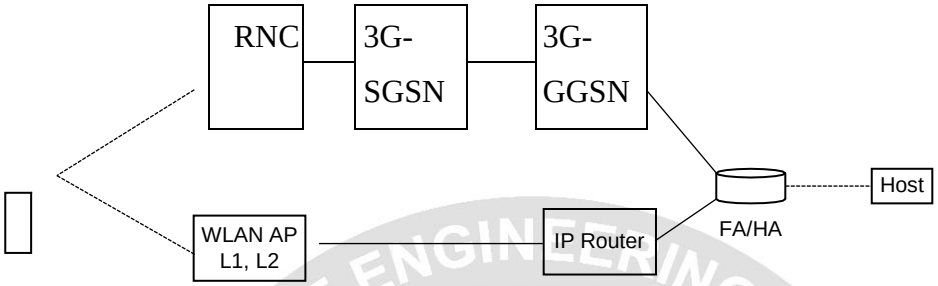
Interworking Schemes to Connect WLANs and3G Networks

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 cou pling approach), introduces mobile IP to two networks. Mobile IP mechanisms can be implemented in the mobile nodes and installed on the network devices of 3G and WLANs. This approach provides IP mobility for roaming between 3G and 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 also a 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 networks are 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 intersystem roaming. The 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

UE: User Equipment AP: Access Point

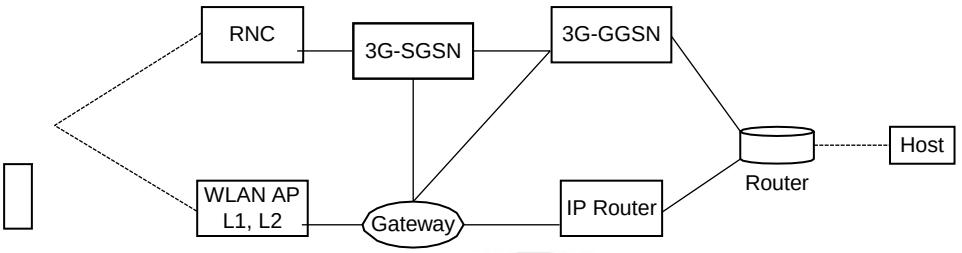
RNC: Radio Network Controller

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]

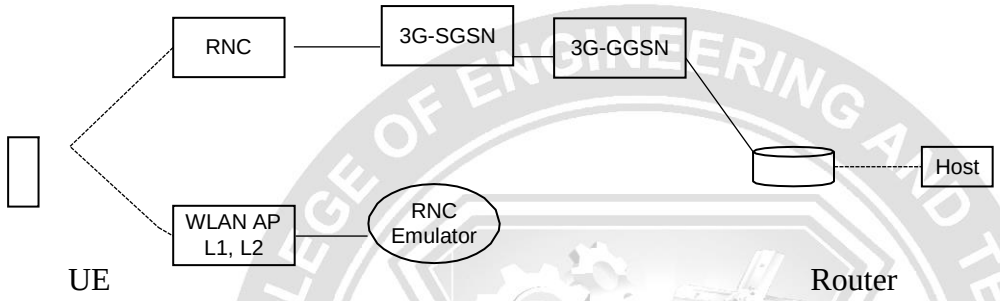


UE: User Equipment
AP: Access Point
3G-SGSN :3G Serving GPRS Support Node 3G-GGSN :3G Gateway GPRS Support NodeRNC: Radio Network Controller

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 ofthis approach is that mobile IP is not required. All packet routing and forward-ing are processed by a 3GPP core network. The packet loss and delay can be reduced significantly. However, this approach lacks flexibility since two networks



UE: User Equipment AP:

Access Point

RNC: Radio Network Controller

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 become the bottleneck.

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- ing 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 22.4enables IP connectivity between the WLAN terminal and IP networks over its WLAN interface. A *dynamic host configuration protocol* (*DHCP*) server is neededto 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.

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

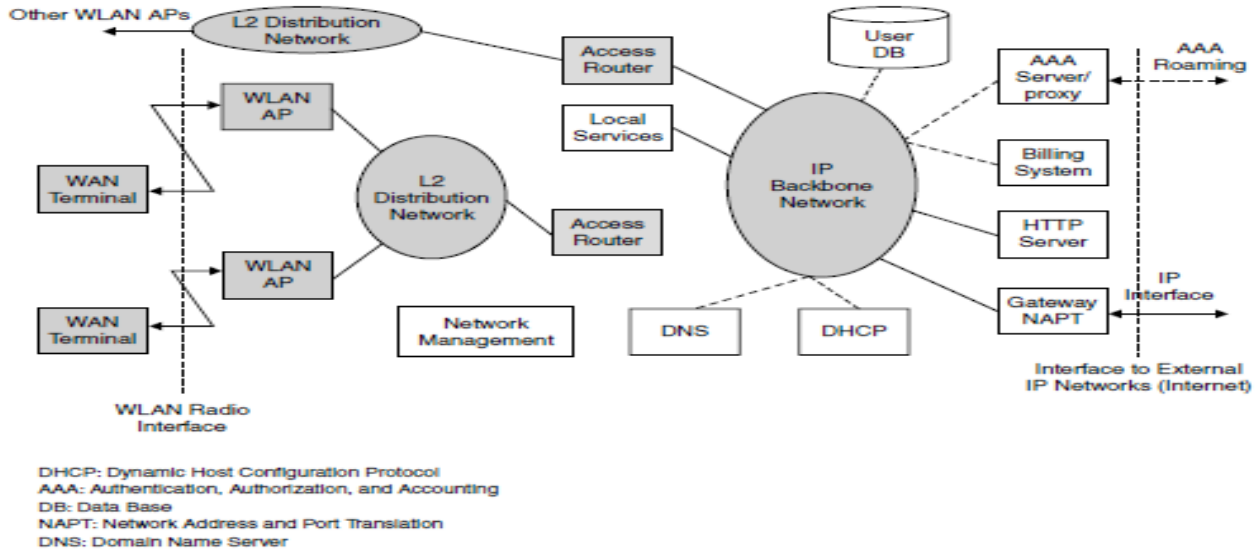


Figure 22.4 A de facto WLAN system.

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 can be prompted to enter their credit card number and pay for the connection without

establishing 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.