**Integração entre Redes Locais sem Fio (WLANs) e Redes de Sistemas Celulares**

*Roberto Bresil*

**Trabalho Final de Mestrado Profissional**

Instituto de Computação
Universidade Estadual de Campinas

# Integração entre Redes Locais sem Fio (WLANs) e Redes de Sistemas Celulares

**Roberto Bresil**

Agosto de 2004

**Banca Examinadora:**

- Prof. Dr. Nelson Luis Saldanha da Fonseca (Orientador)
- Prof. Dr. Fabrizio Granelli
  University of Trento - Italy
- Prof. Dr. Ricardo Dahab
  Instituto de Computação - UNICAMP
- Prof. Dr. Edmundo R. M. Madeira
  Instituto de Computação - UNICAMP

**FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP**

Bresil, Roberto

B754i Integração entre redes locais sem fios (WLANs) e redes dos sistemas celulares / Roberto Bresil – Campinas, [S.P. :s.n.], 2004.

Orientadores : Nelson Luis Saldanha da Fonseca; Omar Carvalho Branquinho

Trabalho final (mestrado profissional) – Universidade Estadual de Campinas, Instituto de Computação.

1. Redes locais de computação. 2. Telefonia celular. 3. Computadores - Controle de acesso. 4. Convergência tecnológica. 5. Sistemas de comunicação sem fio. I. Fonseca, Nelson Luis Saldanha da. II. Branquinho, Omar Carvalho. III. Universidade Estadual de Campinas, Instituto de Computação. IV. Título.

# Integração entre Redes Locais sem Fio (WLANs) e Redes de Sistemas Celulares

Este exemplar corresponde à redação final do Trabalho Final devidamente corrigida e defendida por Roberto Bresil e aprovada pela Banca Examinadora.

Campinas, 13 de Outubro de 2004

Prof. Dr. Nelson Luis Saldanha da Fonseca
(Orientador)

Prof. Dr. Omar Carvalho Branquinho
(Co-Orientador)

Trabalho Final apresentado ao Instituto de Computação, UNICAMP, como requisito parcial para a obtenção do título de Mestre em Computação na área de Redes de Computadores.

## Resumo

As WLANs conseguem atingir altas taxas de transmissão de dados quando comparadas às taxas de transmissão de dados atingidas pelos sistemas celulares. Estas altas taxas de transmissão têm chamado a atenção das operadoras de redes celulares as quais começam a ver a possibilidade de uso das WLANs como um complemento às suas redes de acesso para transmissão de dados, cujo objetivo principal é o de prover maiores taxas de transmissão de dados aos usuários de telefones celulares em localidades públicas, conhecidas como *hotspots*, onde existem WLANs instaladas.

Esta dissertação tem foco na convergência entre as redes WLAN padrão IEEE 802.11 e os sistemas celulares GSM/GPRS/UMTS, visando a integração destas duas redes através da utilização dos cartões SIM/USIM. São comparadas as arquiteturas de acoplamento *Loose Coupling* e *Tight Coupling*, considerando aspectos relacionados ao controle de acesso e segurança, *roaming*, mobilidade, tarifação e suporte das redes WLANs e celulares.



## Abstract

WLANs can reach high data transmission rates when compared to the data transmission rates reached by the cellular systems. These high data transmission rates are getting attention from the cellular network operators that starting looking at the WLANs as a complement to their access data network. The main target is to provide high data transmission rates to their subscribers in public locations, known as hotspots, where there are WLANs installed.

This work focuses in the interworking between the IEEE 802.11 WLAN and the GMS/GPRS/UMTS cellular systems, considering services for SIM/USIM card users. Two interworking architectures, Loose Coupling and Tight Coupling, are compared considering aspects like access control and security, roaming, mobility, billing and support for the WLAN and cellular networks.

# Dedicatória

Dedico este trabalho aos meus pais Reinaldo e Clara.

# Agradecimentos

Agradeço a Deus pela ter me dado a oportunidade de realizar este trabalho.

Aos meus pais, Reinaldo e Clara, e às minhas irmãs, Elizete e Célia, pelo apoio recebido.

Aos funcionários do IC, especialmente à Claudia, Ione e Olívia pelos favores e pelos problemas resolvidos com toda atenção e simpatia durante o curso.

Aos amigos de trabalho e do curso de Mestrado Profissional Luis Lemos, Sidney Kawamura, Paulo Roberto Dias Martins, Rogério Moreira, Vinícius Asta Pagano, Rodrigo Burger, Sandro Dangui, Alessandro Santos, Ana Cristina Cabral, Mauricio Sanches, Valéria Reis, Helder Pinho, Paulo Henrique Tavares e todos os outros amigos que de alguma forma contribuíram para a realização deste trabalho.

Aos mestres Nelson e Omar pela orientação, paciência, apoio e atenção fornecidos durante a realização deste trabalho.

# Conteúdo

Resumo ..... vi
Abstract ..... vi
Dedicatória ..... vii
Agradecimentos ..... viii
Conteúdo ..... ix
1. Introdução ..... 1
2. As Redes de Sistemas Celulares GSM, GPRS e UMTS ..... 5
2.1. As Redes GSM/GPRS ..... 5
2.1.1. Plano de Transmissão em GPRS ..... 7
2.2. As Redes UMTS ..... 8
2.2.1. Arquitetura de Protocolos do UMTS ..... 9
2.2.2. Integração de Sistemas GSM, GPRS e UMTS ..... 10
3. Rede Local sem Fio ..... 12
3.1. O Padrão IEEE 802.11 ..... 12
3.1.1. A Arquitetura 802.11 ..... 14
3.1.2. As Camadas da Arquitetura 802.11 ..... 15
3.1.3. Associação e Reassociação das Estações 802.11 aos AP ..... 15
3.1.4. Evolução das WLANs ..... 16
3.1.5. Segurança e Autenticação no 802.11 ..... 16
3.1.6. Melhorias de Segurança e Autenticação no 802.11 ..... 18
3.2. Wireless Switches ..... 24
3.2.1. Pilha de Protocolos nas Arquiteturas *fat AP* e *thin AP* ..... 26
3.2.2. Interoperabilidade e Padronizações ..... 27
3.2.3. Modelo da arquitetura *thin AP* ..... 27
3.3. WLANS Públicas (PWLAN) ..... 28
3.3.1. Arquitetura de uma WLAN pública ..... 29
4. Integração das WLANs com os Sistemas Celulares ..... 31
4.1. Padronizações ..... 32
4.1.1. Cenário 1: Tarifação e Atendimento ao Cliente Comuns. ..... 33
4.1.2. Cenário 2: Controle de Acesso e Tarifação Baseado no Sistema Celular ..... 33
4.1.3. Cenário 3: Acesso aos Serviços de 3GPP/GPRS ..... 33
4.1.4. Cenário 4: Continuidade de Serviços ..... 34
4.1.5. Cenário 5: Continuidade de Serviço sem Interrupções ..... 34
4.1.6. Cenário 6: Acesso aos Serviços de Comutação por Circuito do Sistema celular 35
4.2. Arquiteturas de Interconexão entre Sistemas Celulares e WLANs ..... 35
4.3. Acoplamento de Redes UMTS/GPRS com WLAN 802.11 ..... 38
5. A Arquitetura *Loose Coupling* ..... 39
5.1. Autenticação e Acesso aos Serviços ..... 41
5.1.1. Autenticação GSM/GPRS ..... 42
5.1.2. Autenticação UMTS ..... 44
5.1.3. Formato de Identificação do Usuário ..... 47

5.1.4. Autenticação EAP SIM ..... 49
5.1.5. Autenticação EAP AKA ..... 52
5.1.6. Plano de Controle de Autenticação EAP SIM/AKA ..... 55
5.2. Billing e Accounting ..... 56
5.3. Mobilidade ..... 59
5.4. Roaming de Usuários ..... 61
5.5. Plano de Controle do Usuário ..... 63
6. A Arquitetura *Tight Coupling* ..... 65
6.1. Pilha de Protocolos no Terminal ..... 68
6.2. A Função "Inter-Working" ..... 70
6.3. A Função de Adaptação para WLAN ..... 71
6.4. O Protocolo EAP GPRS ..... 73
6.5. O Plano de Controle de Sinalização e Dados de Usuário ..... 78
7. Conclusões ..... 80
7.1. A Evolução da WLAN IEEE 802.11 ..... 80
7.2. Wireless Switch como Elemento Centralizador ..... 81
7.3. Comparação entre os acoplamentos Tight e Loose Coupling ..... 82
7.3.1. Servidor de Autenticação ..... 82
7.3.2. Mobilidade ..... 83
7.3.3. O Sistema de *Billing* ..... 84
7.3.4. O Controle de Acesso ..... 84
7.3.5. Suporte do AP ao Controle de Acesso ..... 85
7.3.6. Suporte ao Terminal ..... 85
7.3.7. Plano de Dados de Usuário e o Processamento de Dados Enviados e Recebidos no Terminal ..... 86
7.3.8. Velocidade de Acesso à Internet ..... 87
7.3.9. A Conexão da WLAN ao CN GPRS/UMTS ..... 87
7.3.10. Interconexão com Hotspots já Existentes ..... 88
7.4. Considerações Finais ..... 89
7.5. Trabalhos Futuros ..... 91
8. Lista de Abreviações ..... 92
9. Referências Bibliográficas ..... 105

# 1. Introdução

As redes sem fio vêm apresentando um grande desenvolvimento nos últimos anos e atualmente estão presentes em vários ambientes com diferentes tipos de soluções. Elas atuam desde o ambiente doméstico, o chamado *home cell* ou *Wireless Personal Area Network* (WPAN), fazendo a comunicação entre dispositivos dentro de uma residência ou escritório, até as redes de sistemas celulares, as chamadas *Wireless Wide Area Network* (WWAN), passando pelas *Wireless Local Area Network* (WLAN) e *Wireless Metropolitan Area Network* (WMAN)

A Figura 1.1 ilustra a classificação das redes sem fio.

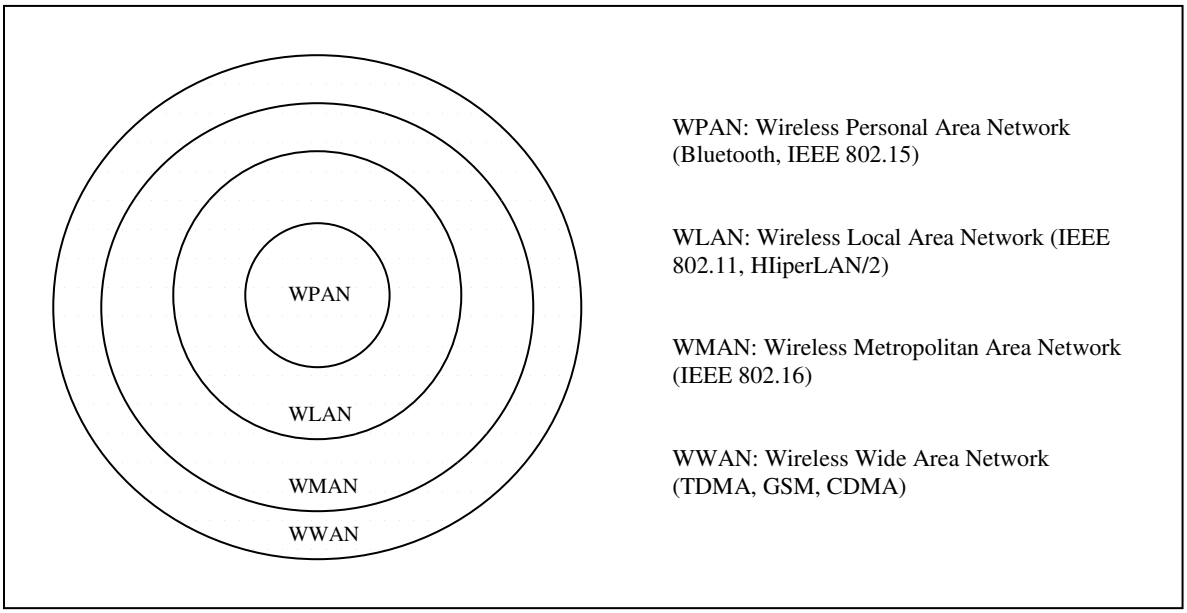


Figura 1.1. Classificação das redes sem fio.

Existe uma tendência de integração entre estes tipos de redes, apesar de existir conflitos entre diferentes soluções para o mesmo ambiente, como é o caso das WPANs e WLANs.

As WLANs conseguem atingir altas taxas de transmissão de dados quando comparadas às taxas de transmissão de dados atingidas pelos sistemas celulares. Estas altas taxas de transmissão têm chamado a atenção das operadoras de redes celulares, as quais começam a ver a possibilidade de uso das WLANs complementando suas redes atuais a fim que seus clientes

possam usufruir maiores taxas de transmissão de dados. A interconexão entre as WLANs e a redes celulares tem como objetivo principal prover maiores taxas de transmissão de dados aos usuários de telefones celulares em localidades públicas, conhecidas como *hotspots*, onde existem WLANs instaladas.

As redes dos sistemas celulares vêm crescendo dia a dia e o telefone celular já não é mais um dispositivo caro e considerado de luxo; ao contrário, passou a ser barato e acessível para muitas pessoas. Os primeiros sistemas celulares móveis, os chamados 1G ou primeira geração, foram disponibilizados comercialmente no início da década de 80 e eram todos analógicos. Durante a década de 80 surgiram os sistemas digitais 2G, ou segunda geração, como o GSM, o TDMA e o CDMAOne, os quais foram implantados na década de 90. Mais recentemente, outros sistemas conhecidos como 2,5G, ou segunda geração e meia, como o GPRS e CDMA2000 1xRTT, e 3G, ou terceira geração, como o UMTS, o CDMA 1xEV-DO e o CDMA 1xEV-DV, vêm sendo disponibilizados comercialmente, apresentando características de transmissão de dados por pacote, não existente em sistemas 2G.

Inicialmente, as operadoras das redes celulares ofereciam somente o serviço de voz, mas a massificação dos dispositivos móveis, o barateamento dos equipamentos e a expansão das redes celulares fizeram com que outros serviços pudessem ser agregados juntos aos dispositivos móveis, por exemplo, acesso à Internet. No entanto, as taxas de transmissão suportadas pelas redes celulares e pelos dispositivos móveis 2G, eram insuficientes para atender certos tipos de serviços. O sistema GSM, por exemplo, é capaz de oferecer serviços de transferência de dados, no entanto, a taxa de transmissão chega até 14,4 Kbps [De Vriendt]. Com isso houve um grande movimento por parte de fabricantes e operadoras em busca de equipamentos e soluções que pudessem suportar taxas maiores de transmissão de dados em redes por pacotes. Este movimento levou a padrões conhecidos como 2,5G (segunda geração e meia) e 3G (terceira geração), os quais começam aos poucos a aparecer no mercado. Exemplos de sistemas 2,5G são o GPRS, com taxas máximas de 172 kbps [Ala-Laurila] e o CDMA2000 1xRTT, com taxas máximas de 144 kbps [De Vriendt]. Exemplos de sistemas 3G são o UMTS, com taxas máximas de 2 Mbps [Ala-Laurila], o CDMA 1xEV-DO e o CDMA 1xEV-DV com promessas de taxas máximas de 2,4 Mbps e 3 Mbps, respectivamente [De Vriendt].

Paralelamente às redes de sistemas móveis, a tecnologia de comunicações sem fio também promoveu um grande desenvolvimento na área das redes locais, surgindo as redes

locais sem fio (WLANs), as quais conseguem atingir taxas de transmissão mais altas que aqueles atingidas pelas redes de telefonia celular 3G. Atualmente as WLANs conseguem taxas de até 54 Mbits/s [802.11a] [80211g] e existem promessas de se atingir 100 Mbps [802.11n], sendo o padrão predominante o 802.11b, também conhecido como Wi-Fi, com taxas máximas de 11 Mbps.

As operadoras de redes de telefonia celular e fabricantes de equipamentos de Telecomunicações começaram então a ver a possibilidade de uso das WLANs complementando as redes celulares a fim de usufruir das altas taxas de transmissão das WLANs para o acesso a dados dos dispositivos móveis.

As redes celulares 2G se mostraram incapazes de prover uma taxa satisfatória para transmissão de dados em dispositivos móveis. A necessidade de altas taxas de transmissão levou aos padrões 2.5G e 3G os quais podem estabelecer conexões de até 172 kbps e 2 Mbps, respectivamente.

Já as WLANs apresentam maiores taxas de transmissão e baixo custo de instalação quando comparado com os sistemas celulares. Os operadores de redes celulares reconhecem que as WLANs apresentam um importante papel em comunicação de dados sem fio e começam a enxergar as WLANs como um forte aliado para integração em suas redes de dados. O interesse das operadoras nas WLANs também baseia-se no fato de que se espera que as WLANs sejam instaladas em lugares públicos como hotéis, aeroportos, bares e cafés. Uma vez que as WLANs estejam integradas às redes celulares, os usuários do sistema celular podem usufruir das altas taxas providas pela WLAN nos lugares públicos, conhecidos como *hotspots*.

Tem sido intensamente debatido ultimamente a interconexão entre as WLANs e os sistemas celulares. Especula-se que as WLANs podem vir a substituir a tecnologia 3G, bem como inibir seu desenvolvimento. Por outro lado, o UMTS Fórum [UMTSForum] descreve a WLAN como sendo um complemento para os serviços 3G [Report 22].

O 3GPP (*Third Generation Partnership Project*), o qual é uma associação de organizações padronizadoras da Europa, EUA, Japão, e Coréia do Sul, também tomou a iniciativa de desenvolver uma arquitetura de interconexão entre as WLANs e os sistemas GPRS e UMTS [3GPP 23.234]. Este estudo está atualmente dentro do Release 6 do 3GPP. Por outro lado, o 3GPP2 (*Third Generation Partnership Project 2*), que padroniza a evolução do

CDMA2000, não apresenta nenhum grupo de trabalho até o momento que analisa o acoplamento entre o CDMA2000 e a WLAN [3GPP2]. Uma proposta de interconexão entre o CDMA2000 e a WLAN IEEE 802.11 pode ser vista em [Buddhikot].

A interconexão entre as redes celulares e as WLANs traz grandes desafios como, por exemplo, controle de acesso e segurança dos usuários de telefones celulares nas WLANs, mobilidade dos usuários entre as redes celulares e as WLANs, *roaming* através das WLANs, tarifação quando o usuário da rede celular utiliza a WLAN como meio de acesso, Qualidade de Serviço, suporte do *Core Network* da rede celular às WLANs bem como suporte ao terminal para o acesso através das WLANs.

Esta dissertação tem foco na convergência entre as redes WLAN e WWAN, mais especificamente entre a rede WLAN padrão IEEE 802.11 e os sistemas celulares GSM/GPRS e UMTS, visando a integração da rede WLAN com as redes de sistemas celulares através da utilização dos cartões SIM/USIM.

Esta dissertação tem por objetivo o estudo e comparação entre duas arquiteturas propostas para este tipo de interconexão, conhecidas como *Loose Coupling* e *Tight Coupling*. Estas arquiteturas são propostas pela ETSI (*European Telecomunications Standard Institute*) [ETSI 101 957], e são também exploradas por vários fabricantes e outras instituições, para a interconexão entre as WLANs e os sistemas celulares. No entanto, esta dissertação leva em conta a interconexão entre os sistemas celulares GPRS e UMTS com a WLAN padrão 802.11 e não o HiperLan/2, como proposto pela ETSI [ETSI 101 957], visto que o padrão IEEE 802.11 é o predominante no mercado atualmente.

Esta dissertação está estruturada da seguinte forma. O Capítulo 2 descreve a arquitetura das redes celulares GSM, GPRS e UMTS, a evolução de uma rede GSM até a rede UMTS e como estas redes se integram. O Capítulo 3 foca na arquitetura da WLAN padrão IEEE 802.11, suas extensões em termos de capacidade de transmissão de dados e melhorias de segurança. *Wireless Switches* também são mostradas neste capítulo. O Capítulo 4 apresenta a integração entre WLANs e sistemas celulares proposta pelo 3GPP e possíveis arquiteturas para esta integração. O Capítulo 5 descreve a arquitetura de acoplamento *loose coupling*. O Capítulo 6 descreve a arquitetura de acoplamento *tight coupling*. O Capítulo 7 compara as diferenças entre as arquiteturas *loose coupling* e *tight coupling* apresentando vantagens e desvantagens de cada uma considerando vários aspectos de integração.

# 2. As Redes de Sistemas Celulares GSM, GPRS e UMTS

A rede GSM é a mais difundida atualmente e conta com aproximadamente 2/3 dos usuários dos sistemas celulares no mundo [De Vriendt]. É considerada uma rede 2G e é utilizada principalmente na Europa, em algumas partes da Ásia, da África e nos últimos anos vem sendo introduzida também no Brasil, na banda de 1,8 GHz.

O sistema UMTS é o sistema de terceira geração (3G) sucessor do sistema GSM/GPRS e também é chamado de W-CDMA. Este sistema vem sendo desenvolvido pelo grupo 3GPP e com ele espera-se obter taxas de transmissão de até 2 Mbps.

Este capítulo descreve a arquitetura das redes GSM, GPRS e UMTS, assim como a evolução da rede GSM para a UMTS, passando pela rede GPRS.

## *2.1. As Redes GSM/GPRS*

A rede GSM é composta por várias células, sendo que cada célula é composta por uma BTS, a qual tem uma determinada área de cobertura. A BTS é a estação transmissora e receptora dos sinais que terminam e se original no dispositivo móvel. Cada BTS está conectada a uma BSC. O conjunto de BTSs e BSC é chamado de BSS (*Base Station Subsystem*). O roteamento das ligações dentro de uma rede GSM é feito pelo MSC (*Mobile Switching Center*) e o tráfego originado ou terminado de outras redes (da rede pública, por exemplo, a PSTN) é tratado pelo GMSC (*Gateway MSC*). Bancos de dados, como o HLR (*Home Location Register*), o VLR (*Visitor Location Register*), o AuC (*Authentication Center*) são utilizados para a autenticação, autorização e controle de acesso.

O sistema GPRS foi desenvolvido para ser uma rede de dados por pacote trabalhando como um *overlay* do sistema GSM. Ele utiliza técnicas de transmissão por pacotes para envio de dados entre o terminal e a uma rede externa de dados. A rede GPRS é na verdade uma rede de sobreposição à rede GSM. Esta sobreposição foi pensada a fim de se minimizar o impacto de implantação e custo de um novo sistema que oferece uma maior taxa de transmissão aos novos usuários GPRS e ainda garante a continuidade dos serviços oferecidos pelo GSM. A rede de sobreposição GPRS provê um aumento na taxa de transmissão de dados por pacote de 14,4 (do sistema GSM) para 172 Kbps.

O conceito da sobreposição à rede GSM levou à adição de novos elementos na rede GPRS para tornar possível o tráfego de dados utilizando comutação por pacotes dentro da já existente infra-estrutura de rede do GSM. Estes elementos de redes são chamados de GSNs (*GPRS Support Nodes*) e são responsáveis pelo roteamento e direcionamento dos pacotes entre o terminal e a rede de pacotes externa (PDN – *Packet Data Network*):

- SGSN (*Serving GPRS Support Node*)

  É o elemento de rede que representa o centro da comutação por pacotes nas redes GPRS.

  As principais funções do SGSN são: roteamento e direcionamento dos pacotes, gerenciamento de mobilidade (MM), gerenciamento de localização, atribuição de canais, autenticação e tarifação das chamadas.

- GGSN (*Gateway GPRS Support Node*)

  Este elemento age como uma interface entre um SGSN e uma outra rede de pacotes GPRS (PLMN) ou uma rede externa de pacotes de dados (PDN). Executa a função de PDP (*Packet Data Protocol*), ou seja, converte os pacotes GPRS oriundos do SGSN para pacotes no formato IP antes de direcioná-los para a rede externa. Do mesmo modo, ele converte os pacotes oriundos da rede externa em pacotes GPRS e os direciona para o SGSN apropriado.

A Figura 2.1 ilustra a arquitetura de uma rede GSM/GPRS.

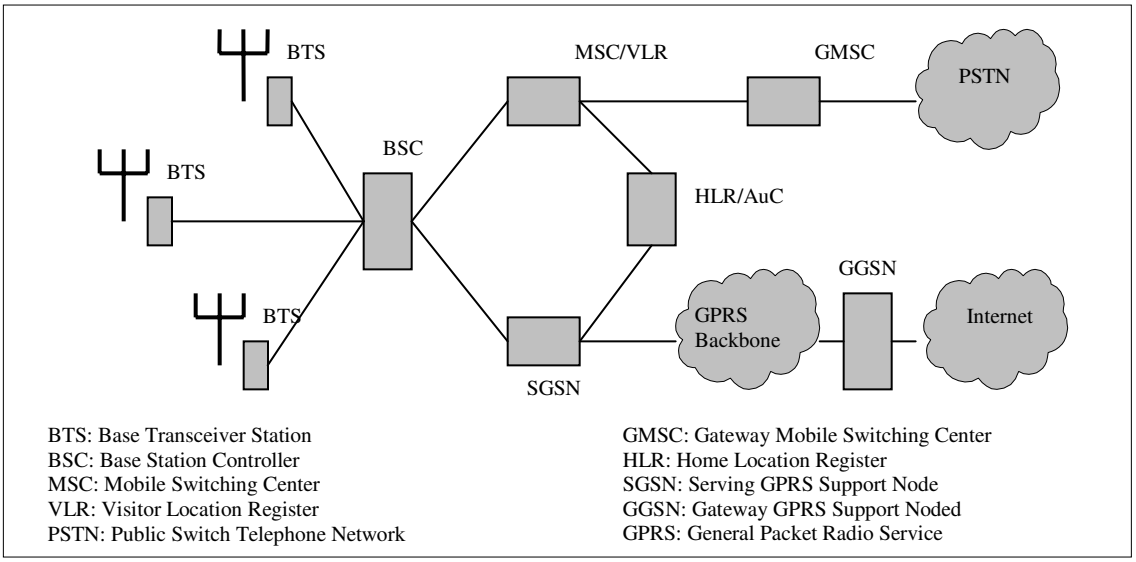


Figura 2.1. Arquitetura de uma rede GSM/GPRS.

Os diferentes componentes da arquitetura GSM são conectados por interfaces abertas que são definidas através de normalização, o que possibilita a interoperabilidade entre equipamentos de diversos fabricantes. O sistema GPRS acrescentou algumas novas interfaces ao sistema GSM a fim de suportar a comutação por pacotes. Estas novas interfaces foram definidas principalmente entre o SGSN e o GGSN e os outros componentes. A definição das interfaces GSM e GPRS pode ser vista em [Rai].

### 2.1.1. Plano de Transmissão em GPRS

O plano de transmissão em GPRS consiste de um conjunto de protocolos divididos em camadas e provê a transferência de dados de usuário e informações de controle como, por exemplo, controle de fluxo, detecção de erros e controle de potência.

A Figura 2.2 ilustra a pilha de protocolos utilizados no plano de transmissão em GPRS.

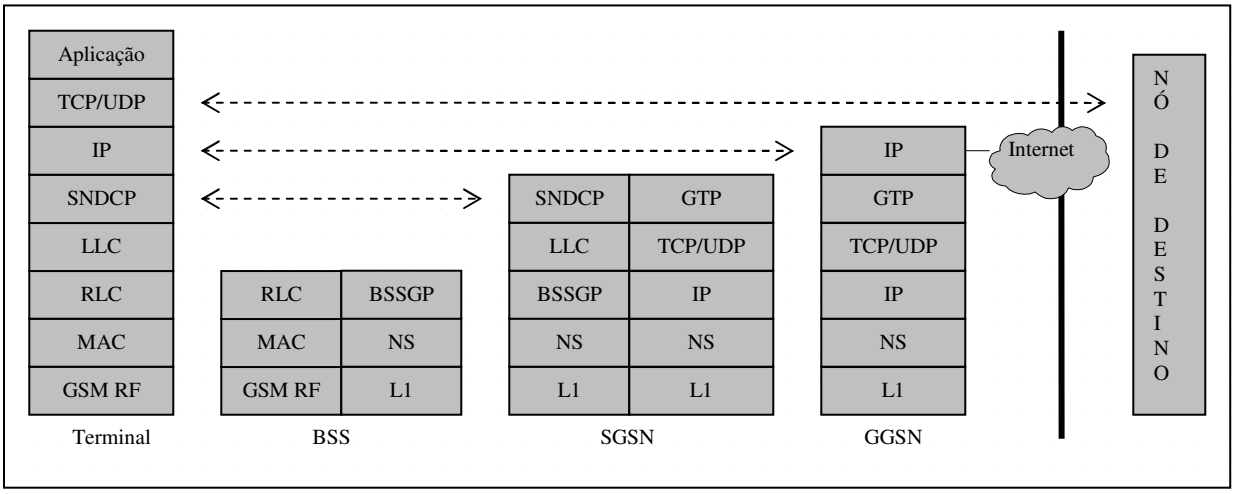


Figura 2.2. Plano de Transmissão em GPRS.

Entre os GSNs a comunicação acontece utilizando o protocolo GTP (*GPRS Tunneling Protocol*) que por sua vez utiliza os serviços do TCP/UDP e IP para encapsulamento de dados no backbone da rede GPRS.

O terminal utiliza-se dos serviços IP para transmissão de dados até o GGSN. No GGSN acontece o processamento dos pacotes IP oriundos tanto do terminal como da Internet.

## 2.2. As Redes UMTS

O sistema UMTS pode ser dividido em um conjunto de domínios lógicos e em um conjunto de interfaces que os interconectam.

A Figura 2.3 ilustra uma arquitetura em alto nível do sistema UMTS.

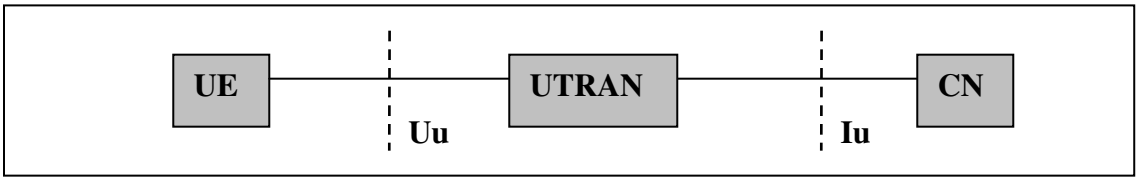


Figura 2.3. Domínios e Interfaces do Sistema UMTS.

O sistema UMTS utiliza o mesmo *Core Network* (CN) do GPRS, mas utiliza uma nova interface de acesso de rádio. A nova interface de radio do UMTS é o UTRAN, a qual é conectada ao CN via interface Iu.

Os domínios lógicos do UMTS são o UE (*User Equipment*), que é o equipamento do usuário, o UTRAN (*UMTS Terrestrial Radio Access Network*), que é a rede de acesso, e o CN (*Core Network*), que é o responsável pela comutação, autenticação, direcionamento de dados, encaminhamento e acesso às redes externas.

O UMTS é um sistema modular que pode ser dividido em várias sub-redes. Cada uma dessas sub-redes pode conter um ou mais elementos de redes. O requisito básico para uma sub-rede é pelo menos um elemento de rede de cada tipo. Este conceito de sub-redes chama-se PLMN (*Public Land Mobile Network*). Estas podem funcionar sozinhas ou podem se interconectar com outras PLMN ou com outras PDNs como, por exemplo, a Internet. Uma PLMN UMTS, seus principais elementos e suas interfaces de rede são ilustrados na Figura 2.4.

O UE é composto pelo ME (*Mobile Equipment*), que é o terminal de rádio que faz a comunicação de RF. O UE utiliza a interface aérea Uu e o cartão USIM (*UMTS Subscriber Identity Module*), o qual contém a identidade do assinante. No cartão USIM estão armazenadas chaves de autenticação e códigos criptográficos.

Os elementos de redes do UTRAN são o Node B e o RNC (*Radio Network Controller*), que são equivalentes a BTS e BSC no sistema GSM/GPRS, respectivamente.

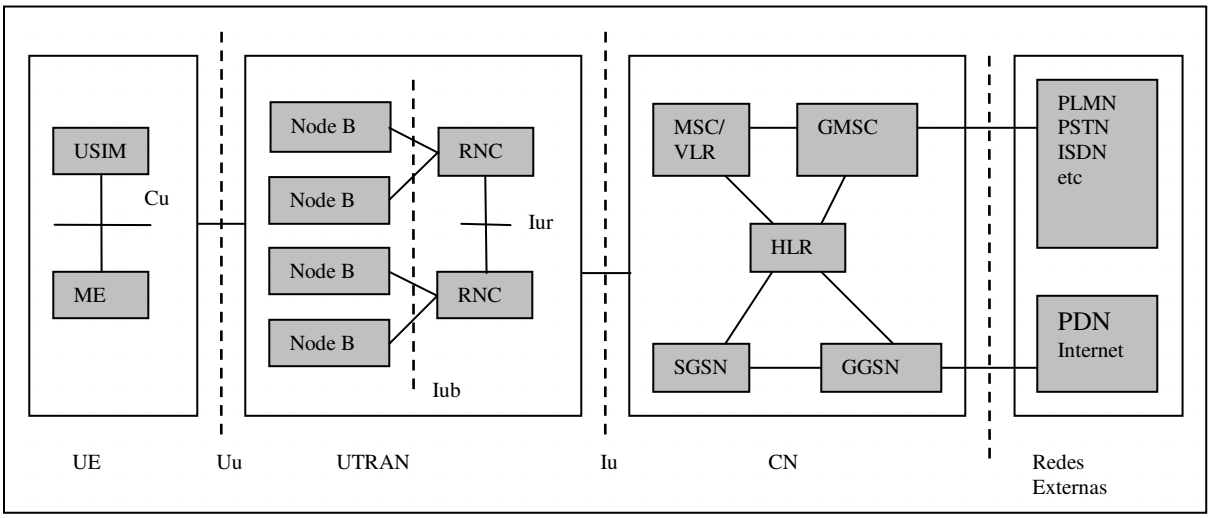


Figura 2.4. Principais elementos de uma PLMN do sistema UMTS.

Os principais elementos de rede do CN são o HLR, que é o banco de dados que guarda as informações dos usuários daquele sistema, o MSC/VLR e o GMSC, que prestam serviços de comutação por circuitos, e o SGSN e GGSN, que prestam serviços de comutação por pacotes.

Da mesma forma que os sistemas GSM e GPRS, as normas do sistema UMTS também definem interfaces abertas entre os seus elementos de redes, possibilitando interoperabilidade entre diferentes fabricantes. A definição das interfaces UMTS pode ser vista em [Rai].

### 2.2.1. Arquitetura de Protocolos do UMTS

A Figura 2.5 ilustra uma estrutura simplificada dos elementos que compõem a estrutura de protocolos do UMTS [Garcia]. A interface Iur não está presente nesta figura.

A estrutura do UTRAN foi projetada utilizando-se camadas e planos que são logicamente independentes uns dos outros a fim de que mudanças em determinadas partes da estrutura de protocolos não afetem outras partes. As especificações da primeira versão do UMTS [3GPP 21.101] estabelecem o ATM como tecnologia de transporte dentro do *Transport Network Layer* (TNL). Recentemente o 3GPP definiu uma solução alternativa para o transporte no UTRAN baseado em IP [3GPP 25.933].

Os detalhes das estruturas de protocolos das interfaces UTRAN podem ser vistos em [3GPP 25.401] e os detalhes da interface Uu podem ser vista em [3GPP 25.301].

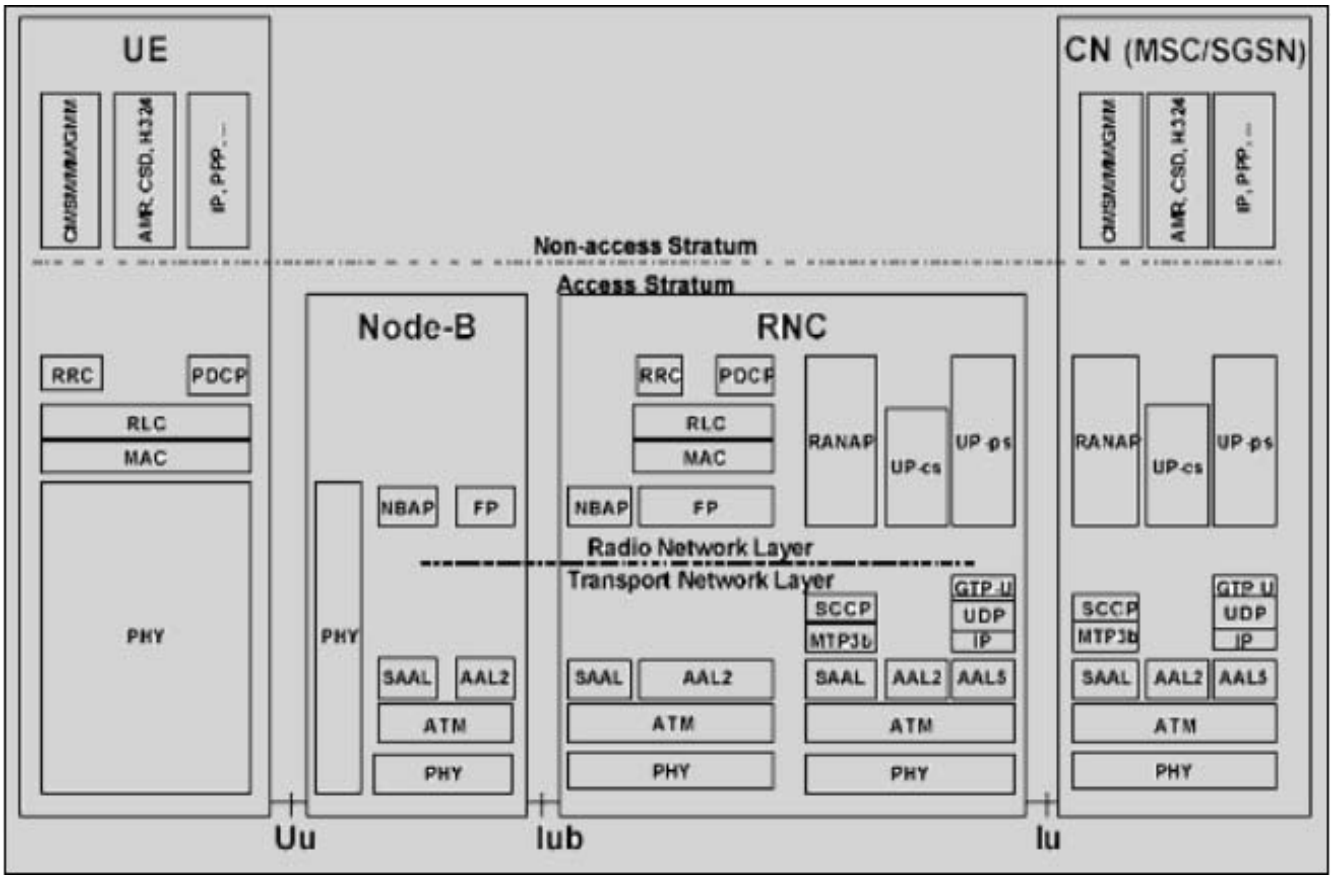


Figura 2.5. Arquitetura simplificada dos protocolos do UMTS.

Detalhes dos planos de transmissão e sinalização do UMTS podem ser vistos em [Park].

### 2.2.2. Integração de Sistemas GSM, GPRS e UMTS

O sistema UMTS foi elaborado para ser o sucessor do sistema GSM. No entanto, uma evolução do GSM para o UMTS passa pelo GPRS, pois o GPRS adiciona ao GSM os elementos de rede no CN necessários para o tratamento de pacotes que são também necessários para o UMTS.

Com terminal operando em *dual system* GSM/GPRS e UMTS, uma rede GSM/GPRS pode evoluir para uma rede UMTS com a adição gradativa do UTRAN, co-existindo com os BSS (BTS + BSC) do sistema do GSM/GPRS.

A Figura 2.6 ilustra o sistema UMTS co-existindo com o GSM/GPRS.

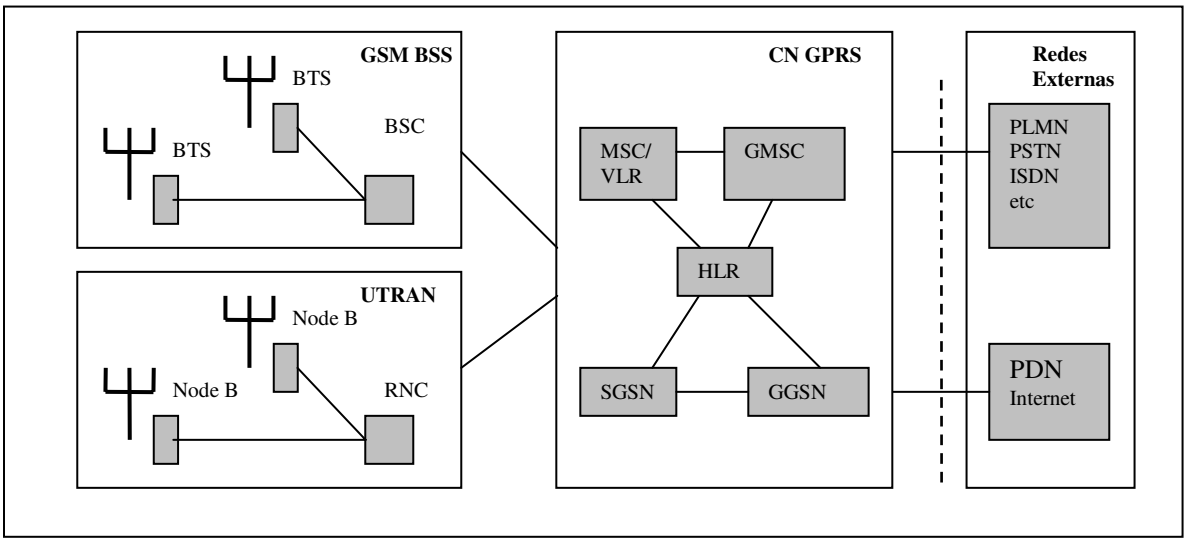


Figura 2.6. Integração dos sistemas UMTS e GSM/GPRS.

# 3. Rede Local sem Fio

Uma rede local sem fio (do Inglês *Wireless Local Area Network*, WLAN) é um sistema de comunicação que utiliza a tecnologia de RF para a transmissão de dados sem fio e é utilizada como uma extensão ou alternativa de uma rede cabeada. A grande vantagem da WLAN sobre a rede cabeada é a mobilidade do usuário, além de custos mais atrativos para manutenção e mobilidade física de redes dentro de residências, escritórios e de ambientes corporativos.

A tecnologia WLAN já vem sendo utilizada acerca de 10 anos. Entretanto, o grande impulso na tecnologia WLAN aconteceu com o surgimento do padrão 802.11 do IEEE, publicado inicialmente em 1997 [802.11], permitindo a interoperabilidade entre equipamentos de diversos fabricantes. Com a publicação deste padrão, tanto a indústria quanto provedores de serviços começaram a considerar as WLANs como um serviço público a ser oferecido à população. Neste papel de acesso público a dados existe uma sobreposição de funções entre WLAN e sistemas celulares.

## *3.1. O Padrão IEEE 802.11*

O padrão IEEE 802.11 refere-se à família de especificações desenvolvidas pelo IEEE para a tecnologia WLAN. O IEEE 802.11 especifica uma interface aérea entre um *Access Point* (AP) e um terminal ou entre dois terminais. Este padrão define uma subcamada *Media Access Control* (MAC), os protocolos de gerenciamento e serviços do MAC e ainda três camadas físicas: infravermelho, *Frequency Hopping Spread Spectrum* (FHSS) na faixa de 2,4 GHz e *Direct Sequence Spread Spectrum* (DSSS) também na faixa de 2,4 GHz. Todas as três camadas físicas suportam taxas máximas de 1 e 2 Mbps.

Existem diferentes especificações para a camada física dentro do 802.11, as quais operam em diferentes freqüências e possuem diferentes taxas de transmissão:

- 802.11

  Este é o padrão original de 1997 o qual suporta taxas de transmissão de 1 ou 2 Mbps. A faixa de freqüência de operação é em 2,4 GHz. Esta faixa de freqüência é livre, ou seja, não licenciada, e é conhecida como *Industrial Scientific and Medical* (ISM) *band*. Esta

é a mesma faixa de freqüência de operação do Bluetooth, de alguns telefones sem fios e dos fornos de microondas.

- 802.11b

  É um suplemento ao padrão original, publicado em 1999, especificando as taxas de 5,5 e 11 Mbps e também opera na faixa de freqüência de 2,4 GHz (ISM), mantendo a mesma MAC. É o padrão mais utilizado mundialmente, sendo também conhecido como Wi-Fi.

  Wi-Fi é uma marca registrada pela Wi-Fi Alliance, anteriormente conhecida com WECA (*Wireless Ethernet Compatibility Alliance*), uma organização formada por fornecedores de equipamentos e software de WLAN cuja missão é garantir a interoperabilidade do padrão IEEE 802.11. Produtos certificados como Wi-Fi pela WECA podem interoperar uns com os outros mesmos sendo de fabricantes diferentes.

- 802.11a

  Também é um suplemento ao padrão original, publicado em 1999. Esta extensão suporta taxas de transmissão de até 54 Mbps na faixa de freqüência de 5 GHz, mantendo a mesma MAC. Esta faixa de freqüência também é livre (não licenciada) e é conhecida como *Unlicensed National Information Infrastructure* (UNII) *band.*

- 802.11g

  Este é outro suplemento do 802.11, publicado em 2003. O 802.11g é suposto a oferecer o melhor de ambos os padrões 802.11a e 802.11b com suporte a taxas de até 54 Mbps na banda de 2,4 GHz. O 802.11g é compatível com o 802.11b.

A Figura 3.1 ilustra a arquitetura das extensões do padrão 802.11 e suas taxas de transmissão.

| Camada 2 | 802.2 – LLC<br>802.11 - MAC | | | |
|---|---|---|---|---|
| Camada 1 | 802.11<br>1 e 2 Mbps em 2,4 GHz | 802.11a<br>6, 9, 12, 18, 36, 54 Mbps em 5 GHz | 802.11b<br>1, 2, 5,5 e 6 Mbps em 2,4 GHz | 802.11g<br>6, 9, 12, 18, 36, 54 Mbps em 2,4GHz |

Figura 3.1. Extensões do padrão 802.11.

### 3.1.1. A Arquitetura 802.11

Os principais componentes da arquitetura 802.11 são ilustrados na Figura 3.2.

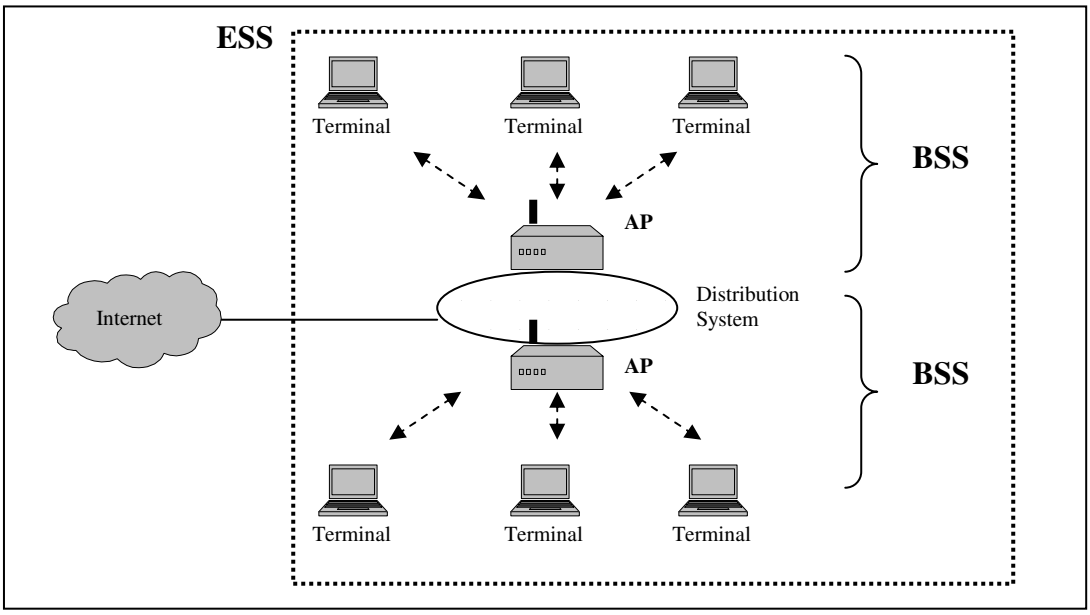


Figura 3.2. Principais componentes da arquitetura 802.11.

O bloco fundamental da arquitetura 802.11 é uma célula conhecida como *Basic Service Set* (BSS). O BSS contém um ou mais terminais wireless e uma estação central, conhecida como *Access Point* (AP). O terminal deve possuir um *Network Interface Card* (NIC) que provê a interface aérea de rádio com o AP.

Vários AP podem estar conectados uns aos outros através do *Distribution System* (DS). O DS pode ser implementado utilizando Ethernet ou ainda um outro canal wireless. Para as camadas de protocolos superiores (o IP, por exemplo), o DS aparece como uma única rede 802 do mesmo modo que uma *bridge* em uma rede Ethernet 802.3 aparece como um único elemento de rede para os protocolos de camadas superiores [Kurose].

Um *Extended Service Set* (ESS) é a união de vários BSS através de seus APs. O DS é o elemento lógico que interconecta os BSSs e provê serviços que permitem o *roaming* das estações entre os BSSs [802.11f_draft]. Uma rede WLAN que contém pelo menos um AP é chamada também de rede WLAN do tipo infra-estrutura.

Os terminais 802.11 também podem se comunicar entre si sem a necessidade de um AP e DS. Neste caso a rede é chamada de *Independent Basic Set Service* (IBSS), ou rede *ad hoc* e é formada somente pelos terminais.

### 3.1.2. As Camadas da Arquitetura 802.11

O padrão 802.11 foca nas duas últimas camadas da pilha da Internet, a camada física e a camada de enlace (*Data Link Layer*). Na camada de enlace o modelo 802.11 define duas subcamadas: o *Logical Link Control* (LLC) e o *Media Access Control* (MAC). Para a subcamada LLC, o padrão 802.11 utiliza o padrão 802.2 e endereços de 48 bits do mesmo modo que outras redes LAN 802 (por exemplo, Ethernet), permitindo a interconexão das redes wireless com as redes cabeadas, conforme ilustrado na Figura 3.3.

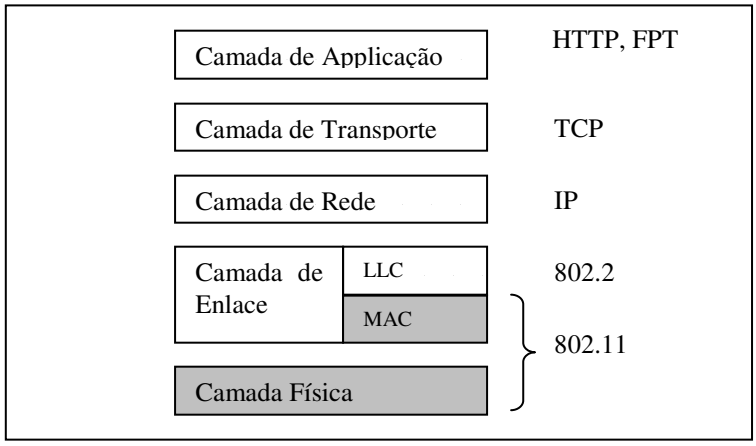


Figura 3.3. O padrão 802.11 e a pilha de protocolos da Internet.

### 3.1.3. Associação e Reassociação das Estações 802.11 aos AP

Quando um terminal 802.11 entra na área de alcance de um ou mais AP ele escolhe um AP para se associar. A associação entre o terminal e o AP é baseada na intensidade do sinal recebida pelo terminal e acontece antes do inicio de transmissão de dados. Periodicamente o terminal busca por outros canais 802.11 a fim de verificar se algum outro AP oferece uma intensidade de sinal mais forte. Se um outro AP oferece um sinal melhor que o anterior, o terminal muda sua sintonia para o canal do outro AP. Este processo é conhecido como

reassociação e normalmente acontece devido à mobilidade do terminal em relação ao AP no qual ele esta associado.

Este processo dinâmico de associação e reassociação entre os terminais e diferentes APs possibilita a mobilidade de usuários dentro de uma área com cobertura de vários APs, entretanto requer um planejamento adequado de reuso de canais pelos APs a fim de que um AP não cause interferência em outro.

### 3.1.4. Evolução das WLANs

Os padrões iniciais do IEEE, o 802.11 [802.11], o 802.11a [802.11a] e o 802.11b [802.11b], são referenciados como WLAN de primeira geração, ou WLAN 1G [NN103740]. Na WLAN de primeira geração, aspectos como segurança, Qualidade de Serviço, interoperabilidade e *roaming* não são atendidos ou não são suficientemente adequados. O caso mais crítico é o de segurança nas WLANs de primeira geração, o qual é baseado no WEP (*Wired Equivalent Privacy*) e mostrou, ao longo do tempo, não apresentar segurança suficiente para a instalação de WLANs em termos corporativos [Salkintziz][NN101960].

Estas limitações levaram o surgimento de novos padrões dentro do projeto 802.11, a fim de resolver os problemas anteriormente verificados nas WLANs de primeira geração. Com isso surgiu então a WLAN de segunda geração, ou WLAN 2G, envolvendo novos padrões os quais podemos destacar as especificações de melhoria de segurança [802.11i] e autenticação e controle de acesso [802.1x], melhoria de Qualidade de Serviço, *roaming* e interoperabilidade [NN103740] [802.11_Family]. Muitos destes padrões ainda estão em desenvolvimento, mas já prometem melhorias para a WLAN 802.11.

### 3.1.5. Segurança e Autenticação no 802.11

Do ponto de vista de rede, o problema mais importante é o controle de acesso. A rede deve decidir, de alguma forma, se um determinado terminal deve ou não ter acesso aos recursos da rede. Nas redes cabeadas os dados são transmitidos através de fios e interceptar a comunicação requer acesso físico nas instalações da rede. Nas redes sem fios, os dados são transmitidos em difusão através de uma antena e por este motivo o sinal pode ser interceptado por qualquer pessoa que possua um cartão WLAN padrão 802.11. Isso pode ocorrer, por

exemplo, nas imediações de prédios onde existe a instalação de uma WLAN, e o invasor pode utilizar antenas de alto ganho que amplificam o sinal da WLAN para tentar acessar os recursos da rede.

Quanto à segurança, originalmente, o padrão 802.11 provê os seguintes mecanismos:

- Identificação da rede

  É a identificação do AP, ou *Service Set Identification* (SSID). Neste caso, cada AP é configurado com um SSID que é requisitado de cada cliente que deseja se associar a este AP.

- Registro de cartões NIC

  É uma lista de controle de acesso através do MAC, ou MAC *Access Control List* (ACL). Neste caso somente as estações que estão na ACL do MAC podem se associar com o AP.

- Criptografia

  Este mecanismo é conhecido como *Wired Equivalent Privacy* (WEP), o qual provê serviços autorização e de criptografia contra usuários não autorizados dentro da WLAN.

Quanto à autenticação existem, originalmente, dois algoritmos especificados pelo padrão 802.11[Ergen]:

- Autenticação de sistema aberto

  Neste caso qualquer estação com o SSID do AP pode se conectar na rede. Nenhuma verificação é feita neste tipo de autenticação.

- Autenticação com chave compartilhada.

  Este tipo de autenticação depende que a estação e o AP tenham a cópia de uma chave compartilhada (WEP) para que o acesso seja permitido. Se a estação tiver uma chave inválida, que não é aquela esperada pelo AP, o processo de autenticação falha e a associação da estação não é permitida com o AP.

O processo de autenticação é diferente da associação. A autenticação é o processo de validação das credencias de um usuário para se conectar a uma rede e usar os seus serviços, seja a rede cabeada ou sem fio. A associação de uma estação é o processo de associar um

terminal a um AP dentro de uma WLAN. A associação é uma pré-condição necessária para o processo de autenticação 802.1x.

Estes mecanismos de autenticação do 802.11 apresentam limitações e não tem um nível de proteção suficiente contra ataques na rede, especialmente quando a WLAN é instalada em grande escala, com muitos AP e muitos terminais. Os valores de SSID e endereços de MAC podem ser facilmente obtidos através de *Sniffers* e a principal preocupação com o mecanismo de criptografia, usado pelo WEP, é que ele já foi quebrado e existem ferramentas disponíveis para a quebra deste mecanismo [NN101960].

### 3.1.6. Melhorias de Segurança e Autenticação no 802.11

Muitas especificações vem sendo adicionadas no padrão 802.11 desde a sua publicação original. Com relação à segurança, novos padrões vêm sendo desenvolvidos e sendo introduzidos no padrão original:

- 802.11i

  Este padrão incorpora o controle de acesso e autenticação 802.1x, assim como outros mecanismos de criptografia, de distribuição de chaves e algoritmos de autenticação. Este padrão também é chamado de *Robust Security Network* (RSN). Até a publicação deste trabalho, este documento ainda estava em desenvolvimento.

- 802.1x

  O objetivo do 802.1x é prover autenticação e controle de acesso para os AP, através do uso do protocolo *Extensible Authentication Protocol* (EAP) definido na RFC 2284 [RFC2284]. Com o 802.1x a autenticação e controle de acesso é feita ao nível de usuário e não ao nível de lista de controle de acesso de MAC ou SSID. Este padrão foi publicado em 2001.

O EAP é um protocolo de uso geral para autenticação que suporta vários mecanismos de autenticação, tais como chaves públicas, certificação de usuários, *token cards*, etc. O 802.1x define um padrão para o encapsulamento de mensagens EAP em ambientes LAN, definido o *EAP over LAN* ou EAPOL. O encapsulamento de mensagens EAP em ambiente 802.11 WLAN é chamado de *EAP over WLAN* ou EAPOW. Com o 802.1x, as mensagens

EAP são encapsuladas em frames Ethernet e não utilizam o PPP. A autenticação é feita através de servidores de autenticação, tais como o RADIUS, Kerberos e Diameter.

A arquitetura do EAP é ilustrada na Figura 3.4 [Mishra][CISCO].

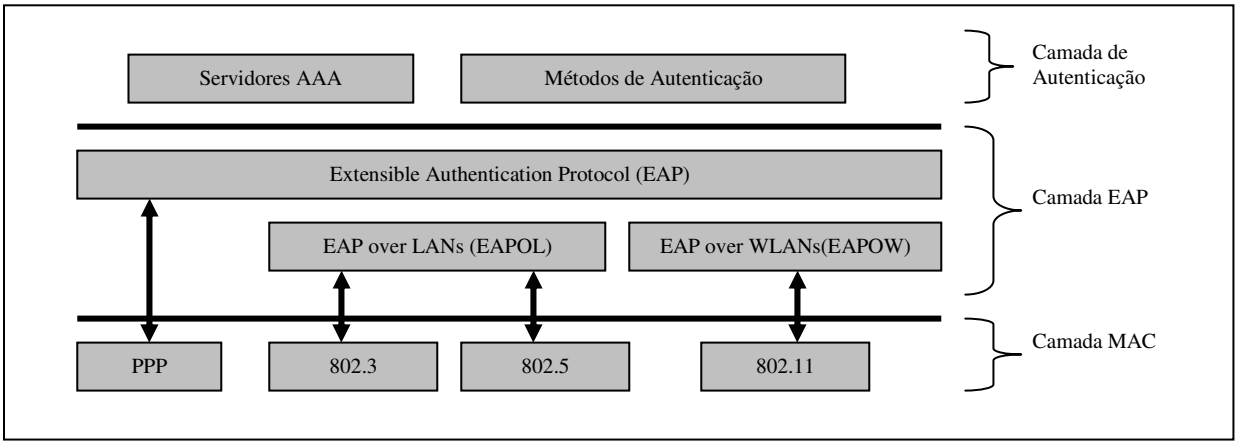


Figura 3.4. Arquitetura do EAP.

A arquitetura do padrão 802.1x define três elementos [802.1x]:

- Suplicante

  É a entidade que requer a autenticação para se conectar na rede. Em redes sem fio, o suplicante é a estação que deseja autorização para se associar a um AP.

- Autenticador

  É a entidade que força a autenticação de um suplicante antes de permitir acesso aos serviços da rede. Em uma rede sem fio, o autenticador é um AP. O autenticador habilita o controle de acesso ao suplicante baseado no resultado da autenticação.

- Servidor de Autenticação

  Este é o servidor que verifica as credencias do suplicante a fim de liberar ou negar acesso aos serviços da rede.

A Figura 3.5 ilustra a terminologia 802.1x aplicada em uma WLAN 802.11[Congdon].

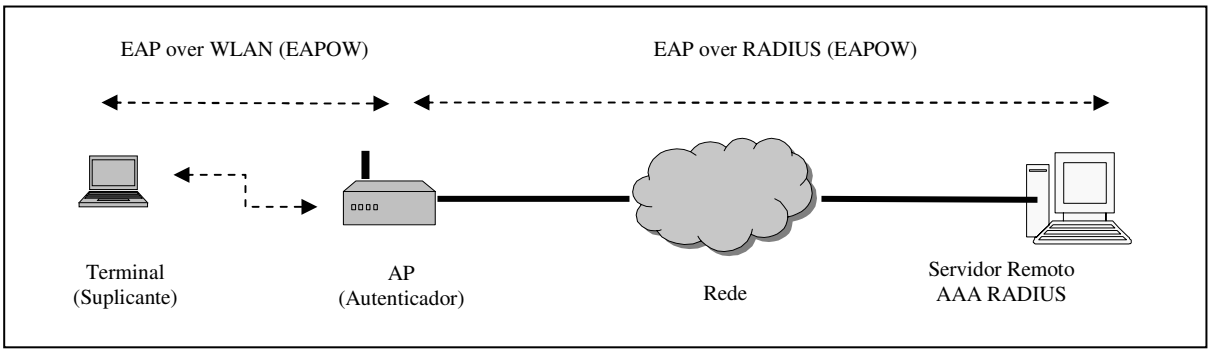


Figura 3.5. 802.1x para 802.11.

O protocolo EAP permite o uso de um servidor remoto para *Authorization, Authentication and Accounting* (AAA), o qual implementa os vários mecanismos de autenticação enquanto que o autenticador simplesmente repassa as mensagens entre o suplicante e o servidor de autenticação e vice-versa. Os equipamentos que atuam como autenticador, tais como AP em redes sem fios e *switches* em redes cabeadas, não precisam entender necessariamente cada tipo de pedido entre o suplicante e o servidor de AAA e podem agir simplesmente como um gateway, fazendo a interface entre os diferentes protocolos utilizados entre o suplicante (EAP) e o servidor AAA, o qual realiza o trabalho de autenticação. Além disso, o autenticador contém uma máquina de estado que verifica o protocolo EAP, a fim de verificar se o servidor remoto foi capaz de autenticar o usuário ou não. Se a autenticação foi positiva, o AP permite que a estação acesse a rede livremente, caso contrário, o acesso à rede é negado.

O padrão 802.1x não define um servidor de AAA específico. Exemplos de servidores que podem ser utilizados são o RADIUS, o Diameter e o Kerberos. O servidor remoto pode ainda acessar outros servidores ou databases a fim de obter dados necessários para a autenticação do usuário, mas acessos a outros servidores por parte do servidor de AAA não estão no escopo do 802.1x. O 802.1x é um padrão aberto e permite melhorias de implementação, como é feito no caso do *LEAP CISCO Authentication Server* [CISCO].

O 802.1x segue o modelo de paradigma de comunicação conhecido como *Challenge-Response*. Basicamente, com este modelo, um usuário ao requisitar uma conexão em uma WLAN através de um AP será questionado pelo AP a respeito de sua identificação, a qual será transmitida pelo AP para um servidor remoto para autenticação. O servidor remoto pede ao AP uma prova da identificação do usuário, o AP obtém esta informação do usuário e a envia

para o servidor a fim de completar a autenticação. Uma troca de mensagens para autenticação do 802.1x, com permissão de acesso, é ilustrada na Figura 3.6 utilizando o RADIUS [Congdom][Cisco].

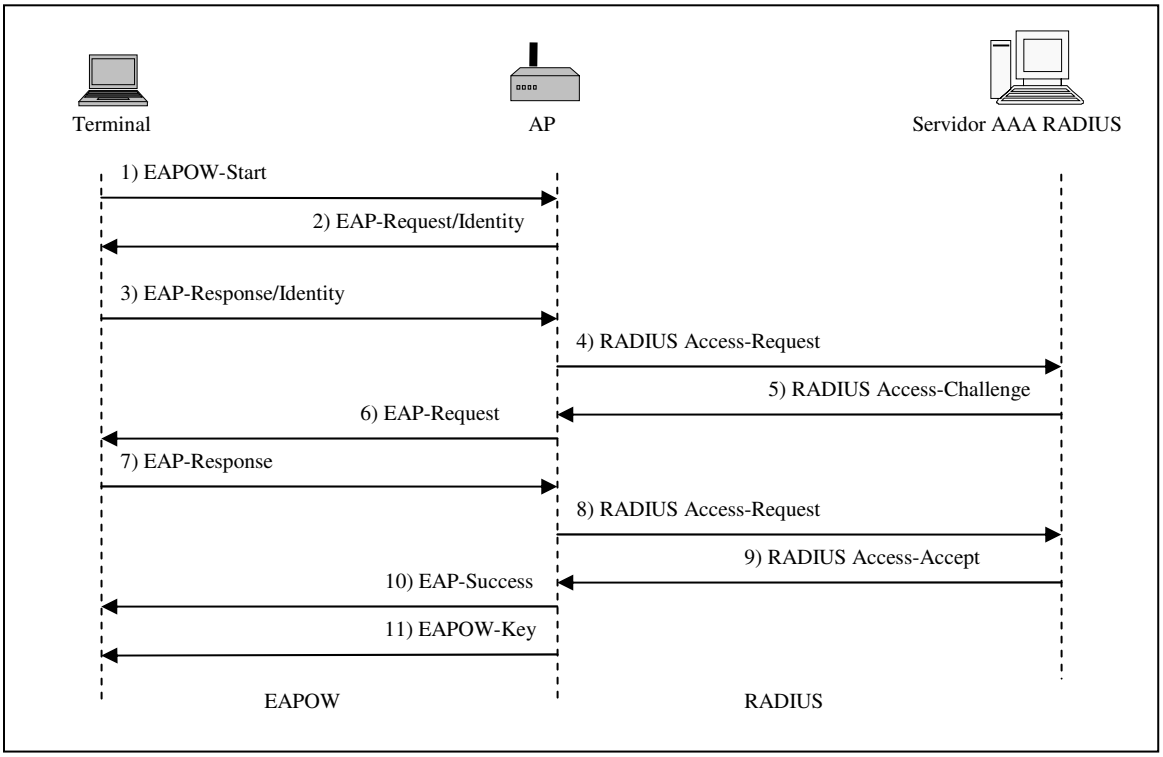


Figura 3.6. 802.1x para 802.11.

A fase de inicialização compreende as mensagens 1, 2 e 3 e são trocadas entre o terminal e o AP:

1. A mensagem *EAPOW-Start* (ou *EAPOL-Start*, para o caso de redes cabeadas) é utilizada para iniciar o processo de autenticação. É enviada pelo terminal, para o AP. Esta mensagem é definida no padrão 802.1x [802.1x];
2. A mensagem *EAP-Request/Identity* é utilizada pelo AP, para requisitar a identidade do usuário no terminal. Esta mensagem é definida na RFC 2284 [RFC2284];
3. A mensagem *EAP-Response* é utilizada pelo terminal para enviar sua identidade para o AP. Esta mensagem é definida na RFC 2284 [RFC2284].

A fase de autenticação compreende as mensagens 4, 5, 6, 7 e 8 e são trocadas entre o AP e o servidor de AAA, como o RADIUS [RFC2865], por exemplo. Esta seqüência pode variar de acordo com o método de autenticação escolhido entre o suplicante e o servidor de AAA.

4. A mensagem *RADIUS Access-Request* é utilizada pelo AP para enviar a identificação do usuário (nome) para o servidor RADIUS. Esta mensagem é definida na RFC 2865 [RFC2865]. Neste momento, o servidor RADIUS pode consultar um outro servidor ou database a fim de autenticar o usuário;
5. A mensagem *RADIUS Access-Challenge* não é obrigatória e é somente enviada quando o servidor RADIUS deseja fazer mais uma verificação de dados do usuário. Esta mensagem é enviada pelo servidor RADIUS para o AP requisitando credencias do usuário (senha). Esta mensagem é definida na RFC 2865 [RFC2865];
6. Se o AP suporta mensagens do tipo *Challenge/Response*, a mensagem *RADIUS Access-Chalenge* é repassada para o terminal como uma nova requisição de credencias na forma da mensagem *EAP-Request*. Se o AP não suporta mensagens do tipo *Challenge/Response*, então o AP deve tratá-la como se tivesse recebido uma mensagem do tipo *RADIUS Access-Reject* e enviar um *EAP-Failure* para o suplicante. Esta mensagem é definida na RFC 2284 [RFC2284];
7. A mensagem *EAP-Response* é enviada pelo terminal para o AP com as credencias do usuário que foram requisitadas na requisição anterior. Esta mensagem esta definida na RFC 2284 [RFC2284];
8. A mensagem *RADIUS Access-Request* é enviada pelo AP para o servidor RADIUS com as credencias do usuário que foram requisitadas anteriormente na mensagem. Esta mensagem é definida na RFC 2865 [RFC2865];
9. A mensagem *RADIUS Access-Accept* é enviada pelo servidor RADIUS para o AP se o usuário é válido, caso contrário uma mensagem *RADIUS Access-Reject* será enviada para o AP [RFC2865];
10. A mensagem *EAP-Success* é envida do AP para o terminal quando o AP recebe a mensagem *RADIUS Access-Accept*. Se o AP receber a mensagem *RADIUS Access-*

*Reject* do servidor RADIUS, uma mensagem *EAP-Failure* é enviada para o terminal [RFC2284];

11. A mensagem *EAP-Key* é enviada pelo AP para o terminal contendo informação sobre a chave que será utilizada para a criptografia dos dados naquela sessão [802.1x];

A Figura 3.6 ilustra somente a troca de mensagens que existe entre o terminal, o AP e servidor de AAA, que no exemplo é o RADIUS. O método de autenticação não é ilustrado. O EAP na verdade é um conjunto de mensagens que transportam métodos de autenticação e negociação entre a estação e o servidor de AAA. Outros métodos de autenticação são suportados pelo EAP, tais como o *Message Digest 5* (MD5), no qual o cliente requer autenticação através de *password*, o *Transport Layer Security* (TLS), que usa *Public Key Infrastructure* (PKI) para autenticação, e o *Tunneled Transport Layer Security* (TTLS), que combina informações de certificação de rede e outras autenticações como *tokens* ou *passwords*. Independentemente do método de autenticação a ser utilizado, é importante que todos os componentes 802.1x suportem o mesmo método.

Segurança adicional também vem sendo obtida através de melhorias nos algoritmos de criptografia. Enquanto o 802.1x define regras para autenticação e controle de acesso, o padrão 802.11i (RSN) define novos métodos de criptografia. A Wi-Fi Alliance também introduziu um novo método de criptografia mais robusto chamado de *Wi-Fi Protected Access* (WPA) como uma solução provisória. O WPA utiliza o modelo de autenticação do 802.1x e tecnologia *Temporal Key Integrity Protocol* (TKIP) que gera novas chaves de segurança a cada 10 kbytes de dados transmitidos pela rede, dificultando o acesso de pessoas não autorizadas na rede. Um novo algoritmo de criptografia em desenvolvimento e que deverá ser parte do 802.11i é o *Advanced Encryption Standard* (AES), que promete ser mais robusto que o WPA e que poderá ser utilizado como na autenticação juntamente com o 802.1x.

Outro fator importante de segurança é o *roaming* de uma estação dentro de uma WLAN. O padrão 802.1x estabelece que toda estação deve se autenticar novamente com o AP no qual esta em roaming [NN101960]. Um padrão, chamado de 802.11f [802.11f_draft], também esta sendo desenvolvido e deve estabelecer a interoperabilidade entre os APs.

Um exemplo de AP que suporta o 802.1x com suporte ao RADIUS é o *Orinoco AP-600*. Um exemplo de AP convencional, sem suporte ao 802.1x é o *DLink DWL-900AP+*.

## 3.2. Wireless Switches

Na arquitetura convencional de uma WLAN o AP é responsável pelo controle de RF, autenticação, controle de acesso, segurança e mobilidade dentro de seu domínio. Nesta arquitetura, o AP é conhecido como *fat AP*. É adequada para WLANs pequenas, tipicamente com menos de 10 APs. Quando a WLAN cresce, uma arquitetura com controle e gerenciamento centralizados torna-se mais adequada. Nesta arquitetura, o AP é conhecido como *thin AP*. Esta arquitetura define um novo elemento de rede, chamado de *wireless switch.*

*Wireless switches* são elementos de redes de uma WLAN que centralizam funções como segurança, autenticação, controle de acesso, QoS (quando disponível) e mobilidade de usuários dentro de um domínio de vários APs. A concentração de funcionalidades no *wireless switch* permite a redução de custo na instalação de grandes redes WLAN e também uma simplicidade maior de gerenciamento.

Na arquitetura *fat AP*, o AP é responsável pelo processamento das camadas físicas e de enlace (L1 e L2 do modelo OSI) do 802.11. Já na arquitetura *thin AP*, o AP somente é responsável pelo processamento da camada física, ou seja, limita-se somente ao tratamento de acesso de rádio que é feito pelos terminais. A camada de enlace do 802.11 (802.11MAC e 802.2 LLC) está presente no *wireless switch*. Por este motivo, na arquitetura *thin AP*, o AP não é mais chamado de *Access Point*, mas sim de *Access Port* (APo) visto que sua responsabilidade agora é só o tratamento de RF. Todo o processamento das camadas MAC e LLC está embutido no *wireless switch.*

A Figura 3.7 ilustra a arquitetura de uma WLAN com um *wireless switch* [Airspace].

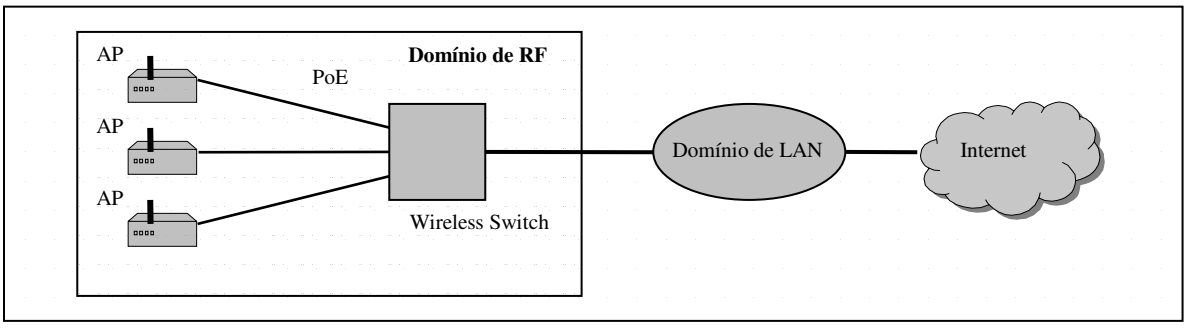


Figura 3.7. Arquitetura de uma WLAN com *wireless switch* e *thin APs*.

A arquitetura de *thin APs* com um *wireless switch* inteligente vem ganhando um grande suporte da indústria pois simplifica o gerenciamento e reduz o custo de instalações em grande escala. O objetivo desta nova arquitetura é reduzir o processamento dentro do AP, limitando-o somente ao acesso de RF das estações. O *wireless switch* é o elemento responsável por aspectos como autenticação, segurança, balanceamento de usuários entre os APo´s, criptografia, gerenciamento de mobilidade e *roaming* mais rápidos entre os APs.

Algumas vantagens da arquitetura *thin AP* sobre a *fat AP* são:

- Configuração de AP

  A configuração de AP inclui a atribuição de canais de RF e níveis de potência para cada AP da WLAN. No caso de *fat AP* a configuração deve ser feita para cada AP, enquanto que no caso de *thin AP* a configuração de muitos APo´s podem ser feitas através de uma única interface de um *wireless switch*.

- Atualizações de software

  Visto o grande desenvolvimento dos procedimentos de autenticação e criptografia do 802.11 nos últimos anos, atualizações de software no AP é esperada freqüentemente. Na arquitetura *fat AP* a atualização deve ser feita para todos os APs da WLAN enquanto que na arquitetura *thin AP* somente a atualização do *wireless switch* é necessária.

- Segurança

  Os *fat APs* contém informações de configurações de rede, de roteamento, de criptografia e de servidores de autenticação, ou seja, eles contêm informações importantes da infra-estrutura da rede e o roubo destes elementos de rede poderiam revelar possíveis alvos de ataque. Os *thin APs* só contém as características de RF para o acesso de rádio das estações.

Além das vantagens acima, APs e *wireless switches* que suportam *Power over Ethernet* (PoE), uma solução onde a corrente elétrica é enviada através dos cabos Ethernet, facilitam a instalação e mudanças de localização de APs dentro ou fora de prédios, visto que não há a necessidade de cabos de energia elétrica.

### 3.2.1. Pilha de Protocolos nas Arquiteturas *fat AP* e *thin AP*

As Figuras 3.8 e 3.9 ilustram a pilha de protocolos utilizados pelo *Access Point* na arquitetura *fat AP* e pelo *Access Port* e *wireless switch* na arquitetura *thin AP*.

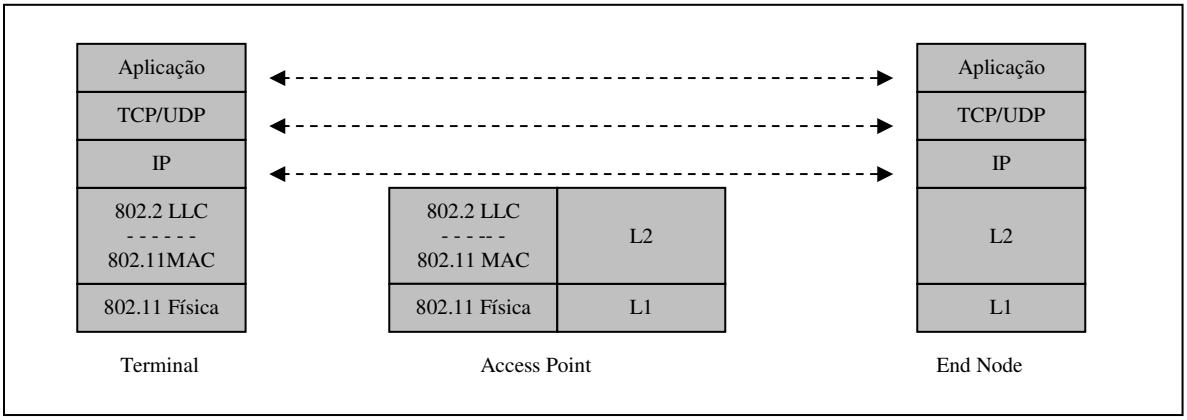


Figura 3.8. Pilha de protocolos na arquitetura *fat AP*.

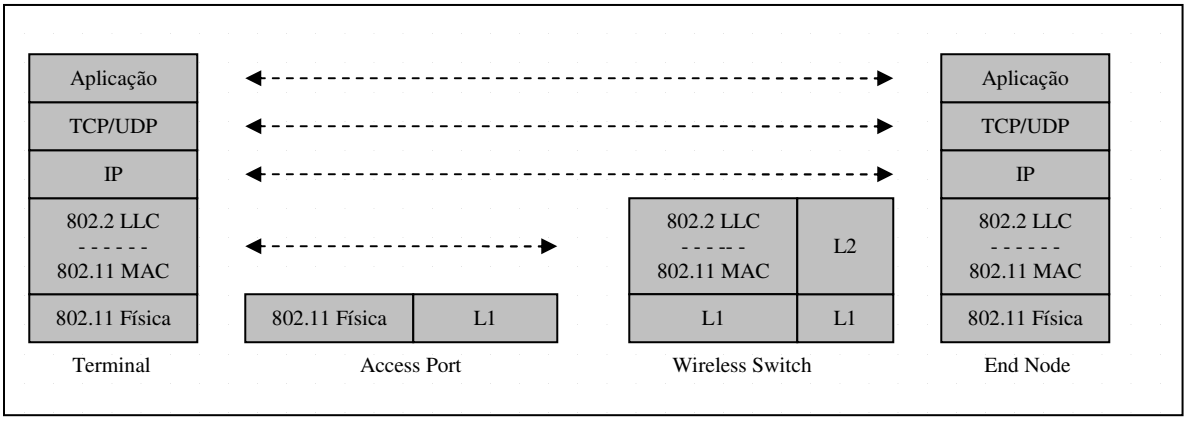


Figura 3.9. Pilha de protocolos na arquitetura *thin AP*.

Na arquitetura *fat AP*, o AP faz processamento das camadas físicas e de enlace (L1 e L2 do modelo OSI) do 802.11. Na arquitetura *thin AP*, o APo somente é responsável pelo processamento da camada física. A camada de enlace do 802.11 (802.11MAC e 802.2 LLC) está presente no *wireless switch*.

### 3.2.2. Interoperabilidade e Padronizações

Os *wireless switches* já se encontram disponíveis no mercado através de diversos fabricantes [Symbol][Airespace] e com isso com novo protocolo vem sendo desenvolvido pelo *Internet Engineering Task Force* (IETF), visando a interoperabilidade entre APs e *wireless switches* de diferentes fornecedores. Este protocolo é conhecido como *Light Weight Access Point Protocol* (LWAPP) e sua finalidade principal é um padrão de comunicação aberto entre *wireless switches* e APs.

O LWAPP pretende estabelecer padrões como:

- Gerenciamento e controle da comunicação entre o *wireless switch* e os APs.
- Configuração, descoberta e controle de software dos APs pelos *wireless switches*.
- Formatação, fragmentação e empacotamento de pacotes ente APs e *wireless switch*.

Até a publicação deste trabalho, este protocolo estava em fase de desenvolvimento pelo IETF, ou seja, é uma especificação *Internet-draft* [LWAPPdraft].

### 3.2.3. Modelo da arquitetura *thin AP*

O modelo utilizado pela arquitetura *thin AP* se aproxima do modelo utilizado pelas redes de telefonia celular como GSM e UMTS quanto ao uso de um elemento centralizador.

Na arquitetura *thin AP* a presença da *wireless switch* se aproxima da função da BSC no GSM, e RNC no UMTS, como um elemento centralizador de gerenciamento, e o *Access Port* se aproxima da função da BTS como um elemento de acesso de rádio. A *wireless switch* é conectada a um roteador ou *bridge*, a qual é conectada a uma LAN.

A Figura 3.10 ilustra a arquitetura de uma rede GSM e a arquitetura de WLAN com *wireless switch*, *hub* e *Access Ports*, onde a BSC e o *wireless switch* aparecem como elementos de gerenciamento dos nós de acesso de rádio.

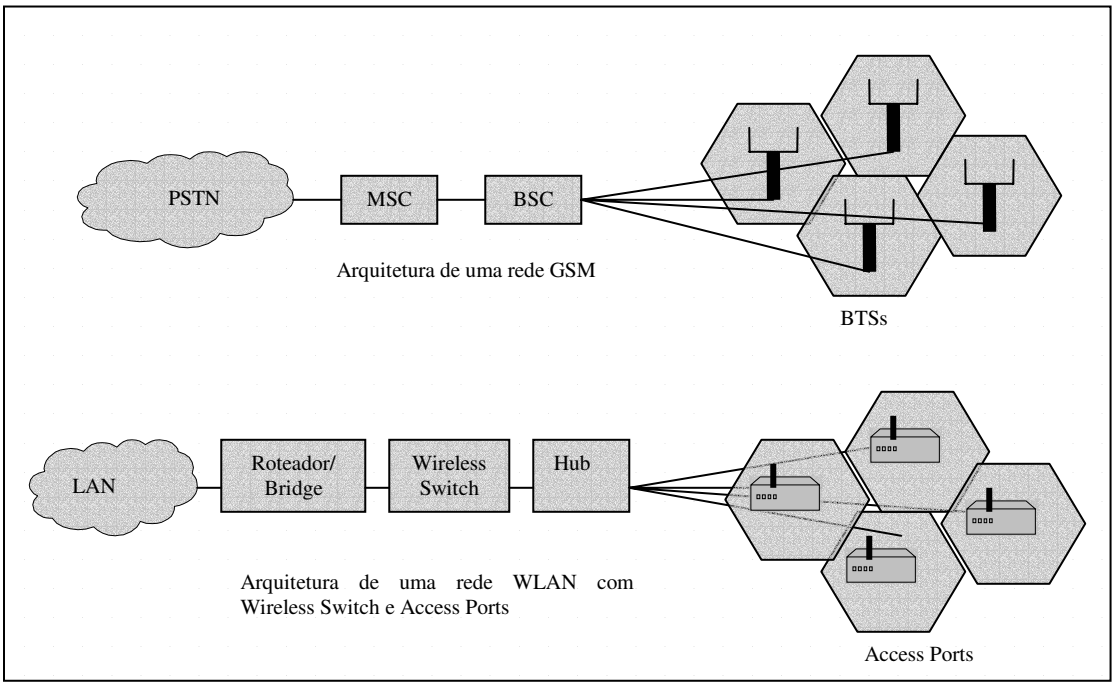


Figura 3.10. Comparação entre a arquitetura GSM e a arquitetura WLAN com *thin AP*.

## 3.3. WLANS Públicas (PWLAN)

WLANs públicas são redes que vem sendo instaladas em lugares públicos denominados *hotspots*. Os *hotspots* são áreas públicas como aeroportos, estações ferroviárias, *shopping centers*, hotéis, bares e cafés onde o público tem acesso à Internet através de WLANs.

Neste segmento surgem os operadores de WLANs públicas, os quais são denominados de *Wireless Internet Service Providers* (WISPs). Muitas categorias de WISP atualmente são previstas, tais como [Thorngren]:

- Operadoras de redes celulares que integram WLAN com seus serviços já existentes.
- Provedores de Internet (ISP) que estendem seus negócios.
- Novas companhias que operam somente no ramo de WISP.
- Localidades específicas, tais como aeroportos, centros de convenções, etc, que possuem as suas próprias facilidades para o fornecimento do serviço.

Neste contexto, um usuário pode acessar o *hotspot* através de uma conta mensal ou cartões pré-pago. Além de acesso à Internet, uma outra aplicação do *hotspot* é a integração do

*hotspot* com os sistemas celulares, onde o usuário tem a habilidade de *roaming* de uma rede celular para a WLAN e vice-versa. Atualmente, alguns fabricantes de celulares já disponibilizam aparelhos capazes de se registrar tanto em redes celulares como também em redes 802.11b [Beeby].

### 3.3.1. Arquitetura de uma WLAN pública

A arquitetura de alto nível de uma WLAN pública, contento as arquiteturas *fat* e *thin AP*, é ilustrada na Figura 3.11.

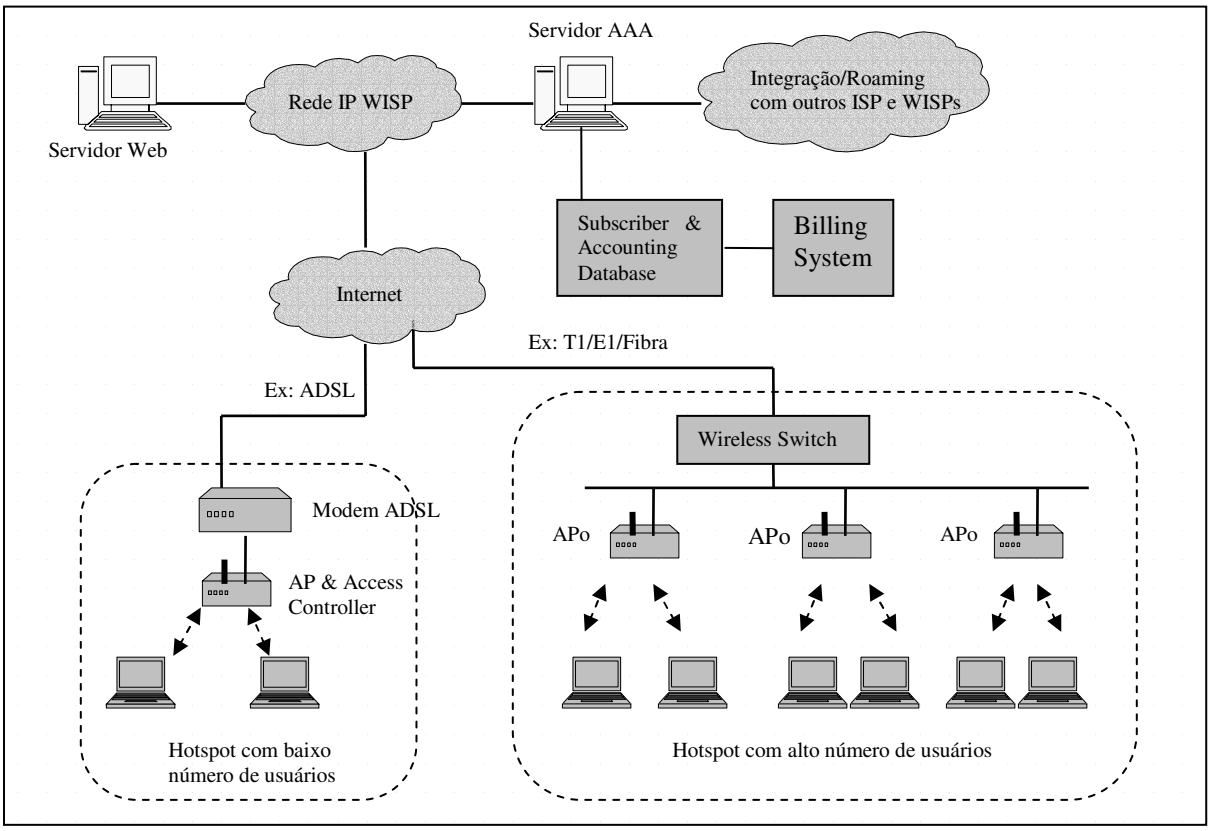


Figura 3.11. Arquitetura de alto nível de uma WLAN pública.

Basicamente, a instalação de um WISP requer um servidor AAA para o controle de acesso, um banco de dados com as informações dos usuários e o sistema de *billing*. O *roaming* de ISP *accounts* são obtidos através de acordos entre WISPs e ISPs através de conexões dedicadas ou ainda utilizando a Internet.

Para *hotspots* com alto número de usuários, como aeroportos e estações ferroviárias, é recomendado o uso de *wireless switch* como concentrador de autenticação e gerenciamento (arquitetura *thin AP*). Para o acesso à Internet é recomendado links E1/T1 ou fibras ópticas a fim de suportar o alto tráfego na rede. Nos *hotspots* com baixo número de usuários o uso de um *fat AP* é mais vantajoso em termos de custo e manutenção. Também nestas localidades um link ADSL apresenta uma boa alternativa de redução de custo, embora pode-se usar outras tecnologias.

No caso das redes WLAN públicas também é recomendável o uso de ferramentas que garantam segurança de informação fim-a-fim em níveis mais altos da aplicação, como VPN, além de segurança de controle de acesso provido pelo 802.11. VPNs utilizam criptografia e métodos de autenticação como mecanismos de esconder e mascarar dados da rede privada do WISP de potencias ataques na rede pública.

A Figura 3.12 ilustra uma arquitetura simplificada da pilha protocolos em uma WLAN pública e no WISP.

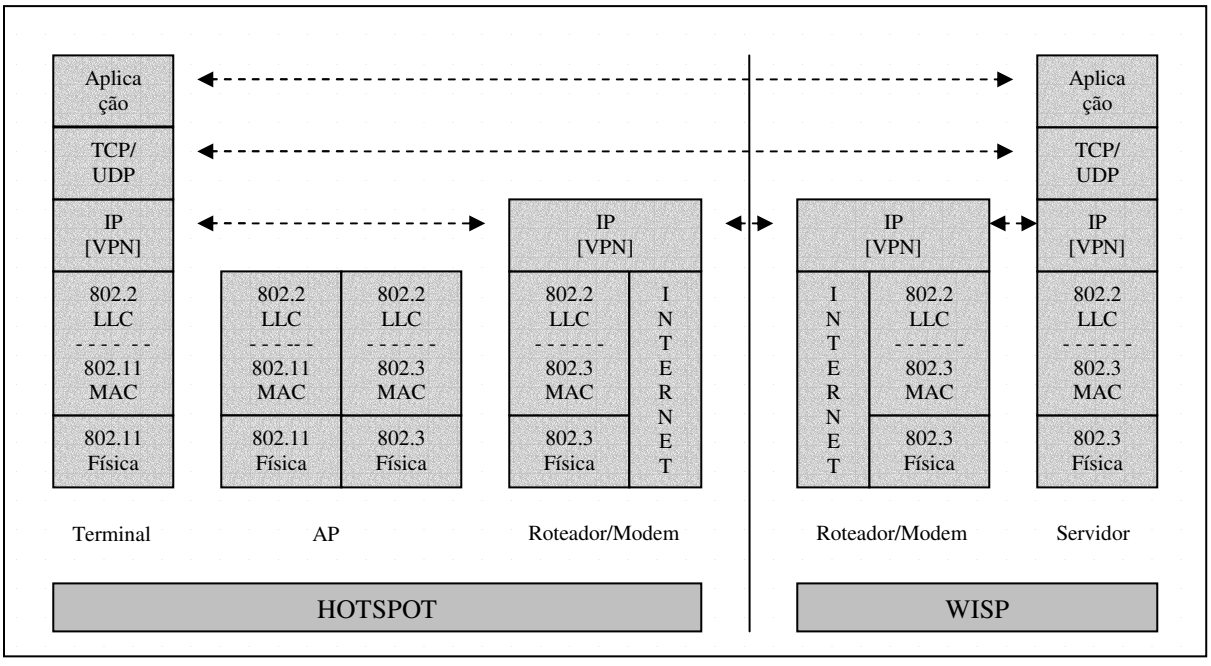


Figura 3.12. Pilha de protocolos em uma WLAN e no WISP, na arquitetura *fat AP*.

# 4. Integração das WLANs com os Sistemas Celulares

As WLANs vem sendo instaladas em locais públicos como aeroportos, estações ferroviárias, hotéis, campus universitários, bares e cafés, os quais são conhecidos como *hotspots*. Um dos possíveis serviços a serem oferecidos pelos operadores de telefonia celular é a integração dos *hotspots* WLANs à sua rede atual, fornecendo áreas com maiores taxas de transmissão de dados e conseqüentemente, um acesso mais rápido à Internet. A intenção de integração entre sistemas celulares e WLANs é estender os serviços e funcionalidades dos sistemas celulares para o ambiente WLAN. Assim as WLANs passam a ser uma tecnologia de acesso a dados por pacotes com taxas mais altas não suportadas pelos sistemas celulares.

Atualmente as redes de sistemas celulares GPRS provêem uma taxa de acesso de até 172 kbps, com promessas de até 2 Mbps para sistemas UMTS, em grandes áreas de cobertura. Já as WLANs conseguem prover taxas de 11 Mbps e 54 Mbps com os padrões 802.11b e 802.11a/802.11g, respectivamente, em pequenas áreas. Uma integração entre estas duas tecnologias reúne as vantagens de cada uma, resultando em um sistema com grande cobertura capaz de fornecer um serviço de conexão à Internet cujas taxas podem variar de valores relativamente baixas até altas taxas em *hotspots* estratégicos.

A Figura 4.1 ilustra um ambiente onde o usuário de telefonia celular tem mais de uma opção para acesso à Internet, à medida que se movimenta.

Os *hotspots* disponíveis para os usuários podem variar em termos de proprietários da WLAN, ou seja, ele pode ser propriedade da própria operadora da rede celular que faz o gerenciamento da WLAN, pode ser de um WISP ou ainda o *hotspot* pode estar dentro de uma empresa ou organização. Mesmo com estes diferentes proprietários das WLANs, os usuários das operadoras de celulares podem fazer uso dos *hotspots*. Para isso, acordos de *roaming* entre as operadoras e os diferentes proprietários das WLANs, tais como WISP e organizações, são necessários para permitirem o uso dos *hotspots* por parte dos usuários das operadoras de redes celulares. Nestes casos, serviços de autenticação e *billing* ainda são responsabilidades da operadora de celular. Em termos de custos, a operadora compartilha as receitas com os proprietários das WLANs baseados nos acordos de *roaming*. Neste contexto, um usuário estando em um *hotspot* pode acessar os serviços providos pelo operador e realizar operações

que exigem maiores taxas de transmissão como, por exemplo, envio de e-mails com arquivos atachados.

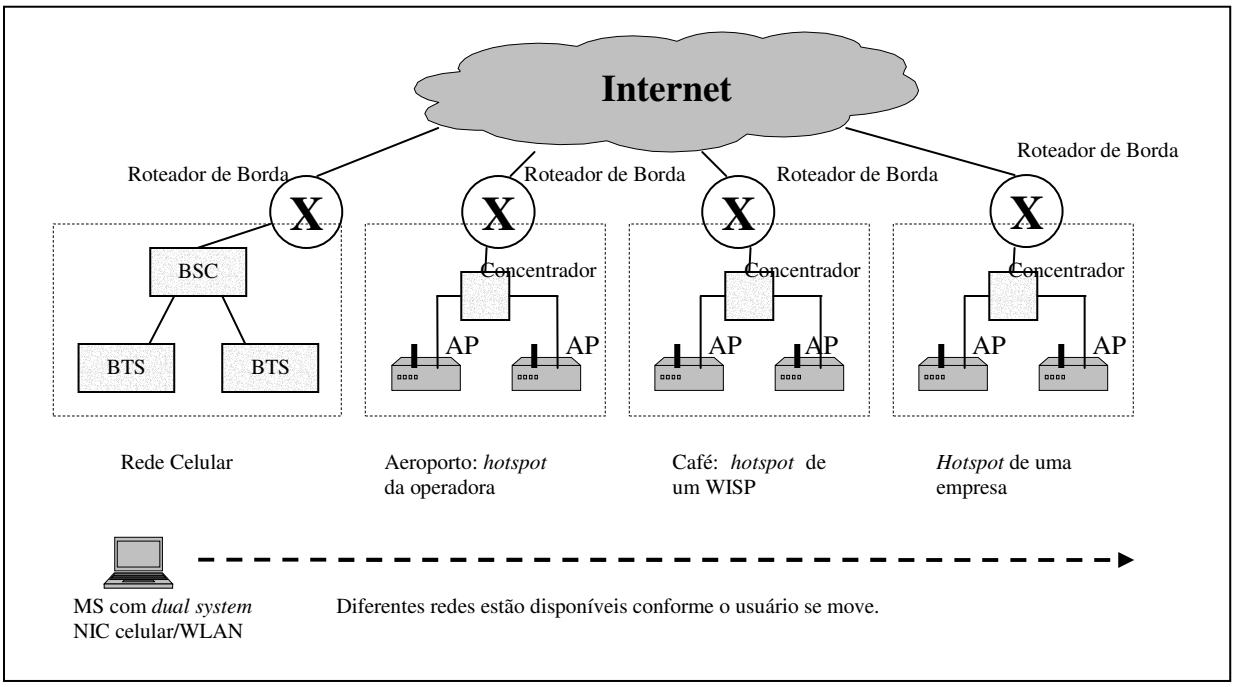


Figura 4.1 – Múltiplas opções de acesso em um ambiente integrado.

Para acesso aos *hotspots*, os usuários precisam de um *dual system* NIC, com as funções de WLAN e sistema celular disponível. Um exemplo deste cartão é o Nokia D211 GPRS/Edge/WLAN [Beeby].

## 4.1. Padronizações

Atualmente existem propostas de integração entre as WLANs e os sistemas celulares. Alguns órgãos de padronizações, como 3GPP e o ETSI BRAN já possuem estudos para este tipo de integração [3GPP 22.934] [ETSI 101 957].

O 3GPP é o órgão que vem realizando maiores atividades em termos de padronizações nesta área. Dentro deste contexto o 3GPP definiu seis cenários de integração entre as WLANs e os sistemas celulares [3GPP 22.934], os quais focam no tipo e na Qualidade de Serviço que são oferecidos aos usuários. Cada um destes seis cenários habilita uma capacidade específica e requer um determinado nível de integração. Estes cenários são ilustrados a seguir.

### 4.1.1. Cenário 1: Tarifação e Atendimento ao Cliente Comuns.

Este é o nível de integração mais simples que existe. Somente os sistemas de tarifação e atendimento ao cliente são comuns. Não existe nenhum outro tipo de interconexão entre os sistemas celulares e WLANs. Este tipo de interconexão não requer modificação algumas nos padrões já existentes do 3GPP.

Neste caso, o operador do sistema celular oferece a cada cliente uma conta e uma senha para acesso à Internet via WLAN. O usuário tem acesso aos serviços da Internet providos dentro da WLAN, mas não tem acesso aos serviços e recursos providos exclusivamente pelo sistema celular.

### 4.1.2. Cenário 2: Controle de Acesso e Tarifação Baseado no Sistema Celular

Neste cenário, o sistema de AAA para os usuários de WLAN é baseado no mesmo procedimento de AAA utilizado pelos usuários do sistema celular. O usuário pode utilizar o cartão SIM/USIM para autenticação e acesso aos serviços da WLAN do mesmo modo que utiliza para ter acesso ao sistema celular. Neste caso, a *profile* do usuário é alterada pelo operador de sistema celular para que o usuário também tenha acesso na rede WLAN.

Um exemplo deste cenário é o de um usuário com um laptop que contém um *dual system* NIC 3GPP/WLAN. O usuário pode acessar os serviços do sistema celular e da WLAN utilizando sessões separadas no laptop, mas não precisa fazer troca de hardware (NIC) no laptop.

Este cenário não adiciona outros serviços na WLAN além daqueles que são oferecidos normalmente na Internet.

### 4.1.3. Cenário 3: Acesso aos Serviços de 3GPP/GPRS

Este cenário permite que o operador de sistema celular estenda os serviços do sistema celular, como por exemplo, WAP, serviços de localização e multimídia IP, para o ambiente de WLAN. Entretanto, mesmo o usuário tento acesso aos mesmos serviços do sistema celular no

ambiente WLAN, a continuidade de serviços não é garantida entre os dois sistemas, ou seja, um usuário que está utilizando um determinado serviço dentro de uma WLAN pode perder a conexão com este serviço ao sair da cobertura da WLAN e entrar na cobertura do sistema celular e vice-versa. Neste caso o usuário, se quiser ter acesso ao serviço novamente, precisa restabelecer a chamada novamente.

Um exemplo deste cenário é um usuário que contém um *dual system* NIC 3GPP/WLAN em seu laptop e deseja acessar serviços disponível na rede celular. Quando o usuário se move e acontece transição entre ambientes, o serviço será descontinuado.

### 4.1.4. Cenário 4: Continuidade de Serviços

O objetivo deste cenário é a garantia da continuidade dos serviços oferecidos no cenário 3 durante mudanças entre o ambiente do sistema celular e o ambiente WLAN. A mudança pode ser observada pelo usuário em termos de Qualidade de Serviço na transição entre ambientes visto que os dois ambientes podem ter capacidades e características diferentes devido a diferentes tecnologias de acesso e suas redes.

Embora a continuidade de serviço é requerida por este cenário, é possível que alguns serviços não possam ser suportados por outro ambiente e aí seja descontinuado na transição.

Um exemplo deste cenário é um usuário que contém um *dual system* NIC 3GPP/WLAN em seu laptop e deseja acessar um serviço de e-mail. Quando o usuário se move e acontece transição entre ambientes, o NIC 3GPP/WLAN faz o chaveamento automático para o outro ambiente e o serviço continua. O usuário pode sentir interrupções passageiras durante a transição, mas não é necessária uma nova conexão.

### 4.1.5. Cenário 5: Continuidade de Serviço sem Interrupções

Este cenário é o cenário 4 com melhorias no momento da transição e com Qualidade de Serviço. O objetivo é obter um serviço continuado entre o sistema celular e o a WLAN onde usuário não perceba diferenças significativas entre as transições e na Qualidade de Serviço entre os dois ambientes.

Um exemplo deste cenário é um usuário utilizando serviços multimídia em uma WLAN. Ao deixar o ambiente WLAN e passar para o sistema celular, o serviço multimídia continua sem o usuário sentir interrupções.

### 4.1.6. Cenário 6: Acesso aos Serviços de Comutação por Circuito do Sistema celular

Este cenário permite acesso aos serviços de comutação por circuitos de uma rede 3G. O objetivo é permitir que a operadora forneça acesso aos serviços fornecidos pelos componentes de comutação por circuitos dentro do C*ore Network* 3G como, por exemplo, chamadas de voz normais, em um ambiente WLAN.

## *4.2. Arquiteturas de Interconexão entre Sistemas Celulares e WLANs*

Os seis cenários definidos pelo 3GPP levam em consideração os tipos e a Qualidade de Serviço que são oferecidos aos usuários. Do ponto de vista de arquitetura para transmissão de dados por pacotes, os 5 primeiros cenários podem ser reduzidos em 4 tipos de interconexão, ou acoplamento, entre os sistemas celulares e as WLANs [Cristache]. O cenário 6 leva em conta o acesso aos serviços de comutação por circuitos e não será levado em conta nesta dissertação.

O primeiro nível de acoplamento entre redes UMTS e WLANs é o chamado *open coupling*, o qual define duas redes de acesso e duas redes de transporte separadas, uma para o sistema celular e uma para a WLAN. Somente o sistema de *billing* é comum neste tipo de acoplamento. Este tipo de arquitetura preenche somente os requisitos do cenário 1.

A Figura 4.2 ilustra o acoplamento *open coupling*.

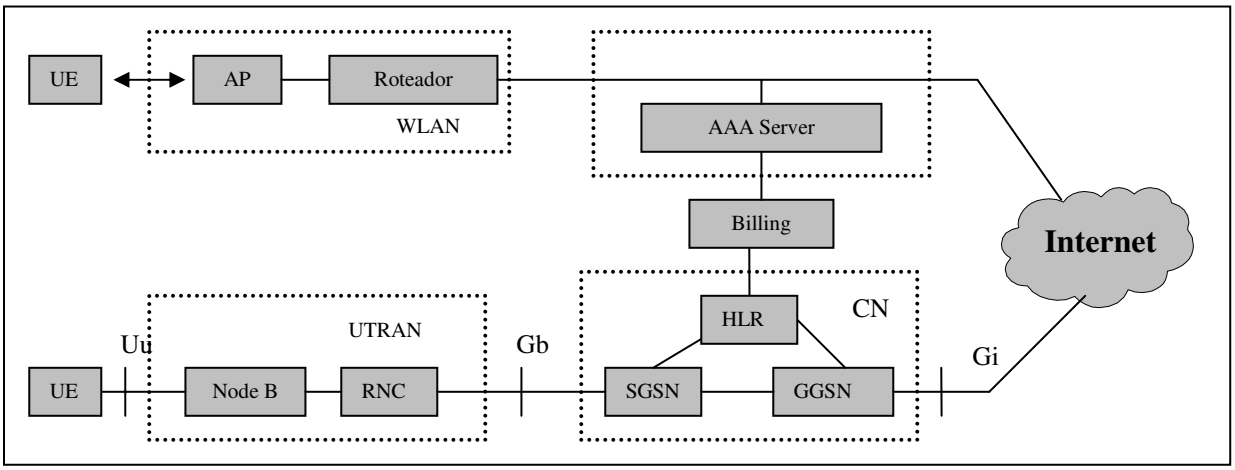


Figura 4.2. Interconexão o*pen coupling* entre UMTS e WLAN.

Um segundo nível de acoplamento é o chamado *loose coupling*, que provê um uso de autenticação comum entre a rede de sistema celular e a WLAN através de uma conexão entre o servidor AAA da WLAN e o HLR do sistema celular, os quais são mantidos separados. Este cenário preenche os requisitos dos cenários 1, 2, 3 e 4. Dependendo da Qualidade de Serviço suportada pela WLAN, este cenário pode preencher os requisitos do cenário 5.

A Figura 4.3 ilustra o acoplamento *loose coupling*.

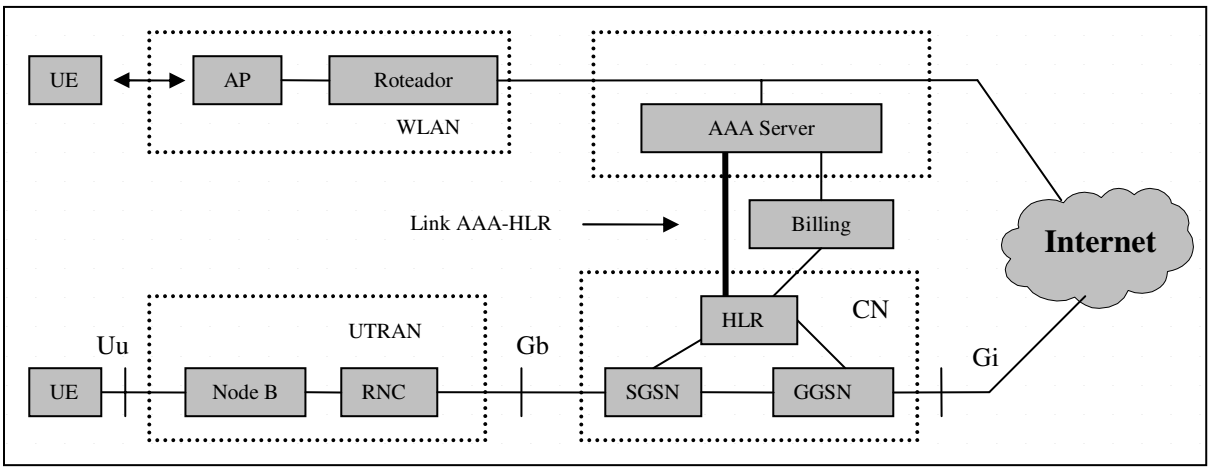


Figura 4.3. Interconexão *loose coupling* entre UMTS e WLAN.

O próximo nível de acoplamento é o *tight coupling* onde o AP é conectado diretamente ao SGSN, através do módulo *Inter Working Function* (IWF). Este cenário também preenche

os requisitos dos cenários 1, 2, 3 e 4 e depende da Qualidade de Serviços suportada pela WLAN para preencher também os requisitos do cenário 5.

A Figura 4.4 ilustra a arquitetura do acoplamento *tight coupling*.

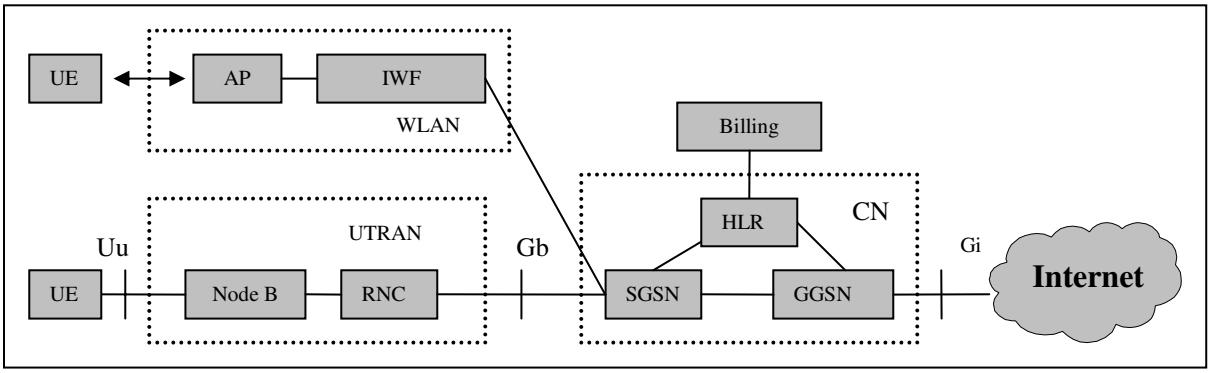


Figura 4.4. Interconexão *tight coupling* entre UMTS/GPRS e WLAN.

O último nível de acoplamento é o *very tight coupling* onde o AP é conectado ao RNC através de um módulo de *Inter Working Function* (IWF) e torna-se parte da UTRAN. Este cenário também preenche os requisitos dos cenários 1, 2, 3 e 4 e também depende da Qualidade de Serviços da WLAN para preencher os requisitos do cenário 5.

A Figura 4.5 ilustra a arquitetura do acoplamento *very tight coupling*.

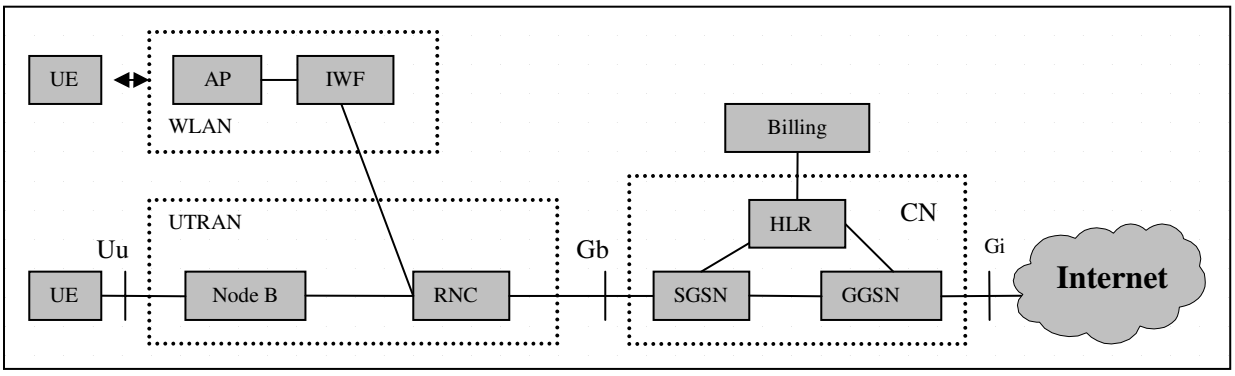


Figura 4.5. Interconexão *very tight coupling* entre UMTS e WLAN.

A complexidade de implementação varia de acordo com o grau de acoplamento, quanto maior o acoplamento (*very tight coupling*) maior o grau de impacto nos elementos de rede UMTS, que passam a ter que suportar as interfaces das WLANs.

## 4.3. Acoplamento de Redes UMTS/GPRS com WLAN 802.11

Esta dissertação concentra-se nas arquiteturas de acoplamento *loose coupling* e *tight coupling*. Os motivos são:

- A arquitetura *open coupling* não traz alteração nos padrões atuais do 3GPP. A condição necessária para o uso dos recursos da WLAN neste tipo de acoplamento é a necessidade de definição de uma nova conta e senha para o usuário do sistema celular a fim de que ele possa se autenticar e então utilizar os recursos da Internet.
- A arquitetura *very tight coupling* apresenta um grau de implementação complexo, visto que o acoplamento acontece no nível de rede de acesso. A grande desvantagem do *very tight coupling* é que as redes de acesso UMTS e GPRS apresentam tecnologias diferentes, UTRAN e GPRS RAN respectivamente, e, portanto, diferentes padrões teriam que ser desenvolvidos para cada rede.
- As arquiteturas *loose coupling* e *tight coupling* são as arquiteturas em estudo pela ETSI para a interconexão de redes HIPERLAN/2 aos sistemas celulares de terceira geração [ETSI 101 957].

No entanto, o escopo deste trabalho será a integração de sistemas celulares GPRS e UMTS com WLANs do padrão 802.11, visto que o padrão 802.11 é o mais difundido mundialmente.

Visto que o as redes 2,5 GPRS e 3G UMTS utilizam o mesmo *Core Network* (CN) para tráfego de pacotes, como visto na Figura 2.6, no restante deste trabalho será utilizada a nomenclatura CN GPRS/UMTS para se referir à rede de pacotes que pode ser implementada tanto na rede 2,5 GPRS ou 3G UMTS.

Do ponto de vista dos cenários de integração descritos pelo 3GPP, este trabalho estará focado nos requisitos do cenário 4, ou seja, acesso aos serviços de dados (Internet) tanto pelas redes WLAN como pelas redes celulares com continuidade de serviço, sem levar em consideração a Qualidade de Serviço. O cenário 5, continuidade de serviço sem interrupções (ou seja, com Qualidade de Serviço), e o cenário 6, acesso aos serviços de comutação, estão fora do escopo desta dissertação.

# 5. A Arquitetura *Loose Coupling*

A arquitetura *loose coupling* é um tipo de interconexão entre as redes WLANs e GPRS que provê o uso de autenticação comum para as duas redes. A Figura 5.1 ilustra a arquitetura deste tipo de acoplamento.

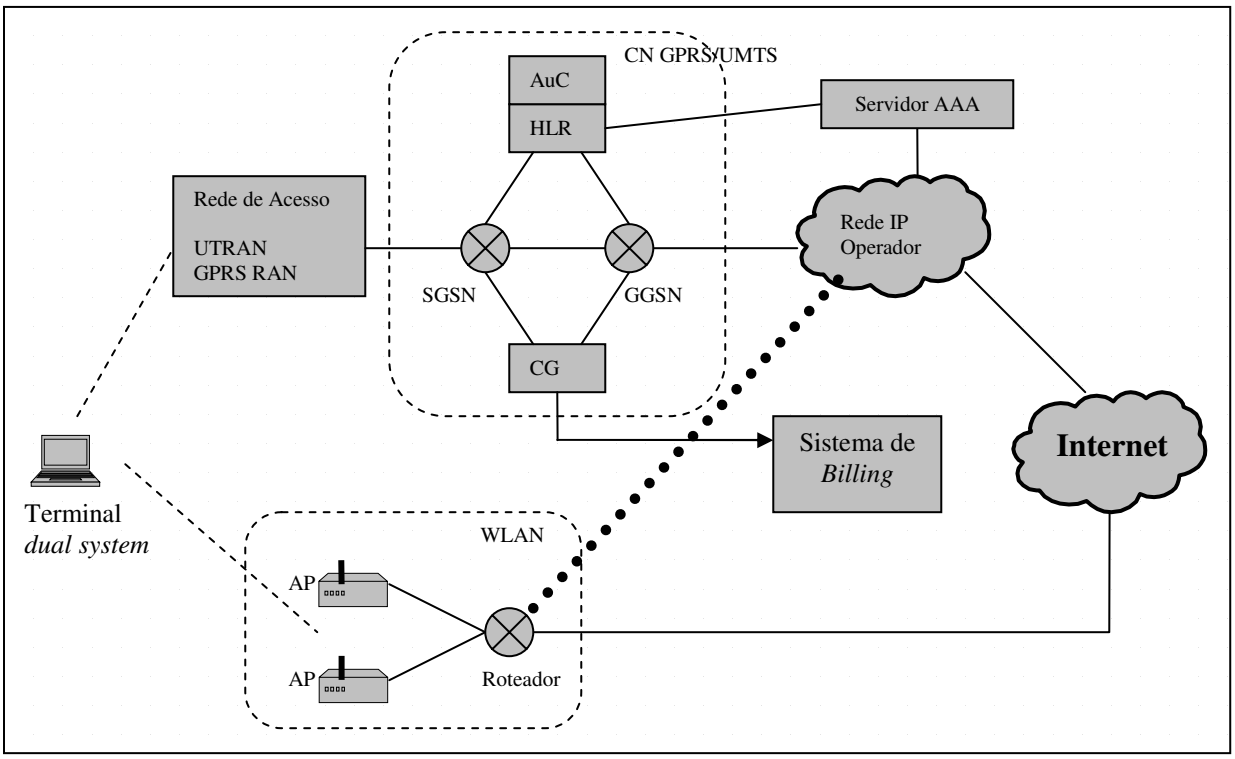


Figura 5.1. Integração entre uma rede GPRS e WLAN utilizando-se o *loose coupling*.

Como pode ser visto neste tipo de arquitetura, a WLAN é acoplada na rede GPRS via a rede IP do operador e o tráfego de dados das WLANs não passa pelo CN GPRS/UMTS, mas vai direto para a Internet ou para a rede IP do operador.

A mobilidade e o *roaming* entre as duas redes podem ser suportados através de:

- Uma conexão dedicada entre a WLAN e a rede IP do operador, como ilustra a linha pontilhada entre a WLAN e a rede IP na Figura 5.1.
- Através de uma rede pública como, por exemplo, a Internet.

No caso onde a WLAN não é propriedade da operadora, ou seja, pertence a outros operadores WISP, acordos de *roaming* são necessários para mobilidade e *roaming*.

Este tipo de arquitetura utiliza os protocolos padronizados pelo IETF para autenticação, autorização e mobilidade. Por isso não é necessário utilizar nenhuma tecnologia de sistema celular nas redes WLAN. Neste tipo de arquitetura, a autenticação baseada nos cartões SIM/USIM pode ser suportada para que o usuário ganhe acesso aos serviços do operador em ambas as redes, celular e WLAN.

Em termos sistêmicos, na arquitetura *loose coupling*, pode-se visualizar a conexão de uma WLAN no sistema celular como ilustra a Figura 5.2 [Haverinen].

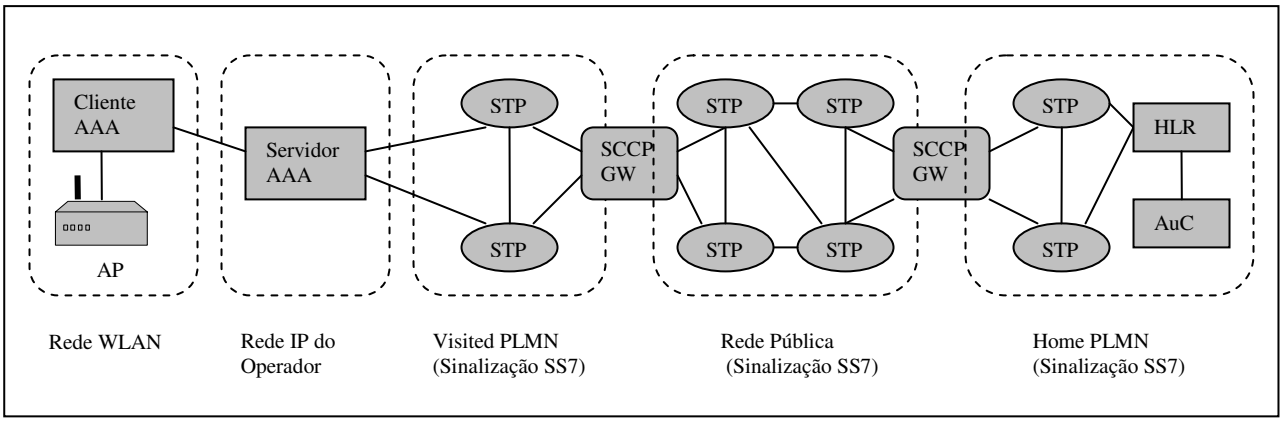


Figura 5.2. Componentes de sistema da rede celular e WLAN.

A união entre os dois sistemas, WLAN e celular, acontece graças ao servidor AAA. Para a rede WLAN, o servidor AAA é o servidor de autenticação de usuários, enquanto que para o sistema celular ele atua como se fosse um VLR (*Visitor Location Register*), requisitando credenciais de usuários para o AuC da PLMN onde o usuário esta registrado, através da sinalização SS7. Por isso, o servidor AAA deve possuir a pilha de protocolo SS7 a fim de poder contatar os serviços do HLR/AuC.

Na rede de sistema celular, o STP (*Signaling Transfer Point*) e o SCCP Gateway (*Signaling Connection Control Part*) têm a função de rotear as mensagens SS7 para os nós correspondentes dentro das PLMN, baseado nos endereços da sinalização SS7, os chamados DPC (*Destination Point Code*). A operação do STP e do SCCP Gateway é semelhante à de roteadores dentro de uma rede IP, ele avalia o DPC de cada mensagem recebida e encaminha para o nó de destino.

## 5.1. Autenticação e Acesso aos Serviços

Dentro das WLANs, a autenticação e o acesso aos serviços do operador de telefonia celular devem ser feitos baseados nos cartões SIM, para os usuários GPRS, e nos cartões USIM, para os usuários UMTS. Nas WLANs 802.11, a autenticação é baseada nos padrões 802.1x [802.1x], onde o servidor de AAA provê a funcionalidade de autenticador dentro da rede IP do operador. O terminal e o AP também devem suportar os métodos e protocolos de autenticação do 802.1x, os quais são baseados no protocolo EAP.

A fim de suportar a interconexão de sistemas celulares GPRS e UMTS com as WLANs, dois novos métodos de autenticação EAP foram criados: EAP SIM (*Subscriber Identity Module*) e EAP AKA (*Authentication and Key Agreement*). O EAP SIM [EAP SIM] e o EAP AKA [EAP AKA] especificam mecanismos baseados no EAP para autenticação e distribuição de chaves utilizando os cartões GSM SIM e UMTS SIM (USIM). O EAP SIM especifica métodos de autenticação para redes GSM enquanto que o EAP AKA especifica métodos de autenticação para as redes GSM e UMTS. Até a data de publicação deste trabalho, o EAP SIM e EAP AKA estavam em fase de desenvolvimento pelo IETF, ou seja, são especificações *Internet-draft.*

Como já foi mencionado anteriormente, o EAP é um protocolo que suporta vários tipos de autenticação. Na realidade o EAP encapsula métodos de autenticação entre um cliente (um autenticador) e um servidor de autenticação. No caso das WLANs e dos sistemas celulares o EAP SIM/AKA tem como cliente o terminal móvel e o servidor de autenticação EAP está na rede IP do operador, implementado no servidor de AAA, como, por exemplo, o RADIUS. O EAP tem um campo que define o tipo do método de autenticação que esta sendo realizado [RFC2284] de modo que o cliente e o servidor de autenticação possam se sincronizar quanto à autenticação a ser realizada.

O AP não precisa saber qual o tipo de autenticação esta sendo realizada. Sua função, durante o processo de autenticação, é somente repassar os pacotes de um lado para outro. No entanto, o AP é único interessado no resultado da autenticação, se a autenticação for um sucesso o AP libera acesso do terminal na rede pela WLAN, caso contrário o terminal terá acesso negado.

Neste tipo de arquitetura o AP é um AP padrão 802.11 e não precisa de nenhuma funcionalidade específica de tecnologia celular GSM, GPRS ou UMTS. No entanto, ele deve suportar o padrão 802.1x.

O servidor de AAA, além dos serviços de autenticação, autorização e *accounting*, também suporta operações de *roaming*, que permite que um usuário de um determinado operador de telefonia celular utilize outra rede de acesso. Atualmente, o RADIUS [RFC2865] é o protocolo de AAA mais utilizado pela indústria IP e é considerado como o *de facto* protocolo para o AAA. O Diameter [Diameter], considerado o sucessor do RADIUS, ainda está em fase de padronização pelo IETF.

### 5.1.1. Autenticação GSM/GPRS

A rede GSM/GPRS provê um processo de autenticação e segurança dos terminais que estão requisitando serviços na rede a fim de que outras pessoas não consigam obter informações dos usuários durante o fluxo de dados entre o usuário e a rede. O processo de autenticação é baseado no paradigma de *Challenge-Response*, no qual o usuário móvel tem que responder a uma determinada requisição para que seja aceito na rede.

O processo de autenticação nas redes GSM/GPRS é baseado em dois algoritmos chamados de A3 e A8 e de ainda uma chave Ki, que é específica para cada usuário e nunca é transferida do terminal para a rede ou vice-versa. A Figura 5.3 [Haverinen][Nyström] ilustra o processo de autenticação de um terminal em uma rede GSM/GPRS.

Ao tentar acessar os serviços da rede, o terminal envia sua identificação para o SGSN, que contata a central de autenticação AuC, passando a identificação do usuário, que pode ser a identificação permanente IMSI ou uma identificação temporária TMSI (*Temporary Mobile Subscriber Identity*). O AuC contém a chave secreta de autenticação de cada usuário Ki, que é obtida através do IMSI ou TMSI, e os chamados algoritmos de autenticação A3 e A8. Baseado na chave de identificação do usuário Ki e em um número aleatório, RAND de 128 bits, gerado automaticamente, o AuC executa os algoritmos A3 e A8 produzindo assim os valores SRES e Kc, respectivamente.

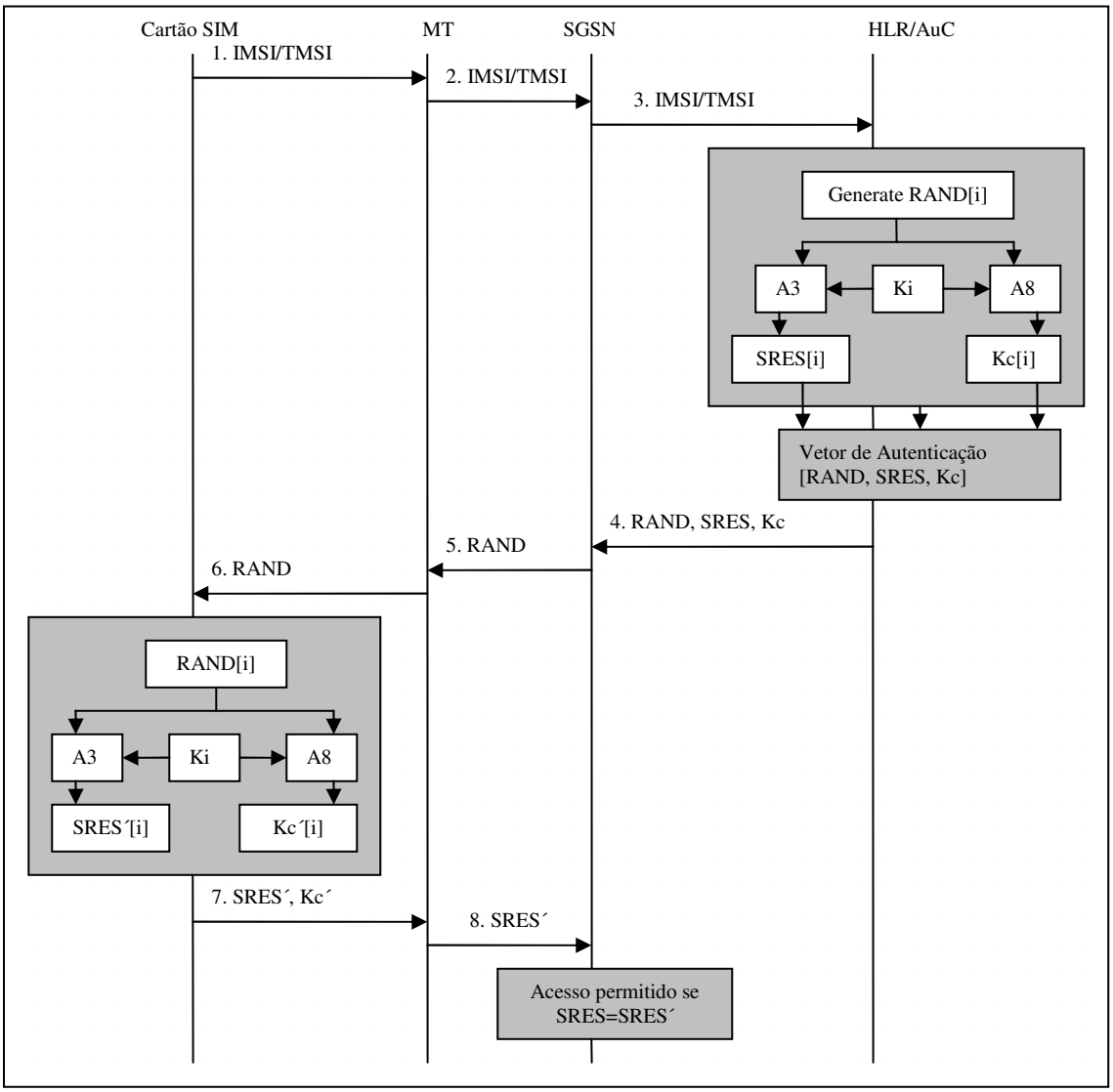


Figura 5.3. Autenticação de acesso em GSM/GPRS.

Os algoritmos A3 e A8 são funções matemáticas *one-way* do tipo hash, ou seja, para cada entrada RAND[i] e Ki, o algoritmo gera uma saída SRES[i] = A3(RAND[i], K[i]) e Kc[i] = A8(RAND[i], K[i]), sendo praticamente impossível obter os valores RAND[i] e K[i] a partir dos valores SRES[i] e Kc[i]. O conjunto destes três valores [RAND, SRES, Kc] é chamado de vetor de autenticação triplo ou ainda *GSM triplet*. SRES é a resposta de assinatura (S*ignature Response*) a ser utilizada no paradigma de *Challenge-Response* e possui 32 bits. Kc é a chave de criptografia e possui 64 bits.

Após obter o vetor de autenticação GSM, o SGSN envia o valor de RAND para o usuário móvel como uma mensagem de *Challenge-Request*. O usuário móvel deve responder a esta requisição a fim de que a autenticação seja confirmada.

O cartão SIM, do mesmo modo que o AuC, também possui chave secreta de autenticação Ki e os algoritmos A3 e A8. O cartão SIM recebe a requisição do SGSN e roda as algoritmos A3 e A8 baseado no valor recebido RAND[i] e na chave Ki, gerando então os valores SRES´[i] e Kc´[i]. O valor de SRES´[i] é então enviado para o SGSN como reposta (*Challenge-Response*) à requisição feita anteriormente.

O SGSN compara os valores de SRES´[i] e SRES[i] e se estes valores forem iguais, a acesso a rede é então permitido.

### 5.1.2. Autenticação UMTS

As redes UMTS utilizam uma arquitetura de autenticação chamada *Authentication and Key Agreement* (AKA). O mecanismo de autenticação UMTS AKA provê autenticação mútua, ou seja, o terminal autentica a rede e a rede autentica o terminal. Do mesmo jeito que nas redes GSM/GPRS, o UMTS AKA segue o paradigma de *Challenge-Response*.

O processo de autenticação do UMTS é baseado em uma chamada Ki, definida para cada usuário, que é compartilhada entre o cartão USIM e o AuC do *Home Environment* (HE) onde o usuário está registrado. Assim como nas redes GSM/GPRS, a chave Ki é permanente para cada usuário e nunca é transferida de um lado para outro. No UMTS, a chave Ki tem 128 bits.

A autenticação UMTS é baseada na chave secreta do usuário Ki, em números randômicos que são gerados pelo AuC e nos chamados algoritmos de autenticação f1, f2, f3, f4 e f5, os quais são utilizados para a geração do vetor de autenticação UMTS.

A Figura 5.4 [Abid][Vala-Sipilä] ilustra o processo de autenticação AKA de um terminal em uma rede UMTS.

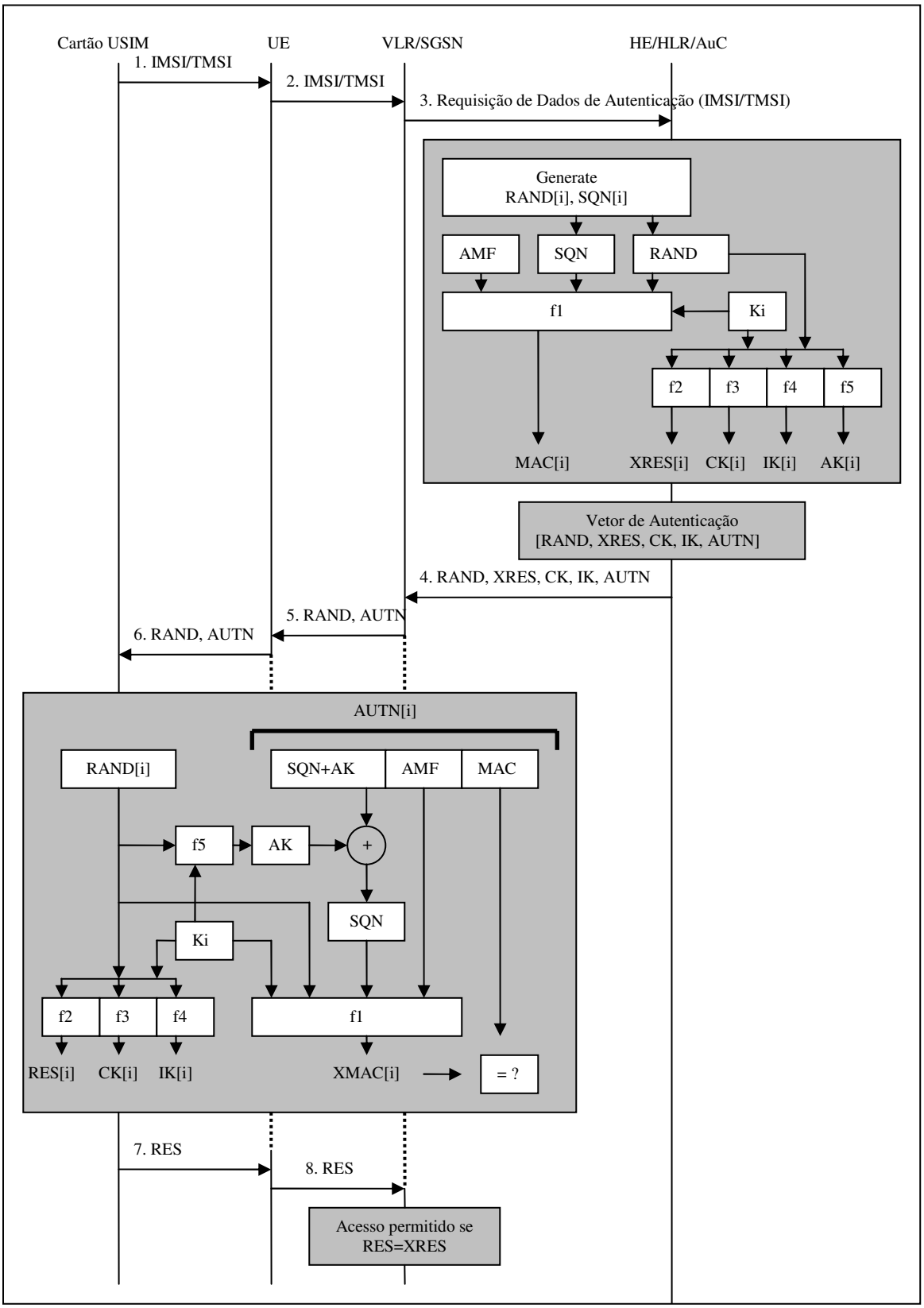


Figura 5.4. Autenticação de acesso UMTS AKA.

Inicialmente o terminal envia sua identificação para o VLR ou SGSN. Esta identificação pode ser a identificação permanente IMSI ou uma identificação temporária TMSI do terminal. O VLR ou SGSN envia uma mensagem requisitando as informações de autenticação para o AuC onde o usuário está registrado (o HE do usuário) contento sua identificação (IMSI ou TMSI). Com a identificação do usuário, o AuC inicia o processo para obter o vetor de autenticação para aquele usuário, o qual consiste da execução de vários algoritmos de criptografia (f1, f2, f3, f4 e f5). Os algoritmos de autenticação do UMTS são funções matemáticas do tipo *one-way*, ou seja, é praticamente impossível obter o valor das entradas baseando-se nos resultados da saída.

O resultado do processo de autenticação UMTS gera os seguintes valores:

- Um número seqüencial SQN, gerado pelo AuC;
- Um valor aleatório RAND, gerado pelo AuC, de 128 bits;
- O *Message Authentication Code* (MAC), de 64 bits, obtido através da chave Ki, de RAND, de SQN e um campo administrativo *Authentication Management Field* (AMF). Este valor é calculado através do algoritmo f1;
- Uma *Expected Response* (XRES), de 32 a 128 bits, obtido através da chave Ki e de RAND. Este valor é calculado através do algoritmo f2. Este é valor que será verificado pela rede UMTS durante o processo de *Challenge-Request*;
- Uma *Ciphering Key* (CK), de 128 bits, obtido através da chave Ki e de RAND. Este valor é calculado através do algoritmo f3;
- Uma *Integrity Key* (IK), de 128 bits, obtido através da chave Ki e de RAND. Este valor é calculado através do algoritmo f4;
- Uma *Authentication Key* (AK), de 64 bits, obtido através da chave Ki e de RAND. Este valor é calculado através do algoritmo f5;
- Um *Authentication Token Number* (AUTN), composto de SQN embaralhado com AK, de AMF e de MAC.

O AuC compõe então o vetor de autenticação UMTS, formado por [RAND, XRES, CK, IK, AUTN], e o envia para o VLR ou SGSN. O VLR ou SGSN extrai os valores RAND e AUTN do vetor de autenticação e os envia como uma mensagem de *Challenge-Request* para o terminal.

O cartão USIM também participa do processo de autenticação. Ele também possui a chave secreta de identificação do usuário Ki e os algoritmos f1, f2, f3, f4 e f5 e é capaz de extrair os valores RES, CK, IK e XMAC a partir de RAND e AUTN.

A autenticação da rede pelo USIM é feita através dos valores de XMAC e MAC. Se XMAC e MAC forem iguais, o cartão USIM assume que os valores RAND e AUTN foram gerados por uma rede que conhece o valor de Ki, ou seja, pelo AuC onde o usuário está registrado (HE) e o processo de autenticação continua com o terminal enviando o valor de RES (*Challenge-Response*) para o VLR ou SGSN. Se os valores de XMAC e MAC forem diferentes, o processo de autenticação é interrompido pelo terminal.

O VLR ou SGSN faz a autenticação do terminal comparando os valores de RES e SRES e se estes valores forem iguais, a acesso à rede é então permitido.

### 5.1.3. Formato de Identificação do Usuário

Em ambas as redes de acesso, WLAN e GPRS, a identificação completa do usuário tem um formato estruturado que é composto pela identificação da rede (*Home Network*), que é utilizada para efeitos de *roaming*, e a identificação do usuário (*UserId*) dentro da rede.

No caso das redes GPRS e UMTS, o usuário é identificado pelo IMSI que é armazenado no cartão SIM/USIM. O IMSI é composto pelos seguintes campos [Haverinen][EAP SIM]:

- *Mobile Country Code* (MCC): este número é composto por 3 dígitos e define o país da operadora;
- *Mobile Network Code* (MNC): identificação da operadora dentro de um país. Este código é composto por 2 ou 3 dígitos;
- *Mobile Subscriber Identification Number* (MSIN): identificação do usuário dentro da rede da operadora. Este número é composto por no máximo 10 dígitos.

Através do MCC e MNC pode-se localizar a rede GSM *Home* do usuário a fim de se localizar o HLR que contém todos os dados do usuário.

Já nas redes de acesso à Internet, o usuário é identificado pelo NAI [RFC2486], o qual consiste de um nome de um usuário e de um domínio, separados pelo símbolo @. Um

exemplo de um NAI válido é *nome.sobrenome@meuwisp.com*. O *roaming* de usuários é feito pelo servidor AAA, que direciona o usuário para a rede apropriada baseado no domínio do NAI. Os servidores AAA são configurados de modo a localizarem o servidor AAA correto baseado no domínio do NAI.

Quando um usuário de telefonia celular tenta acessar a Internet via WLAN, ele precisa de um NAI a fim de poder realizar a autenticação na WLAN e conseguir acesso na rede. Visto que a identificação do usuário de telefonia celular é baseada no IMSI, um mapeamento de IMSI para NAI é então necessário. Um exemplo deste mapeamento é ilustrado na Figura 5.5 [Haverinen][EAP SIM].

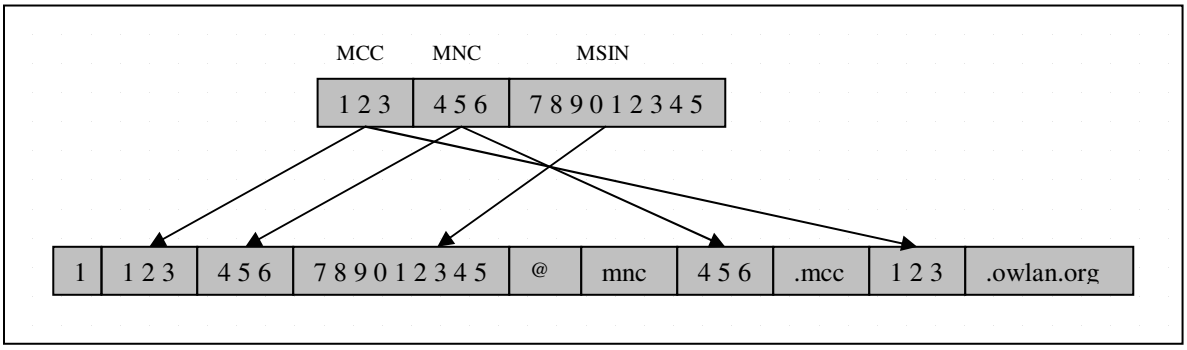


Figura 5.5. Mapeamento de um IMSI em NAI.

O terminal faz o mapeamento incluindo o IMSI como usuário do NAI. O domínio do NAI é derivado dos campos MCC e MNC. No exemplo, um IMSI 123456789012345 é mapeado para o NAI *1123456789012345@mnc456.mcc123.owlan.org*. O campo de usuário é preenchido pelo IMSI e um prefixo indiciando o tipo de autenticação, 0 para EAP AKA [EAP AKA] e 1 para o EAP SIM [EAP SIM]. O campo do domínio é preenchido contendo as informações do MNC e do MCC, os quais possibilitam que os servidores AAA consigam direcionar as requisições para os HRL/AuC apropriados. O último campo "*owlan.org"* é reservado para as autenticações do tipo SIM/AKA.

Os detalhes e recomendações da conversão do IMSI para o NAI podem ser encontrados em [EAP SIM], [EAP AKA] e [3GPP 23.234]

### 5.1.4. Autenticação EAP SIM

O EAP SIM [EAP SIM] utiliza o cartão GSM SIM com a intenção de prover autenticação de terminais em ambientes WLANs que estão interconectadas aos sistemas celulares GPRS.

Como já mencionado anteriormente, a rede GSM/GPRS faz a autenticação dos terminais na rede baseada no vetor de autenticação [RAND, SRES, Kc] (*GSM triplets*), que é gerado pelo AuC. Esta funcionalidade já está disponibilizada nos terminais GSM/GPRS e um meio de autenticação em ambientes WLAN levando em conta o vetor de autenticação é também necessário. O EAP SIM [EAP SIM] tem a finalidade de prover a autenticação de terminais GPRS em ambientes WLANs utilizando o cartão GSM SIM e o vetor de autenticação gerado pelo AuC.

Do mesmo jeito que na autenticação GSM/GPRS SIM, o EAP SIM também segue o paradigma de *Challenge-Response*, onde o terminal tem que responder a uma requisição da rede para que seja autenticado. Nas redes GSM/GPRS somente o terminal é autenticado na rede, muito embora os mecanismos de autenticação suportem a autenticação mútua [Haverinen]. Já no ambiente WLAN, que apresenta riscos maiores a ataques por parte de invasores, o EAP SIM realiza autenticação mútua, ou seja, a rede autentica o terminal e o terminal autentica a rede. Além disso, durante o processo de autenticação, de um a três vetores de autenticação podem ser requisitados ao AuC para se gerar múltiplas chaves Kc, a fim de se obter uma criptografia mais segura.

O processo de autenticação EAP SIM é ilustrado na Figura 5.6 [3GPP 23.934][Haverinen]. O procedimento de autenticação é baseado no IEEE 802.1x [802.1x] e no EAP SIM [EAP SIM].

Nesta arquitetura o servidor AAA, o RADIUS, por exemplo, provê a funcionalidade de um servidor EAP e interage com o HLR/AuC para obter as credenciais do usuário, do mesmo modo que o SGSN faz durante o procedimento de autenticação GSM/GPRS. As credenciais do usuário são necessária para a criação da mensagem de autenticação *challenge-request* que é enviada para o terminal. O AP é um cliente RADIUS que direciona as mensagens EAP do terminal para o servidor AAA e vice-versa, e aguarda o resultado final da autenticação, liberando ou não acesso à rede para o terminal.

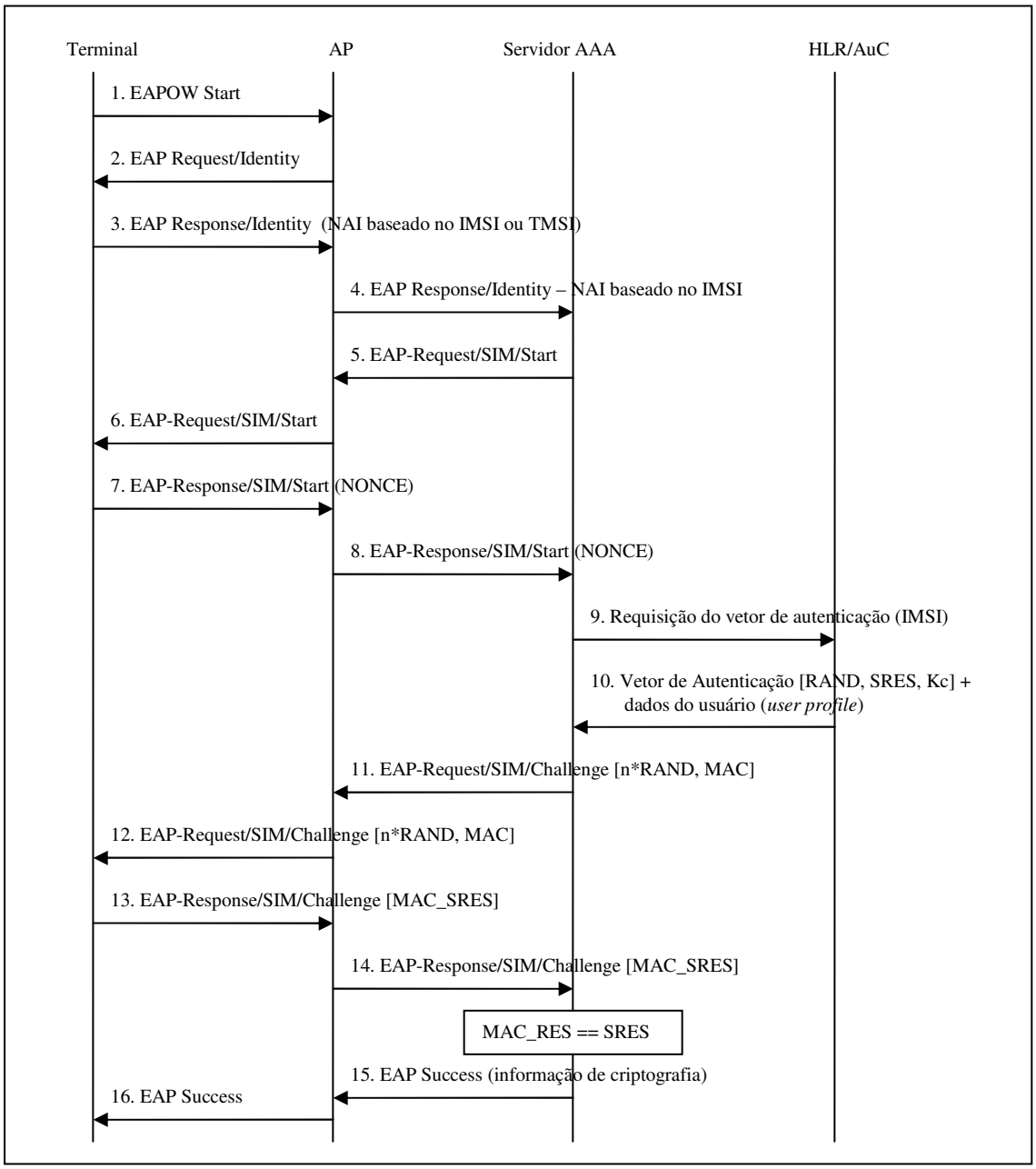


Figura 5.6. Autenticação EAP SIM em rede GPRS.

Os passos neste tipo de autenticação são descritos a seguir:

1. O processo de autenticação começa logo após a associação entre o terminal e o AP. O terminal envia uma mensagem *EAPOW-Start* [802.1x], que inicia a autenticação 802.1x;
2. O AP envia uma mensagem *EAP Request/Identity* [RFC2284], requisitando a identidade do terminal;

3. O terminal envia uma mensagem *EAP Response/Identity* [RFC2284] contendo sua identidade, o IMSI ou TMSI, no formato NAI [RFC2486];
4. Baseado no domínio do NAI recebido, a requisição é enviada para o servidor AAA apropriado. No caso de uso do RADIUS como servidor AAA, a mensagem *EAP Response/Identity* é encapsulada na mensagem *RADIUS Access-Request* [RFC2865];
5. O servidor AAA, baseado no NAI, verifica que o requisitante é um usuário GSM/GPRS e inicia a autenticação SIM enviando uma mensagem *EAP-Request/SIM/Start* [EAP SIM] para o AP. Esta mensagem é encapsulada na mensagem *RADIUS Access-Accept* [RFC2865];
6. O AP repassa a mensagem *EAP-Request/SIM/Start* [EAP SIM] para o terminal;
7. O terminal escolhe um número aleatório NONCE, o qual será utilizado mais tarde pelo próprio terminal para fazer a autenticação da rede, e o envia na mensagem *EAP Response/SIM/Start*. O valor de NONCE pode ser entendido como um *challenge-request* que o terminal faz para a rede;
8. O AP encapsula a mensagem *EAP Response/SIM/Start* [EAP SIM] na mensagem *RADIUS Access-Request* [RFC2865] e a envia para o servidor AAA;
9. O servidor AAA faz a requisição do vetor de autenticação [RAND, SRES, Kc] e os dados do usuário para o HLR/AuC, baseado no NAI. O servidor AAA utiliza a mesma pilha de protocolos SS7 utilizado na rede SS7 do GSM/GPRS, assim o roteamento da requisição do vetor de autenticação é direcionado para o HLR/AuC apropriado;

   Múltiplas requisições de vetores de autenticação podem ser feitas ao HLR/AuC, a fim de se obter chaves de criptografia mais seguras. O número de requisições, *n*, varia de 1 a 3;
10. O HLR/AuC retorna o(s) vetor(es) de autenticação;
11. O servidor AAA envia a mensagem *EAP-Request/SIM/Challenge* [EAP SIM], encapsulada na mensagem *RADIUS Access-Challenge* [RFC2865], contendo *n* valores de RAND e um *Message Authentication Code* (MAC), que serão utilizados pelo terminal a fim de confirmar a autenticação. O MAC é calculado com base no número NONCE que foi enviado pelo móvel (passo 7) e pode ser entendido como um *challenge-response* da rede GPRS ao NONCE;

12. O AP repassa a mensagem *EAP-Request/SIM/Challenge* [EAP SIM] para o terminal. O terminal, através do cartão SIM, executa os algoritmos de autenticação A3 e A8 para cada RAND recebido, obtendo assim várias chaves de criptografia Kc. A chave de criptografia a ser utilizada é obtida das várias chaves Kc e do número NONCE gerado anteriormente no item 7. O terminal também calcula uma cópia do MAC, baseada no número NONCE, e verifica se o valor recebido MAC recebido é igual a MAC calculado. Se os valores forem diferentes, a autenticação da rede falhou e o terminal ignora as mensagens EAP recebidas. Se os valores são iguais, o processo de autenticação continua e o terminal calcula o valor MAC_SRES (*MAC Signature Response*), que é a resposta ao *challenge-request* feito pelo servidor AAA (passo 11);
13. O terminal então envia uma mensagem do tipo *EAP-Response/SIM/Challenge* [EAP SIM], contendo o valor de MAC_SRES, para o AP;
14. O AP repassa a mensagem *EAP-Response/SIM/Challenge* [EAP SIM] com o valor de MAC_SRES, para o servidor AAA, encapsulando-a na mensagem *RADIUS Access-Request* [RFC2865];
15. O valor de MAC_SRES é comparado com o valor de MAC. Se os valores forem iguais o servidor AAA envia uma mensagem *EAP-Success* [RFC2284] ao AP através da mensagem *RADIUS Access-Accept* [RFC2865]. Esta mensagem inclui informação criptográfica para o AP, que será utilizada para fins de segurança na interface aérea do 802.11;

    Se os valores de MAC_SRES e MAC forem diferentes, uma mensagem *EAP-Failure* [RFC2284] é enviada ao AP através de uma mensagem *RADIUS Access-Reject* [RFC2865];
16. O AP envia a mensagem *EAP-Success [RFC2284]* (ou *EAP-Failure* [RFC2284]) para o terminal;

### 5.1.5. Autenticação EAP AKA

O EAP AKA [EAP AKA] define um tipo de EAP que permite que um terminal GSM ou UMTS seja autenticado em ambientes WLANs, provendo um nível de segurança maior que o EAP SIM [Nyström][S3-020549]. Do mesmo modo que no EAP SIM, os mecanismos de

autenticação do EAP AKA são baseados no cartão SIM/USIM. Para o modo UMTS, a autenticação múltipla é suportada, enquanto que no modo GSM somente a autenticação do terminal pela rede é suportada. O EAP AKA também segue o paradigma de *Challenge-Response*.

O processo de autenticação EAP AKA para um terminal UMTS é ilustrado na Figura 5.7 [3GPP 23.934]. O procedimento de autenticação é baseado no IEEE 802.1x [802.1x] e no EAP AKA [EAP AKA]. Assim como no EAP SIM, esta arquitetura tem um servidor AAA, o RADIUS, por exemplo, que provê a funcionalidade de um servidor EAP e interage com o HLR/AuC, do mesmo modo que o VLR ou SGSN faz durante o procedimento de autenticação de um terminal UMTS. O AP é um cliente RADIUS que repassa as mensagens EAP do terminal para o servidor AAA e vice-versa, e provê acesso à rede de acordo com o resultado final da autenticação.

Os passos na autenticação EAP AKA são descritos a seguir:

1. O processo de autenticação começa logo após a associação entre o terminal e o AP. O terminal envia uma mensagem *EAPOW-Start* [802.1x],que inicia a autenticação 802.1x;
2. O AP envia uma mensagem *EAP Request/Identity* [RFC2284], requisitando a identidade do terminal;
3. O terminal envia uma mensagem *EAP Response/Identity* [RFC2284] contendo sua identidade, o permanente IMSI ou o temporário TMSI, no formato NAI [RFC2486].
4. Baseado no domínio do NAI recebido, a requisição é enviada para o servidor AAA apropriado. No caso de uso do RADIUS como servidor AAA, a mensagem *EAP Response/Identity* é encapsulada na mensagem *RADIUS Access-Request* [RFC2865];
5. O servidor AAA faz a requisição do vetor de autenticação [RAND, XRES, CK, IK, AUTN] e os dados do usuário para o HLR/AuC, baseado na informação do NAI. O servidor AAA utiliza a mesma pilha de protocolos SS7 utilizado na rede SS7 do UMTS. Assim o roteamento da requisição do vetor de autenticação é direcionado para o HLR/AuC apropriado;
6. O HLR/AuC retorna o vetor de autenticação;

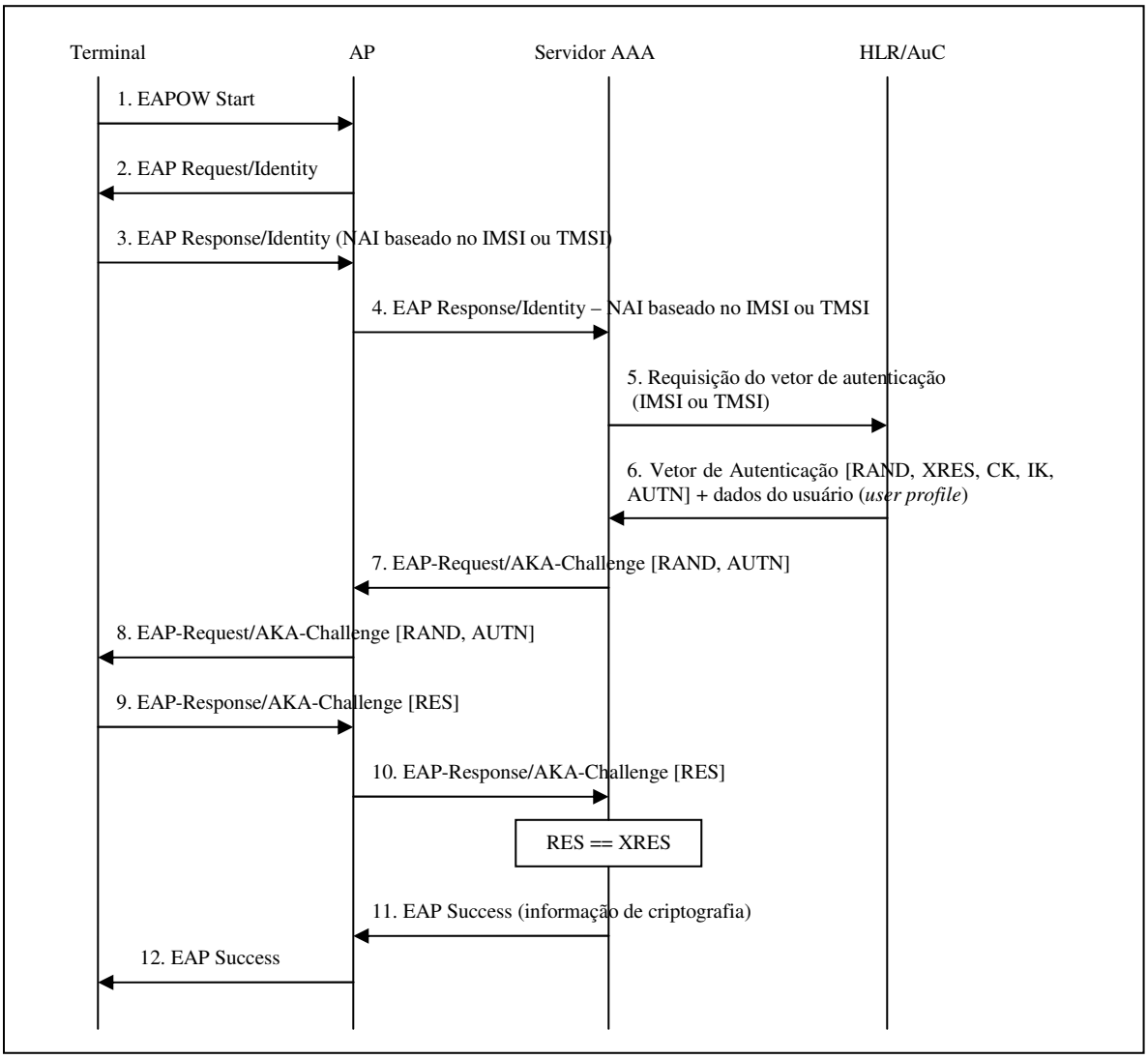


Figura 5.7. Autenticação EAP AKA em rede UMTS.

7. O servidor AAA envia a mensagem *EAP-Request/AKA-Challenge* [EAP AKA], encapsulada na mensagem *RADIUS Access-Challenge* [RFC2865], contendo *n* valores de RAND e AUTN, os quais serão utilizados pelo cartão USIM a fim de confirmar a autenticação da rede pelo terminal;
8. O AP repassa a mensagem *EAP-Request/AKA-Challenge* [EAP AKA] para o terminal. O terminal, através do cartão USIM, executa os algoritmos de autenticação para os valores de RAND e AUTK recebidos. Se XMAC for diferente de MAC, a autenticação é rejeitada pelo terminal. Se XMAC for igual ao MAC recebido no AUTN, a rede é

autenticada e o USIM calcula os valores RES, CK e IK. O valor RES, que é a resposta ao *challenge-request* feito pelo servidor AAA;

9. O terminal então envia uma mensagem do tipo *EAP-Response/AKA-Challenge* [EAP AKA], contendo o valor de RES, para o AP;
10. O AP repassa a mensagem *EAP-Response/AKA-Challenge* [EAP AKA] com o valor de RES, para o servidor AAA, encapsulando-a na mensagem *RADIUS Access-Request* [RFC2865];
11. O valor de RES é comparado com o valor de XRES. Se os valores forem iguais o servidor AAA envia uma mensagem *EAP-Success* [RFC2284] ao AP através da mensagem *RADIUS Access-Accept* [RFC2865]. Esta mensagem inclui informação criptográfica para o AP, que será utilizada para comunicação entre o AP e o terminal na interface aérea do 802.11;

    Se os valores de RES e XRES forem diferentes, uma mensagem *EAP-Failure* [RFC2284] é enviada ao AP através de uma mensagem *RADIUS Access-Reject* [RFC2865];
12. O AP envia a mensagem *EAP-Success* [RFC2284] (ou *EAP-Failure* [RFC2284]) para o terminal.

O mesmo fluxo de mensagens também é usado no modo GSM, com a exceção do vetor de autenticação GSM retornado pelo AuC (passo 6) e de que somente o atributo RAND é enviado para o terminal (passos 7 e 8).

### 5.1.6. Plano de Controle de Autenticação EAP SIM/AKA

Nos procedimento EAP SIM e EAP AKA a autenticação do usuário na rede depende do HLR onde o usuário está registrado (*Home PLMN*). O AP na WLAN implementa o 802.1x e atua como um cliente RADIUS. O servidor AAA implementa o protocolo RADIUS e acessa os dados do usuário no HLR/AuC via sinalização SS7, através dos serviços oferecidos pelo MAP. A autenticação propriamente dita depende dos dados do HLR da PLMN na qual o usuário esta registrado.

O plano de controle com os protocolos utilizados pelo processo de autenticação é ilustrado na Figura 5.8 [Salkintziz]. Pode-se observar que o terminal é autenticado pelos métodos de autenticação SIM ou AKA presentes no terminal e HLR.

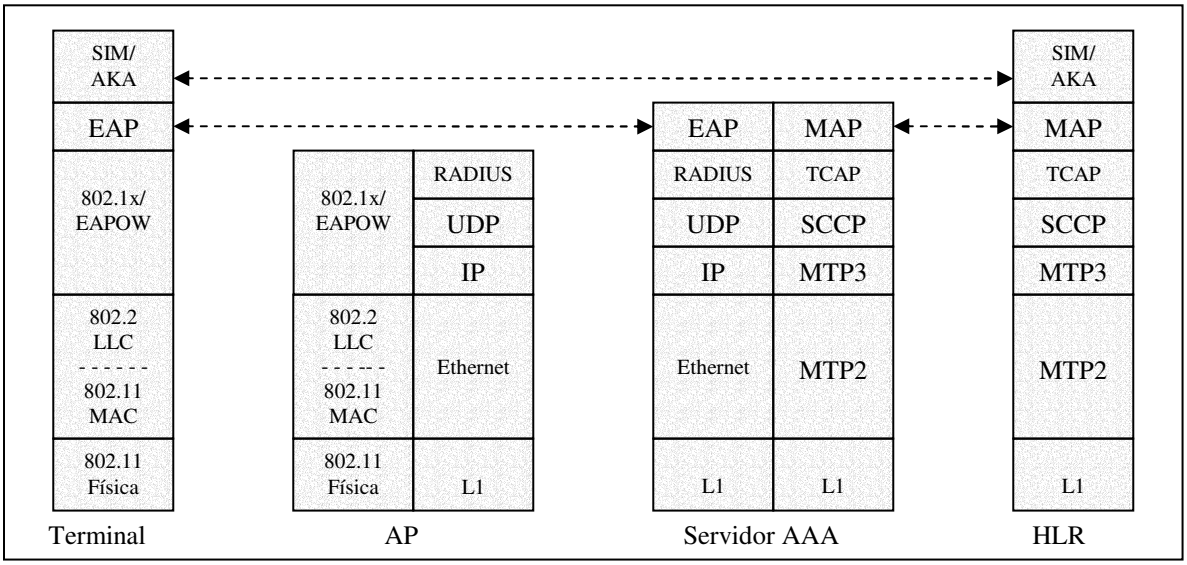


Figura 5.8. Plano de controle de autenticação.

Pode-se observar na Figura 5.8 que o servidor AAA possui uma pilha de protocolos MAP (*Mobile Application Part*), que o habilita a requisição de serviços do HLR/AuC através da sinalização SS7.

A sinalização SS7 é responsável por localizar a *Home PLMN* onde o usuário está registrado.

## 5.2. Billing e Accounting

As redes GPRS e WLAN têm requisitos específicos com relação a *accounting*. Ambas as redes são baseadas em pacotes e devem estar aptas a prover um serviço permanente para o usuário, os quais podem ser baseados em tempo de utilização da rede ou em termos de dados transferidos pela rede. Devido a estas características, vários métodos de *accounting* podem ser suportados pelo operador como, por exemplo, *accounting* baseado em tempo de uso da rede, onde os tempos de conexão inicial e final são reportados, *accounting* baseado em volume de dados transmitidos, onde a quantidade de dados transmitida é reportada, ou ainda uma taxa

única mensal, onde o usuário tem tempo de uso e volume de dados a serem transmitidos ilimitados.

No caso da rede GPRS, vários nós são utilizados pelo usuário quando ele acessa os serviços de *packet-switch* e o SGSN e o GGSN fazem o monitoramento do tráfego do usuário pela rede para efeitos de *accounting*. A fim de consolidar os dados de tráfego de usuários, o sistema GPRS define um elemento lógico de rede chamado *Charging Gateway Functionality* (CGF), o qual provê uma interface lógica entre o SGSN e GGSN e o sistema de *billing*. A interface entre SGSN/GGSN e o CGF é a interface Ga, que é a responsável pela transmissão dos *Call Detail Records* (CDR), como ilustra a Figura 5.9.

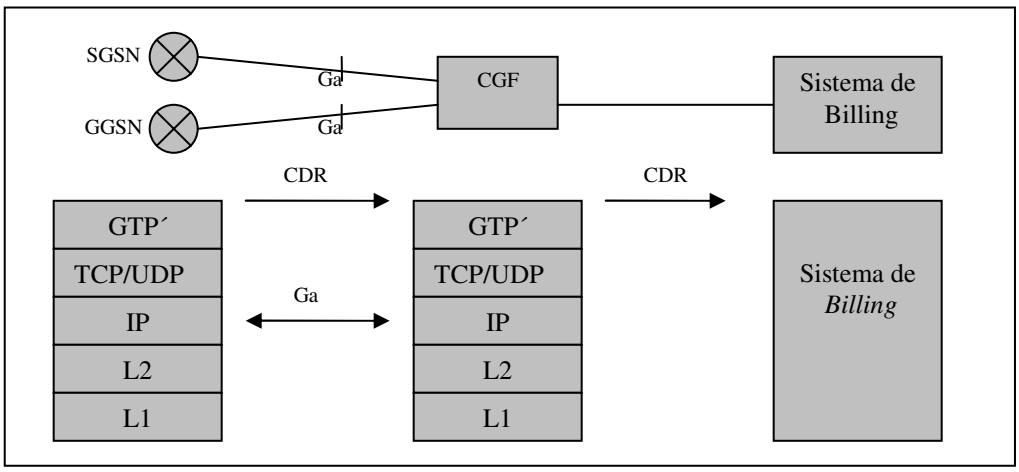


Figura 5.9. A interface Ga entre SGSN/GGSN e o CGF.

O CFG é um elemento de rede que age como um nó intermediário de armazenamento de CDRs e sua função é de filtrar, pré-processar e consolidar todos os CDR enviados pelo SGSN e GGSN antes de enviá-los para o sistema de *billing*, o que ajuda a diminuir a carga de processamento no sistema de billing.

Os CDRs gerados pelo SGSN e GGSN são enviados para o CGF através do protocolo *GPRS Tunneling Protocol for Charging*, ou GTP´, o qual é derivado do GTP. A interface entre o CGF e o sistema de *billing* depende do sistema de *billing* que esta sendo utilizado pelo operador e normalmente requer algum tipo de configuração no CGF. Exemplos desta interface são o FTAM (*File Transfer, Access and Management*) e o FTP (*File Transfer Protocol*) [Nyström].

O CGF é uma entidade lógica dentro da rede GPRS que é conectado ao sistema de *billing*. Ele pode estar integrado junto ao SGSN e GGSN ou ainda estar localizado em um nó separado chamado de *Charging Gateway* (CG), como ilustra a Figura 5.10 [Haverinen].

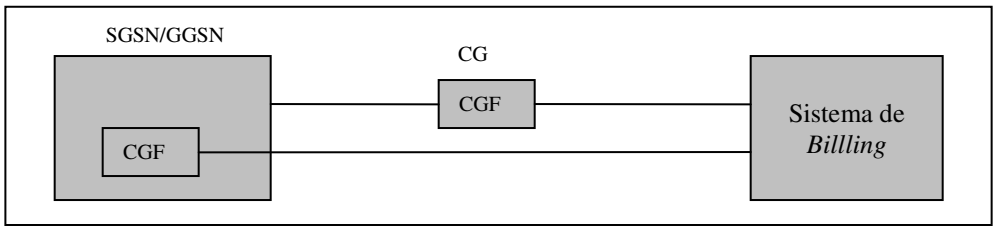


Figura 5.10. CGF conectado no sistema de *billing*.

Na arquitetura *loose coupling* da Figura 5.1, a funcionalidade do CGF está no elemento de rede CG.

Dentro da rede WLAN, os protocolos AAA também incluem a funcionalidade de *accounting*. O AP, que agrega a funcionalidade de cliente AAA, coleta informações a respeito de recursos que estão sendo utilizados pelo usuário, como, por exemplo, tempo inicial e final de conexão e volume de dados transmitidos, e os envia para o servidor AAA.

O servidor AAA RADIUS [RFC2865], inclui extensões para a transmissão de dados de *accounting*. O Diameter, também inclui tais extensões. Como já mencionado anteriormente, a solução da arquitetura *loose coupling* utiliza os protocolos padronizados pelo IETF e, por isso, suporta a solução RADIUS para *accounting*.

O AP envia dados para o servidor AAA contendo informações como tempo conexão e volume de dados transmitidos e recebidos. O servidor AAA verifica a identificação do terminal (IMSI ou TMSI) e converte a informação de *accounting* recebida para o formato CDR no padrão GPRS. Um código dentro do CDR identifica que o CRD é de origem de uma WLAN [Ala-Laurila].

Durante a conexão, o AP também pode enviar relatórios intermediários para o servidor AAA, e o servidor AAA pode também ser configurado de modo a enviar CDRs intermediários para o CG. O servidor AAA envia os CDRs para o CG utilizando o protocolo GTP´.

Ao terminar a conexão, o relatório final contendo todos os dados necessários para efeitos de tarifação é enviado ao servidor AAA. O servidor de AAA, ao receber o relatório final, prepara o CDR para aquela conexão e envia para o CG. Uma vez recebido o relatório

final, o CG consolida todos os CDR recebidos durante aquela conexão e envia uma CDR final para o sistema de *billing*.

Para aumentar a segurança dos dados de accounting, visto que estes dados são os responsáveis pelas contas dos usuários, é recomendado o uso de criptografia entre o AP e o servidor AAA. Os dados podem ser criptografados utilizando-se o protocolo IPSEC ou ainda pode-se utilizar o mecanismo *shared secret* provido pelo RADIUS [Ala-Laurila].

## 5.3. Mobilidade

O conceito de mobilidade dentro de um sistema celular refere-se ao fato de um usuário poder atravessar diferentes células de um operador sem perder a conexão, onde uma célula é definida como sendo a área geográfica coberta por uma BTS. O mesmo conceito estende-se para o caso das WLANs e para os sistemas híbridos WLAN e redes celulares, onde o usuário deve estar habilitado a se mover entre diferentes células da rede celular e das WLANs sem perder a conexão.

No caso dos telefones celulares, os usuários já dispõem da possibilidade de se locomover entre diferentes células sem perda de conexão. Da mesma maneira, os terminais móveis que provêem comunicação de dados, como os laptops e PDAs, devem também ter a mesma possibilidade de mobilidade entre as WLANs e os sistemas celulares. No entanto, as transmissões de dados dos terminais móveis entre as redes são feitas através de conexões que usam IP, as quais serão desconectadas durante o processo de *handoff* entre as redes de acesso, devido à mudança de endereço IP entre as conexões. Por este motivo, um suporte externo é necessário ao IP a fim se obter a mobilidade para os terminais.

Um exemplo de suporte para a mobilidade entre as WLANs e os sistemas celulares é o Mobile IP (MIP) [RFC2002]. O Mobile IP utiliza dois endereços IP que estão ligados a um terminal móvel. Um endereço IP é o IP local e é registrado na *Home Network*. Um outro endereço é o *Care-of-Address* (COA), o qual é variável, que é utilizado na *Foreign Network*, onde o terminal está correntemente conectado.

A arquitetura Mobile IP é composta pelos seguintes elementos:

- Um *Mobile Node* (MN), que é o terminal que viaja entre diferentes redes de acesso;

- Um *Correspondent Node* (CN), que é a entidade na rede com o qual o MN está se comunicando;
- Um *Home Agent* (HA), que está localizado na rede onde MN está registrado (a *Home Network*) e suporta o endereço IP e a conexão da rede quando o MN visita diferentes redes de acesso;
- Um *Foreign Agent* (FA), que atua como servidor de rede de acesso e faz o roteamento do tráfego do MN para o HA.

O Mobile IP define também o conceito de *Care-of-Address* (COA), que está relacionado com o endereço IP para o qual o HA irá rotear os pacotes IP destinados ao MN. Maiores detalhes da arquitetura Mobile IP podem ser vistos em [RFC2002].

Para o caso da arquitetura *loose coupling*, uma solução para a mobilidade é adição de um FA na rede GPRS e um FA na rede WLAN, como ilustra a Figura 5.11.

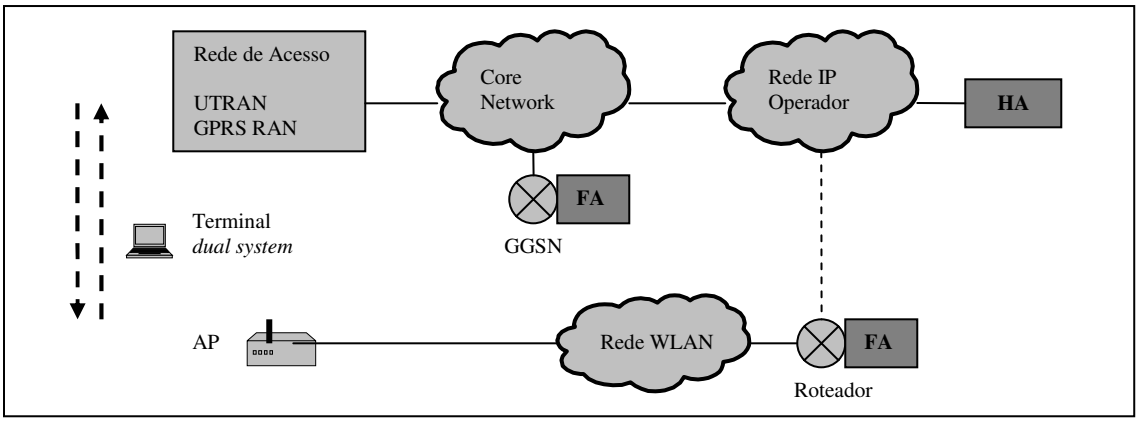


Figura 5.11. Integração GPRS/UMTS e WLAN utilizando Mobile IP.

Na rede GPRS, o FA é adicionado junto ao GGSN e na rede WLAN o FA reside no roteador de acesso para a rede privada do operador ou Internet. O HA está localizado na rede IP privada do operador.

O processo de *handoff* de um terminal na rede WLAN para a rede GPRS acontece da seguinte maneira. A potência do sinal recebido do AP pelo móvel é inicialmente forte o suficiente para que a conexão permaneça na WLAN. À medida que o usuário se afasta da WLAN, o sinal oriundo do AP se torna cada vez mais fraco, até o algoritmo de *handoff* no

terminal decidir se desassociar da WLAN e se associar à rede GPRS. Quando o terminal se associa à rede GPRS ele envia um registro MIP utilizando o FA da rede GPRS, que é o GGSN. O FA completa o registro MIP juntamente com o HA, fornecendo um endereço IP COA para o HA, o qual será utilizado pelo HA a fim de rotear os pacotes para o terminal. O FA faz a associação do endereço IP COA com o endereço IP do terminal e atua como um *proxy agent* em nome do terminal durante aquela conexão.

O mesmo processo também acontece quando o terminal se desassocia de uma rede GPRS e se associa a uma rede WLAN. O terminal detecta a presença de uma rede WLAN e decide então se desassociar da rede GPRS e se associar com a rede WLAN, enviando um registro MIP utilizando o FA da rede WLAN, que está localizado no roteador de acesso da WLAN. O registro é completado entre o FA e o HA, com o FA da WLAN enviando o endereço IP COA para o HA, que passa a atuar como *proxy-agent* para o terminal dentro da WLAN.

Outros exemplos de suporte para mobilidade podem ser vistos em [Sun].

## 5.4. Roaming de Usuários

O conceito de *roaming* está relacionado ao fato de usuários registrados em uma determinada empresa de rede celular possam também utilizar redes de acesso de outros operadores. Os operadores de telefonia celular já dispõem da infra-estrutura necessária para suportar *roaming* entre diferentes redes de acesso e os acordos de *roaming* já permitem mecanismos de autenticação, *accounting* e *billing* entre redes de acesso de diferentes operadores.

Nas redes híbridas, celulares e WLAN, o *roaming* é obtido através de acordos que permitem os servidores de AAA das redes WLAN contatarem o HLR/AuC dede diferentes operadores de rede celular. Quando um terminal tenta utilizar os serviços de uma WLAN, o servidor de AAA contata o HLR/AuC da PLMN onde o usuário está registrado e obtém os dados necessários para a autenticação do usuário.

A Figura 5.12 ilustra o *roaming* entre diferentes operadores durante o acesso pela WLAN.

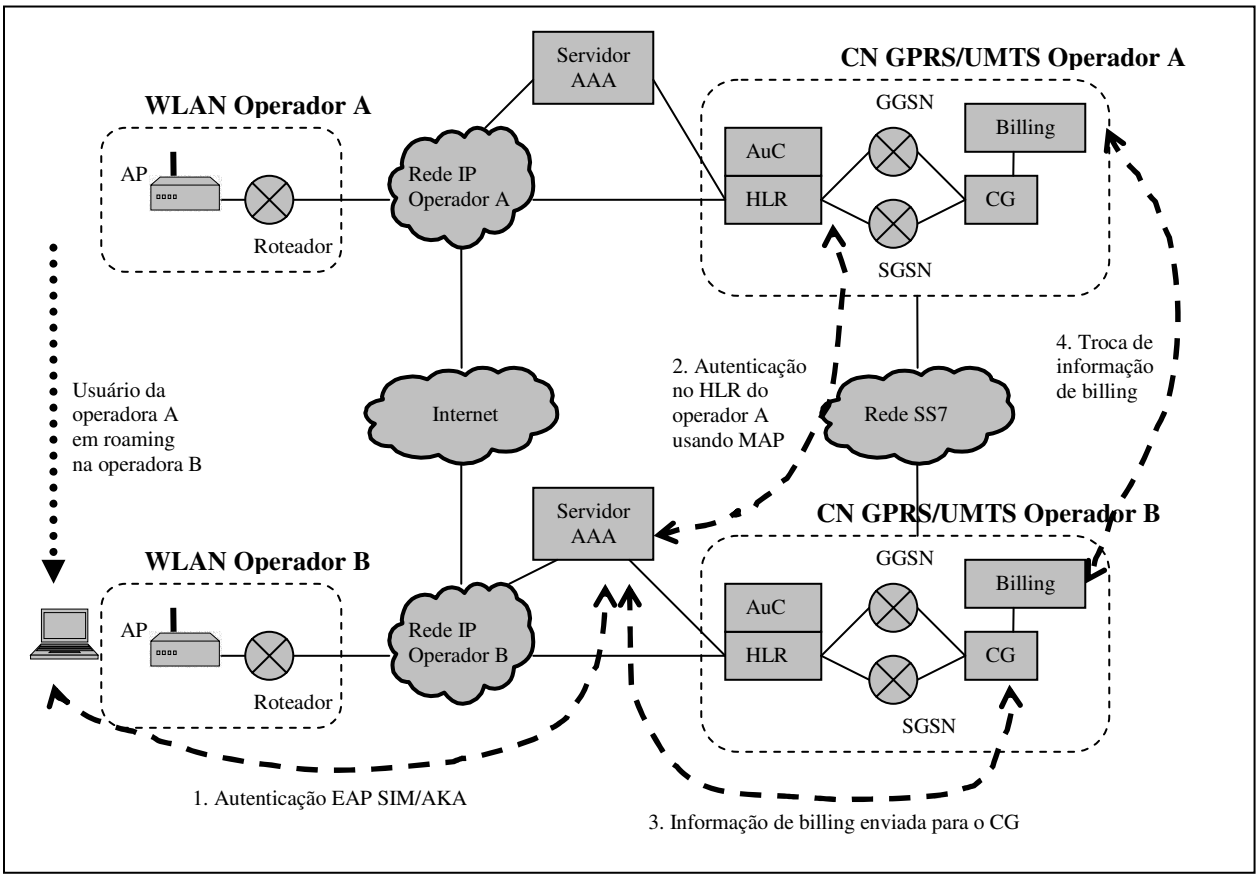


Figura 5.12. *Roaming* entre operadores utilizando WLAN como rede de acesso.

Podemos destacar os seguintes passos no processo de *roaming*:

1. Início da autenticação EAP SIM/AKA.

   O terminal, que contém um cartão SIM/USIM na rede do operador A, ao se aproximar da WLAN do operador B, inicia o processo de associação com a WLAN. Logo em seguida começa o processo de autenticação EAP SIM/AKA com o servidor AAA do operador B.

2. Autenticação no HLR/AuC no *Home PLMN*.

   O servidor AAA do operador B identifica o IMSI do terminal através do NAI recebido durante a autenticação e verifica que os operadores A e B têm um acordo de *roaming* para WLANs. O servidor AAA do operador B, utilizando os serviços da camada MAP da sinalização SS7, envia a requisição de autenticação para o HLR do operador A.

O HLR do operador A responde a requisição feita pelo servidor AAA do operador B com o vetor de autenticação e a *profile* do usuário e o processo de autenticação do terminal é completado.

A partir deste ponto o terminal passa a ter acesso aos serviços da rede.

3. Informação de *billing* da chamada.

   Quando o terminal se desconecta, o servidor AAA envia um CDR com as informações de accounting para o CG do operador B. O CDR tem a indicação de que foi gerado por um terminal em *roaming*. Outros CDRs intermediários também podem ser enviados enquanto o usuário acessa a rede.

4. Troca de informação de billing entre os operadores.

   Regularmente, os sistemas de *billing* dos operadores se comunicam entre si e trocam informações com relação entre CDRs de terminais em *roaming*. Este mecanismo garante que os CDRs do tipo WLAN gerados pelo terminal em *roaming* são enviados para o sistema de billing do operador A e daí então submetidos na conta final do usuário.

## 5.5. Plano de Controle do Usuário

Se o resultado da autenticação do usuário foi bem sucedido, o AP libera o acesso para o usuário à Internet. A partir deste momento o usuário não necessita mais entrar em contato com a rede GPRS, pois o acesso à Internet é feito diretamente pela rede WLAN.

O AP, que contém um cliente AAA, armazena as informações de tempo de acesso e quantidade de dados enviados e recebidos do cada usuário e notifica o servidor AAA na rede IP do operador para efeitos de adicionar estas informações na conta do usuário, como ilustra a Figura 5.13 [ETSI 101 957].

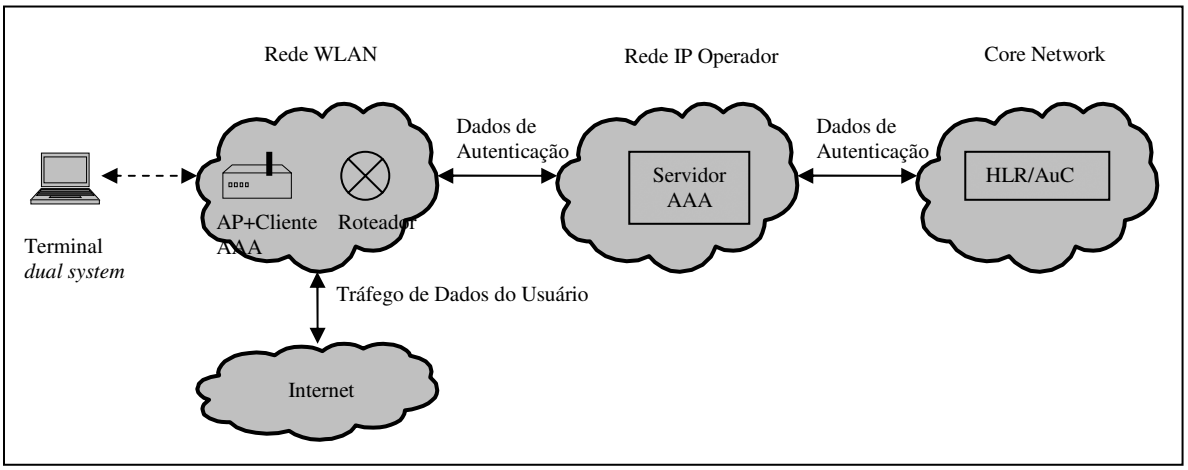


Figura 5.13. Dados de usuário e dados de autenticação na arquitetura *loose coupling*.

O plano de transmissão dos dados do usuário é ilustrado na Figura 5.14. A notação L2/L1 denota as duas camadas mais baixas utilizadas na pilha de protocolos.

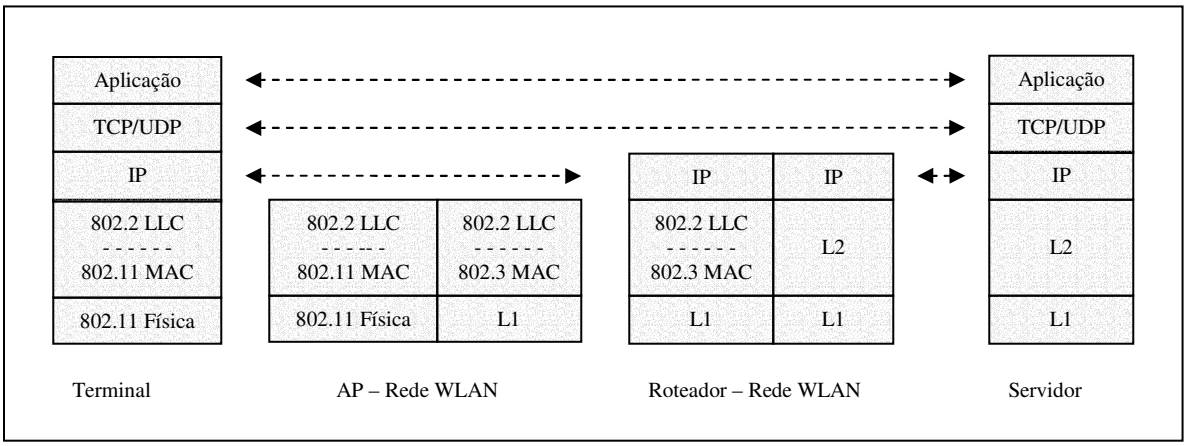


Figura 5.14. Plano de transmissão de dados do usuário.

# 6. A Arquitetura *Tight Coupling*

A arquitetura *tight coupling* é um tipo de interconexão entre as redes WLANs e o CN GPRS/UMTS no qual a WLAN é conectada ao CN GPRS/UMTS da mesma maneira que as redes de acesso do GPRS (GPRS RAN) e UMTS (UTRAN). Neste tipo de arquitetura, tanto o tráfego de sinalização como os dados do usuário passam pela CN GPRS/UMTS.

As principais características deste tipo de arquitetura são o reuso dos serviços de infra-estrutura já existentes no CN GPRS/UMTS, como, por exemplo, mobilidade, Qualidade de Serviço, segurança, sistema de *billing*, database de usuários, acesso aos serviços e recursos básicos da CN GPRS/UMTS e ainda um serviço comum de *Customer Care* para os acessos GPRS/UMTS e WLAN.

A Figura 6.1 ilustra a arquitetura deste tipo de acoplamento [Salkintzis].

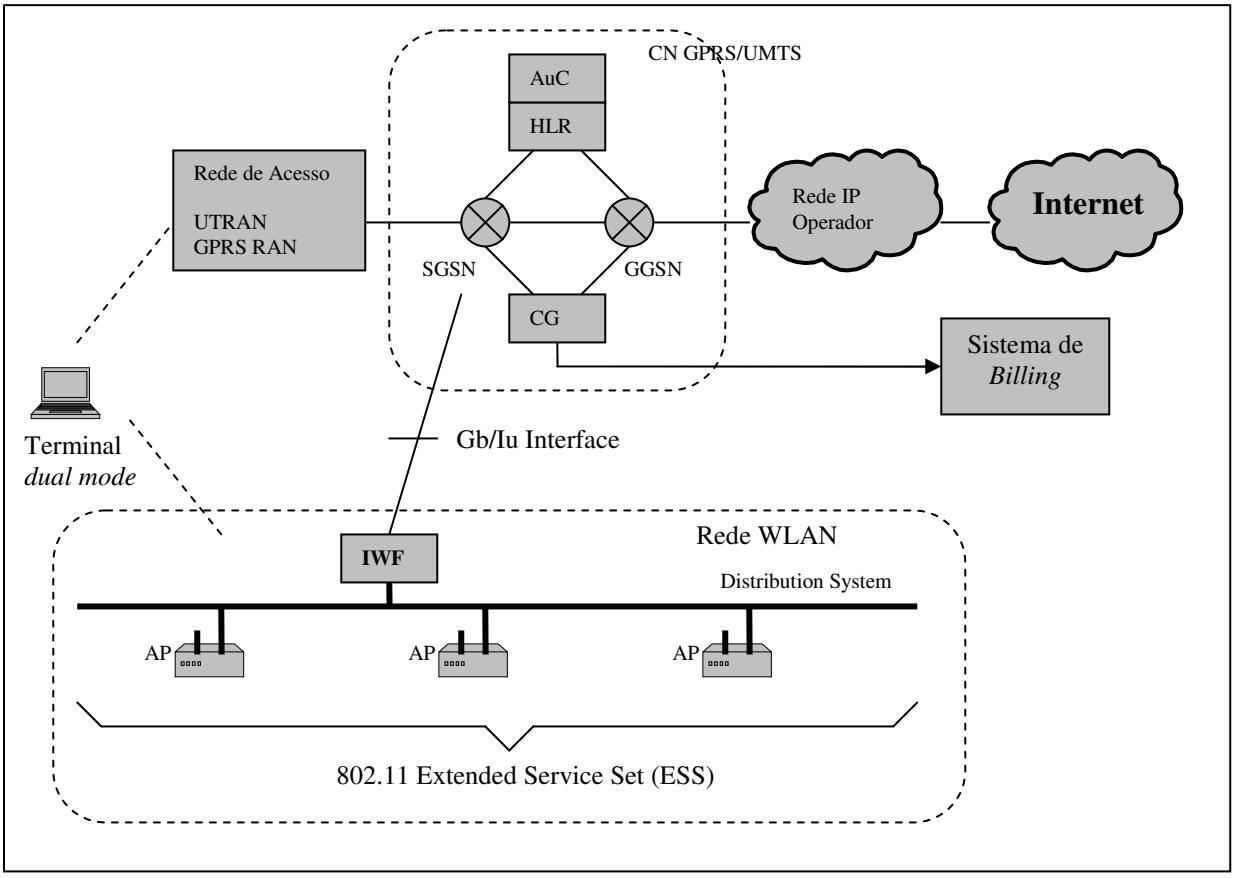


Figura 6.1. Integração entre a CN GPRS/UMTS e WLAN na arquitetura *tight coupling*.

A rede WLAN é constituída por um ou mais APs 802.11 conectados através de um *Distribution System* (DS), o qual, neste tipo de sistema, é tipicamente uma LAN padrão IEEE 802.3 (Ethernet). A rede WLAN utiliza a configuração de infra-estrutura, onde os APs têm a funcionalidade de uma BTS. A área coberta por um único AP é conhecida como *Basic Service Set* (BSS) e o conjunto de vários BSS forma a configuração *Extended Service Set* (ESS) [802.11].

Neste tipo de acoplamento, a rede WLAN funciona como uma rede de acesso RAN (*Radio Access Network*) alternativa e se conecta ao CN GPRS/UMTS através da interface GPRS Gb (entre a BSC e o SGSN) ou da interface UMTS Iu (entre a RNC e o SGSN), como ilustra a Figura 6.2.

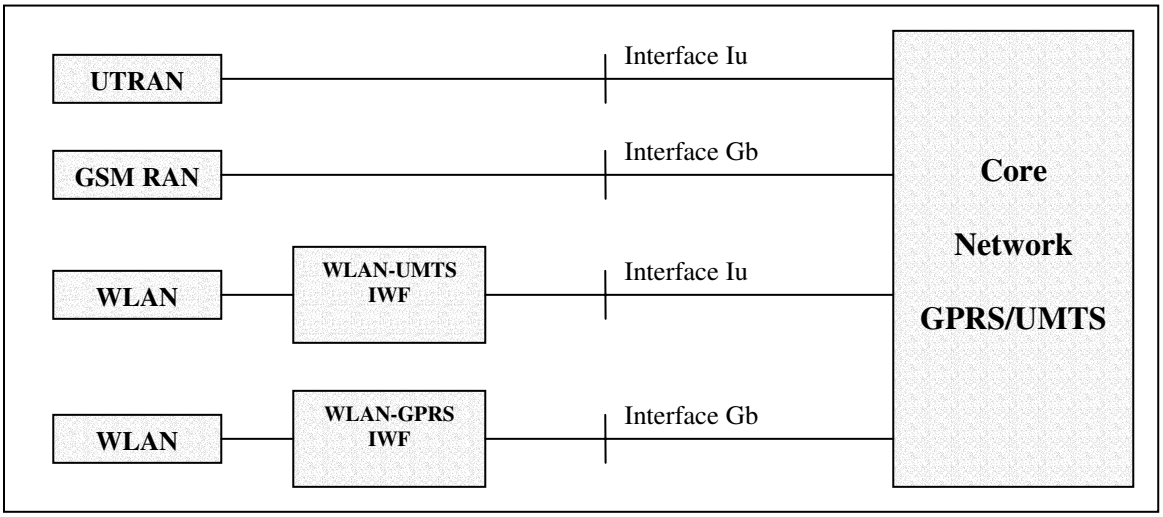


Figura 6.2. Diferentes redes de acesso na arquitetura *tight coupling*.

Do ponto de vista do CN GPRS/UMTS a rede WLAN é considerada como qualquer outra rede de acesso, ou seja, o CN GPRS/UMTS não consegue identificar diferenças entre o acesso feito por uma rede WLAN ou por uma rede com tecnologia GPRS/UMTS. Isto é conseguido através de um novo elemento de rede, o *Inter Working Function* (IWF), necessário dentro da arquitetura *tight coupling*.

O IWF é responsável pela conexão da rede WLAN ao CN GPRS/UMTS. Ele conecta o *Distribution System* da rede WLAN ao SGSN através da interface GPRS Gb ou da interface UMTS Iu. Este novo elemento é necessário para que o SGSN considere a rede WLAN como sendo uma outra rede de acesso GPRS RAN ou UTRAN. Sua principal função é prover uma

interface padrão entre as redes WLAN e o CN GPRS, escondendo assim as características específicas das redes WLAN.

Do lado do terminal, os protocolos de camadas superiores do GPRS e UMTS são utilizados também quando o terminal está operando dentro de uma WLAN. A arquitetura de um terminal para este tipo de acoplamento, suportando as interfaces GPRS, UMTS e WLAN, é ilustrada na Figura 6.3.

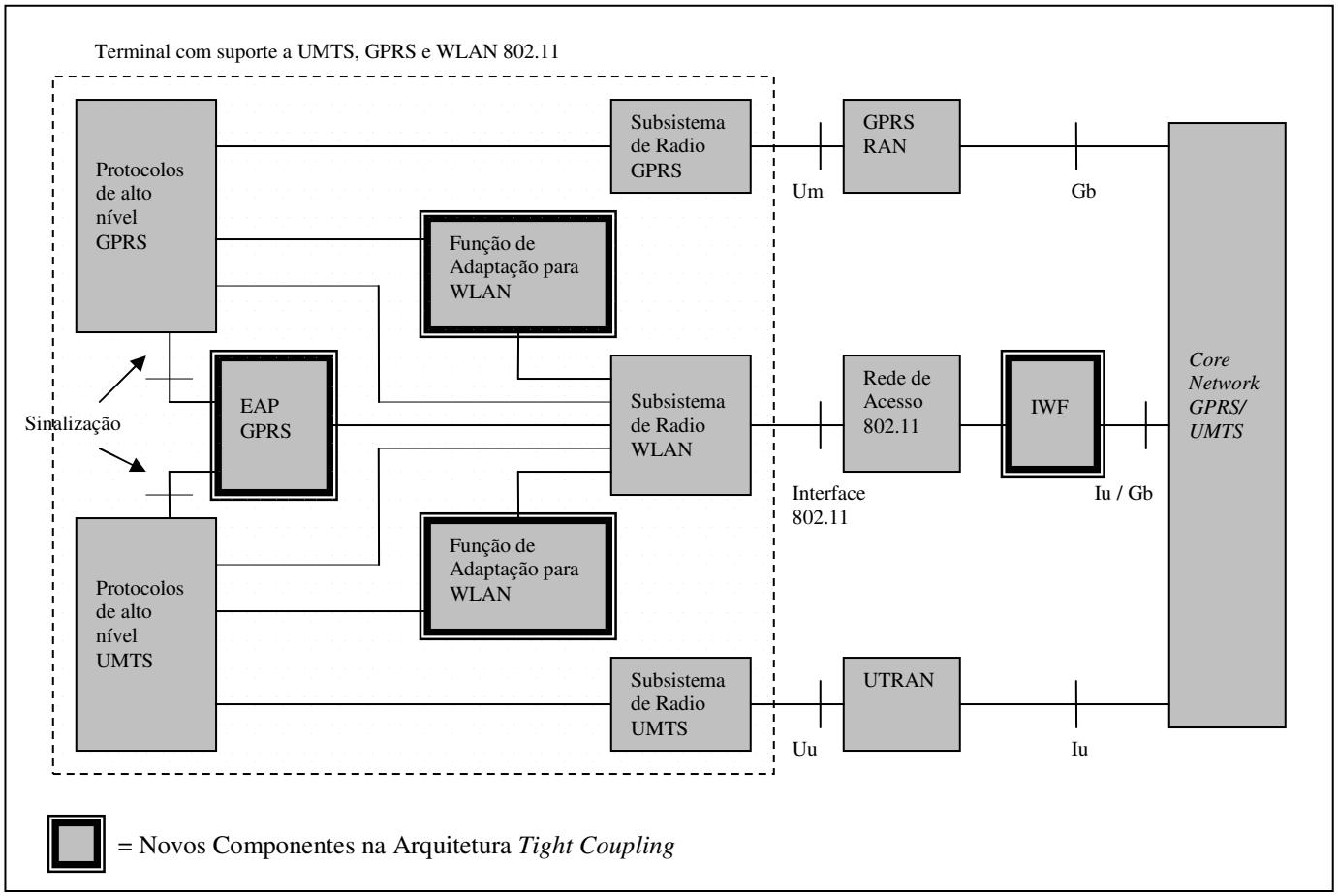


Figura 6.3. Arquitetura de um terminal no acoplamento *tight coupling*.

Novos componentes são definidos para o acoplamento *tight coupling*:

- EAP GPRS

  Este protocolo é uma extensão do EAP e é responsável pelo transporte de sinalização GPRS do terminal para a CN GPRS e vice-versa.

- Módulo *Inter-Working Function* (IWF)

A função principal do IWF é prover uma interface padrão entre as redes WLAN e o CN GPRS. Funciona como uma *bridge* entre os protocolos da interface Gb ou interface Iu com os protocolos do DS da WLAN, como, por exemplo, o 802.3 (Ethernet).

- Função de Adaptação para WLAN

  Este módulo é responsável para suportar funções de interconexão entre o terminal e o IWF.

## 6.1. Pilha de Protocolos no Terminal

Do lado do terminal, os protocolos de nível superior do GPRS e UMTS são reutilizados. O objetivo principal é fazer com que a WLAN simplesmente forneça um outro meio de transporte para estes protocolos.

No caso do GPRS, os protocolos LLC (*Logical Link Control*), SNDCP (*SubNetwork Dependent Convergence Protocol*) e os protocolos de gerenciamento de mobilidade GMM (*GPRS Mobility Management*) e de sessão SM (*Session Management*) são utilizados para o acesso tanto em GPRS como em WLAN, como ilustra a Figura 6.4.

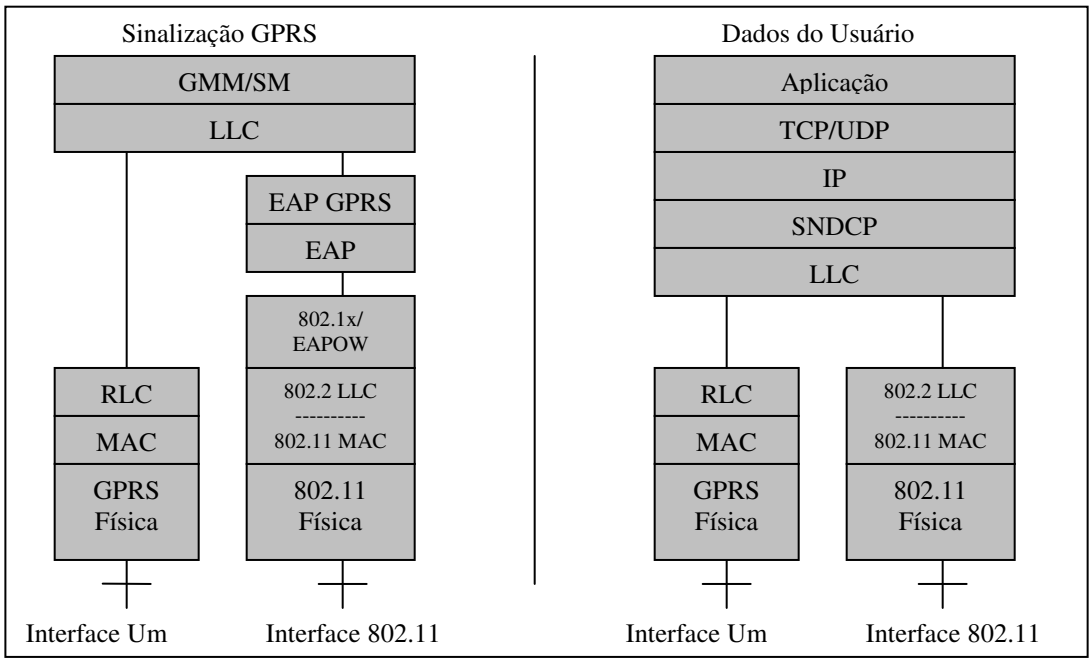


Figura 6.4. Pilha de Protocolos no terminal GPRS para a arquitetura *tight coupling*.

Do mesmo jeito, no caso do UMTS, os protocolos RRC (*Radio Resource Control*), PDCP (*Packet Data Convergence Protocol*) e os protocolos GMM e SM também são utilizados em ambos os acessos, WLAN e UMTS, como ilustra a Figura 6.5.

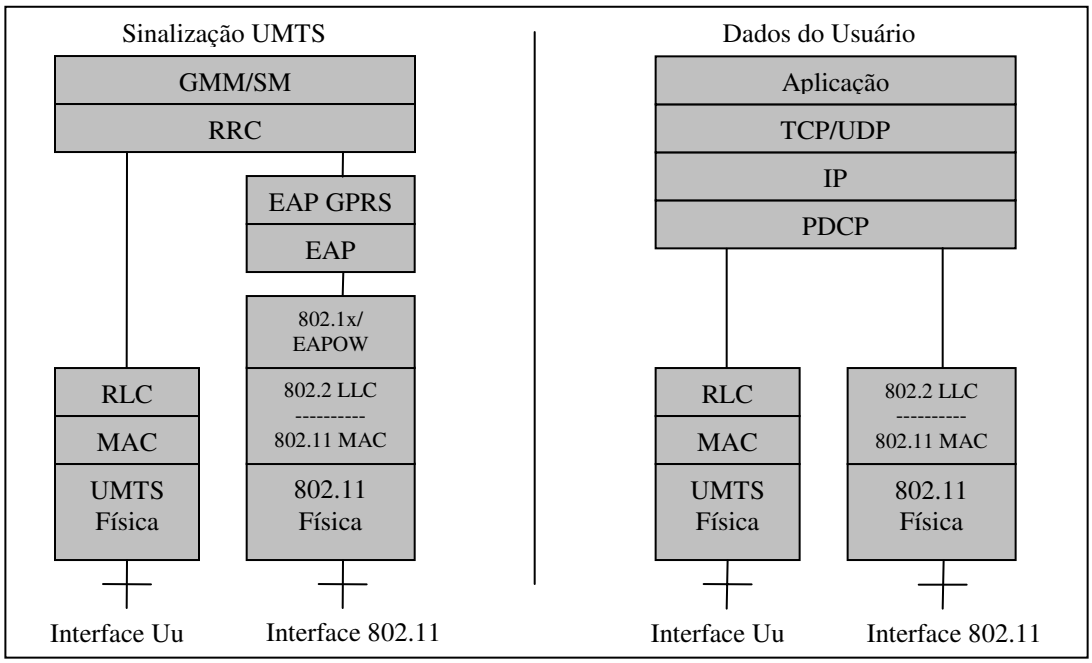


Figura 6.5. Pilha de Protocolos no terminal UMTS para a arquitetura *tight coupling*.

Pelas figuras acima se observa que a WLAN provê um outro meio de transporte para os protocolos das camadas superiores do GPRS e UMTS. No entanto, alterações ou extensões destes protocolos são necessárias para suporte das interfaces da WLAN 802.11.

A mobilidade entre as diferentes tecnologias é obtida através de procedimentos de atualização de RAN (*Radio Access Network*). Os terminais devem possuir cartões com funções de acesso a mais de uma tecnologia, por exemplo, GSM/GPRS, UMTS e 802.11. A interface WLAN do terminal deve regularmente fazer o *scan* dentro da sua faixa de freqüência procurando por um AP válido. O AP periodicamente faz o broadcast de um sinal chamado *beacon*, o qual contém informações como SSID do AP, intervalo de *beacon*, *time stamp* e as características do AP [Pahlavan]. O terminal utiliza as informações do sinal de *beacon* para detectar a presença da WLAN e se associar ao AP.

Quando o terminal entra em uma área de cobertura de WLAN, o processo de atualização de RAN verifica a presença da WLAN através da presença de sinais *beacon* e tenta

se associar ao AP. Após a associação, o terminal executa os procedimento de autenticação e controle de acesso, através do EAP GPRS, para acesso os serviços da rede WLAN. Do mesmo modo, quando o terminal deixa a área de cobertura da WLAN, o processo de atualização de RAN verifica a ausência da WLAN e inicia o processo de autenticação e sinalização para a rede GPRS/UMTS.

## 6.2. A Função "Inter-Working"

O *Inter-Working Function* (IWF) tem um papel fundamental na arquitetura *tight coupling*. Do lado da WLAN, o IWF é conectado ao *Distribution System* (DS) da WLAN e do lado do CN GPRS/UMTS ele é conectado ao SGSN. Ele é responsável por fornecer uma interface Gb, para terminais GPRS, ou uma interface Iu, para terminais UMTS. O IWF é o elemento de rede que faz com que o SGSN considere a WLAN como sendo uma GPRS *Routing Area* (RA) dentro do sistema, ou seja, o IWF é responsável para que o CN GPRS/UMTS não consiga diferenciar uma RA com acesso WLAN de outra RA com acesso GPRS ou UMTS. Uma RA é uma região onde o terminal pode se mover sem atualizar o SGSN [3GPP 23.002]. Neste sentido, o IWF atua como uma "*bridge"* entre os protocolos do padrão 802.3 (Ethernet) e os protocolos do GPRS (interface Gb) ou do UMTS (interface Iu).

Como já foi mencionado, o IWF é conectado ao DS da WLAN e ao SGSN. O DS é tipicamente uma LAN na qual os dispositivos conectados a ela se comunicam através de endereços da camada MAC. Os terminais que estão atachados na WLAN através dos APs também utilizam os seus endereços MAC para se comunicarem através do DS. Ou seja, o IWF e os terminais estão na mesma LAN. Assim, o tráfego GPRS/UMTS do terminal para o SGSN é enviado para o endereço MAC do IWF. Da mesma maneira, quando o IWF recebe tráfego GPRS/UMTS do SGSN ele deve enviá-lo para o endereço MAC do terminal. Portanto, o IWF é responsável pela manutenção de uma tabela de mapeamento entre endereços MAC dos terminais na WLAN e a identificação do terminal GPRS/UMTS pelo SGSN.

## 6.3. A Função de Adaptação para WLAN

A Função de Adaptação para WLAN é implementada no terminal e tem a finalidade de notificar os protocolos de nível superior do GPRS e UMTS da presença da WLAN e ainda executar o procedimento de descoberta e armazenamento do endereço MAC do IWF e da identificação da WLAN como *Routing Area*, o chamado *Routing Area Identity* (RAI).

O processo de descoberta do endereço MAC do IWF e da identificação da WLAN deve ser suportado pelo IWF, conforme ilustra a Figura 6.6 [Salkintzis].

O endereço MAC do IWF é utilizado como endereço de destino das PDUs da camada MAC do 802.11, carregando sinalização GPRS/UMTS ou dados do usuário com destino ao SGSN.

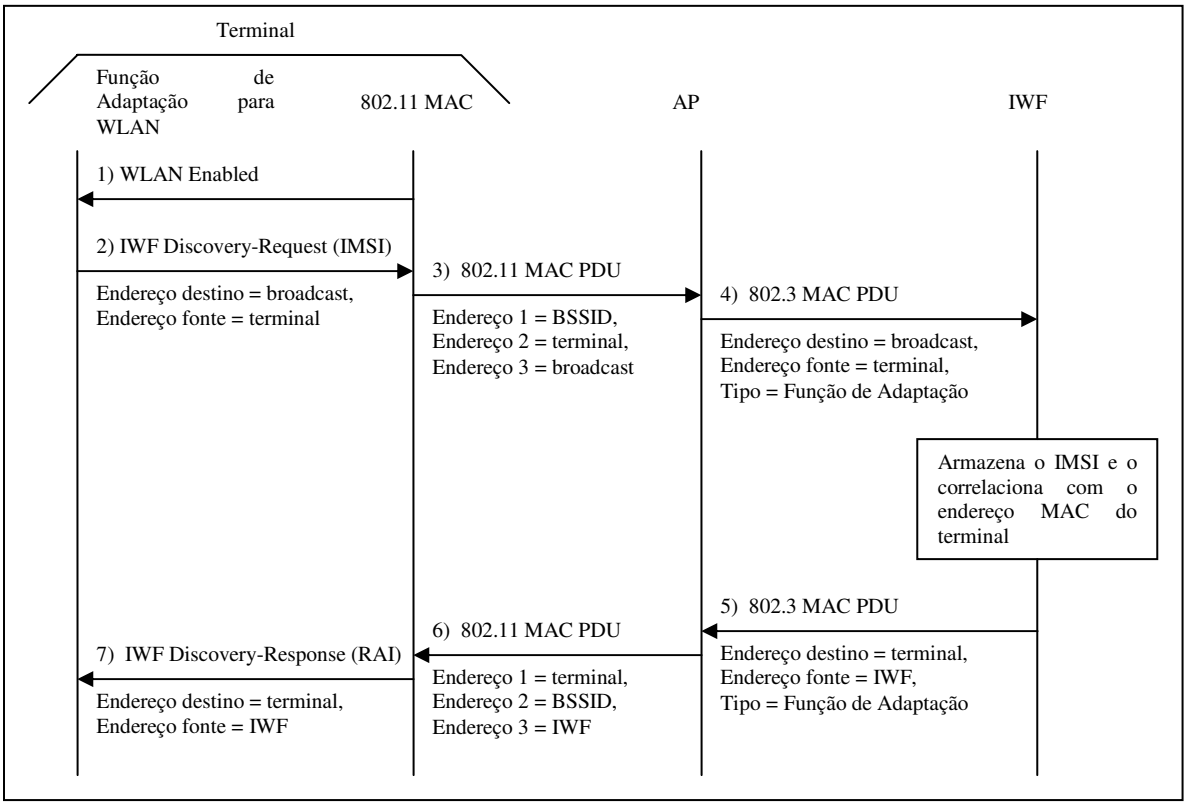


Figura 6.6. Procedimento de descoberta do endereço MAC do IWF pelos terminais.

O procedimento de descoberta do endereço MAC do IWF e do RAI da WLAN é descrito a seguir:

1. O procedimento inicia-se após a associação entre o terminal e o AP, quando a camada 802.11 MAC é habilitada. A camada MAC do 802.11 envia uma mensagem para a Função de Adaptação para WLAN notificando a presença de uma WLAN;
2. A Função de Adaptação para WLAN envia uma mensagem *IWF Discovery-Request* para a camada MAC 802.11 para que esta transmita uma PDU com o endereço destino igual a *broadcast* e endereço fonte igual ao MAC do terminal;

   A mensagem *IWF Discovery-Request* carrega a informação de identificação do terminal (IMSI);
3. A camada MAC envia então uma PDU para o AP com as seguintes informações de endereço:
   - Endereço 1: o BSSID
   - Endereço 2: o endereço MAC do terminal
   - Endereço 3: o endereço de *broadcast*
4. O AP faz o *broadcast* desta mensagem para o DS. A PDU enviada pelo AP tem o campo tipo no cabeçalho 802.3 preenchido com um novo valor, específico para este tipo de contexto: "Função de Adaptação para WLAN";

   O IWF, ao receber este tipo de PDU, sabe que é uma mensagem de um terminal que quer se registrar. O IWF armazena o endereço MAC do terminal e o associa com o IMSI recebido;
5. O IWF então responde com uma PDU que contém o seu endereço MAC como fonte. A PDU enviada pelo AP tem o tipo preenchido como "Função de Adaptação" e contém a informação do RAI da WLAN;
6. O AP envia esta PDU para o terminal apropriado, de acordo com o endereço destino que recebeu;
7. A camada MAC do 802.11 envia uma mensagem *IWF Discovery-Response* para a Função de Adaptação para WLAN no terminal contendo o RAI da WLAN. O endereço MAC do IWF é obtido do endereço fonte da PDU.

Após este procedimento, o terminal conhece o endereço MAC do IWF e o RAI da WLAN. O IWF, por sua vez, guarda o endereço MAC do terminal associado com o IMSI.

## 6.4. O Protocolo EAP GPRS

O acesso da rede WLAN ao CN GPRS/UMTS é obtido através do protocolo EAP GPRS [EAP GPRS], o qual permite que terminais GPRS/UMTS em de uma WLAN executem procedimentos de sinalização com a rede CN GPRS/UMTS através de equipamentos que utilizam controle de acesso baseado no protocolo EAP, como, por exemplo, um AP baseado no 802.1x [802.1x]. Até a data de publicação deste trabalho, o EAP GPRS estava em fase de desenvolvimento pelo IETF, ou seja, é uma especificação *Internet-draft*.

O EAP GPRS não é um novo método de autenticação, mas sim um novo mecanismo de transporte de sinalização para protocolos de alto nível tanto do GPRS como do UMTS, os quais são referenciados como *User Applications* (UA). Neste sentido, a autenticação é feita pelos protocolos de alto nível, as UAs, enquanto que o EAP GPRS somente provê o mecanismo de transporte para estes protocolos.

O EAP GPRS não provê serviços de detecção e correção de erros, controle de fluxo, retransmissão, sequenciamento, etc. Estes procedimentos, se necessário, devem ser tratados pelos protocolos que utilizam o EAP GPRS, ou seja, as UAs.

A arquitetura de protocolos do EAP GPRS é ilustrada na Figura 6.7 [EAP GPRS].

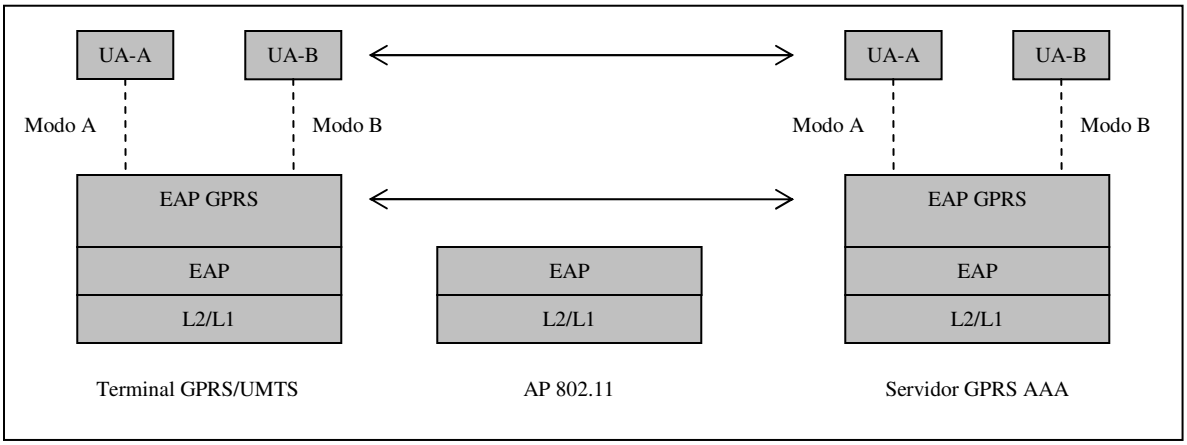


Figura 6.7. Arquitetura de Protocolos do EAP GPRS.

Neste tipo de arquitetura, o AP segue o padrão 802.11, com suporte ao padrão de segurança 802.1x. O AP não requer nenhuma funcionalidade específica de tecnologia celular GSM, GPRS ou UMTS.

Do lado da CN GPRS é exigido um servidor GPRS de AAA. Este é o servidor onde o protocolo EAP GPRS termina e provê a autenticação e controle de acesso para o terminal GPRS/UMTS em uma WLAN. Esta funcionalidade, na CN GPRS/UMTS, pode ser implementada juntamente com o SGSN, ou ainda em outro elemento específico para esta funcionalidade.

O EAP GPRS pode operar em vários modos, o que, na prática, significa que ele pode suportar vários protocolos de alto nível (UAs). Como exemplos de UAs pode-se citar os protocolos LLC [3GPP 04.64] e RRC [3GPP 25.331], os quais são utilizados como serviço de transporte para as mensagens GMM de terminais GPRS e UMTS utilizando as interfaces Gb e Iu, respectivamente. O uso dos protocolos LLC e RRC junto ao EAP GPPR pode trazer modificações ou mesmo extensões, mas estas alterações não estão no escopo do EAP GPRS.

Para acessar os serviços da CN GPRS através de uma WLAN, o terminal GPRS/UMTS precisa ter liberação de acesso tanto do AP como também da CN GPRS. Com o uso do EAP GPRS as mensagens dos procedimentos de mobilidade do GPRS/UMTS (GMM) são transportadas através do contexto do procedimento 802.1x. Este mecanismo faz a correlação entre os dois mecanismos de segurança, no qual o acesso do terminal ao AP só terá sucesso se o procedimento de mobilidade GMM também tiver sucesso. Isto significa que quando um terminal GPRS ou UMTS tentar acessar a rede WLAN (seja no processo de ligar o terminal ou durante um processo de *handoff*) ocorre a troca de sinalização de autenticação entre o terminal e o SGSN, as quais são encapsuladas dentro do EAP GPRS, e o AP só tem acesso liberado se este processo finalizar com sucesso, ou seja, o terminal ganha acesso na rede WLAN somente se for aceito na rede GPRS. Se o processo de autenticação na rede GPRS falhar, o AP não tem acesso liberado e o terminal não consegue acesso na WLAN. Do mesmo modo que nas outras extensões do EAP, o AP, que neste caso é o autenticador, não também precisa saber qual o tipo de autenticação esta sendo realizada. Sua função é somente verificar o resultado final da autenticação.

Um cenário típico do uso do EAP GPRS é o caso quando um terminal é ligado e percebe a presença de uma WLAN. Este procedimento é ilustrado na Figura 6.8.

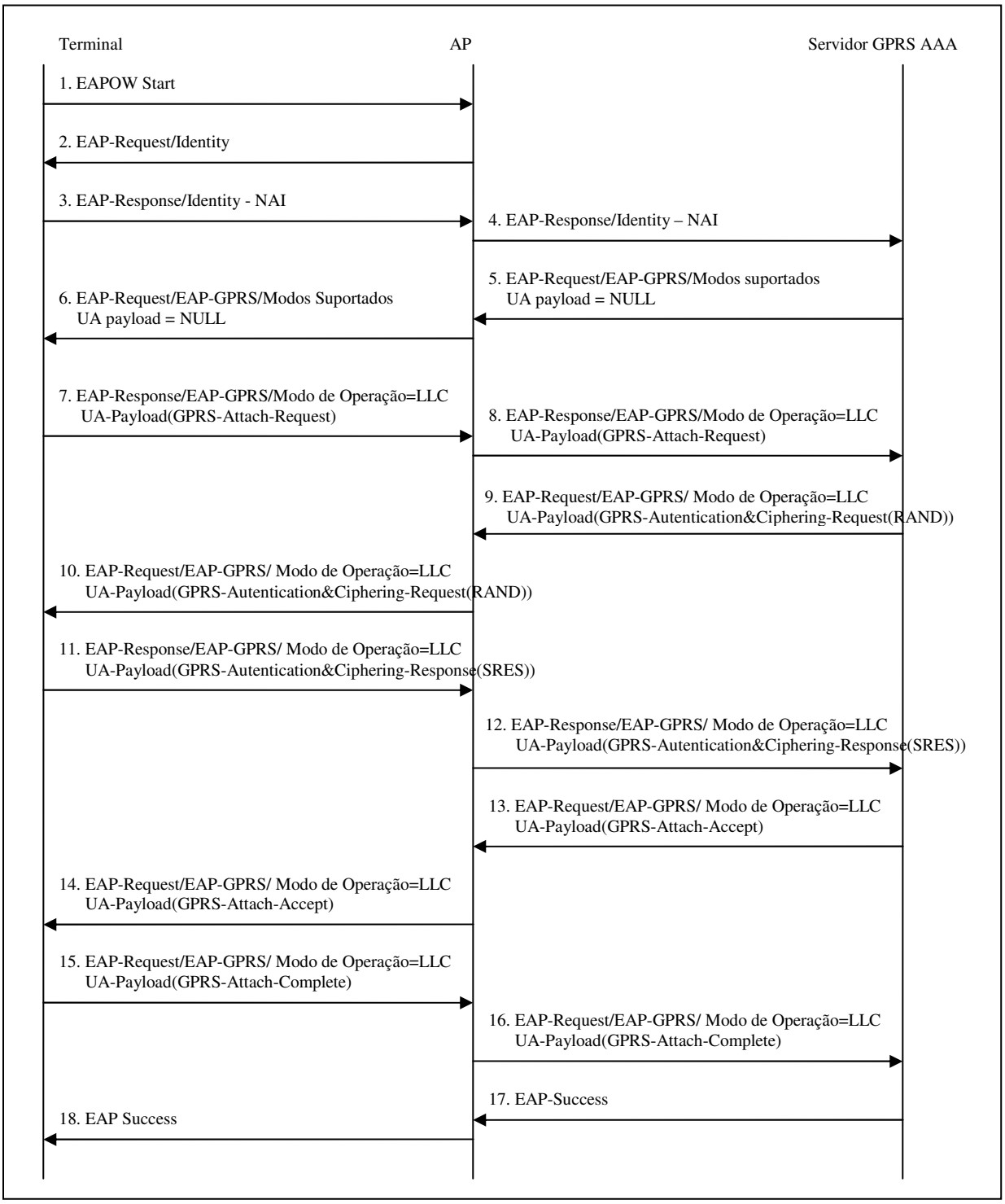


Figura 6.8. Terminal GPRS conectando na rede WLAN via EAP GPRS.

Os passos neste tipo de autenticação são descritos a seguir:

1. O processo de autenticação começa logo após a associação entre o terminal e o AP. O terminal envia uma mensagem *EAPOW-Start* [802.1x] para o AP, que inicia o processo de autenticação 802.1x;
2. O AP envia uma mensagem *EAP-Request/Identity* [RFC2284] para o terminal, requisitando a sua identidade;
3. O terminal envia uma mensagem *EAP-Response/Identity* [RFC2284] contendo sua identidade no formato NAI [RFC2486], no formato *nome.do.usuario@dominio.com*. Entretanto, como o EAP GPRS não faz autenticação de usuário (esta responsabilidade é dada aos protocolos de nível superior, as UAs), o EAP GPRS não precisa saber da identidade do cliente GPRS. Assim a identificação do usuário no NAI ("*nome.do.usuário*") pode ser um nome aleatório qualquer.

   A identidade real do terminal será transmitida durante a troca de sinalização entre os protocolos superiores que utilizarão o EAP GPRS como meio de transporte.

   O domínio do NAI ("*domínio.com*") é utilizado para efeitos de *roaming* e deve ser um domínio válido, contento as informações de *Mobile Country Code* (MCC) e *Mobile Network Code* (MNC), como ocorre nos métodos de autenticação EAP SIM e EAP AKA;
4. Baseado no domínio do NAI recebido, a requisição é enviada para o servidor GPRS AAA apropriado;
5. O servidor GPRS AAA, inicia então a transação EAP GPRS enviando uma mensagem *EAP-Request/EAP-GPRS* [EAP GPRS] de inicialização contento os protocolos de nível superior (as UAs) que são suportados por ele, por exemplo, o LLC (interface Gb) e RRC (interface Iu).

   Não há mensagem de UA sendo enviada como *payload* nesta mensagem de inicialização. Ela é utilizada para notificar o terminal de que uma transação EAP GPRS está se iniciando e quais as interfaces são suportados pelo servidor GPRS AAA;
6. O AP repassa a mensagem *EAP-Request/EAP-GPRS* [EAP GPRS] para o terminal;
7. Ao receber a mensagem de inicialização do EAP GPRS, o terminal envia uma mensagem *EAP-Response/EAP-GPRS* [EAP GPRS] contendo o modo selecionado (neste exemplo foi escolhido o protocolo LLC) e inclui um frame LLC, contendo a mensagem *GPRS-Attach-Request* [3GPP 24.008], como *payload* de UA nesta

mensagem de resposta. A mensagem *GPRS-Attach-Request* inclui a identificação do usuário;

8. O AP repassa a mensagem *EAP-Response/EAP-GPRS* [EAP GPRS] para o servidor GPRS AAA;
9. Ao receber a mensagem *GPRS-Attach-Request*, o servidor GPRS AAA decide autenticar o terminal GPRS e então transmite a mensagem EAP-*Request/EAP-GPRS* [EAP GPRS] contento uma mensagem *GPRS-Autentication&Ciphering-Request* [3GPP 24.008] como *payload* de UA.

   Neste momento, o servidor verifica se o terminal é um cliente GSM ou UMTS e decide pelo método de autenticação. Se o cliente for GSM, como no exemplo, a mensagem *GPRS-Autentication&Ciphering-Request* contém o número aleatório RAND. No caso da autenticação UMTS esta mensagem tem um atributo adicional (RAND e AUTN);
10. O AP repassa a mensagem *EAP-Request/EAP-GPRS* [EAP GPRS] para o terminal;
11. O terminal quando recebe a mensagem *GPRS-Autentication&Ciphering-Request* executa o algoritmo de autenticação do GSM e gera o número SRES (*Signature Response*). O terminal envia então uma mensagem *EAP-Response/EAP-GPRS* [EAP GPRS] contendo a mensagem *GPRS-Autentication&Ciphering-Response* [3GPP 24.008], a qual recebe o valor de SRES como parâmetro de retorno para verificação da rede.

    Se a autenticação fosse UMTS, a função teria como parâmetro o valor de RES;
12. O AP repassa a mensagem *EAP-Response/EAP-GPRS* [EAP GPRS] para o servidor GPRS AAA;
13. Baseado no valor de SRES, o servidor GPRS AAA verifica se o terminal é um cliente GPRS válido e envia então uma mensagem *EAP-Request/EAP-GPRS* [EAP GPRS] contendo uma mensagem *GPRS-Attach-Accept* [3GPP 24.008] encapsulada como *payload* de UA.

    A mensagem *GPRS-Attach-Accept* é enviada para o terminal indicando que a requisição de conexão foi aceita. Esta mensagem pode incluir uma nova identificação temporária para o terminal;
14. O AP repassa a mensagem *EAP-Request/EAP-GPRS* [EAP GPRS] para o terminal;

15. O terminal quando recebe a mensagem *GPRS-Attach-Accept* envia uma mensagem de reconhecimento da nova identificação temporária recebido para o servidor GPRS AAA através de uma mensagem *EAP-Response/EAP-GPRS* [EAP GPRS] contendo a mensagem *GPRS-Attach-Complete* [3GPP 24.008] encapsulada como *payload* de UA. A mensagem *GPRS-Attach-Complete* é enviada para a rede quando uma nova identificação foi designada para o terminal dentro da mensagem GPRS-Attach-Accept;
16. O AP repassa a mensagem *EAP-Response/EAP-GPRS* [EAP GPRS] para o servidor GPRS AAA;
17. O servidor recebe a mensagem *GPRS-Attach-Complete* e envia a mensagem *EAP-Success* [RFC2284] para o terminal;
18. O AP repassa a mensagem *EAP-Success* [RFC2284] para o terminal.

## 6.5. O Plano de Controle de Sinalização e Dados de Usuário

O plano de controle de transmissão de sinalização para autenticação e controle de acesso, considerando um terminal GPRS com a interface Gb, é ilustrado na Figura 6.9.

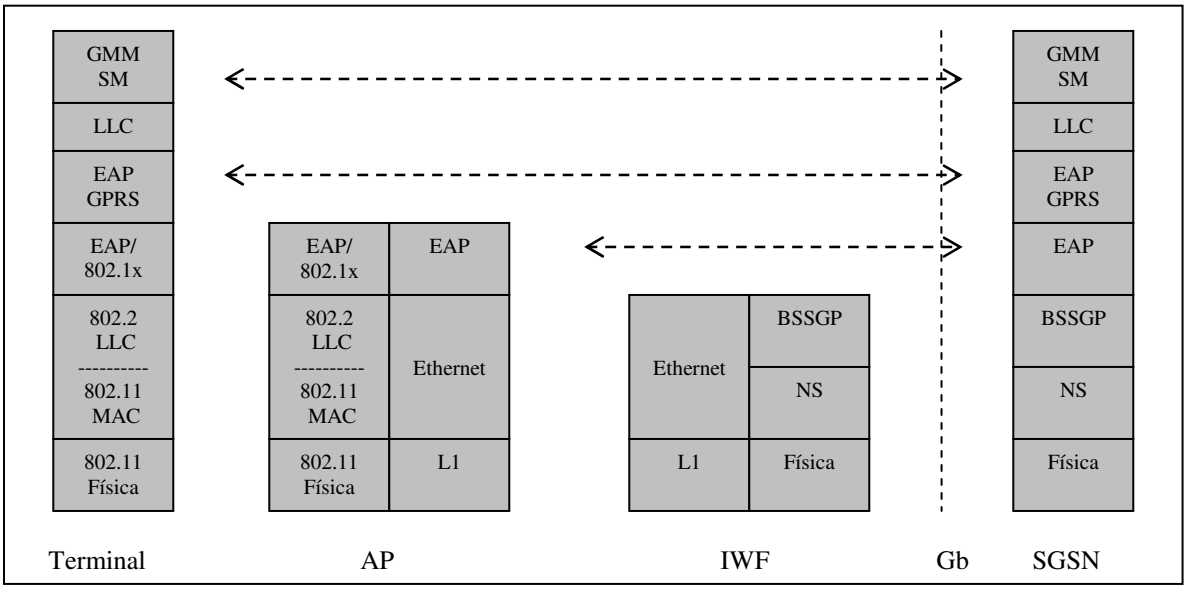


Figura 6.9. Plano de controle de sinalização de um terminal GPRS em uma WLAN via EAP GPRS.

Pode-se observar na Figura 6.9 que o EAP GPRS somente encapsula mensagens do protocolo LLC para transporte. A autenticação do terminal é concluída pelo protocolo GMM no terminal e SGSN.

Se o resultado da autenticação do terminal foi bem sucedido, o AP libera o acesso na WLAN e, conseqüentemente, o usuário passa então ter acesso à rede. Ao contrário do que acontece no acoplamento *loose coupling*, todo o tráfego de dados do usuário passa agora por toda a CN GPRS.

O plano de controle de dados do usuário é ilustrado na Figura 6.10, considerando também um terminal GPRS com a interface Gb.

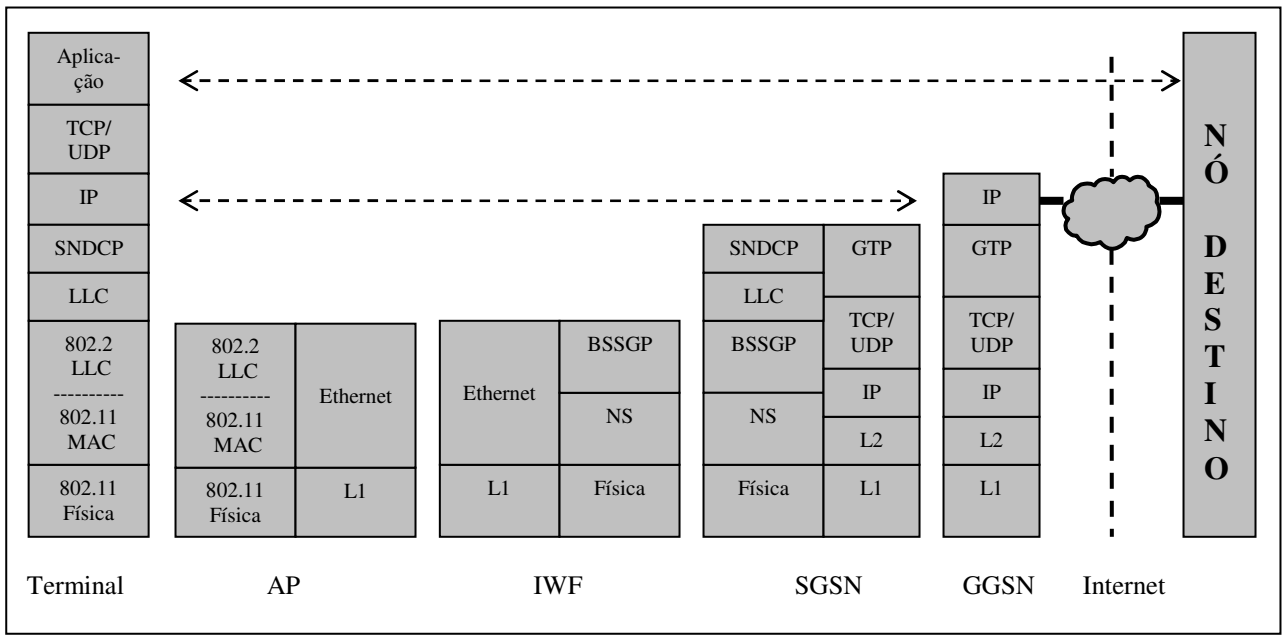


Figura 6.10. Plano de controle do usuário do usuário com um terminal GPRS.

A Figura 6.10 ilustra que todo o tráfego de dados do usuário passa pelo SGSN e GGSN, que são elementos internos da CN GPRS. O roteamento IP para a Internet é feito no GGSN.

# 7. Conclusões

Como visto anteriormente, a arquitetura *tight coupling* conecta a WLAN diretamente no SGSN utilizando as interfaces Gb ou Iu através do IWF. Ela provê um acoplamento mais firme entre a WLAN e o CN GPRS no qual os usuários utilizam toda a infra-estrutura do CN GPRS/UMTS para acesso à Internet. Já a arquitetura *loose coupling* apresenta um acoplamento mais leve entre o CN GPRS/UMTS e a WLAN, onde o usuário não necessita da infra-estrutura da CN GPRS/UMTS para o acesso à Internet.

Neste capítulo compara-se estes dois tipos de arquitetura sob diversos aspectos, apontando-se vantagens e desvantagens de cada um deles. É interessante comentar a evolução das WLAN e como esta evolução influencia o comportamento das WLANs e o acoplamento com as redes celulares.

## *7.1. A Evolução da WLAN IEEE 802.11*

Um ponto importante descrito neste trabalho é a evolução da tecnologia das redes sem fio a partir do padrão 802.11. Inicialmente o padrão 802.11 fornecia um conjunto básico de normas para prover conectividade de uma estação à uma LAN ou para um agrupamento de estações poder se comunicar no modo *ad-hoc*.

Este conjunto básico mostrou-se insuficiente para o uso da WLAN dentro de corporações e escritórios, principalmente devido à falhas de segurança. Estas limitações levaram ao surgimento de novos suplementos, padrões e extensões dentro do IEEE 802.11 [802.11_Family]. Muitos ainda em fase de desenvolvimento, mas já prometem melhorias para o uso empresarial. Pode-se destacar como grande melhoria a segurança, com os padrões 802.11i e 802.1x, os quais definem autenticação e controle de acesso mais robustos e seguros.

Com o surgimento do 802.1x, o AP passa a ser um dos elementos responsáveis pelo controle de acesso suportando o EAP e também atuando como um cliente RADIUS, como no caso da arquitetura *loose coupling*.

Portanto, com os novos padrões de segurança, o AP deixa de ser uma simples "*bridge*" entre a interface de rádio, o 802.11, e uma outra interface como, por exemplo, a Ethernet (802.3). Ele ganha novas atribuições como autenticador do 802.1x. Estas novas atribuições e funcionalidades do AP, juntamente com novos métodos de autenticação, como o EAP-SIM,

EAP-AKA e EAP-GPRS, são utilizados para integração das WLANs com os sistemas celulares, e permitem o controle de acesso dos usuários com cartões SIM/USIM junto aos bancos de dados de usuários dos operadores de redes celulares (HLR).

## 7.2. Wireless Switch como Elemento Centralizador

Outro ponto a considerar na evolução das WLANs é o surgimento do *Wireless Switch*, o qual se caracteriza pela centralização das funções da MAC. Este novo conceito traz uma nova arquitetura onde o gerenciamento, a configuração, o controle de potência dos *Access Points*, a autenticação e o controle de acesso na rede passam a serem centralizados em um único elemento e com certeza influenciam na implementação, manutenção e gerenciamento de um *hotspot*.

Além destes fatores, pode-se citar uma outra característica importante desta arquitetura para o caso específico dos *hotspots*: a segurança física do *Access Port*. O *hotspot* é uma área pública onde, na maioria dos casos, não existem restrições de acesso para as pessoas. É o caso, por exemplo, de aeroportos onde as pessoas circulam livremente e com certeza tem acesso físico aos pontos de acesso das WLAN. O uso do *Access Points* neste caso pode comprometer a segurança da rede, visto que o *Access Point* pode conter informações de configurações de roteadores e servidores de controle de acesso e autenticação da rede (802.1x).

Neste caso, o uso de *Access Ports*, utilizado pela arquitetura da *Wireless Switch*, mostra-se mais adequado, pois todas as informações de controle de acesso e autenticação da rede (802.1x) estão presentes na *Wireless Switch*. O *Access Port* atua simplesmente como uma *bridge* entre a camada física de RF da WLAN para uma outra camada física e não representa mais um perigo em caso de roubo. A *Wireless Switch*, por sua vez, pode ficar em uma sala com acesso restrito, evitando assim o acesso de pessoas não autorizadas às informações de segurança da rede.

Outro fato interessante é o uso de *Power over Ethernet* (PoE) dentro da arquitetura *Wireless Switch*. Esta característica facilita a instalação do *Access Port* dispensando a necessidade do uso de cabos de energia elétrica.

Podemos citar ainda como vantagem desta arquitetura a existência de soluções com MAC centralizado com desempenho superior ao sistema com MAC distribuído [Corrêa].

Portanto, a arquitetura de WLAN com *Wireless Switch*, além de ser recomendada para *hotspots* com grande número de APs, facilitando o gerenciamento, manutenção e instalação, é também recomendada como um elemento adicional de segurança para lugares públicos, como aeroportos, universidades e hospitais.

## 7.3. Comparação entre os acoplamentos Tight e Loose Coupling

A arquitetura *tight coupling* faz a conexão da WLAN diretamente ao SGSN e tem como principal vantagem o fato de reutilizar os mecanismos de autenticação, segurança e mobilidade fornecidos pela rede GPRS. Sendo assim a rede WLAN precisa entender as operações GPRS de modo que possa executar as atividades que são requisitadas pela rede GPRS, como se fosse qualquer outra rede de acesso GPRS. Por este motivo, a presença do IWF é necessária como o elemento que faz a *bridge* entre os protocolos do GPRS e os protocolos da WLAN. Este elemento deve prover diferentes interfaces com a CN GPRS quando o terminal for GPRS (interface Gb) ou UMTS (interface Iu).

Já a arquitetura *loose coupling*, faz a integração entre a WLAN e a rede celular através de um servidor AAA baseado nos protocolos do IETF e utiliza a Internet ou uma linha dedicada entre o *hotspot* e a rede do operador para transporte de sinalização de controle e dados de usuário. Neste tipo de arquitetura, a WLAN não precisa conhecer os protocolos GPRS ou UMTS e por isso as modificações dentro das WLANs são menores.

### 7.3.1. Servidor de Autenticação

Dentro da CN GPRS, a arquitetura *tight coupling* exige um servidor AAA GPRS, responsável pela autenticação do terminal, ou seja, é o ponto na CN GPRS onde o protocolo EAP-GPRS termina. Este servidor pode ser implementado como um elemento separado, o que exige da operadora um outro nó dentro da rede que suporte os protocolos de gerenciamento de mobilidade e controle de acesso do GPRS/UMTS (GMM/SM). Outra solução é a presença da funcionalidade do servidor AAA GPRS no SGSN, o qual já é o responsável pela autorização, controle de acesso e mobilidade dos terminais na rede GPRS. De qualquer maneira, o EAP-

GPRS exige um servidor AAA GPRS que traz alterações também na CN GPRS/UMTS, com modificações na pilha de protocolos de suporte ao GMM/SM a fim de suportar o EAP-GPRS, seja em um outro nó separado ou dentro do SGSN, como ilustra a Figura 6.9.

A arquitetura *loose coupling* também exige um servidor AAA na rede IP do operador para autenticação do terminal, o qual é baseado nos protocolos do IETF, como o EAP e o RADIUS, ou o seu sucessor, o DIAMETER. Diferentemente da arquitetura *tight coupling*, este servidor não é o ponto onde a autenticação termina. Na arquitetura *tight coupling*, os protocolos GMM/SM são os responsáveis pelo acesso aos dados do usuário no HLR. Já o servidor AAA da arquitetura *loose coupling* precisa acessar o HLR da operadora para completar a autenticação, como ilustra a Figura 5.4. Na verdade, este servidor atua como uma ponte entre os protocolos do IETF e a pilha do protocolo MAP, que faz o acesso ao HLR. Portanto, ao contrário do servidor AAA GPRS da arquitetura *tight coupling*, o servidor AAA da arquitetura *loose coupling* não exige mudanças de protocolos na CN GPRS/UMTS.

### 7.3.2. Mobilidade

Em termos de mobilidade, a arquitetura *tight coupling* reutiliza a mobilidade provida pela CN GPRS/UMTS através dos protocolos GMM e SM. A sinalização de controle dos protocolos GMM e SM entre o terminal e a CN GPRS, e vice-versa, é transportada com o auxilio do EAP-GPRS/UMTS e, neste caso, nenhuma funcionalidade adicional é necessária. Na arquitetura *tight coupling*, a CN GPRS considera a WLAN como sendo uma outra *Routing Area* (RA) GPRS e, portanto, nenhum suporte adicional é requerido.

Por outro lado, a arquitetura *loose coupling* não permite o reuso dos protocolos GMM e SM do GPRS/UMTS. Esta arquitetura necessita de suporte para mobilidade, como, por exemplo, o Mobile IP. O *Home Agent* (HA) é implementado na rede IP do operador, enquanto que o *Foreign Agent* (FA) é implementado no SGSN, do lado da CN GPRS, e no roteador de acesso da WLAN. Portanto, considerando-se o suporte Mobile IP, a arquitetura *loose coupling* exige um complemento de funcionalidade na rede IP do operador (HA), na CN GPRS (FA no SGSN) e na WLAN (FA no roteador de acesso).

### 7.3.3. O Sistema de *Billing*

A arquitetura *tight coupling* também reutiliza o sistema de *billing* do CN GPRS. Uma vez que a WLAN é vista pela CN GPRS como qualquer outra RA GPRS e que todo o tráfego originário da rede WLAN passa pela CN GPRS, o SGSN e o GGSN contabilizam o tráfego da WLAN da mesma forma que o tráfego GPRS, ou seja, os relatórios de tarifação (CDRs) são enviados pelo SGSN e GGSN para o *Charging Gateway Functionality* (CGF) da CN GPRS e aí então consolidados no sistema de *billing*. Portanto, nenhuma funcionalidade adicional é requisitada pelo *tight coupling* em termos de *billing*.

Por outro lado, a arquitetura *loose coupling* faz a tarifação baseado nos funcionalidades de *accounting* providas pelo RADIUS. O AP, que é um cliente RADIUS, envia relatórios para o servidor AAA contendo informações como tempo de uso e volume de bytes enviados e recebidos. O servidor AAA prepara relatórios de tarifação no formato GPRS (os CDRs) e os envia para o CGF. Portanto, o acoplamento *loose coupling* não requer alterações na CN GPRS para efeitos de *billing*.

### 7.3.4. O Controle de Acesso

Os dois tipos de acoplamentos utilizam o controle de acesso baseado no 802.1x, no qual o AP só libera acesso ao terminal se o resultado da autenticação for positivo.

O controle de acesso na arquitetura *tight coupling* é baseado no EAP-GPRS, que na verdade, não define um novo método de autenticação, mas sim um mecanismo de transporte para as mensagens dos protocolos GMM e SM entre a CN GPRS e o terminal e vice-versa. Na realidade, o EAP-GPRS não transporta diretamente as mensagens dos protocolos GMM e SM, mas sim as mensagens dos protocolos LLC (interface GPRS Gb) e RRC (interface UMTS Iu), os quais fornecem serviços de transporte L2 (retransmissão, sequenciamento, etc) para os protocolos GMM e SM. O EAP-GPRS opera imediatamente abaixo do LLC e do RRC e, por isso, alterações ou extensões nos protocolos LLC e RRC são necessárias para suporte ao EAP-GPRS.

Na a arquitetura *loose coupling* o controle de acesso é baseado no EAP-SIM e EAP-AKA. Diferentemente do EAP-GPRS, o EAP-SIM e o EAP-AKA definem novos métodos de autenticação. O EAP-SIM utiliza o cartão SIM para a autenticação de terminais GPRS em

ambientes WLAN. O EAP-AKA provê a autenticação de terminais GSM/GPRS e UMTS baseados no cartão GSM SIM ou UMTS USIM, respectivamente. Ambos os métodos utilizam um servidor AAA RADIUS para a autenticação, o qual faz a interface com o HLR concluir a autenticação.

O EAP-AKA provê um nível de segurança maior que o EAP-SIM, e tem sido recomendado como o protocolo a ser utilizado na arquitetura *loose coupling* [Nyström] [S3-020549].

Os protocolos GMM e SM do GPRS não são envolvidos na autenticação EAP-SIM e EAP-AKA nem do lado do terminal e nem do lado da CN GPRS. O servidor AAA RADIUS deve possuir a interface necessária para acessar o HLR (pilha de protocolos MAP), conforme ilustra a Figura 5.4. Assim, não é necessária alterações dentro da CN GPRS para suporte ao EAP-SIM e EAP-AKA.

### 7.3.5. Suporte do AP ao Controle de Acesso

Tanto na arquitetura *tight coupling* como na *loose coupling* o AP tem a funcionalidade de autenticador do 802.1x, e deve suportar o EAP.

Na arquitetura *loose coupling* o AP também tem o papel de um cliente RADIUS, responsável pelo acesso e suporte ao servidor AAA com relação ao controle de acesso e sistema de *billing*. Por isso, deve-se também oferecer o suporte como cliente do servidor AAA da rede IP do operador.

### 7.3.6. Suporte ao Terminal

A arquitetura *tight coupling* pressupõe que o terminal implementa a pilha do GRPS ou do UMTS, como ilustram as Figuras 6.4 e 6.5. No caso desta arquitetura, a WLAN simplesmente provê um outro meio de transporte para as camadas superiores do GPRS ou UMTS no terminal. Assim sendo, modificações ou extensões dos protocolos superiores do GPRS/UMTS são necessárias para o acesso à interface 802.11. Além disso, a presença de uma Função de Adaptação é também necessária para o suporte ao processo de descobrimento de endereçamento MAC do IWF, o que exige um nível maior de complexidade do lado do terminal e apresenta uma outra restrição para a arquitetura *tight coupling*.

Por outro lado, na arquitetura *loose coupling*, o terminal não precisa do suporte aos protocolos GPRS ou UMTS, como ilustram as Figuras 5.4 e 5.12. O terminal exige um nível de complexidade menor, o que representa uma vantagem quando comparado com o terminal destinado à arquitetura *tight coupling*.

### 7.3.7. Plano de Dados de Usuário e o Processamento de Dados Enviados e Recebidos no Terminal

Um importante ponto a se considerar é o plano de transmissão de dados do usuário das duas arquiteturas e a questão do processamento dos dados enviados e recebidos. O plano de transmissão de dados da arquitetura *loose coupling* é ilustrado na Figura 5.12 e o da *tight coupling*, considerando um terminal GPRS com interface Gb, é ilustrado na Figura 6.10.

Para efeito ilustrativo, a Figura 7.1 ilustra lado a lado a pilha de protocolos no terminal para a arquitetura *tight coupling*, considerando ambas interfaces Gb e Iu, e para a arquitetura *loose coupling*.

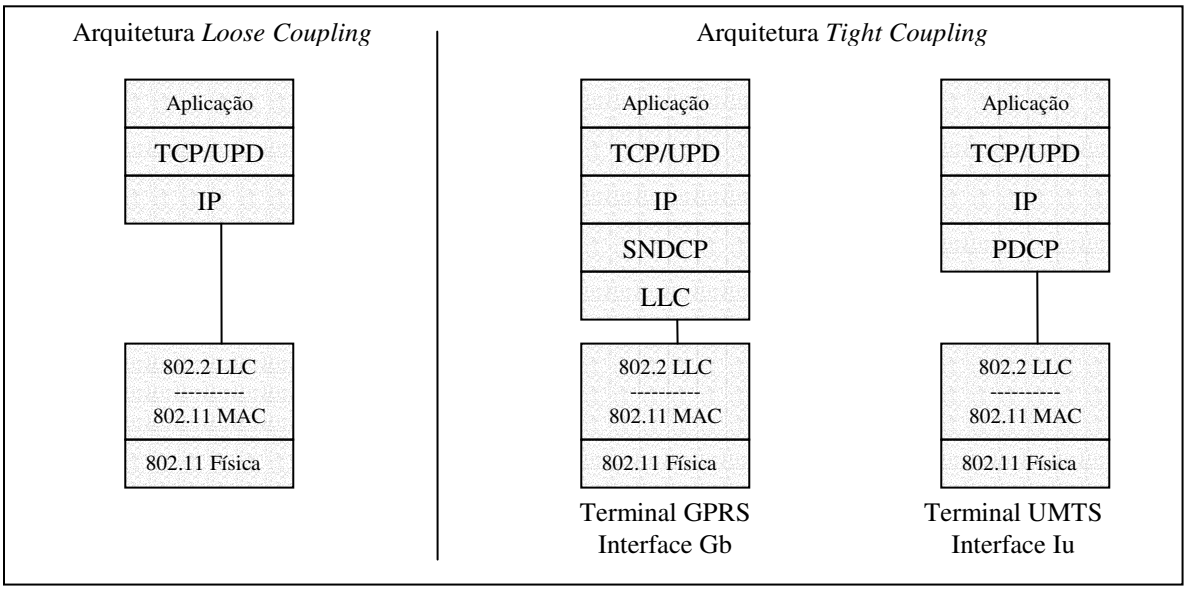


Figura 7.1. Comparação entre o Plano de Transmissão das arquiteturas *tight* e *loose coupling* dentro de um terminal.

Na arquitetura *loose coupling*, uma PDU TCP/UDP é encapsulada em uma PDU IP e então enviada diretamente ao 802.2 LLC da interface de rádio da WLAN.

Já a arquitetura *tight coupling* apresenta um *overhead* maior em termos de encapsulamento e processamento de dados a serem transmitidos. Uma PDU IP deve ser encapsulado nos outros protocolos como o SNDCP e o LLC, no caso de um terminal GPRS com interface Gb, e como o PDCP, no caso de um terminal UMTS com interface Iu.

Portanto, um terminal na arquitetura *tight coupling* apresenta um *overhead* maior quanto ao volume total de bytes a serem transmitidos quando comparado com a mesma quantidade de dados ao nível de aplicação da arquitetura *loose coupling*. Além disso, o terminal na arquitetura *tight coupling* exige um processamento maior dos dados a serem enviados e recebidos, devido ao maior número de protocolos na sua pilha.

### 7.3.8. Velocidade de Acesso à Internet

Na arquitetura *loose coupling* o usuário tem acesso direto à Internet, sem passar pela CN GPRS. A taxa de dados transmitidos e recebidos pelo usuário vai depender diretamente do tipo de acesso do *hotspot* à Internet. Para *hotspots* pequenos, como o caso de cafés, bares e restaurantes, o acesso à Internet pode ser feito, por questões de viabilidade econômica, através de linhas ADSL. Neste caso, a limitação de acesso é a linha ADSL, pois esta linha possui taxas de transmissão de dados da ordem de centenas de Kbps, e a WLAN possui taxas de Mbps. Para *hotspots* maiores, como é caso de aeroportos, universidades e *shopping centers*, o acesso pode contar com uma LAN interna, roteadores e acesso externo à Internet com altas taxas de transmissão e, neste caso, a rede fixa pode não representar limitações para os usuários de WLAN.

A arquitetura *tight coupling* se caracteriza por prover acesso à Internet através da CN GPRS, onde uma linha dedicada conecta ao IWF, na WLAN, e ao SGSN, no CN GPRS/UMTS. Neste caso, os pontos de limitações podem ser a linha dedicada entre o IWF, o próprio IWF e a CN GPRS/UMTS, onde tanto o SGSN e o GGSN podem não ser capazes de suportar taxas de Mbps, providas pelas WLANs.

### 7.3.9. A Conexão da WLAN ao CN GPRS/UMTS

Na arquitetura *loose coupling*, a conexão entre a WLAN e a CN GPRS é feita utilizando um roteador e/ou modem utilizando o protocolo IP. Já a arquitetura *tight coupling*

exige o IWF, ou seja, um equipamento dedicado para este tipo de interconexão e pode representar custo maior, além da complexidade, que um roteador e/ou modem IP, já disponíveis no mercado.

### 7.3.10. Interconexão com Hotspots já Existentes

Um fato importante que deve ser considerado na integração entre as WLANs e os sistemas celulares é a presença dos *hotspots* já existentes. É o caso, por exemplo, de bares e restaurantes que já possuem suas próprias WLANs independentes, ou ainda, operadores WISP que também já possuem *hotspots* em várias localidades. Podemos ainda considerar WLANs dentro de empresas que desejam fornecer a seus empregados, clientes e fornecedores acesso à Internet utilizando os cartões SIM/USIM como controle de acesso.

A presença de *hotspots* vem crescendo ao longo dos anos, muito embora nos Estados Unidos alguns WISP pararam suas atividades por dificuldades financeiras e muitas discussões são feitas em nível de viabilidade econômicas dos serviços WiFi [Henry]. Nos Estados Unidos, a presença de *hotspots* vem se consolidando através de serviços e agentes como o franqueador, o WISP (ou *carrier*) e o agregador [Henry]:

- A franquia é o modelo mais simples onde um franqueador, como por exemplo, Joltage [Joltage] faz um acordo com um proprietário de um *hotspot* independente, por exemplo, um bar, uma livraria ou um restaurante, que já possui sua própria WLAN. O franqueador fornece conexão a um servidor AAA central para que seus usuários tenham acesso aos serviços naquele *hotspot*.
- O WISP é a empresa que já possui algumas localidades com redes WLANs. Exemplos de WISP são SurfAndSip [SurfAndSip] , Wayport [Wayport] e AirPath [AirPath].
- O agregador é a empresa que faz acordos com vários *carriers*, provendo acesso a seus usuários a um grande número de *hotspots*, os quais realmente pertencem aos *carriers*. Exemplos de agregadores são a Boingo [Boingo] e a WiFinder [WiFinder]. Estas companhias oferecem um diretório com uma lista de *hotspots* que estão disponíveis para o usuário na sua localidade mais próxima ou dentro de uma determinada rota de viagem. O agregador aumenta seu número de localidades atendidas através de acordos com outros provedores de infra-estrutura.

Neste cenário, os operadores de redes celulares não precisam instalar suas próprias redes, mas sim utilizar acordos de *roaming* com os WISP e agregadores permitindo o acesso de seus usuários para aquelas localidades que já possuem infra-estrutura disponível.

Neste tipo de situação a arquitetura *loose coupling* mostra-se como a mais adequada, pois acordos de *roaming* entre os operadores de redes celulares e os WISP e agregadores podem fornecer acessos aos usuários com cartões SIM/USIM. Conexões e configurações entre os servidores de acesso, mais o suporte ao MIP dentro dos *hotspots* já existentes podem ser necessárias. Uma arquitetura do tipo *tight coupling* mostra-se inviável para *hotspots* que já estão em operação e que pertencem a outros proprietários, devido a mudanças que exigiria na WLAN já existente.

## 7.4. Considerações Finais

A arquitetura *tight coupling* provê um acoplamento mais firme entre a WLAN e a CN GPRS/UMTS, por isso apresenta uma complexidade maior. Ela apresenta a vantagem de aproveitar recursos internos da rede celular, como o gerenciamento de mobilidade e sistema de *billing*. No entanto, apresenta desvantagens com relação à integração com outros *hotspots* já existentes e mudanças de protocolos dentro da CN GPRS/UMTS. Não suportam terminais que não implementam a pilha de protocolos do GPRS e UMTS, e ainda podem apresentar limitações de alto tráfego e desempenho dentro da CN GPRS/UMTS. A arquitetura *tight coupling* pode ser atraente para *hotspots* que pertencem exclusivamente a um determinado operador de rede celular.

A arquitetura *loose coupling* apresenta um acoplamento mais leve e por isso menos complicado. O acoplamento é inteiramente baseado nos protocolos do IETF e as mudanças esperadas dentro das WLANs são mínimas. Esta arquitetura não reutiliza os recursos internos do CN GPRS/UMTS e por isso requer o suporte externo para mobilidade, como, por exemplo, o Mobile IP. Também apresenta vantagens com relação à interconexão com *hotspots* já existentes e maior simplicidade do lado do terminal.

A Tabela 7.1 ilustra um resumo da comparação entre as duas arquiteturas.

| Categoria | Arquitetura *Tight Coupling* | Arquitetura *Loose Coupling* |
|---|---|---|
| Servidor de Autenticação | Exige um servidor AAA GPRS que altera pilha de protocolos do GPRS/UMTS | Exige um servidor AAA baseado nos protocolos do IETF. Não há alteração nos protocolos do GPRS/UMTS. |
| Mobilidade | Reutiliza a mobilidade provida pela CN GPRS/UMTS através dos protocolos do GPRS/UMTS. | Exige um complemento de funcionalidade dentro da rede IP do operador, como por exemplo, o Mobile IP. |
| Sistema de *Billing* | Reutiliza o sistema de *billing* da CN GPRS/UMTS. | O sistema de billing é baseado nas funcionalidades de *accounting* dos protocolos do IETF. |
| Controle de Acesso | Baseado no 802.1x (EAP GPRS). | Baseado no 802.1x (EAP SIM e EAP AKA). |
| Suporte do AP ao Controle de Acesso | Deve suportar o 802.1x. | Deve suportar o 802.1x e as funcionalidades de cliente de protocolos do IETF (RADIUS, por exemplo). |
| Suporte ao Terminal | Exige suporte dos protocolos do GPRS/UMTS e função de adaptação para suporte ao IWF, por isso apresenta maior complexidade. | Não exige suporte da tecnologia GPRS/UMTS nem de funções. |
| Transmissão de Dados no Terminal | A camada IP acessa os protocolos do GPRS/UMTS e por isso apresentam maior *overhead* de cabeçalho nos pacotes. | A camada IP acessa diretamente a interface de rádio 802.11. |
| Processamento de Dados no Terminal | Maior processamento nos dados transmitidos e recebidos devido à presença dos protocolos do GPRS/UMTS no plano de transmissão. | Menor processamento de dados visto que a camada IP acessa diretamente a camada de rádio do 802.11. |

| | | |
|---|---|---|
| Velocidade de Acesso à Internet | A velocidade de acesso depende da conexão com o CN GPRS/UMTS, do IWF e do próprio CN GPRS/UMTS, onde o SGSN e o GGSN podem apresentar limitações para altas taxas de transmissão providas pela WLAN. | A velocidade de acesso depende da conexão do *hotspot* e dos roteadores. |
| Conexão da WLAN ao CN GPRS/UMTS | Necessita de um equipamento dedicado, o IWF. | Necessita de roteadores IP, já disponíveis comercialmente. |
| Conexão com *Hotspots* já existentes | Não são recomendadas para integração com *hotspots* já existentes, pois exigem outra conexão da WLAN com o CN GPRS/UMTS além da instalação do IWF. | Pequenas alterações são esperadas, como configurações e suporte de mobilidade. |
| Usuários que podem utilizar a WLAN | É voltada para usuários de redes de sistemas celulares. | Tem um uso mais geral. Aplicado também para usuários de outros WISP através de acordo de *roaming*. |

Tabela 7.1. Comparação entre as arquiteturas *tight* e *loose coupling*.

Podemos concluir que a arquitetura *loose coupling* é a mais indicada para a interconexão entre as WLANs e as redes de operadores celulares GPRS/UMTS.

## 7.5. Trabalhos Futuros

Nesta dissertação foi levado em conta o cenário de integração 4 proposto pelo 3GPP, ou seja, continuidade de serviço, porém sem garantias de Qualidade de Serviço.

Um próximo passo a questão da interconexão entre as WLANs e os sistemas celulares é o estudo do cenário 5 do 3GPP, ou seja, continuidade de serviço associada à Qualidade de Serviço. Um possível trabalho é o estudo do mapeamento de requisitos de Qualidade de Serviço a serem oferecidos pelo 802.11e com os requisitos de Qualidade de Serviço das redes celulares do GPRS e UMTS e ainda com outros requisitos de Qualidade Serviço destinados à Internet, como o IntServ e o DiffServ.

# 8. Lista de Abreviações

**1G**
First-Generation

**2G**
Second-Generation

**3G**
Third-Generation

**3GPP**
Third-Generation Partnership Project

**3GPP2**
Third-Generation Partnership Project 2

**802.3**
IEEE 802.3 CSMA/CD (Ethernet)

**802.5**
IEEE 802.5 Token Ring

**A3**
Algoritmo de Autenticação do GSM

**A8**
Algoritmo de Geração de Chave do GSM

**AAA**
Authorization, Authentication and Accounting

**AAL**
ATM Adaptation Layer

**ACL**
Access Control List

**AES**
Advanced Encryption Standard

**ADSL**
Asymmetric Digital Subscriber Line

**AIFS**
Arbitration Interface Space

**AK**
Authentication Key

**AKA**
Authentication and Key Agreement

**AMF**
Administrative Management Field

**AP**
Access Point

**APo**
Access Port

**ATM**
Asynchronous Transfer Mode

**AuC**
Authentication Center

**AUTN**
Authentication Token Number

**BRAN**
Broadband Radio Access Network

**BSC**
Base Station Controller

**BSS**
Base Station Subsystem (BSC + BTS)
Basic Service Set

**BTS**
Base Transceiver Station

**CDMA**
Code Division Multiplex Access

**CDR**
Call Detail Records

**CGF**
Charging Gateway Functionality

**CK**
Ciphering Key

**CN**
Core Network
Correspondent Node

**CRNC**
Controlling RNC

**COA**
Care of Address

**CSMA/CD**
Carrier Sense Multiple Access with Collision Avoidance

**DCF**
Distributed Coordination Function

**DMZ**
Demilitarized Zone

**DSSS**
Direct Sequence Spread Spectrum

**DRNC**
Drift RNC

**DPC**
Destination Point Code

**DS**
Distributed System

**EAP**
Extensible Authentication Protocol

**EAPOL**
EAP over LAN

**EAPOW**
EAP over WLAN

**EDCF**
Enhanced Distributed Coordination Function

**EIR**

Equipment Identity Register

**ETSI**
European Telecommunication Standards Institute

**ESS**
Extended Service Set

**EU**
User Equipment

**f1**
Algoritmo de Autenticação UMTS para geração de MAC

**f2**
Algoritmo de Autenticação UMTS para geração de XRES

**f3**
Algoritmo de Autenticação UMTS para geração de chave CK

**f4**
Algoritmo de Autenticação UMTS para geração de IK

**f5**
Algoritmo de Autenticação UMTS para geração de AK

**FHSS**
Frequency Hopping Spread Spectrum

**FA**
Foreign Agent

**FTAM**
File Transfer, Access and Management

**FTP**
File Transfer Protocol

**GHz**
Giga Hertz

**GGSN**
Gateway GPRS Support Node

**GMSC**
Gateway Mobile Switching Center

**GMM**
GPRS Mobility Management

**GSM**
Global System for Mobile Communication

**GPRS**
General Packet Radio Service

**GTP**
GPRS Tunneling Protocol

**GTP´**
GPRS Tunneling Protocol for Charging

**GTP-U**
GPRS Tunneling Protocol for User Plane

**GSN**
GPRS Support Node

**HA**
Home Agent

**HE**
Home Environment

**HIPERLAN**
High Performance Radio Local Area Network

**HLR**
Home Location Register

**IBSS**
Independent Basic Service Set

**IEEE**
Institute of Electrical and Electronics Engineers

**IETF**
Internet Engineering Task Force

**IK**
Integrity Key

**IMSI**
International Mobile Subscriber Identity

**Interface GPRS Gb**
Interface GPRS entre a BSC e o SGSN

**Interface GPRS Um**
Interface GPRS entre o MS e a BTS

**Interface UMTS Cu**
Interface UMTS entre o cartão USIM e o ME.

**Interface UMTS Iu**
Interface UMTS entre a UTRAN e a CN

**Interface UMTS Iub**
Interface UMTS entre o RNC e o Node B

**Interface UMTS Iur**
Interface UMTS entre dois RNC

**Interface UMTS Uu**
Interface aérea UMTS entre o ME e o Node B, também chamada de WCDMA

**IP**
Internet Protocol

**IPSEC**
IP Security

**IS-95**
Interim Standard 95

**IS-136**
Interim Standard 136

**ISDN**
Integrated Services Digital Networks

**ISM**
Industrial, Scientific and Medical

**ISP**
Internet Service Provider

**ISUP**
ISDN User Part

**IWF**

Inter Working Function

**IWU**
Inter Working Unit

**Kbps**
Kilo bits per second

**Kc**
Chave de Criptografia do GSM

**Ki**
Chave de Autenticação Individual do GSM

**L1**
Layer 1 (camada 1 ou camada física no modelo OSI)

**L2**
Layer 2 (camada 2 ou camada de enlace no modelo OSI)

**L3**
Layer 3 (camada 3 ou camada de rede no modelo OSI)

**LAN**
Local Area Network

**LLC**
Logical Link Control

**LLM**
Logical Link Management

**LWAPP**
Light Weight Access Point Protocol

**Mbps**
Mega bits per second

**MAC**
Media Access Control
Message Authentication Code

**MAC_SRES**
Message Authentication Code Signature Response

**MAP**
Mobile Application Part

**MD5**
Message Digest 5

**ME**
Mobile Equipment

**MIP**
Mobile IP

**MM**
Mobility Management

**MN**
Mobile Node

**MS**
Mobile Station

**MSC**
Mobile Switching Center

**MT**
Mobile Terminal

**MTP1**
Message Transfer Part 1

**MTP2**
Message Transfer Part 2

**MTP3**
Message Transfer Part 3

**NAI**
Network Access Identifier

**NIC**
Network Interface Card

**Node B**
UMTS base station

**NS**
Network Service

**OSI**

Open System Interconnect

**QoS**
Quality of Service

**PCF**
Point Coordination Function

**PDA**
Personal Digital Assistance

**PDC**
Packet Data Protocol

**PDN**
Packet Data Network

**PDU**
Processing Data Unit

**PKI**
Public Key Infrastructure

**PLMN**
Public Land Mobile Network

**PoE**
Power over Ethernet

**PPP**
Point-to-Point Protocol

**PSTN**
Public Switch Telephone Network

**RADIUS**
Remote Authentication Dial In User Service

**RA**
Routing Area

**RAI**
Routing Area Identity

**RAN**
Radio Access Network

**RAND**
Um valor randômico (aleatório)

**RF**
Radio Frequency

**RNC**
Radio Network Controller

**RNL**
Radio Network Layer

**RNS**
Radio Network Subsystem

**RSN**
Robust Security Network

**SCCP**
Signaling Connection Control Part

**SGSN**
Serving GPRS Support Node

**SIM**
Subscriber Identity Module

**SMS**
Short Message Service

**SM**
Session Management

**SNDCP**
SubNetwork Dependent Convergence Protocol

**SQN**
Sequence Number

**SRES**
Signature Response

**SRNC**
Server RNC

**SS7**
Signaling System 7

**SSID**
Service Set Identification

**SSL**
Secure Socket Layer

**STP**
Signaling Transfer Point

**TCAP**
Transaction Capabilities Application Part

**TCP**
Transmission Control Protocol

**TDMA**
Time Division Multiplex Access

**TE**
Terminal Equipment

**TKIP**
Temporal Key Integrity Protocol

**TLS**
Transport Layer Security

**TMSI**
Temporary Mobile Subscriber Identity

**TNL**
Transport Network Layer

**TTLS**
Tunneled Transport Layer Security

**UA**
User Application

**UDP**
User Datagram Protocol

**UMTS**
Universal Mobile Telecommunication System

**UNNI**

Unlicensed National Information Infrastructure

**USIM**
UMTS Subscriber Identity Module

**UTRAN**
UMTS Terrestrial Radio Access Network

**VLAN**
Virtual Local Area Network

**VLR**
Visitor Location Register

**VPN**
Virtual Private Network

**X.25**
Um Protocolo de Rede

**XRES**
Expected Response

**W-CDMA**
Wideband Code Division Multiplex Access

**WECA**
Wireless Ethernet Compatibility Alliance

**WEP**
Wired Equivalent Privacy

**WLAN**
Wireless Local Area Network

**Wi-Fi**
Wireless Fidelity

**WISP**
Wireless Internet Service Provider

**WPA**
Wi-Fi Protected Access

**WMAN**
Wireless Metropolitan Area Network

**WPAN**
Wireless Personal Area Network

**WWAN**
Wireless Wide Area Network

# 9. Referências Bibliográficas


[ETSI 101 957] ETSI TR 101 957 V1.1.1 (2001-08); Broadband Radio Access Networks (BRAN); HIPERLAN Type2; Requirements and Architecture for Interworking between HIPERLAN/2 and 3rd Generation Cellular Systems

[3GPP 04.64] 3GPP TS 04.64 V8.7.0 (2001-12); 3rd Generation Partnership Project; Technical Specification Group Core Network; Digital Cellular Telecommunications System (Phase 2+); General Packet Radio Service (GPRS); Mobile Station – Serving GPRS Support Node (MS-SGSN) Logical Link Control (LLC) Layer Specification (Release 1999)

[3GPP 21.101] 3GPP TR 21.101 V3.11.0 (2003-03); 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3rd Generation mobile system Release 1999 Specifications (Release 1999)

[3GPP 21.905] 3GPP TR 21.905 V6.2.0 (2003-03); 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications; Release 6

[3GPP 22.934] 3GPP TR 22.934 V6.1.0 (2002-12); 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking; Release 6

[3GPP 23.002] 3GPP TR 23.002 V6.0.1 (2003-03); 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Network Architecture; Release 6

[3GPP 23.107] 3GPP TR 25.107 V5.8.0 (2003-03); 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Quality of Service (QoS) concept and architecture (Release5)

[3GPP 23.234] 3GPP TR 23.234 V1.10.0 (2003-05); 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System to Wireless Local Area Network (WLAN) Interworking; System Description (Release 6)

[3GPP 23.934] 3GPP TR 23.934 V1.0.0 (2002-08); 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System to Wireless Local Area Network (WLAN) Interworking; Functional and Architectural Definition (Release 6)

[3GPP 24.008] 3GPP TS 24.008 V6.2.0 (2003-09); 3rd Generation Partnership Project; Technical Specification Group Core Network; Mobile Radio Interface Layer 3 Specifications; Core Network Protocols; Stage 3 (Release 6)

[3GPP 25.301] 3GPP TR 25.301 V5.2.0 (2002-09); 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Radio Interface Protocol Architecture; Release 5

[3GPP 25.331] 3GPP TS 25.331 V5.6.0 (2003-09); 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Radio Resource Control (RRC); Protocol Specification (Release 5)

[3GPP 25.401] 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Overall Description (Release 6)

[3GPP 25.933] 3GPP TR 25.933 V5.2.0 (2003-03); 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; IP transport in UTRAN; (Release 5)

[DTS/BRAN] DTS/BRAN-0020003-2 Broadband Radio Access Network (BRAN); HIPERLAN Type2; Interworking between HIPERLAN/2 and 3rd Generation Cellular and other Public Systems

[802.11_Family] The Family Dynamics of 802.11; Bill McFarland and Michael Wong; May 2003

[802.11] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Institute of Electrical and Electronics Engineers; 1997

[802.11a] IEEE Standard 802.11a; Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-Speed Physical Layer Extension in the 5 GHz Band. Institute of Electrical and Electronics Engineers; 1999

[802.11b] IEEE Standard 802.11b; Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band. Institute of Electrical and Electronics Engineers; 1999

[802.11g] IEEE Standard 802.11g; Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Further Higher Data Rate Extensions in the 2.4 GHz Band. Institute of Electrical and Electronics Engineers; 2003

[802.11n] IEEE Standard 802.11n; Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Enhancements for Higher Effective Throughput. Specification under development.

[802.11f_draft] IEEE Standard 802.11f pre-draft; Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distributed System Supporting IEEE 802.11 Operation, March 2001

[802.11i] IEEE Standard 802.11/D3.0, Draft Supplement to Standard for Telecommunication and Information Exchange Between Systems – LAN/MAN Specific Requirements. Part 11 Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security, November 2002

[802.1x] IEEE Standard 802.1x-2001, IEEE Standard for Local and Metropolitan Area Network, Port-Based Network Access Control, 2001

[Buddhikot] Buddhikot, Milind M. et al; Design and Implementation of a WLAN/CDMA2000 Interworking Architecture; IEEE Communications Magazine, November 2003, Pages 90-100

[De Vriendt] De Vriendt, Johan et al; Mobile Network Evolution: A Revolution on the Move; IEEE Communications Magazine, April 2002, Pages 104-111

[Ala-Laurila] Ala-Laurila, Juha; Mikkonen, Jouni and Rinnemaa, Jyri; Wireless LAN Access Network Architecture for Mobile Operators; IEEE Communications Magazine, November 2001, Pages 82-89

[Haverinen] Haverinen, Henry; Mikkonen, Jouni and Takamaki, Timo; Cellular Access Control and Charging for Mobile Operator Wireless Local Area Networks, IEEE Wireless Communication, December 2002, Pages 52-60

[Salkintzis] Salkintzis, Apostolis K.; Fors, Chad; Pazhyannur, Rajesh; WLAN-GPRS Integration for Next-Generation Mobile Data Networks; IEEE Wireless Communication, October 2002, Pages 112-124

[Pahlavan] Pahlavan, Kaveh et al; Handoff in Hybrid Mobile Data Networks, IEEE Personnel Communications, April 2000, Pages 34-47

[Ahmavaara] Ahmavaara, Kalle; Haverinen, Henry and Pichna, Roman; Interworking Architecture between 3GPP and WLAN Systems; IEEE Communications Magazine, November 2003, Pages 74-81

[Henry] Henry, Paul S. and Luo, Hui; WiFi: What´s Next? ; IEEE Communications Magazine, December 2002, Pages 66-72

[Koien] Koien, GeirM. and Haslested, Thomas; Security Aspects of 3G-WLAN Interworking, IEEE Communications Magazine, November 2002, Pages 82-88

[Doufexi] Doufexi, Angela et al; Hotspot Wireless LANs to Enhance the Performance of 3G and Beyond Cellular Networks; IEEE Communications Magazine, July 2003, Pages 58-65

[Park] Park, Jeong-Hyun; Wireless Internet Access for Mobile Subscriber Based on the GPRS/UMTS Network; IEEE Communications Magazine, April 2002, Pages 38-49

[Thorngren] Thornegre, Björn, Master Thesis, Lund School of Economics and Management, Department of Business Administration, February 2002.

[RFC2002] RFC 2002; Perkins, C.; IP Mobility Support, October 1996

[RFC2284] RFC 2284; Blunk, L and Vollbreach, J; PPP Extensible Authentication Protocol (EAP), March 1998

[RFC2486] RFC 2486; Aboba, B. and Beadles, M.; The Network Access Identifier, January 1999

[RFC2865] RFC 2865; Rigney, C at all; Remote Authentication Dial In User Service (RADIUS), June 2000

[EAP AKA] Arkko, J. and Haverinen, Henry; EAP AKA Authentication; Internet draft draft-arkko-pppext-eap-aka-10.txt, June 2003

[EAP GPRS] Salkintzis, Apostolis K.; The EAP GPRS Protocol; Internet draft draft-salki-pppext-eap-gprs-01.txt, June 2003

[EAP SIM] Haverinen, Henry and Salowey, J.; EAP SIM Authentication; Internet draft draft-haverinen-pppext-eap-sim-11.txt, June 2003

[Diameter] Calhoun, Pat R. et al; Diameter Base Protocol; Internet draft draft-ietf-aaa-diameter-09.txt; March 2002

[Holma] Holma, Harri and Toskala, Antti; WCDMA for UMTS, Radio Access for Third Generation Mobile Communications, John Wiley and Sons, LTD, 2001

[Garcia] Garcia, Ana-Belén et al, Quality of Service Support in the UMTS Terrestrial Radio Access Network. Universidad Politécnica de Madrid.

[IEC] The International Engineering Consortium; Web ProForum Tutorials; UMTS Protocols and Protocol Testing.

[Report 22] Impact & Opportunity: Public Wireless LNAs and 3G Business Revenues; Report from the UMTS Forum, Report 22; July 2002

[Ergen] Ergen, Mustafa; IEEE 802.11 Tutorial, University of California, Berkely, June 2002

[Mishra] Mishra, Arunesh; Arbaugh, William A.; An Initial Security Analysis of the IEEE 802.1x Standard, Department of Computer Science, University of Mariland, February 2002.

[Congdon] Congdon, Paul; Hewlett Packard, IEEE Plenary, Albuquerque, NM, March 2002

[Grillo] Grillo, António; Nunes, Mário; Performance Evaluation of IEEE 802.11E; INESC/IST, Lisboa, Portugal, 2002.

[Doshi] Doshi, Rushadh et all; Using IEEE 802.11e MAC for QoS over Wireless, Computer Science Department, Stanford University.

[Mangold] Mangold, Stefan et all; IEEE 802.11e Wireless LAN for Quality of Service, ComNets RWTH Aachen Univ. of Technology, Philips Research USA and Philips Research Germany.

[Heusse] Heusse, Martin; Rousseau, Franck; Gilles, Berger-Sabbatel; Duda, Andrzej; Performance Anomaly of 802.11b; LSR-IMAG laboratory, Grenoble, France, IEEE INFOCOM, 2003.

[Cisco] Cisco – Security for Next Generation Wireless LANs, Cisco Systems Inc, 2002

[Airespace] Understanding the Lightweight Access Protocol (LWAPP), A Technical Note, 2003 Airspace Inc, www.airespace.com

[Trapeze1] AP Architecture Impact on the WLAN, Part1: Security and Manageability, White Paper WP-AP1-304, Trapeze Networks Inc, 2003

[Trapeze2] AP Architecture Impact on the WLAN, Part2: Scalability, Performance, and Resiliency, White Paper WP-AP2-304, Trapeze Networks Inc, 2003

[Cristache] Cristache, Gabriel et al; Aspects for the Integration of ad-hoc and Cellular Networks; 3rd Scandinavian Workshop on Wireless Ad-hoc Networks, Stockholm, May 6-7th 2003

[Beeby] Beeby, Ian; Standards Required for Integrating WLAN with 3G; WFI Consulting; 10th September 2002

[Nyström] Nyström, Joakim and Seppala, Mikael; Experimental Study of GPRS/WLAN System Integration, Master´s Thesis Performed at Information Networks, Linkoping Institute of Technology, Sweden, May 19th 2003

[Abid] Abid, Muslin; Sulistyo, Selo and Najib, Warsun; UMTS Security, Security in Core Network and UTRAN, Grimstad, November 29th 2002

[Vähä-Sipilä] Välä-Sipilä, Antti; Ciphering in GPRS and UMTS, Encryption in 3G Data Networks, Tampere University of Technology, May 24th 2000

[S3-020549] 3GPP TSG SA WG3 Security – S3#25, Document for discussion S3-020549, On the security of EAP/SIM and EAP/AKA and their use in the WLAN-3G-interworking, Siemens, 8-11 October 2002, Munich, Germany

[NN103740] The Power of One Network – Securing and Scaling the Wireless LAN; Nortel Networks Position Paper NN103740-040203; Nortel Networks; 2003

[NN101960] Secure Network for Wireless LANs in the Enterprise; Nortel Networks White Paper NN101960-110802; Nortel Networks; 2003

[Corrêa] Corrêa, Clademir E.; Fonseca, Nelson L.S; Branquinho, Omar C.; Avaliação de Redes WLAN 802.11b com Arquiteturas Fat e Thin, Universidade Estadual de Campinas, 2004.

[Garg] Garg, Vijay K.; Wireless Network Evolution, 2G to 3G. Prentice Hall, PTR, 2002.

[Sun] Sun, Jun-Zhao, Howie, Douglas and Sauvola, Jaakko; Mobility Management Techniques for the Next Generation Wireless Network. University of Oulu, Finland

[Kurose] Kurose, J.F and Ross, K.W. Computer Networking, a Top-Down Approach Featuring the Internet

[Rai] Rai, Satyajit R.; GPRS and Wireless Networks; Online: http://www.it.iitb.ac.in/~satyajit/seminar/node11.html

[LWAPPdraft] www.airespace.com/html/lwapp.txt

[Colubris] Wireless LAN router for Public Access, Colubris Networks, www.colubris.com

[UMTSForum] www.umts-forum.org

[Symbol] Symbol´s Wireless Switch System, Symbol Technologies, www.symbol.com

[3GPP] www.3gpp.org

[3GPP2] www.3gpp2.org

[Nokia] www.nokia.com

[Joltage] www.joltage.com

[SurfAndSip] www.surfandsip.com

[WayPort] www.wayport.com

[AirPath] www.airpath.com

[Boingo] www.boingo.com

[WiFinder] www.wifinder.com