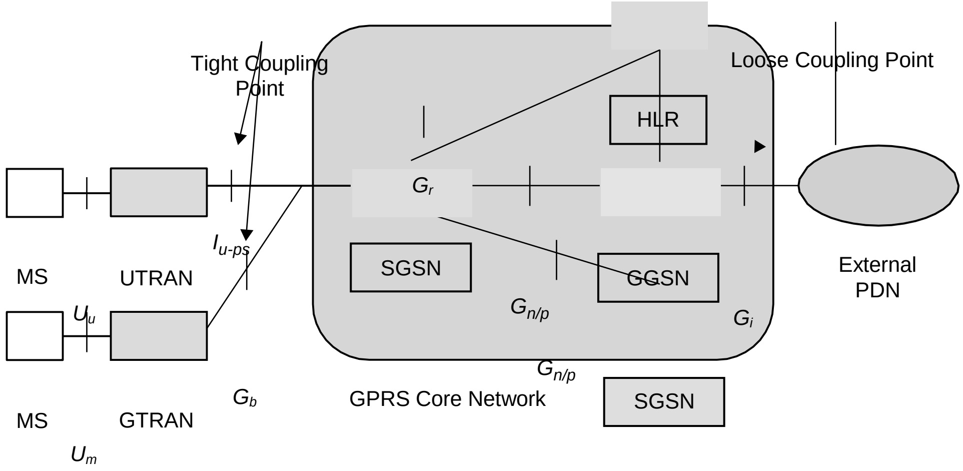
Interworking Architectures for WLAN and GPRS

In this section, we elaborate on the ETSI specified, two generic approaches for interworking — *tight coupling* and *loose coupling*. With tight coupling the WLAN is connected to the 3GPP (GPRS) core network in the same way as any other radio access network (RAN), such as GPRS RAN and UMTS terrestrial RAN (UTRAN). In this case, the WLAN data traffic goes through the GPRS core net- work before reaching the external packet data networks. With tight coupling, the WLAN is connected to either G_b or $I_{u\text{-}ps}$ reference points. On the other hand, with loose coupling, the WLAN is deployed as an access network complementary to the GPRS network. In this case, the WLAN utilizes the subscriber databasein the GPRS network but features no data interfaces to the GPRS core network. Figure shows the GPRS reference diagram for coupling points. The loose



MS: Mobile Station
UTRAN: UMTS Terrestrial Radio Access Network
GTRAN: GPRS Terrestrial Radio Access Network
SGSN: Serving GPRS Support Node
GGSN: Gateway GPRS Serving Node
HLR: Home Location Register
PDN: Packet Data Network

Figure 4.5: A GPRS reference diagram with WLAN coupling points.

[Source: Text book- Wireless Communications and networking, First Edition, Elsevier 2007 by Vijay Garg]

Pulling architecture between the GPRS and the WLAN at the G_i reference pointis indicated. This means that with loose coupling, the WLAN bypasses the GPRS network and provides direct network data access to the external packet data networks (PDNs).

The trend is to follow the loose coupling approach and use SIM or USIM-based authentication and billing. With this approach, a subscriber can reuse the SIM card or the USIM card to access a set of wireless data services over a WLAN.

In the tight coupling approach, 3GPP system-based access control and charging is used. This requires AAA for subscribers in the WLAN to be based on the same AAA procedures used in the GPRS system. An access to 3GPP GPRS-based services is used to allow the cellular operator to extend access to its GPRS-based services to subscribers in a WLAN environment. Also, seamless services scenarios provides seamless service continuity between GPRS and WLAN. The goal of 3GPP circuit- switched services is to allow the operator to offer access to circuit-switched services (e.g., normal voice calls) from a WLAN system. Seamless mobility for these services is provided. The advantages of tight coupling architecture between IEEE 802.11 WLANs and GPRS are the following:

- Seamless service continuation across WLAN and GPRS. The users are able to maintain their data sessions as they move from WLAN to GPRS and vice versa. For services with tight coupling quality of service (Qi's) requirements, seamless service continuation is subject to WLAN Qi's capabilities.
- Reuse of GPRS AAA
- Reuse of GPRS infrastructure (e.g., core network resources, subscriber data-bases, billing systems) and protection of cellular operator's investment
- **Support of lawful** interception for WLAN subscribers

``Increased security, since GPRS authentication and ciphering can be used on top of WLAN ciphering

- Common provisioning and customer care
- Access to core GPRS services such as short message service (SMS), location-based services and multimedia messaging services (MMS)

Internetworking objectives and requirements

Wireless local area networks (WLANs) are subjected to interference because of their operation in the unlicensed spectrum. WLANs' coverage ranges from about 30 to 300 m. Therefore, they are suitable only in high-density areas and thus not able to provide ubiquitous coverage. WLAN technology is relatively inexpensive and quick to deploy. Although WLANs were originally designed to extend LANs in corporate environments, they are becoming increasingly popular to provide IP connectivity in residential, small office home office (SOHO), and campus environments. A new phenomenon in populated areas has emerged to deploy WLANs in public hotspots including airports, coffee houses, convention centers, hotels, and other public areas with a high demand for wireless data.

Both WLANs and 3G are capable of providing higher-speed wireless connections that cannot be offered by earlier 2G cellular technologies. Therefore, they seem to compete. However, each technology has niche market applications. WLANs can cover only a small area and allow limited mobility, but provide higher data rates. Therefore, WLANs are well suited to hotspot coverage where there is a high density of demand for high-data-rate wireless services requiring limited mobility. On the other hand, 3G wireless networks, with their well-established voice support, wide coverage, and high mobility, are more suited to areas with moderate or low-density demand for wireless usage requiring high mobility. Therefore, WLANs and 3G are complementary. The integration of 3G wireless and WLANs is highly significant to make wireless multimedia and other high-data-rate services a reality for a large population. A multimedia 3G/WLAN terminal can access high-bandwidth data services where WLAN coverage is offered, while accessing wide area networks using 3G at other places. However, this approach alone will only allow limited multi-access functionality. To make multi-access solutions effective, we need an integrated solution to provide seamless mobility between accesses

Technologies, allowing continuity of existing sessions. 3G/WLAN integration promises to offer these capabilities seamlessly.

In the standard arena, work is going on both in the 3G partnership project (3GPP) and 3GPP2 on 3G/WLAN integration. 3GPP has specified an interworking architecture that enables users to access their 2G and 3G data services from WLANs. 3GPP2 has been initiated to examine the issues of 3G/WLAN interworking. They are finalizing stage 1 specifications of the interworking system and in the near future will start the architectural activities.

Several WLAN standardization organizations (in particular ETSI BRAN, IEEE 802.11, IEEE 802.15 and multimedia access communication (MMAC)) have agreed to set up a joint wireless interworking group (WIG) to deal with the interworking between WLANs and cellular networks. This activity is being driven primarily from Europe by ETSI BRAN.

In this chapter we focus on interworking issues of WLANs and wireless wide-area networks (WWANs). We also discuss the local multipoint distribution system (LMDS) and the multichannel multipoint distribution system (MMDS).

Interworking Objectives and Requirements

One of the principal objectives of interworking is to allow independent evolution of 3GPP (WWAN) and WLAN standards. The extent of interdependence between these standards should be minimized or localized at the point of interconnection. Support for the legacy WLAN user is perhaps the most important objective of a 3GPP-WLAN interworking setup. A legacy WLAN user is a user with a WLAN-capable device and a subscription to 3GPP services. The user may or may not be 3GPP capable. Such a user should be able to access 3GPP services without substantial hardware/software upgrades. Such a setup would result in a strong business

Case, leading to extend the facility of 3GPP services to the user who, although having a 3GPP subscription, does not want to spend it on additional hardware/software upgrades. The other objective of interworking is the single subscription.

The following are the interworking requirements:

- **Common billing and customer care.** This is the simplest form of interworking that provides a common bill and customer care to the subscriber but otherwise requires no real interworking between the WLAN and 3GPP data networks.
- **3GPP-based access control and charging.** This requires authentication, authorization, and accounting (AAA) for subscribers in the WLAN to be based on the same AAA procedures used in the 3GPP data networks. It means a mobile subscriber can use his or her subscriber identity module/ UMTS-SIM (SIM/USIM) to access WLAN services.

- **Access to 3GPP-based packet switched services.** The aim of this requirements to allow the mobile operator to allow access to its 3GPP data services to subscribers in a WLAN environment. It means a mobile subscriber should be able to access/select 3GPP data services through the WLAN access network. Although the user is allowed access to the same 3GPP data services over both the 3GPP and WLAN access networks, no service continuity across these access networks is required in this scenario.
- **Service continuity.** The goal is to allow seamless service continuity across the 3GPP and WLAN systems. It means that a user session during mobility across these networks should not only continue but also should not have noticeable service change in terms of quality and disruption.

- **Access to 3GPP circuit-switched services.** The goal of this requirement is to allow the 3GPP operator to offer access to circuit-switched services such as voice calls from the WLAN systems. Seamless service continuity is a must for these services.

Local Multipoint Distribution Service

Local multipoint distribution service (LMDS) with two-way capability gives long- distance carriers a relatively cheap entree into the local market with multiple operating benefits.

LMDS is a new type of stationary broadband wireless access technology designed for a mass subscriber marketplace (see Figure 22.18). It is based on millimeter micro frequencies — 2.4 GHz and above. LMDS now offers a potential for cheaper in-building bandwidth than fiber or copper.

Local in LMDS denotes that propagation characteristics of signals in this frequency range limit potential coverage area of a single cell site; ongoing field trials conducted in metropolitan centers place the range of an LMDS transmitter up to 5 miles.

Multipoint indicates that signals are transmitted in the point-to-multipoint or broadcast method; the wireless return path, from the subscriber to the base station, is a point-to-point transmission. *Distribution* refers to the distribution of signals, which may consist of simul- tenuous voice, data, Internet, and video traffic. *Service* implies the subscriber nature of the relationship between the opera- tor and customer; the services offered through an LMDS network are entirely dependent on the operator’s choice of business.

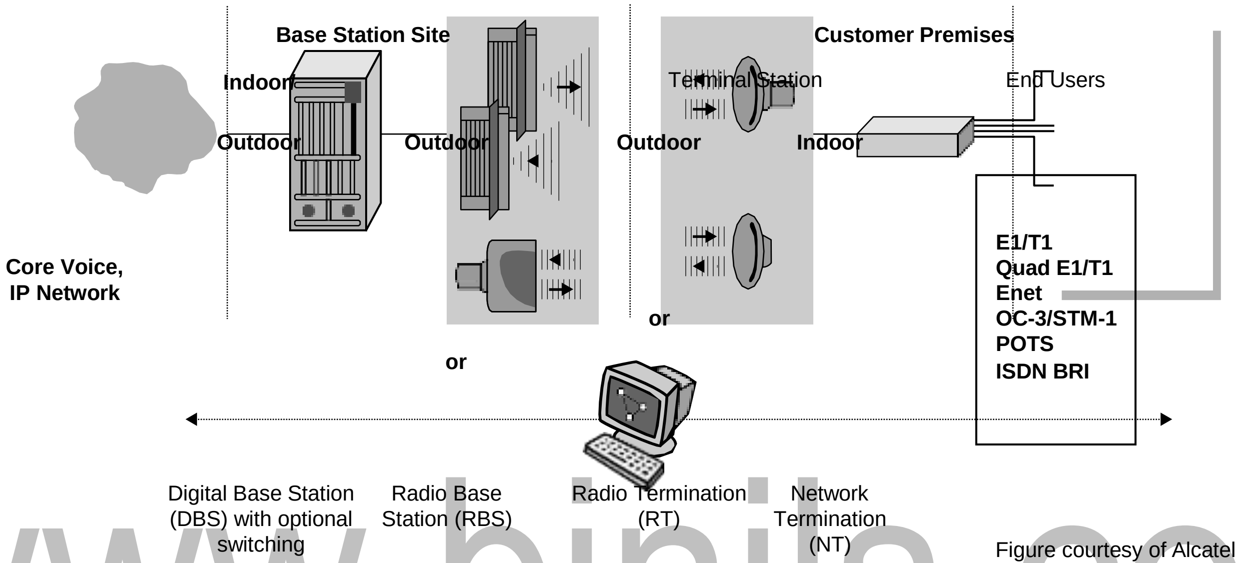


Figure 4.16: Local Multipoint Distribution Service

LMDS transmissions are strictly line-of-sight. For this reason, carriers are apt to target business districts where rooftop mounting of subscriber dishes is permissible. LMDS services are permitted at a number of frequencies: 24 GHz, 28 GHz, 31 GHz, 38 GHz, and soon 40 GHz. The 28 GHz region has a spectrum allocation of 1.3 GHz, and currently offers the greatest potential for bundling diverse services. The capacity of 28 GHz LMDS, consisting of three bands — 27.5 to 28.35 GHz, 29.10 to 29.25 GHz, and 31.0 to 31.5 GHz — is such that the sys- tem can accommodate high-speed Internet access.

Other applications of LMDS include multiple virtual private networks for corporations and government agencies or ATM telephony and streaming video, including video broadcasting. LMDS is seen primarily as a data pipe. LMDS opera- actors have plans for supporting all kinds of corporate network services, including secure file transfer and messaging within a virtual LAN context, video conference- in, and IP telephony. In LMDS, a data access scheme can be FDMA, TDMA, or CDMA. The typical data rate of LMDS is 45 Mbps.

Advantages of LMDS for broadband are:

- Lower entry/deployment costs than wire line
- Ease/speed of deployment
- Fast realization of revenue (resulting from rapid deployment)
- Scalable architecture (demand-based build-out)
- No stranded capital when customers leave
- Cost-effective network maintenance, management, and operations

The IEEE 802.16.2 standard focuses on the coexistence of a fixed broad- band wireless access (BWA) system with other wireless systems and provides rec- commendations for the design and coordinated deployment of fixed broadband wireless access systems in order to control interference ailitate

Coexistence. IEEE 802.16.2 analyzes appropriate coexistence scenarios and provides guidance for system design deployment, coordination, and frequency usage. IEEE 802.16.2 covers 2 to 66 GHz frequencies, with a detailed emphasis on 3.5, 10.5, and 23.5 to 43.5 GHz frequencies.

The following are the present IEEE 802.16 standards:

- *P802.16a*: 2–11 GHz licensed band; addresses point-to-multipoint BWA systems, OFDM, and single-carrier systems
- *P802.16b:* license-exempt bands, with focus on 5–6 GHz; wireless high-speed unlicensed metropolitan area network (HUMAN), OFDM
- *P802.16.2*: focuses on 2–11 GHz frequency band and the coexistence of BWA systems

Multichannel Multipoint Distribution System Multichannel multipoint distribution service (MMDS) is a new technology for wireless access — particularly useful for the Internet (see Figure 22.19). MMD signals have longer wavelengths than that of LMDS and can travel farther without losing significant power. MMDS signals do not get blocked easily by objects and are less susceptible than LMDS to rain absorption. Repeater stations can be used to redirect MMDS signals. With MMDS, a transmitting tower placed at a high elevation can reach customers within a 35-mile radius who have receiving dishes on the side or roof of the building. Several service providers consider MMDSa technology they can use to reach local customers without negotiating access agreements with regional operating companies. LMDS, in contrast to MMDS, covers a smaller radius (only up to 5 miles) and is more expensive to deploy.

MMDS has a narrow spectrum allocation (2.5 to 2.7 GHz in the United States); hence, it has a slower data rate compared to LMDS. The typical data rates of MMDS are 0.5 to 3 Mbps. The access schemes in MMDS are FDMA, TDMA, OFDM, or CDMA. Most of the MMDS are line-of- sight systems, but a non-LOS system is possible. The network topology for MMDS can be either point-to-point or point-to-multipoint. Transmission power used in MMDS is usually in the 1- to-100-watt range, which is substantially below the transmission power requirements of VHF and UHF terrestrial broadcasting stations.

MMDS-favored cell architecture is a single, large microcell. While multicell deployments have been implemented, they are generally not efficient. The reason for this is twofold. The 2.5-GHz frequency band requires either large antennas, which are not well-received consumer client receivers, or smaller antennas with avery broad beam. Often smaller, low-cost antennas are used. The consequence is that multipath is induced, due to reflections of the signal associated with broad antenna beams. This in turn requires that the access method provide significant immunity to the effects of multipath.

In the single cell MMDS deployment, the available bandwidth is limited to the frequency band licensed, which is equal to or less than 200 MHz total. Using this limited bandwidth for two-way, interactive Internet access is certainly feasible, but does not produce broadband access to any reasonably sized population base. However, the use of data casting, which exploits the multiplying effect of data multicast and broadcast, can provide a cost-effective and easily deployed model. The MMDS model is dramatically affected by the combination of bandwidth limitations, propagation characteristics, and the resulting impact of preferred modulation type. Table 22.1 provides a comparison of LMDS and MMDS.

[Source: Text book- Wireless Communications and networking, First Edition, Elsevier 2007 by Vijay Garg]

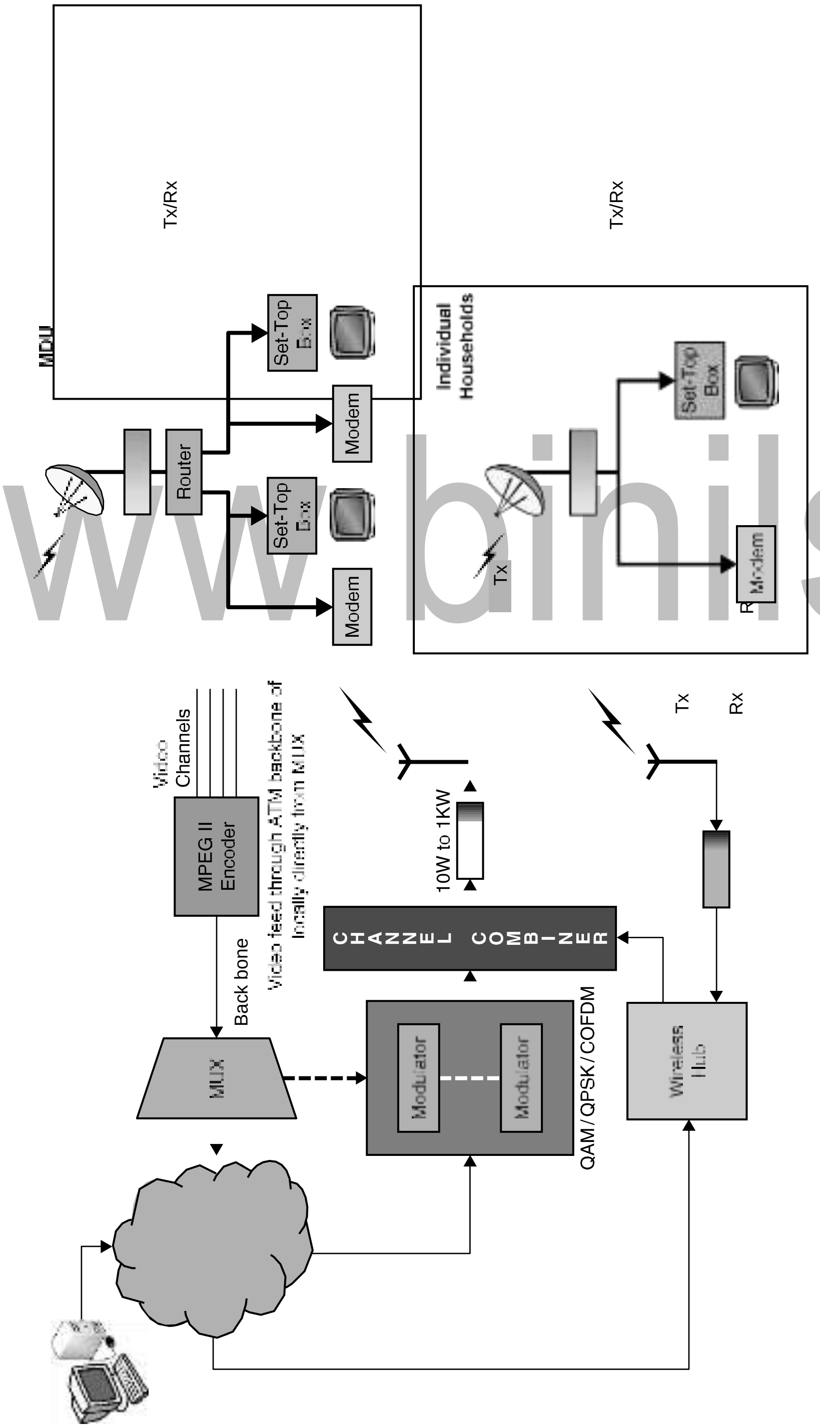


Figure 4.17: Typical MMDS system for digital video and wireless Internet.

Table Comparison of LMDS versus MMDS.

Feature	LMDS	MMDS
Frequency range	28–31GHz (U.S.) 2–42GHz (rest of world)	2.5–2.7 GHz
Propagation characteristics	Good for medium range, LOS, ≤5 miles, free space attenuation	Good for short range, LOS, ≤35 miles, free space attenuation
Favored cell architecture	Multiple, small microcells	Single, large microcell
Impact of cell architecture bandwidth avail-	large Able, which can effectively be increased by decrease- in cell size	Limited bandwidth avail- ability due to no frequency reuse
Ability to support 2-way system architecture	Well suited due to small cell size, large available bandwidth, and highly directive antennas in reason ably small-sized cell	Limited due to bandwidth, antenna characteristics, and propagation characin- touristic
Link pathology	Long range and broad antennas beams ensure significant multipath	Short range and highly directive antennas mean little or no multipath

	te up to 311Mbps	typically 0.5to3Mbps
Access schemes	FDMA, TDMA, CDMA	FDMA, TDMA, OFDM, CDMA
Target market	Large and medium enter- prices	Residential, small enter prices
Customer premises equip-mint costs	High	low to medium

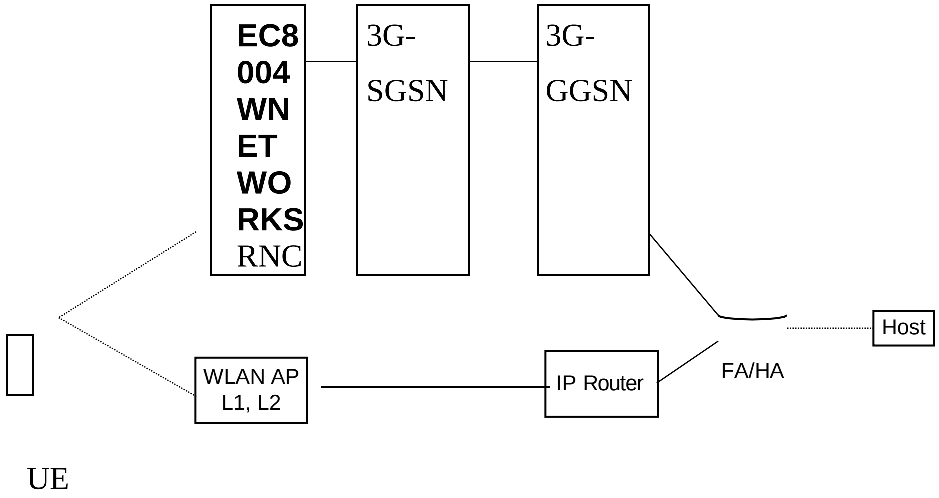
Interworking Schemes to Connect WLANs and3G Networks

Based on the objectives and requirements discussed in the previous section, we present interworking schemes to connect WLANs and 3GPP networks.

Basically, interworking schemes can be categorized as mobile IP approach, gateway approach, and emulator approach. *Mobile IP approach* (called loose coupling approach), introduces mobile IP to two networks. Mobile IP mechanisms can be implemented the mobile nodes and installed on the network devices of 3G and WLANs. This approach provides IP mobility for roaming between 3Gand WLANs. However, this approach requires installing mobile IP devices such as a home agent (HA) and a foreign agent (FA) in both networks, and terminal devices should also implement mobile IP features. Since the user device requires sending the registration back to its home network, packet delay and loss are alsoa problem for handoffs. Moreover, this approach suffers from the triangular routing between networks if mobile IP does not support route optimization.

The *gateway approach* introduces a new logical node to connect two wireless networks.

The new node is located between the two networks and acts as an internal device. It exchanges necessary information between the two networks, converts signals, and forwards the packets for the roaming users. This approach aims to separate the operations of two networks, which implies the two network peer-to-peer networks and can handle their subscriber independently. With the two network operators having a roaming agreement, the logical node helps two networks offer inter sits advantages of this approach are that the two networks can be operated independently; packets for roaming users go through the node without processing by mobile IP; and handoff delay and loss can be reduced .



UE: User

Equipment AP:

Access Point

RNC: Radio Network Controller

3G-SGSN: 3G Serving

GPRS Support Node 3G-

GGSN: 3G Gateway GPRS

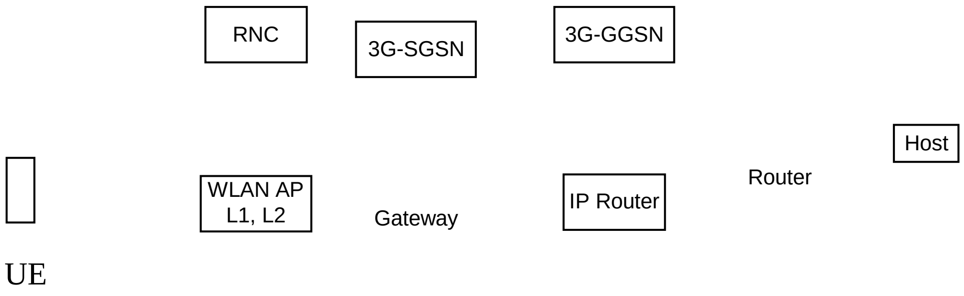
Support Node FA: Foreign

Agent

HA: Home Agent

Figure 4.1: Architecture of the mobile IP approach.

[Source: Text book- Wireless Communications and networking, First Edition, Elsevier 2007 by Vijay Garg]



UE: User
Equipment
AP: Access
Point
3G-SGSN: 3G Serving
GPRS Support Node 3G-
GGSN: 3G Gateway GPRS
Support Node RNC: Radio
Network Controller

Figure 4.2: Architecture of the gateway approach.

[Source: Text book- Wireless Communications and networking, First Edition, Elsevier 2007 by Vijay Garg]

The *emulator approach* (called tight coupling approach), uses WLAN as an access stratum in a 3G network. This approach replaces 3G access stratum by WLAN layer one and layer two. A WLAN access point (AP) can be viewed as a3G network controller or a serving GPRS support node (SGSN). The benefit of this approach is that mobile IP is not required. All packet routing and forward-in are processed by a 3GPP core network. The packet loss and delay can be reduced significantly. However, this approach lacks flexibility since two networks

3G-SGSN: 3G Serving GPRS Support Node

3G-GGSN: 3G Gateway GPRS Support Node

Figure 4.3 Architecture of the emulator approach.

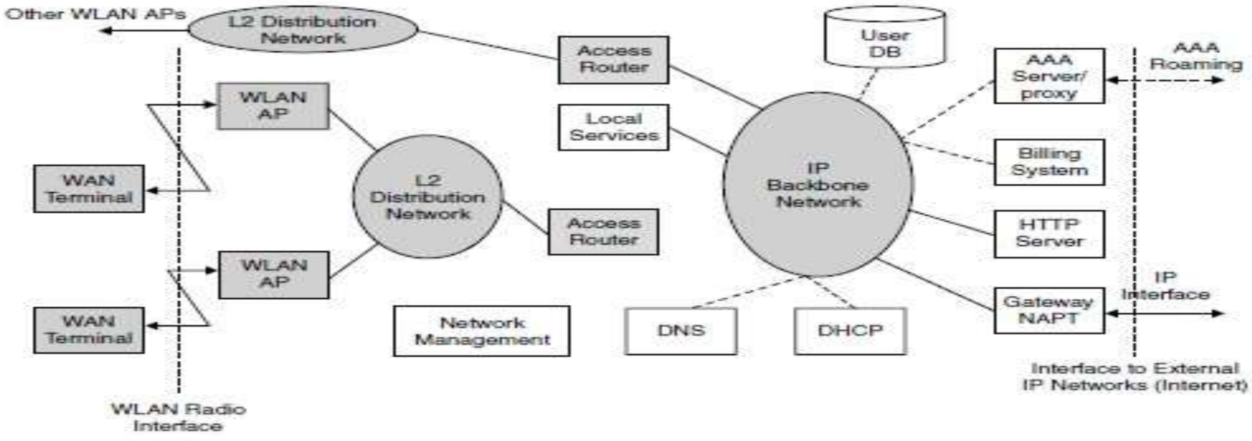
[Source: Text book- Wireless Communications and networking, First Edition, Elsevier 2007 by Vijay Garg]

Are tightly coupled. The operators of two networks should be the same in order to exchange much information. Another disadvantage of this approach is that the gateway GPRS support node (GGSN) will be the single point to the Internet. All packets have to go through the GGSN first. GGSN and the core network be

De Facto WLAN System Architecture

3GPP WLAN interworking architecture design work is focused on the interworking functionality between 3GPP and WLAN systems. To achieve a 3GPP-WLAN interworking architecture that is widely adopted, it is imperative to use the exist- in de facto WLAN access equipment. Unlike the 3GPP system architecture, there is no existing formal standard for a WLAN access network architecture or for a typical public access WLAN system. The WLAN system shown in Figure 22.4 enables IP connectivity between the WLAN terminal and IP networks over its WLAN interface. A *dynamic host configuration protocol* (*DHCP*) server is needed to facilitate configuration of the WLAN terminal's IP stack. A *domain name server* (*DNS*) resolves Internet fully qualified domain name (FQDN) addresses into IP addresses. A Gateway (GW)/network address and port translation (NAPT) is a gateway toward external IP networks such as the Internet. The GW usually also performs IP network address and port translations to enable the WLAN access network operator to use private-space IP addresses inside the WLAN system and enable access to services available outside IP networks at the same time.

A hypertext transfer protocol *(HTTP) server* may offer local application- level service for accessing users. Accounting data is processed in the *billing system server*. The *local services server* is a general box covering services at IP level or



DHCP: Dynamic Host Configuration Protocol
AAA: Authentication, Authorization, and Accounting
DB: Data Base
NAPT: Network Address and Port Translation
DNS: Domain Name Server

Figure 22.4 A de facto WLAN system.

DHCP: Dynamic Host

Configuration Protocol AAA:

Authentication,

Authorization, and Accounting

DB: Data Base

NAPT: Network

Address and Port

Translation DNS:

Domain Name Server

Figure 4.4: A de facto WLAN system.

[Source: Text book- Wireless Communications and networking, First Edition, Elsevier 2007 by Vijay Garg]

Above, such as mail servers and local web content. *Network management* takes care of the management of all network elements at all layers. It is instrumental in network configuration and monitoring.

The WLAN terminal is typically a laptop computer or a personal digital assistant (PDA) with a built-in WLAN module or a PCMCIA WLAN card.

The WLAN AP is mostly a layer 2 bridge between IEEE 802.11 and the Ethernet. The AP can also support IEEE 802.11i/802.1X functionality, in which case it is also a remote authentication dial-in user service (RADIUS) client toward the fixed network and performs radio link encryption toward the WLAN terminal. Access points are attached to *layer 2 distribution* networks such as a switched Ethernet subnet. The layer 2 distribution network may also provide intra-subnet mobility for WLAN terminals. The layer 2 distribution network enables layer 2 connectivity toward the first IP routing device, the *access router* (*AR*). The basic function of AR is to route user IP packets.

Authentication and authorization is one basic prerequisite for providing IP connectivity and other services via a WLAN system. To realize these functions, an authentication, authorization, and accounting (AAA) server and user database are required. An AAA server is typically the RADIUS server used for a WLAN system. The subscribers' user identities such as login names, shared secrets like passwords, and user profiles are stored in the database. The database is accessed from the AAA server over the IP backbone network using lightweight directory access protocol (LDAP) as the de facto standard.

Legacy authentication and authorization is performed using Web browsers. When the user initiates Web browser, its first request is redirected into a WLAN system HTTP server and a landing Web page is displayed. The user is prompted to enter a login name and password. The password can be static, limited time, or even generated ad hoc (using, e.g., Security ID technology). Similarly, users cane prompted to enter their credit card number and pay for the connection out

Establish hinge a more lasting relationship with the WLAN system operator.

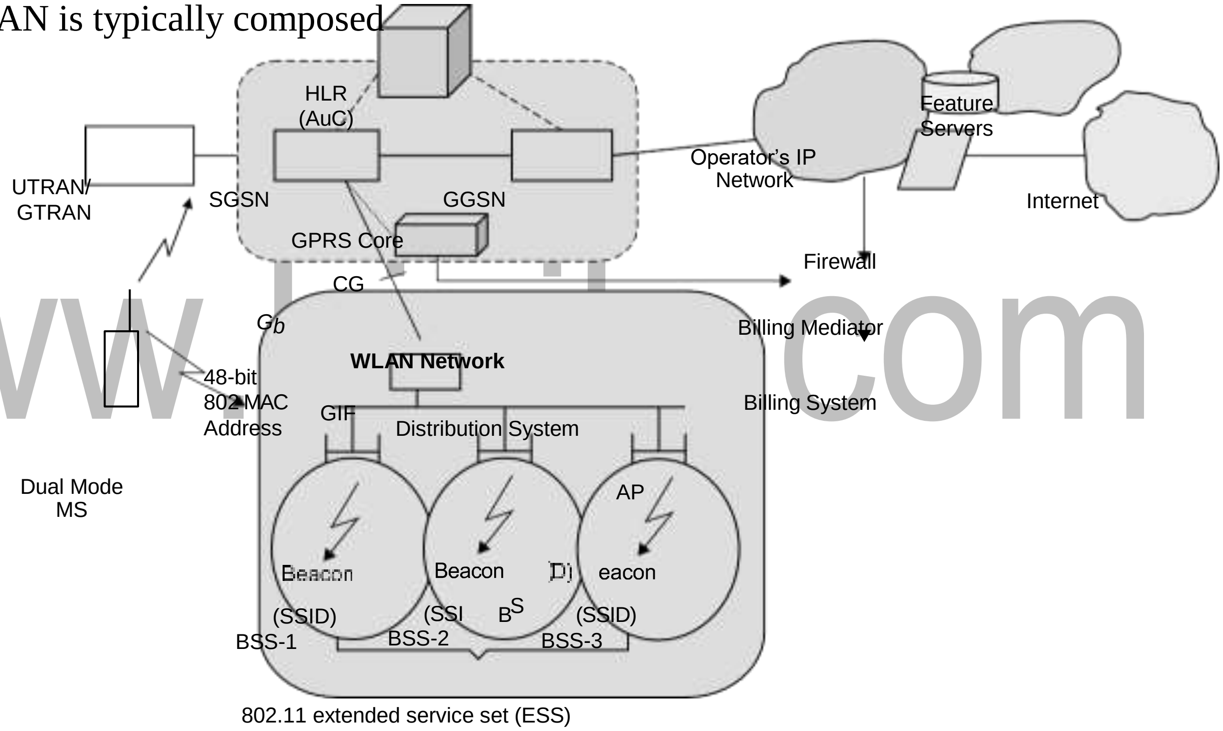
It is also possible to establish a roaming relationship between WLAN systems. Roaming enables a user of a WLAN system to connect to another WLAN system. In this case, the AAA functions are still provided by the user's own WLAN system, while actual WLAN access is provided by other WLAN systems.

Session Mobility

Session mobility may be seen as an evolutionary step from roaming in the integrated environment. Session is defined as a flow of IP packets between the end-user and an external entity; for example, an FTP or HTTP session. We consider a mobile device capable of connecting to the data network through WLANs and 3GPP networks. This could be a laptop with an integrated WLAN-general packet radio service (GPRS) card, or PDA attached to a dual access card. The end-user is connected to the data network and is in a session flow through one access network, say, a WLAN. As the user moves out of the coverage area of the WLAN, the end device detects the failing WLAN coverage and seamlessly switches the flow to the 3GPP network. The end-to-end session remains unaffected. Typically no user intervention would be required to perform the switchover from WLAN to 3GPP. When the user moves back into the coverage of the WLAN system, the flow is handed back to the WLAN.

System Description with Tight Coupling

Figure shows the system architecture with tight coupling. A WLAN is deployed with one or more off-the-shelf access points, which are connected by means of a distribution system. The distribution system is LAN-compliant with IEEE 802.3. The WLAN is deployed in an infrastructure configuration, that is, APs behave like base stations, and mobiles exchange data only with APs. The service area of an AP is called a *basic service set*. Each WLAN is typically composed



GIF: GPRS Interworking FunctionCG: Charging Gateway
HLR: Home Location Register AuC: Authentication Center
SGSN: Serving GPRS Support Node GGSN: Gateway GPRS Support Node BSS: Basic Service Set
AP: Access Point

Figure 4.6: WLAN-GPRS integration with tight coupling system configuration.

[Source: Text book- Wireless Communications and networking , First Edition, Elsevier 2007 by Vijay Garg]

of many basic service sets, which all together form an *extended service set* (*ESS*).

The WLAN network is deployed as an alternative RAN and connects to the GPRS core network through the standard G_b interface. From the core network point of view, the WLAN is considered as other GPRS routing areas (RAs) in the system. The GPRS core network does not identify the difference between an RA with WLAN radio technology and one with GPRS radio technology.

The key functional element in the system is the *GPRS interworking function* (*GIF*), which is connected to a distribution system and to an SGSN via the standard G_b interface. The main function of the GIF is to provide a standardized interface to the GPRS core network and to virtually hide the WLAN particularities. The GIF is the function that makes the SGSN consider the WLAN a typical routing area.

The existing GPRS protocols in mobile are fully reused. The LLC, subnet-work dependent convergence protocol (SNDCP), GPRS mobility management (GMM), and session management are used in both a standard GPRS cell and a WLAN area. Therefore, the WLAN merely provides a new radio transport for these protocols.

When a mobile station (MS) is outside the WLAN area, its WLAN interface is in passive scan mode, that is, it scans a specific frequency band and searches for a beacon signal. When a beacon is received the service set identifier (SSID) is checked and compared against a pre-configured SSID. The SSID serves as a WLAN identifier and can help mobiles attach to the correct WLAN. For example, an operator could use a unique SSID and request that its subscribers configure their mobiles to consider only this SSID valid.

When an MS detects a valid SSID, it performs the typical authentication and association procedures. It then enables its WLAN interface, and further signaling is carried over this interface.

Mobile stations are dual mode, that is, they support both GPRS and WLAN access in a seamless fashion. System mobility is achieved by means of the routing area update (RAU) procedure, which is the core mobility management procedure in GPRS. Typically, when a mobile enters a WLAN area, an RAU procedure takes place, and subsequent GPRS signaling and user data transmission are carried over the WLAN interface. Similarly, when the mobile exits a WLAN area, another RAU procedure takes place, and the GPRS interface is enabled and used to carry further data and signaling traffic. From the core network point of view, handoff between WLAN and GPRS is considered handoff between two individual cells.

Mobile stations in the WLAN send uplink GPRS traffic to the MAC addressof GIF; similarly, downlink GPRS traffic is sent from the GIF to the MAC addresses of mobile stations (see Figure 22.6). The MS has two radio subsystems, one for GPRS access and another for WLAN access (refer to Figure 22.7). The WLAN adaptation function (WAF) identifies when the WLAN radio subsystem is enabled (i.e., when the MS associates with a valid AP) and informs the LLC layer, whichsubsequently redirects signaling and data traffic to the WLAN. Note that all standard GPRS protocols operating on top of the LLC (SNDCP, GMM, SM) function as usual and do not identify which radio subsystem is used. WAF is a key component in a mobile station.

Protocol Stack

The MS supports two radio subsystems (or interfaces) for transporting GPRS signaling and user data (see Figure 22.8). The first interface is implemented with the GPRS-specific radio link control (RLC)/MAC and physical layers, whereas the second interface is implemented with 802.11- specific MAC and physical layers. These two interfaces provide two alternative means for transporting LLC packet data units (PDUs). Typically, when the MS is outside a WLAN area, LLC Desire transmitted over the GPRS interface (U_m). However, when the mobile enters a WLAN area, LLC PDUs are transmitted over the WLAN interface. This switching is performed with the help of WAF and could be completely transparent to the user and to the upper GPRS layers.

The WAF operates in both MS and GIF. It provides an adaptation function for interworking between LLC and 802.11 MAC (in the mobile) and between 802.3 MAC and BSSGP (in GIF). The GIF also implements the GPRS proto- cols specified on G_b interface, frame relay (FR), network service (NS), and base station subsystem GPRS protocol (BSSGP).

WLAN Adaptation Function

The WAF is implemented in every dual mode MS and in the GIF. It supports the appropriate interworking functions. With the aid of WAF it becomes feasible to transport GPRS signaling and data over 802.11 WLANs. The WAF provides the following functions:

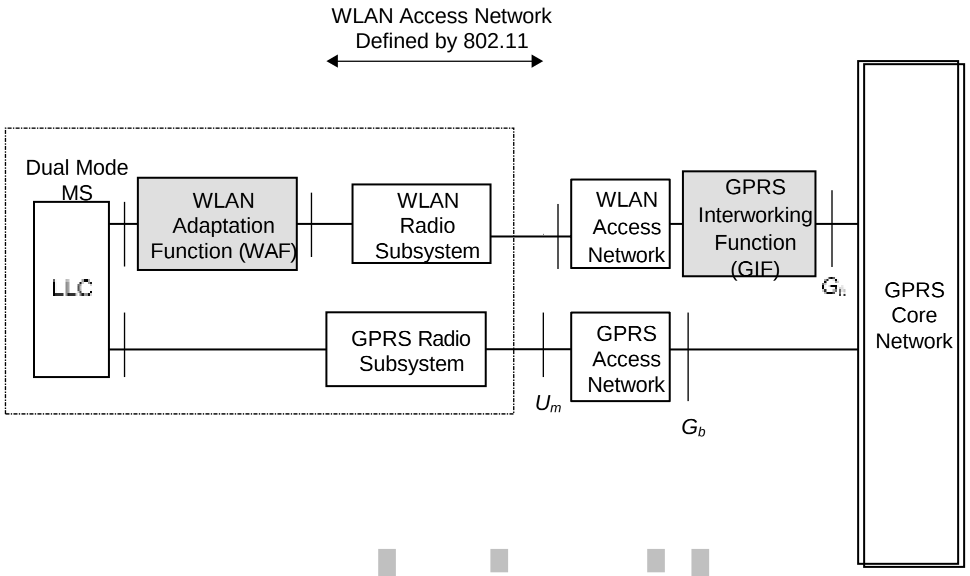


Figure 4.7 Tight coupling over G_b interface: a reference diagr**[Source: Text book-** Wireless Communications and networking , First Edition, Elsevier 2007 by Vijay Garg]

- It signals the activation of the WLAN interface when a mobile enters a WLAN area. It also signals the change of RA to GMM when a mobile enters a WLAN area and gets associated with an AP.

It supports the GIF/RAI discovery procedure, which is initiated by MSs in order to discover the MAC address of GIF and the RA identity (RAI) of the WLAN. It supports the paging procedure on G_b, used when SGSN needs to page an MS. During this procedure, WAF sends an appropriate signaling message to MS in order to alert it and respond to page. It transfers uplink LLC PDUs from MS to the GIF by using the transport services provided the 802.11 MAC. It also transfers downlink LLC PDUs from the GIF and in

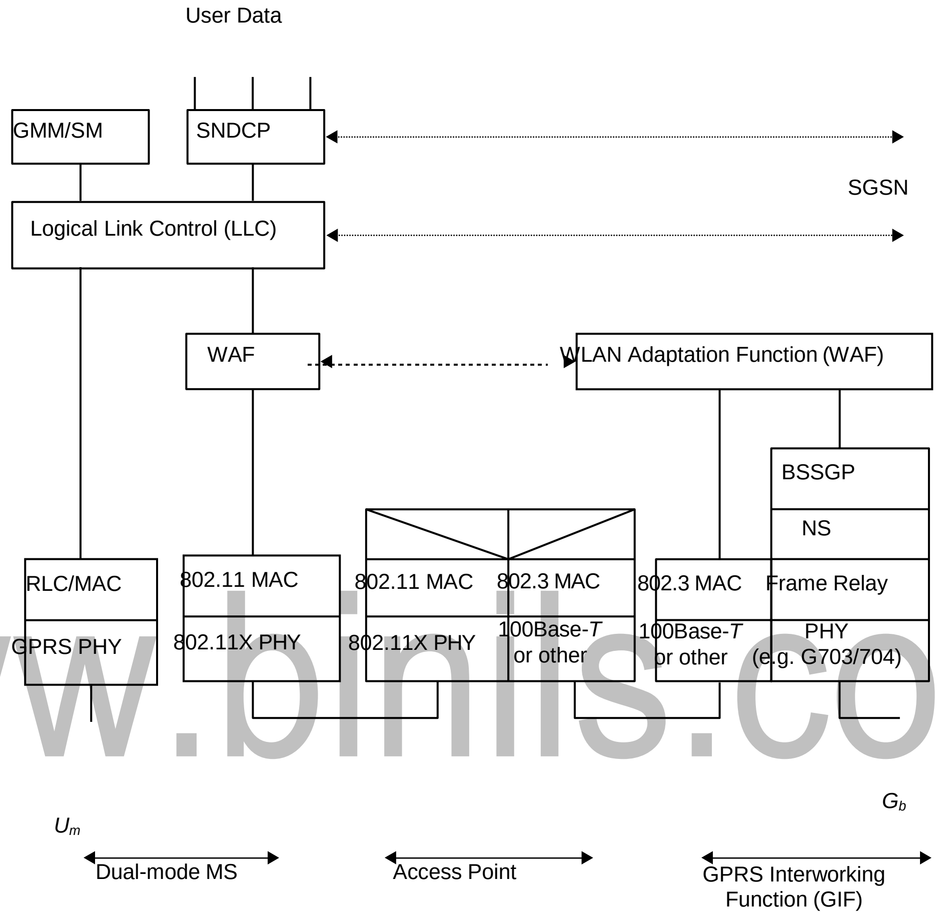


Figure 4.8: Protocol stack for tight coupling over GB *interface*. **[Source: Text book-** Wireless Communications and networking, First Edition, Elsevier 2007 by Vijay Garg]

It supports QoS by implementing transmission scheduling in the GIF and in the MS.

It transfers the temporary logical link identifier (TLLI) and QoS information in the WAF header. The TLLI is a temporary MS identifier used by the LLC layer for addressing purposes.

The encapsulation scheme used in the uplink direction as well a WAF PDU, which includes the TLLI and QoS in the header. The TLLI is used by the GIF to update an internal mapping table that correlates TLLIs with 802 MAC addresses. In order to support the paging procedure, the GIF also needs to correlate IMSIs with 802 MAC addresses. The correlation between TLLIs and 802 MAC addresses is used for forwarding downlink LLC PDUs received on the G_b interface to the correct mobile on the WLAN. Note that the SGSN uses the TLLI

These QoS attributes are primarily used for scheduling in the MS and GIF. In the downlink direction, the QoS may be empty, since there is no need to transfer any QoS parameters to the mobile. The 802.11 and 802.3 MAC headers are the standard headers specified by the 802.11 and 802.3 standards, respectively.

on G_b as address information, whereas the WLAN uses 802 MAC addresses. Inthe uplink direction, QoS contains the following attributes:

- Peak throughput
- Radio priority
- RLC mode

GIF/RAI Discovery Procedure

GIF/RAI discovery is a key procedure carried out immediately after an MS enters an 802.11 WLAN area and gets associated with an AP. The WAF in the MS initiates this procedure:

- To discover the 802 MAC address of GIF. All uplink LLC PDUs are

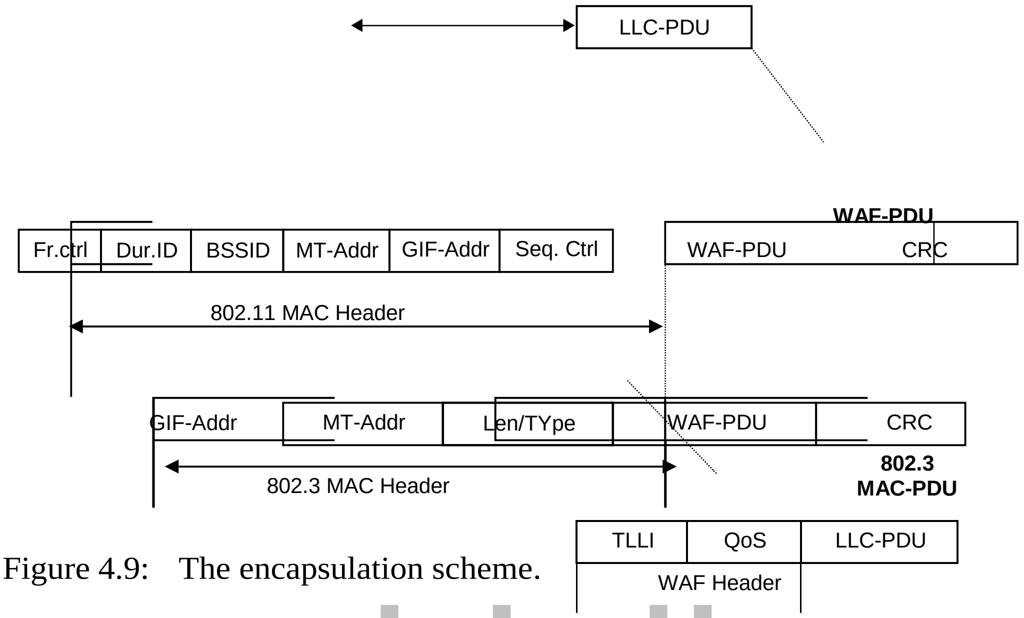


Figure 4.9: The encapsulation scheme.

[Source: Text book- Wireless Communications and networking , First Edition, Elsevier 2007 by Vijay Garg]

- To discover the RAI that corresponds to the WLAN network.
- To send the MS’s IMSI value to GIF. This value is subsequently used by the GIF to support the GPRS paging

Figure shows the signaling flow during the GAF/RAI procedure. The procedure is initiated after the 802.11 MAC layer is enabled (i.e., after the mobile gets associated with a particular AP). The WAF layer in an MS sends a request to

802.11 MAC to transmit a PDU with a source address (SA) equal to MS’s MAC address and a destination address equal to *broadcast*. This PDU is a

GIF/RAI *dis- cover request* message that includes the IMSI value of the MS. The 802.11 MAC layer transmits an 802.11 MAC PDU with the appropriate address information(designated Addr1, Addr2, Addr3). Note that this PDU is directed to the AP with identity BSSID. The AP broadcasts this message to the MS and is finally received by the GIF, which associates the IMSI with the MS's 802.11 MAC address (desig- nated MS). Subsequently, the WAF in the GIF responds with a GIF/RAI discover response that includes the RAI of the WLAN. The MS receives this response, stores the GIF address and the RAI, and notifies the GMM layer that the currentGPRS RA has changed. In response, the GMM layer initiates the normal GPRS RAU procedure and notifies the SGSN that the MS has changed RA. After that, normal GPRS data and signaling is performed over the WLAN.

It should be noted that, with the aid of WAF, MSs can seamlessly move between WLAN and GPRS radio access and use the normal GPRS procedures for mobility management.

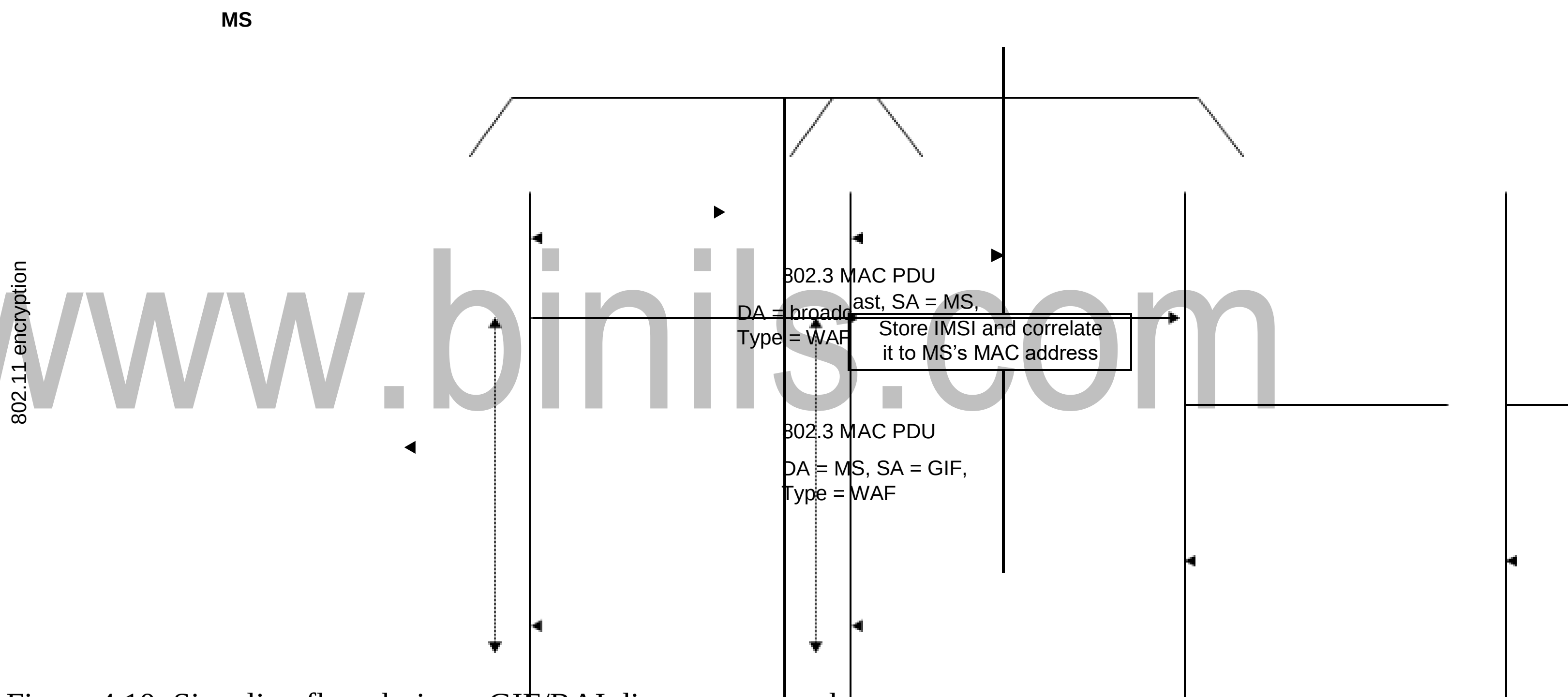


Figure 4.10: Signaling flow during a GIF/RAI discovery procedure.

[Source: Text book- Wireless Communications and networking , First Edition, Elsevier 2007 by Vijay Garg]

System Description with Loose Coupling

Figure shows the system architecture with loose coupling. The WLAN is coupled with the GPRS network in the operator's IP network. Note that, in con- trast to tight coupling, the WLAN data traffic does not pass through the GPRScore network but goes directly to the operator's IP network. In this architecture, SIM-based authentication can be supported in both the GPRS network and the WLAN to gain access to the operator's services. The architecture also supports integrated billing, via the billing mediator, in a common billing system. The WLAN may be owned by a third party, with roaming/mobility enabled via a dedi- cated connection between the operator and the WLAN, or over an existing public network, such as the Internet.

Loose coupling utilizes standard IETF-based protocols for authentication, accounting, and mobility. Roaming can be enabled across all types of WLAN imple- mentations, regardless of who owns the WLAN, solely via roaming agreements.

The WLAN access network connects to the GPRS data network like a different type of radio access network for interworking. This allows for the sup- port of the legacy WLAN access networks, which commonly support RADIUS/ DIAMETER protocols in the WLAN access network. This approach defines some new interfaces with well-defined functions and commonly used protocols. The new interfaces are discussed below (see Figure 22.17).

- ***W_b/W_r* interface.** This interface connects the WLAN access network with the visited 3GPP data network or the home 3GPP data network. The W_r interface transports authentication, authorization, and other related information. The W_b interface transports charging related information. The W_r interface logically connects the WLAN capable user to the AAA server, which resides in the cellular operator home network. The WLAN capable user is authenticated and authorized by the AAA server. The WLAN related subscription information for the user are stored in home location register/home subscriber server (HLR/HSS). The extensible authentication protocol (EAP) is used for this purpose between the WLAN capable user and the AAA server. To accommodate the existing WLAN access networks, which support RADIUS or DIAMETER, the W_r/W_b interface uses DIAMETER protocol toward the AAA server. The principle of authentication is mutual authentication. Two methods of mutual authentication are currently defined, EAP/SIM and EAP/AKA. The EAP/AKA is used for subscribers with USIM and EAP/SIM is used for subscribers with SIM. The existing SIM subscribers' authentication in cellular networks is not based on mutual authentication. This is the reason that the authentication methods are different for SIM- and USIM-based WLAN users.

- ***W***

- **W_n interface.** This interface transports tunneled WLAN user data toward the packet data gateway in the home network and vice versa. The W_n interface is used to transport tunneled data between the home packet data gateway in the home network and the visited data border gateway in the visited network if the WLAN access network is not directly connected to the home network. It is also possible that the packet data is directly routed by the WLAN accessnetwork to the external IP network. This is the reason that this interface is ser-vice specific. If the packet data is routed by the packet data gateway then thereare two ways of transporting the user packet data to the packet data gateway. One method is to establish a secure tunnel between the WLAN access network and the packet data

Gateway. This method is called network based tunneling as the WLAN user is not involved. The other method establishes a direct secure tunnel between the WLAN user client and the packet data gateway. This method is referred to as client based tunneling. The W_{ry} interface is used to inform the WLAN access network about tunneling related information.

***W_x* interface.** This interface connects the AAA server with HLR/HSS. The AAA server retrieves the authentication vectors over this interface from the HLR/HSS. The AAA server also retrieves the WLAN access-related sub- scriber information using this interface. This interface is also used by the AAA server to register itself for an authorized WLAN-capable user with the HLR/HSS. This interface also helps the AAA server to get an indication of subscription-related changes from the HLR/HSS. The AAA server generates temporary identifiers for the WLAN user for security. The temporary identi- fiers are used as far as possible over the WLAN radio access network by the WLAN user. This interface is quite similar to the mobile application part (MAP) G_r interface defined between SGSN and HLR/ HSS. This interface is based on the MAP or DIAMETER protocol.

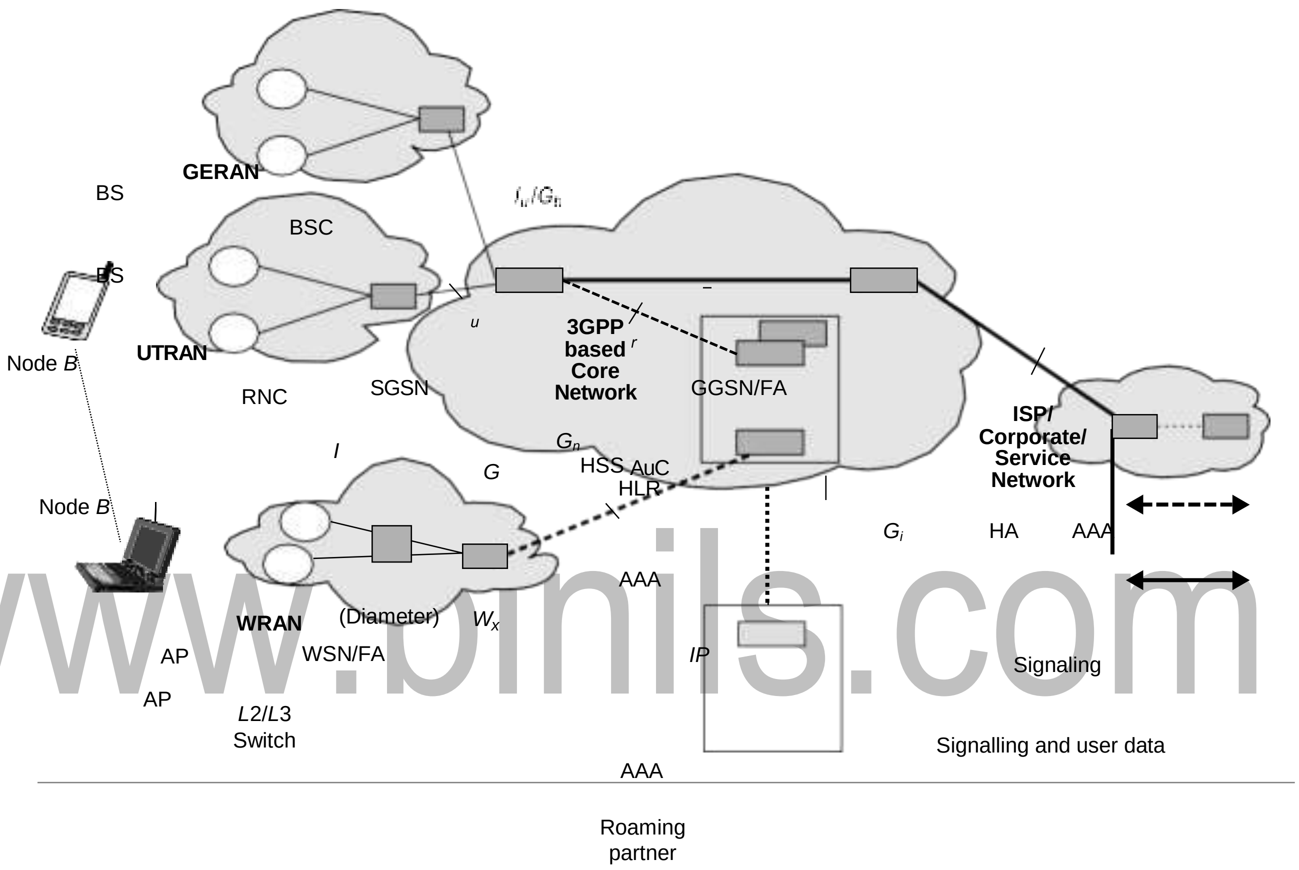


Figure 4.11: WLAN-GPRS integration using loose coupling.

[Source: Text book- Wireless Communications and networking, First Edition, Elsevier 2007 by Vijay Garg

- ***W**$_f$* **interface.** This interface connects the AAA server with the 3GPP charging control function or charging gateway function. This interface transports charging data toward the 3GPP charging control/gateway function. The charging data is collected by the AAA server from either the packet data gateway over the *W$_e$* interface or the *web* interface from the WLAN access network or both. This interface is based on DIAMETER or GPRS tunneling protocol (GTP).
- ***W**$_O$* **interface.** This interface connects the AAA server with the 3GPP on-line charging system for credit control checks for the WLAN-capable user. This interface is based on DIAMETER protocol.
- ***W**$_m$* **interface.** This interface connects the AAA server with the packet gate- way for transport of charging, related information and tunneling related information to the AAA server from packet data gateway. This interface is based on DIAMETER protocol.
- ***W**$_i$* **interface.** This interface connects the packet data gateway with the packet data network. The packet data network may be an external public or private data network or an operator's internal packet data network. The protocol for this interface is dependent upon the packet data network.

Authentication

An authentication similar to GPRS may occur within the WLAN, depending on the implementation. Where the GPRS operator owns the WLAN, it is likely thatthe operator will reuse SIM-based authentication or 3GPP-based USIM au then citation for UMTS subscribers within the WLAN environment. Similarly, for a subscriber to access services provided by a GPRS operator over any WLAN access network, regardless of whether the WLAN is owned by a GPRS opera- tor, (U)SIM-based authentication can be used. To reuse 3GPP subscription, 3GPP interworking WLAN terminals will need access to UICC smart cards with SIM/ USIM applications. A WLAN equipped with a SIM/USIM smart card is called WLAN UE. Given the need for dual-mode (WLAN-cellular) UEs, SIM/USIM will be available in those UEs. The architecture of interworking WLAN access reusing 3GPP USIM/SIM and HSS is shown in Figure 22.12. The authentication procedure shown in Figure 22.13 is based on the deploy-mend of IEEE 802.1X with 802.11. The cellular access gateway provides the AAA server functionality in the cellular operator’s IP core. The access gateway interworks with the home location register (HLR) to obtain the authentication parameters used to create the authentication challenge to the UE and validate the response to the challenge.

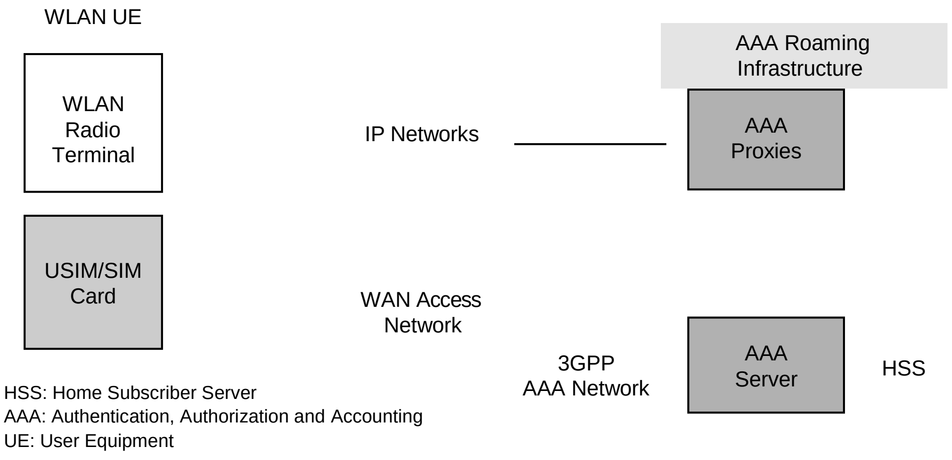


Figure 4.12: WLAN system architecture reusing the 3GPP subscription.

[Source: Text book- Wireless Communications and networking, First Edition, Elsevier 2007 by Vijay Garg]

The authentication process starts after the UE has associated with an AP. The UE sends an EAP-Over-WLAN (EAPOW) Start message to trigger the initiation of 802.1X authentication. In steps 2 and 3 the identity of the UE is obtained with standard EAP-Request/Response messages (see Figure 22.13). Next, the AP initiates a RADIUS dialog with the access gateway by sending an Access-Request message that contains the identity reported by UE. In the SIM-based authentic- ton, this identity typically includes the IMSI value stored in the SIM card. The access gateway uses IMSI and other information included in the identity (i.e., a domain name) to derive the address of the HLR/HSS that contains subscription data for that particular UE. In steps 5 and 6, the access gateway retrieves one or more authentication vectors from every authentication vector. In steps 7 and 8, the random challenges sent to the UE, which runs the authentication algorithm implemented in the (U) SIM card and generates a challenge response value (SRES). In steps 9 and 10, SRES is transferred to the access gateway and compared against the corresponding XRES value received from the HSS. If these values match, a RADIUS Access-Accept is generated in step 11 (otherwise, a RADIUS Access- Reject is generated). This instructs AP to authorize the 802.1X port and allow subsequent data packets from the UE. Note that the RADIUS Access-Accept mes- sage may also include authorization attributes, such as packet filters, which are used for controlling the user's access rights in the specific WLAN environment.

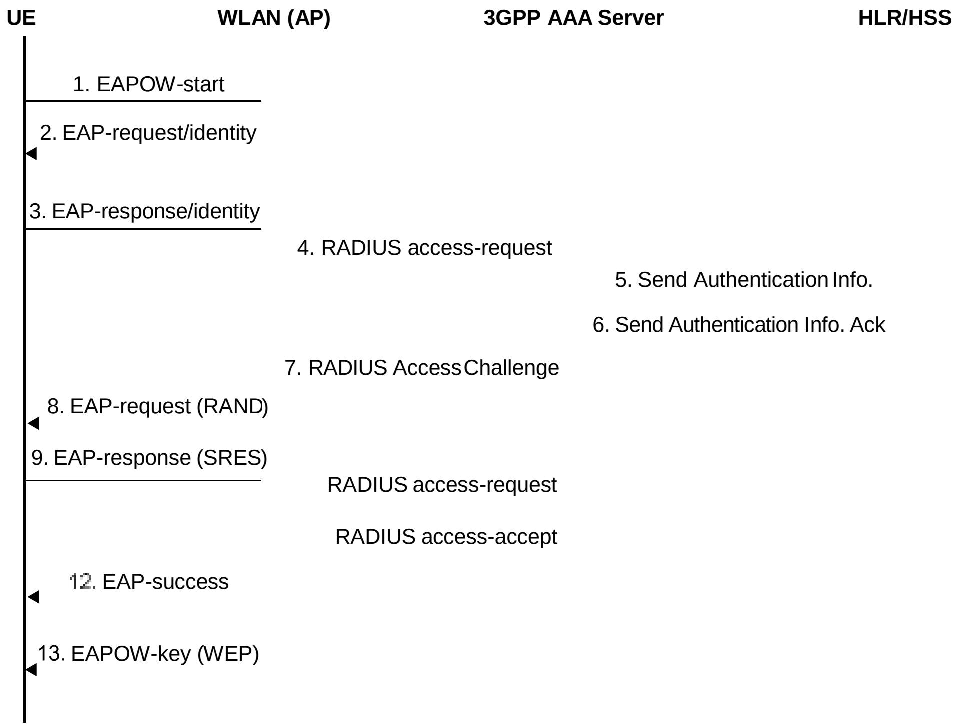


Figure 4.13: SIM-based authentication over WLAN.

[Source: Text book- Wireless Communications and networking, First Edition, Elsevier 2007 by Vijay Garg]

Note that the authentication and authorization in the above procedure is controlled by UE’s home environment (i.e., home GPRS network). The AP in the visited WLAN implements 802.1X and RADIUS but relies on the HSS in the home environment to authenticate the user. Figure 22.14 shows the protocol architecture for the authentication process.

The WLAN access network is connected to a 3GPP AAA proxy via the W_r reference point. The W_r reference point is used for authentication and key agreement signaling, and the protocols in this reference point are extensible authentication protocol (EAP) over DIAMETER or RADIUS. 3GPP AAA proxy forwards authentication signaling between the WLAN access network and the 3GPP AAA server over the W_s reference point. The 3GPP AAA

Server verifies if the subscriber is authorized to use WLAN. The authorization information and authentication vectors needed in the authentication protocols are stored by the HSS. After the user has been successfully authenticated and authorized for network access, the WLAN access network grants UE access to an IP network.

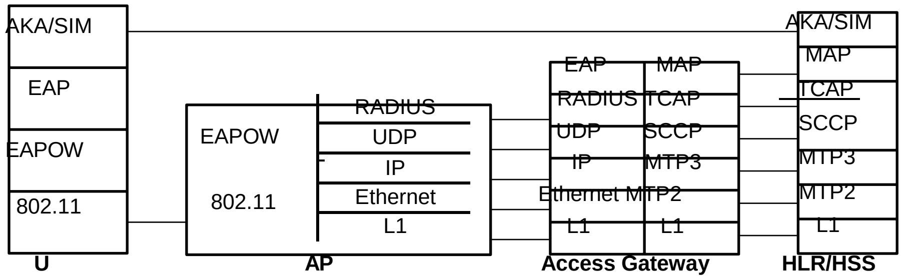
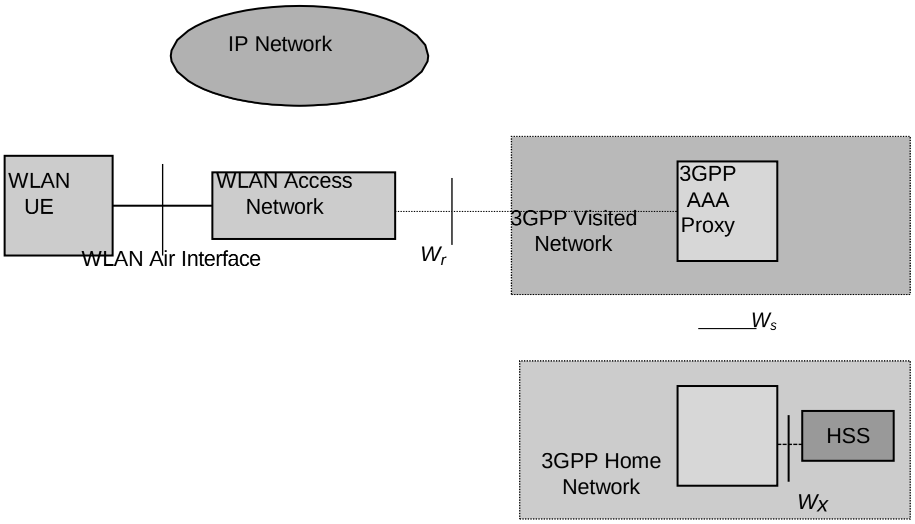


Figure A loosely coupled WLAN control plane for authentication.



HSS: Home Subscriber Server
AAA: Authentication, Authorization, and Accounting
UE: User Equipment

Figure 4.14: 3GPP-WLAN interworking, authentication, ad roaming architecture.

[Source: Text book- Wireless Communications and networking, First Edition, Elsevier 2007 by Vijay Garg]

User Data Routing and Access to Services

The IP network selection is based on a parameter called WLAN access point name (W-APN) similar to the APN parameter used in GPRS. The UE indicates the desired IP network with W-APN. The network authorizes the request, or very- files that the user has the right to use the W-APN. After selecting the IP network, appropriate tunnels are established to route the user data to the selected IP net- work. The tunnel is terminated in the home operator packet data gateway (PDG). The PDG is similar to the GGSN used in GPRS. The W_i reference point between the PDG and the remote network is similar to the G_i reference point used between GGSN and the remote IP networks in GPRS. In the visited 3GPP network, the WLAN access gateway (WAG) is required to implement tunneling. The reference points W_{in}, W_p, W_u, and W_i are used to convey the user data plane, and W_g andW_m are used for control.

3GPP-based Charging for WLAN

The WLAN charging architecture is shown in Figure. Charging informal-ton about WLAN is collected at the WLAN access network and forwarded tithe 3GPP visited and home networks. The AAA server in the home 3GPP net-work authorizes each user's access to a WLAN. Before authorizing a prepaid user to access the WLAN for direct Internet access, the 3GPP AAA server makes a credit reservation from the user's prepaid amount in the OCS (online charging system) over the W_o reference point. The 3GPP AAA server monitors the received accounting information from the WLAN access network. When the downloaded credit is exhausted a new credit request from OCS is triggered to cover the forth- coming accounting reports from the WLAN access network. At the termination of theWLAN

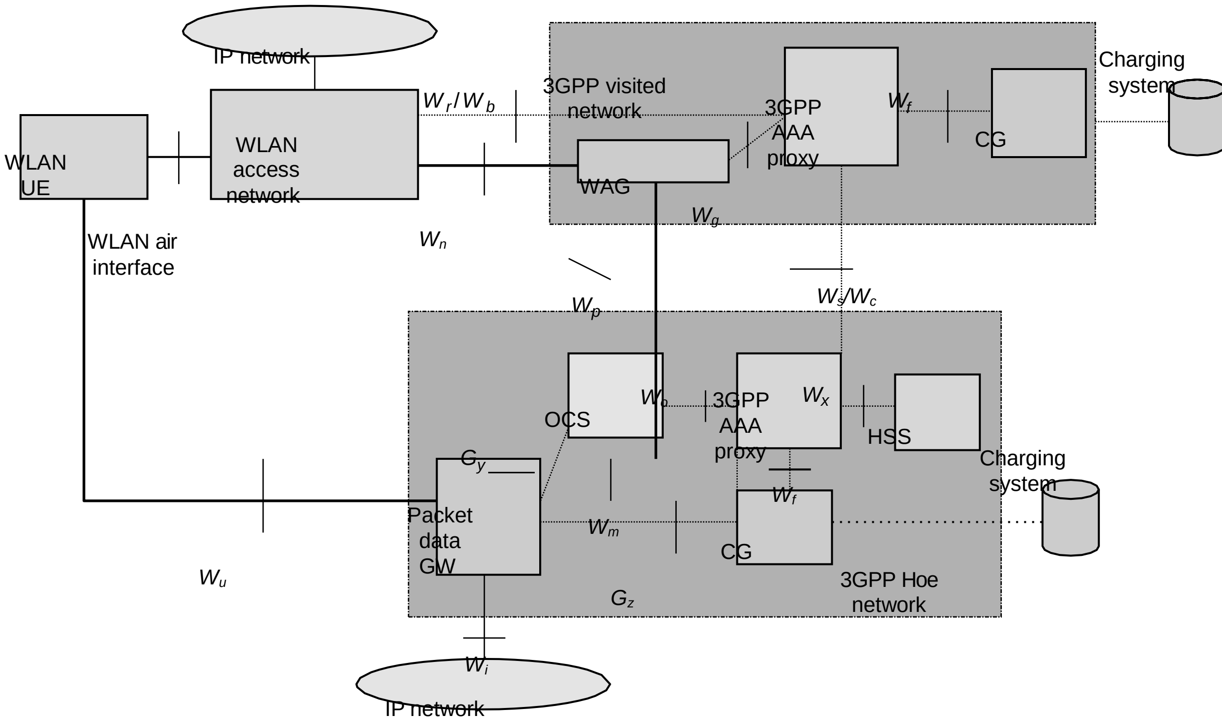
Connection, the 3GPP AAA server returns any unused credit backto the OCS.

After authorization to access the WLAN access network is completed, a user-specific accounting session is established between the WLAN access network and the 3GPP home network. The accounting session is established with standard AAA accounting signaling, and the reference point for this signaling is W_b. At the establishment of the accounting session the 3GPP AAA server indicates to the WLAN a suitable set of accounting criteria, such as an accounting unit (e.g., amount of transferred kilobytes) and reporting threshold to be utilized. After the accounting session establishment the WLAN collects accounting information and reports it to the 3GPP AAA server over the W_b reference point.

All associated IP flows traverse through the PDG; thus, more accurate and service-specific charging information can be collected at the PDG. The resource consumption by each IP flow can be monitored and collected internally at the PDG. For charging of the traversing IP flows, the PDG is also connected to the OCS by the G_y reference point and to the CG (charging gateway) by the G_z ref- erence point. At the establishment of a certain IP flow via the PDG, the PDGrequests credit for IP flow charging from the OCS over the G_y reference point in a similar way as the 3GPP AAA server does over the W_o reference point for WLAN access charging.

Session Mobility

In the loose coupling, mobile IP is used to provide session mobility across GPRS and WLAN. This is in contrast to the tight coupling approach in whichthe GPRS mobility management procedure is used. When the UE moves from



CG: Charging Gateway

OCG: On line Charging System

Figure 4.15: Charging infrastructure and reference points in the 3GPP-WLAN interworking architecture.

[Source: Text book- Wireless Communications and networking , First Edition, Elsevier 2007 by Vijay Garg]