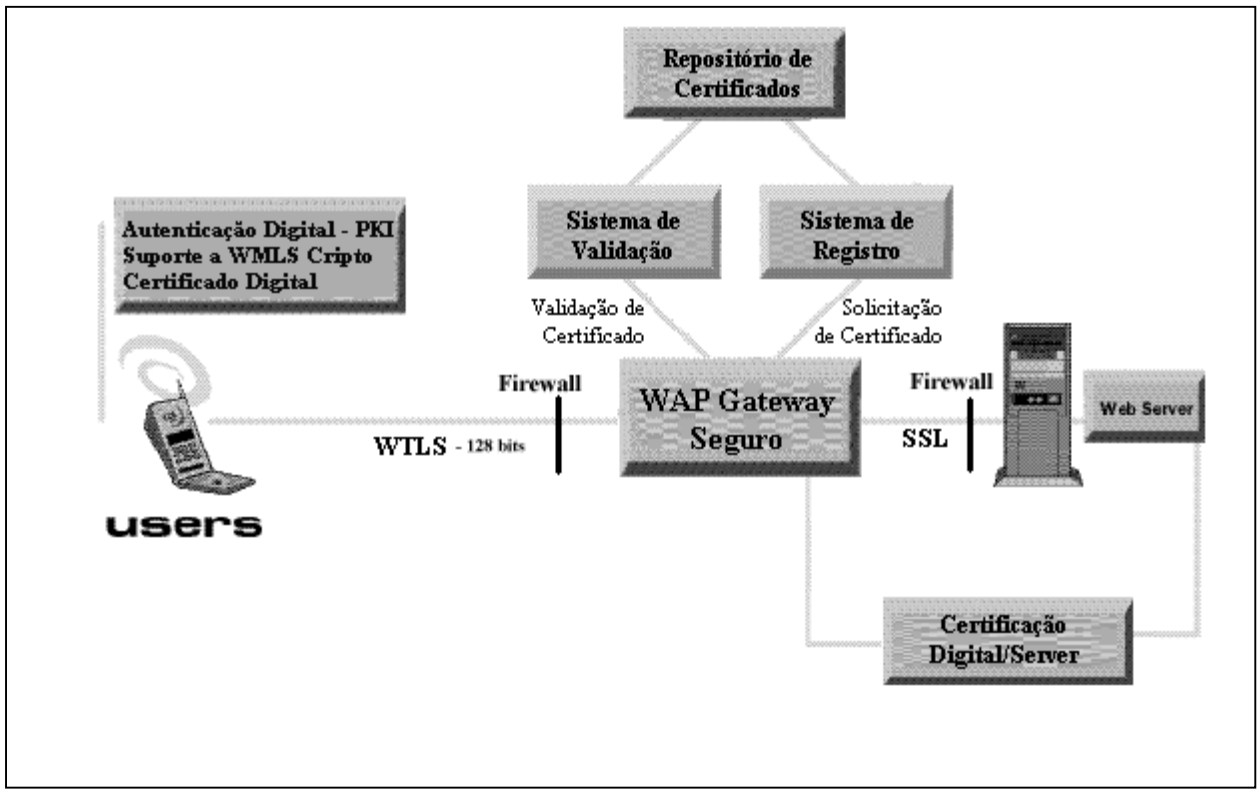


FIGURA 7.5 - REPRESENTAÇÃO DE AMBIENTE WAP SEGURO

# 8 Conclusão

Por tratar-se de uma tecnologia nova, da qual pouco se conhece ainda, torna-se complicado falar sobre o tema "WAP". Duas correntes surgiram em torno do WAP, uma afirma que o WAP é apenas mais uma tecnologia passageira, a outra afirma que esta é a nova revolução no acesso a Internet, e deve firmar-se cada vez mais como tendência de mercado. Nosso objetivo porém não é realizar especulações em torno do futuro comercial da tecnologia WAP, mas sim analisar aspectos técnicos como a arquitetura e principalmente a segurança do mesmo.

Com base no que foi visto durante a realização deste estudo, chega-se a conclusão que as transações realizadas em WAP oferecem um nível de segurança bastante satisfatório, porém, conforme aumentar o volume de transações realizadas, e principalmente, o valor das informações que estarão disponíveis, aumentarão também as tentativas de acesso não autorizado à estas informações. Isto faz com que os desenvolvedores da tecnologia WAP preocupem-se cada vez mais em implementar novas ferramentas para tornar o WAP cada vez mais seguro.

Dois fatores levam os usuários a realizarem operações de comércio eletrônico, segurança e comodidade. Neste caso a segurança diz respeito ao medo de assaltos, seqüestros e outros. Mas se o usuário não sente-se seguro para ir a uma loja realizar compras, é preciso mostrar ao usuário que o nível de segurança apresentado nas operações de comércio eletrônico é realmente confiável, para que o mesmo sinta-se à vontade para disponibilizar informações confidenciais através da Internet. Mas as atividades de comércio eletrônico ainda são um fato recente na vida da maioria dos usuários da Internet, antes acostumados apenas a realizar pesquisas e trocar e-mail. Estes usuários, por mais que sintam-se preparados para as novas tecnologias que surgem a cada dia, sentem-se ainda receosos de realizar operações de comércio eletrônico através de seu telefone celular ou de qualquer outro dispositivo móvel dotado de tecnologia WAP.

Em países da Europa, berço da tecnologia WAP, apenas 2% dos usuários de Internet utilizam os serviços disponibilizados em WAP [OVU00]. Isto deve-se basicamente a falta de qualidade nos serviços oferecidos e  a falta de confiança na tecnologia WAP, por parte dos usuários. Para que o usuário adquira a confiança necessária a utilização do WAP, é necessário que existam estudos como este, demonstrando não somente aspectos relativos a segurança, mas também ao potencial e as facilidades que a tecnologia WAP irá proporcionar.

# Referências Bibliográficas

[BEL98] Belingueres, Gabriel, Balbi, Luciana, Serafino, Sandra. Transport Layer Security 1.0. 1998. Disponível por www em www.geocities.com/SiliconValley/Byte/4170/articulos/tls/index.htm. Acessado em 27/10/2000.

[DIE99] Dierks, T., Allen, C., The TLS Protocol version 1.0, RFC 2246. 1999. Disponível por www em ftp://ftp.isi.edu/in-notes/rfc2046.txt. Acessado em 27/10/2000.

[ECO99] The economist, The end of Privacy. maio 1999. Disponível por www em http://www.economist.com/library/focus/displayStory.cfm?story_id=202103. Acessado em 29/10/2000.

[FER00] Fernandez, P. Juan, Seguridad en WAP. Madri: 2000. Disponível por www em http://www.wmlclub.com/articulos/seguridad.htm. Acessado em 13/10/2000.

[FIE97] Fielding, R. et. Al., Hypertext Transfer Protocol -- HTTP/1.1, RFC 2068, 1997. Disponível por www em ftp://ftp.isi.edu/in-notes/rfc2068.txt. Acessado em 08/10/2000.

[FRE96] Freier, A. O., Karlton, P. y Kocher, P. C. "*The SSL Protocol Specification 3.0*". 1996. Disponível por www em http://home.netscape.com/eng/ssl3/. Acessado em 02/10/2000.

[GSM99] History of GSM, Disponível por www.gsmworld.com/about/history_gm.html Acessado em 12/09/2000.

[IEEE99] IEEE Computer Society. IEEE Standard 802.11, 1999 Edition. 1999. Disponível por www em http://standards.IEEE.org/reading/IEEE/std/lanman/MIB-D6.2.txt. Acessado em 18/09/2000.

[ISO89] ISO. Information Processing Systems - OSI - Basic Reference Model, ISO/IEC IS 7498. 1989.

[LAD00] Ladeira, Marcelo. Telefonia Celular, Poa: UFRGS. Disponível por www em www.penta.ufrgs.br/tp951/tccd_ml.html Acessado em 05/09/2000.

[MOU86] MOURA, J. et al. Redes Locais de Computadores: protocolos de alto nível e avaliação de desempenho, São Paulo: McGraw-Hill, 1986.

[OVU00] OVUM Consultancy Ltda.. 2000. Disponível por www em www.ovum.com. Acessado em Outubro de 2000.

[PHO99] Phone.com. The Wireless Application Protocol. Wireless Internet Today, Redwood City: 1999. Disponível por www em www.phone.com/pub/feb99WAPWP.pdf. Acessado em 05/08/2000

[ROS99] Rosa, Miguel. IPv6 - IP Next Generation - Estudos sobre o protocolo IP de Nova Geração. FCUL - Faculdade de Ciências da Universidade de Lisboa, Departamento de Informática, Lisboa: 1999. Disponível por www em www.ip6.fc.ul.pt. Acessado em 12/09/2000.

[SOA95] Soares, G. Luiz Fernando, Lemos, Guido, Colcher, Sérgio. Redes de Computadores. Das LANs, MANs e WANs às Redes ATM, Rio de Janeiro: Campus, 1995

[SOU99] Souza, B. Lindeberg. Redes de Computadores. Dados, Voz e Imagem, São Paulo: Editora Érica, 1999

[TAN94] Tanenbaum, S. Andrew. Redes de Computadores, Rio de Janeiro: Campus, 1994.

[WAP98] Wap Forum, Wireless Application Protocol Architecture Specification, 1998 Disponível por www em http://www1.wapforum.org/tech/terms.asp?doc=WAP-100-WAPArch-19980430-a.pdf. Acessado em 17/08/2000.

[WAP99] Wap Forum, Wireless Transport Layer Security Specification, 1999 Disponível por www em http://www1.wapforum.org/tech/terms.asp?doc=WAP-100-WTLS-19991105.pdf. Acessado em 17/08/2000.

[WAP00] WAPBrasil, WAP (Wireless Application Protocol). 2000, Disponível por www em www.wapbr.com.br/forum/artigos/wap.asp. Acessado em 09/08/2000.

[WAP00a] WapClub, História do WAP. 2000, Disponível por www em www.wapclub.com.br/wap_historia.asp. Acessado em 26/07/2000.

# Anexo

## A - Funcionamento de Internet Através de Ondas de Rádio

No dia 01 de setembro de 2000, foi realizada visita ao Senac - Bagé, com o propósito de acompanhar o funcionamento do acesso à Internet através de ondas de rádio. A equipe responsável pela implantação deste modo de acesso wireless em Bagé realizou demonstrações relativas a configuração do servidor, qualidade do acesso, e também à segurança, como a utilização de endereço MAC, citado na norma IEEE 802.11.

## B - Participação no V JAT - UFRGS/SOFTSUL

Durante os dias 22 e 23 de novembro de 2000, foi realizado em Porto Alegre - RS, na sede da EMBRATEL, o V JAT (Jornada de Atualização Tecnológica) em convênio com a UFRGS (Universidade Federal do Rio Grande do Sul) e SOFTSUL (Sociedade Sul-Riograndense de Apoio ao Desenvolvimento de Software), com o tema "WAP Aplicações e Serviços". Neste seminário foram realizadas diversas trocas de experiências entre desenvolvedores de aplicações WAP, salientando a preocupação com aspectos como segurança, infra-estrutura e tendências quanto ao futuro desta nova tecnologia, evidenciando a relevância deste trabalho, frente aos anseios apresentados por outros pesquisadores e desenvolvedores WAP presentes ao evento.

## C - Serviços WAP - TAM

Foi apresentado, através dos integrantes da equipe de projetos da TAM - Marcos Roberto Teixeira e Roberto Abreu Mantegassi o sistema de venda de passagens aéreas para ambiente WAP, que permite ao cliente, após a compra do ticket, demonstrada na seqüência de figuras A1.1, A1.2, A1.3 e A1.4, apresentar-se diretamente ao balcão de check-in, munido apenas de um documento de identificação. Este serviço, desenvolvido em parceria com a Telesp, oferece mobilidade ao cliente, pois permite que o ticket seja adquirido até mesmo quando já se estiver a caminho do aeroporto, ou até mesmo dentro dele. Posteriormente, também serão oferecidos serviços como:

- Informações sobre atraso de vôos
- Acompanhamento de Volume Despachado
- Informações e Promoções Personalizadas

Este serviço é oferecido através de um sistema de Broadvision One-to-one demonstrado nas figuras A1.5 e A1.6, possibilitando ao cliente a oportunidade de interagir diretamente com a companhia aérea, ao invés de realizar a compra através de terceiros.

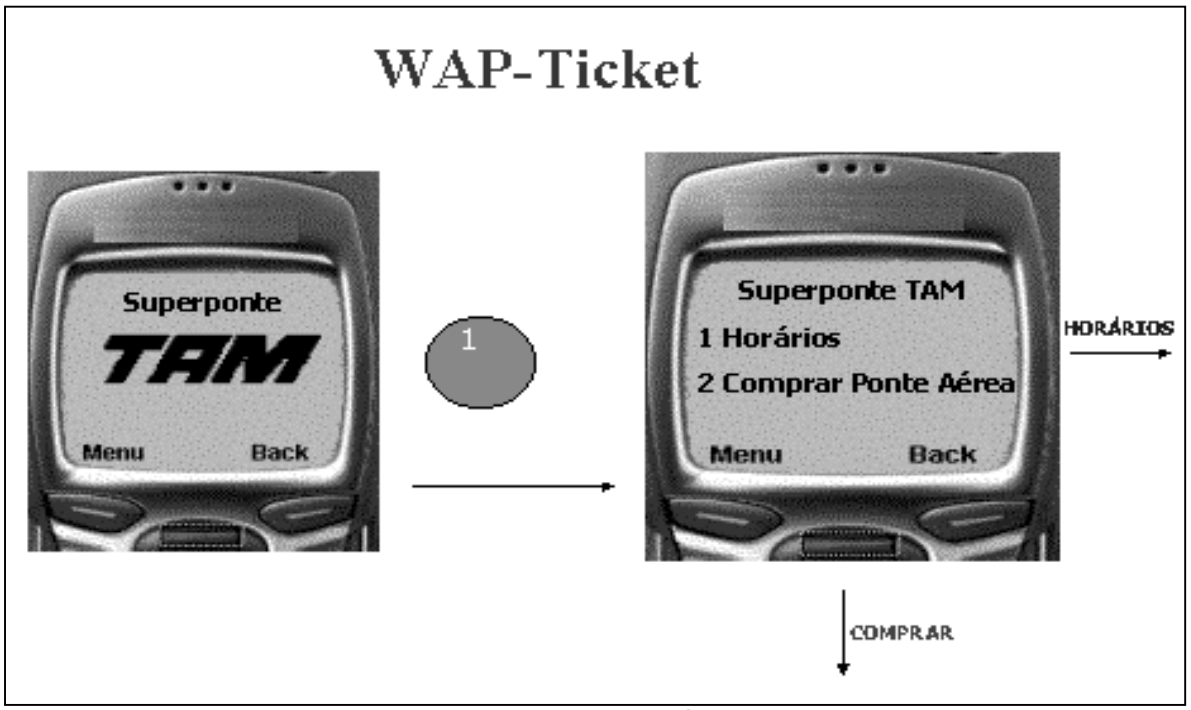


FIGURA A1.1 - SISTEMA DE COMPRA DE PASSAGENS AÉREAS UTILIZANDO WAP

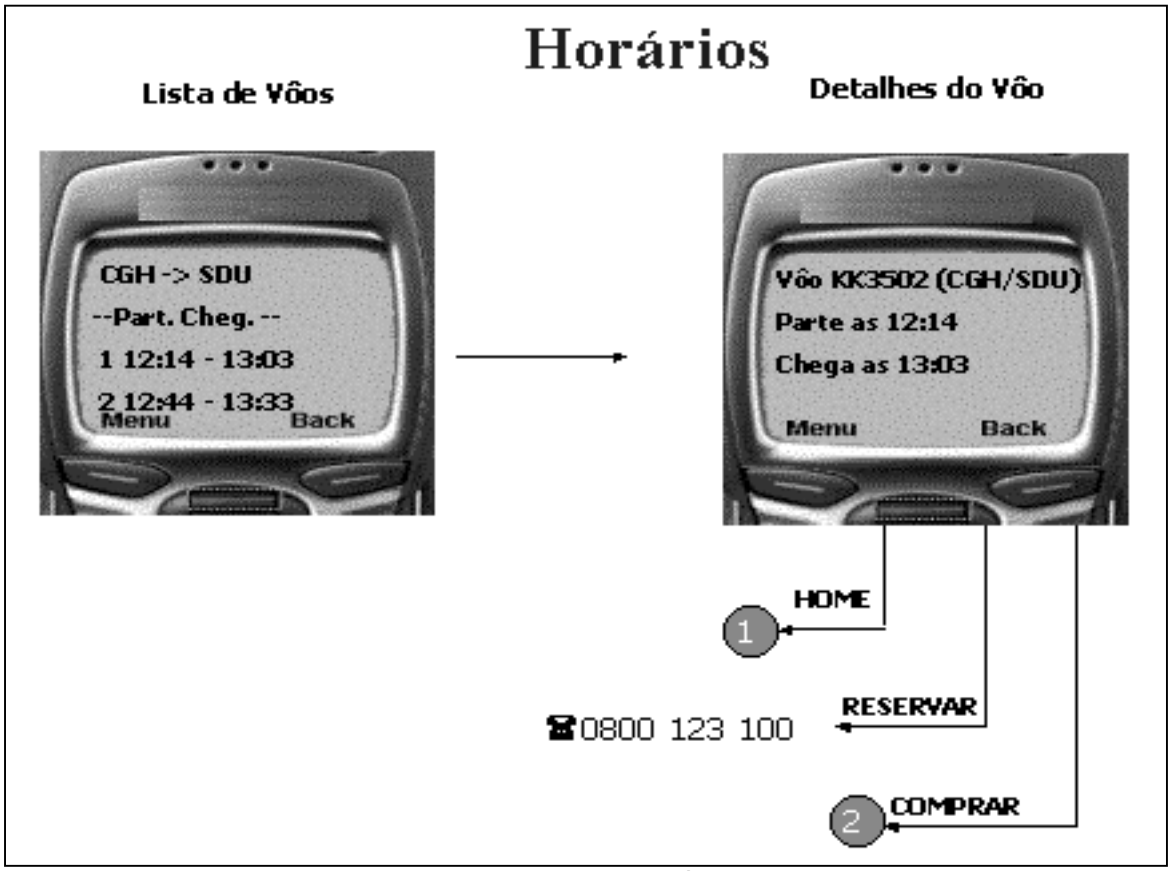


FIGURA A1.2 - SISTEMA DE COMPRA DE PASSAGENS AÉREAS UTILIZANDO WAP

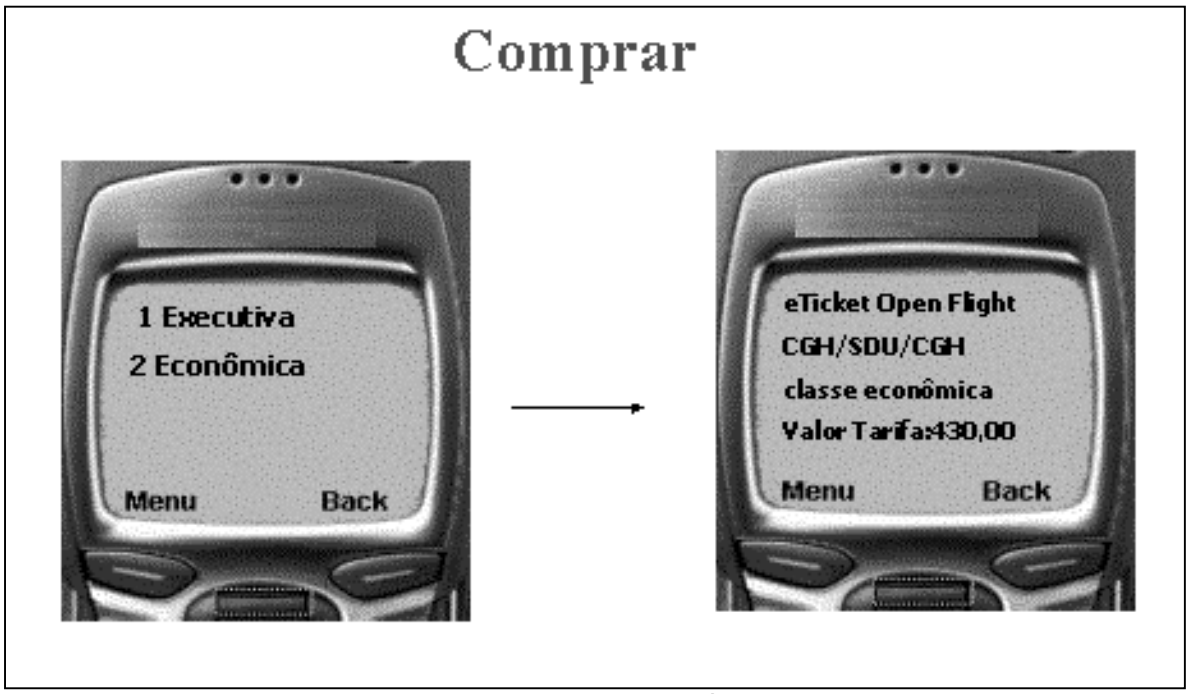


FIGURA A1.3 - SISTEMA DE COMPRA DE PASSAGENS AÉREAS UTILIZANDO WAP

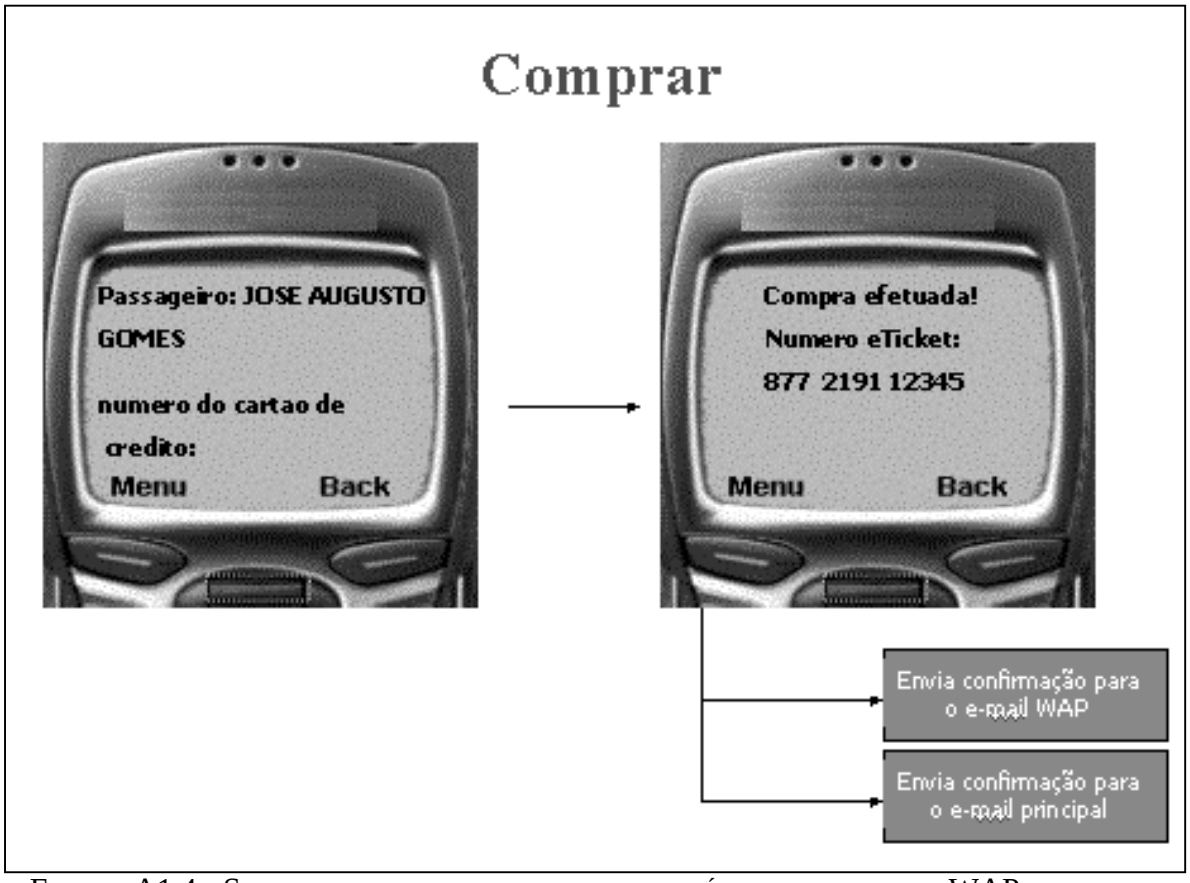


FIGURA A1.4 - SISTEMA DE COMPRA DE PASSAGENS AÉREAS UTILIZANDO WAP

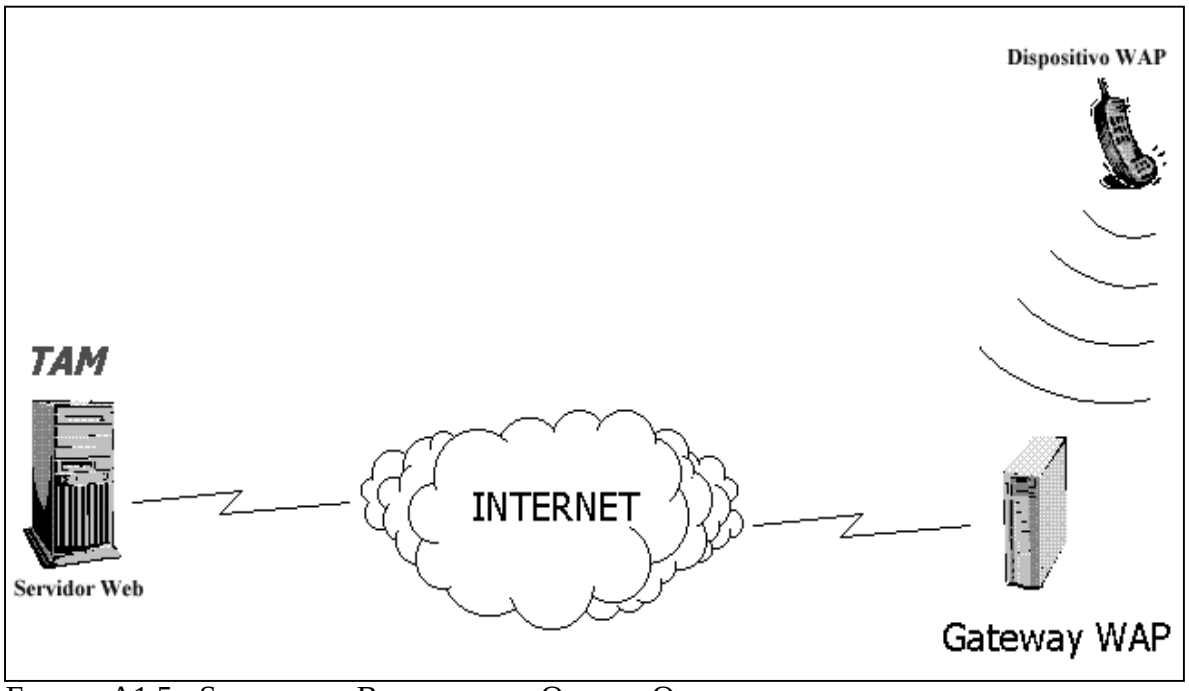


FIGURA A1.5 - SISTEMA DE BROADVISION ONE-TO-ONE

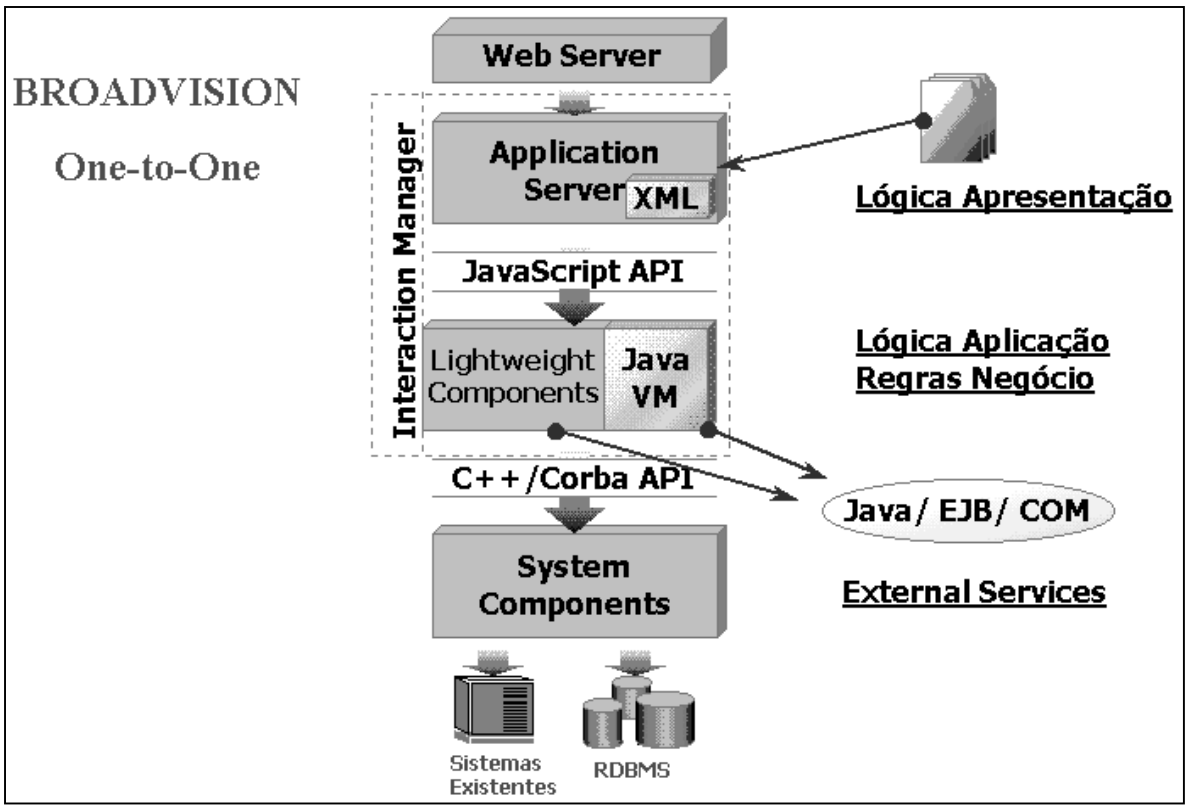


FIGURA A1.6 - SISTEMA DE BROADVISION ONE-TO-ONE