WLAN – GPRS Interworking

Graduate Thesis

Siv.ing. Degree
Information and Communication
Technology

By
Bjørnar Salberg

Grimstad - Norway, May 2001

Abstract

During the last years it has been experienced a huge growth in Internet users. Nearly each household in Norway got a computer attached to the Internet. The trend for further growth seems to be within the concept of mobile Internet, which means that the user can be attached anywhere at any time. The sales of mobile equipments like personal digital assistants (PDAs) and laptops are currently experiencing a great growth. This indicates a need for greater flexibility and mobility and gives therefore a demand for mobile Internet.

The motive for this thesis was to investigate the opportunities to offer mobile Internet on the basis of wireless technologies. The two largest telecom operators in Norway, Netcom and Telenor Mobile, started offer GPRS early year 2001. GPRS is a supplement to GSM, which offers packet switched data traffic. Wireless LAN (WLAN) is another access technology that can be used for wireless access to the Internet. The most used WLAN standard today are 802.11b. This standard is inexpensive and offers relatively high data rata, up to 11Mbps.

GPRS offers a large coverage area and WLAN offers relatively high data rate. Building a bridge between these two access technologies can have the potential of offering the users both large coverage area through GPRS and high data rates through WLAN. Adequate solutions for this needs to fulfill the requirement of not demanding the user to actively change access technology. Neither should the user applications be affected of the change.

Implementation of the bridging technology between WLAN and GPRS can be done at different levels. This thesis discusses solutions based on integration at IP level and integration with the GPRS network at a lower level.

The latter, also called the telecom-integrated solution, investigates the opportunities for connecting a WLAN segment to the GPRS network without affecting existing network nodes. The physical connection of the WLAN segment requires a bridge connected at one of the interfaces specified for the GPRS user plane. Two different solutions are described, one with the bridge connected at the Gn interface and one at the Gi interface. The bridge must include both user plane and the signaling plane for the GPRS network. The user equipment must be modified to handle location management in GPRS, when connected to the WLAN segment.

The IP level solutions, described herein, are based on mobile IPv4 with home agent and foreign agents. The main difference between these solutions is the location of home agent and foreign agents. The home agent can be located at a corporate network, an ISP or on the border of the GPRS network. Foreign agents can be located at any network for the provisioning of connectivity to the mobile nodes.

The solutions based on physical connection of WLAN to the GPRS network are complex and require great adjustments on the user equipment. The mobile IP solutions require less of an effort to implement. The recommended implementation will be to use the solution where the home agent is located at a corporate network or an ISP and foreign agents at WLAN segments. When the user equipment is attached to GPRS or a WLAN network without foreign agent a co-located care-of address will be used. If a foreign agent is implemented into the GGSN node it will be preferred to take use a care-of address belonging to the foreign agent.

Preface

This project is the last part of the master degree education in information and communication technology (sivilingeniør IKT) at Agder College (Høgskolen i Agder, HiA). The thesis has duration of 20 weeks and is valued at ten credits (vektall).

This thesis is written for Telenor R&D in Grimstad, Norway. During the process Thomas Haslestad at Telenor R&D has been my supervisor. I would like to thank him for giving me advice and guidance throughout the project.

Grimstad 2001

Bjørnar Salberg

Original Objectives for this thesis

General Packet Radio Service (GPRS) is a development of GSM that provides packet switched data communication. Wireless LAN (WLAN) is a network technology that is relatively cheap and gives much higher bandwidth than GPRS. The coverage of WLAN would typically be areas like airports, railway stations etc. Combining these two techniques users gets a large coverage area width GPRS and relatively high data speed in WLAN spots.

The essence will be to identify and validate different solutions for interworking. The solutions will differ in the level of integration. A typical solution of tight integration is to physically connect the WLAN segment into the GPRS network, by making a new node that behaves either like a SGSN or a BSC in towards the GPRS network. Another more loose solution is based on the usage of the IP protocol as a bridging technology through the deployment of mobile IPv4 or IPv6.

The goal is to find a line out for a possible solution and if it is time enough left to try to implement a prototype and accomplish a test of the functionality. Access to necessary equipments can set a limit to the practical part of the problem.

Issues like roaming between operators and security will be left out to limit the extent of the problem.

Contents

Definitions and Abbreviations

3GPP	3rd Generation Partnership Project
AAA	Authentication, authorization, and accounting
AKA	Authentication and Key Agreement
AP	Access Point
APN	Access Point Name
BSC	Base Station Controller
BSIC	Base transceiver Station Identity Code
BSS	Base Station System
BSSGP	Base Station System GPRS Protocol
BTS	Base Transceiver Station
COA	Care-of Address
EIR	Equipment Identity Register
ETSI	European Telecommunications Standards Institute
FA	Foreign Agent
GGSN	Gateway GPRS Support Node
GMM	GPRS Mobility Management
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GTP	GPRS Tunnelling Protocol
GTP-C	GTP Control Plane
GTP-U	GTP User Plane
HA	Home Agent
HiperLAN	High Performance LAN
HLR	Home Location Register
IEEE	Institute of Electrical and Electronics Engineers
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
ISP	Internet Service Provider
LA	Location Area
LAN	Local Area Network
LLC	Logic Link Control
MAC	Media Access Control
MAN	Metropolian Area Network
MAP	Mobile Application Part
MN	Mobile Node
MS	Mobile Station
MSC	Mobile Switching Center
MTP	Message Transfer Part
PDA	Personal Digital Assistent
PDN	Packet Data Network
PDP	Packet Data Protocol
PLMN	Public Land Mobile Network
P-TMSI	Packet TMSI
RA	Routing Area
RLC	Radio Link Control
SCCP	Signalling Connection Control Part
SGSN	Serving GPRS Support Node
SNDCP	Sub-Network Dependent Convergence Protocol
TCAP	Transaction Capabilities Application Part
TCP	Transmission Control Protocolo

TE	Terminal Equipment
TEID	Tunnelling Endpoint Identifyer
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
VLR	Visitor Location Register
WAP	Wireless Application Protocol
WLAN	Wireless LAN

Handover

To maintain a path between a Terminal Equipment (TE) and a correspondent node when the (TE) moves between cells of the same radio technology or between different radio technologies with a minimum of involvement from the user.

Terminal Equipment (TE)

The Terminal Equipment (TE) is end system equipment providing the interface towards human beings through a set of applications. The TE includes, among other things, the functions and protocols necessary to provide and handle the communication to both WLAN network and GPRS network.

Roaming

Mobility between administrative domains

1 Introduction

1.1 Motive

During the last years we have seen a huge growth in Internet users. Almost each household in Norway got a computer attached to the Internet. The further growth trend seems to be mobile Internet, which means that the user can be attached anywhere at any time. The sales of mobile equipments like personal digital assistants (PDAs) and laptops great growth, which gives demand for mobile Internet.

Mobile Internet with wireless access is at early stage, but experimental projects bring the development constantly ahead. NTNU and UNINETT accomplish a collaboration project “Trondløst”, which aimed to cover a large part of Trondheim with wireless access to Internet [1]. The purpose with this Metropolitan Area Network (MAN) was to offer a higher data rate and at sight a cheaper alternative to ISDN.

The “I-CELL” project at Telenor R&D treats with interworking between Wireless LAN and GSM Data [2]. This project deals with possibilities to use GSM Data between WLAN spots.

The Wireless Application Protocol (WAP) is an open, global specification that empowers mobile users with wireless devices to easily access and interact with information and services instantly [3].

The two largest cellular phone operators in Norway, Netcom and Telenor Mobile, started offer GPRS early year 2001. GPRS is a supplement to GSM, which offers packet switched data traffic. Billing in GPRS are mainly based the amount of data the user receive, which means the user do not pay for the time he uses. This means the user has opportunity to be always connected. GPRS uses the same radio carrier as GSM, which result in a large coverage area.

Wireless LAN (WLAN) is another access technology that can be used for connection to Internet. The most used WLAN standard today are 802.11b. This standard is inexpensive and offers relatively high data rata, up to 11Mbps[4][5].

If it could be found a method to combine WLAN and GPRS users can be offered both large coverage area and relatively high data rate. An adequate solution demand that the user do not have to actively change access technology. The user applications should not be affected of the change either.

The Interworking between WLAN and GPRS is a foretaste of the opportunities UMTS will bring with higher data rate. UMTS offers a higher data rate than GPRS but still the data rate seems to be unsatisfactory. Telenor and Ericsson have started a collaborative project to offer new wireless access to 3rd generation systems. This project is called H2U, HiperLAN to UMTS.

1.2 Scope

This thesis will treat with the integration of WLAN and GPRS. An adequate implementation will offer the user both high coverage area with GPRS and high data rate with WLAN. WLAN hotspots will typically be located at areas with heavy traffic. These areas can be airports, railway stations, hotels etc.

A concrete example could be to cover Oslo airport Gardermoen and Oslo Central Station with WLAN. A user will then be able to work with a computer, PDA etc. all the way from the airport to the station. When the user is located at the airport the data transfer is done over WLAN. When user comes into the train and moves towards the station he will lose the WLAN access and automatically use GPRS fore data transfer. Applications on the user equipment will not be affected by the change of access technology. When the train arrives the station the user equipment automatically attaches the WLAN without affecting the user.

To do the scenario above possible a bridging technology between WLAN and GPRS is needed. The scope for this thesis will be to identify and validate different solutions for implementation of this bridging technology.

1.3 Method

Accomplishment of this project requires a thorough knowledge of GPRS and Mobile IP. The first phase will be a document study about GPRS and Mobile IP. The GPRS study will be based on the 3GPP document TS 23.060, “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description; Stage 2”. The Mobile IP study will be based on the RFC 2002, “IP Mobility Support”

After the literature stud will a creative phase with identification of possible solution begin. Different solutions will be described an evaluated.

The last phase will be more practical part with implementation of one of the found solutions. This phase of the project can be left out if there is to little time. Access to necessary equipment can be another limitation.

2 Background theory

2.1 GPRS

The General Packet Radio Service (GPRS) is a new bearer service for GSM that greatly improves and simplifies wireless access to packet data networks. It applies a packet radio principle to transfer user data packets in an efficient way between mobile stations and external packet data networks.

2.1.1 System architecture

In order to integrate GPRS into the existing GSM architecture, a new class of network nodes, called GPRS support nodes (GSN), has been introduced. GSNs are responsible for the delivery and routing of data packets between the mobile station and the external packet data network (PDN). The table below shows the functions identified in the functional model assigned to the logical architecture.

Function	2G-MS	BSS	2G-SGSN	GGSN	HLR
Network Access Control:					
Registration					X
Authentication and Authorisation	X		X		X
Admission Control	X	X	X		
Message Screening				X	
Packet Terminal Adaptation	X				
Charging Data Collection			X	X	
Packet Routeing & Transfer:					
Relay	X	X	X	X	
Routeing	X	X	X	X	
Address Translation and Mapping	X		X	X	
Encapsulation	X		X	X	
Tunnelling			X	X	
Compression	X		X		
Ciphering	X		X		X
Mobility Management:	X		X	X	X
Logical Link Management:					
Logical Link Establishment	X		X		
Logical Link Maintenance	X		X		
Logical Link Release	X		X		
Radio Resource Management:	X	X	X		

Table 1 – Mapping of functions to Logic Architecture [7]

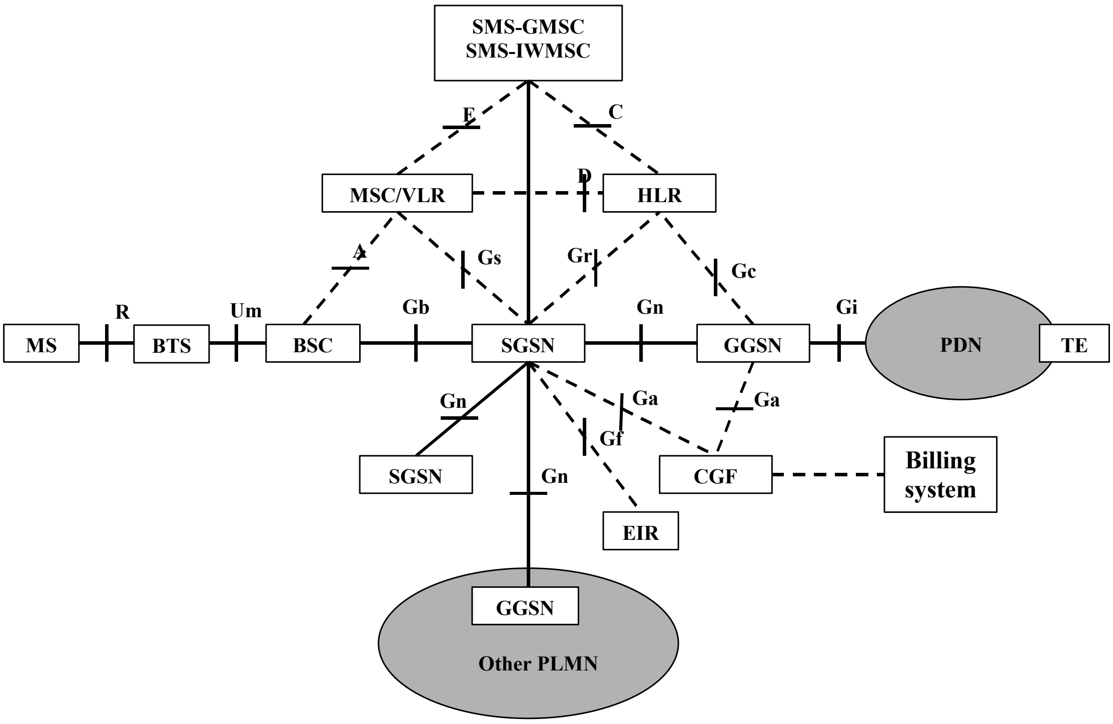


Figure 1 – GPRS system architecture

A serving GPRS support node (SGSN) is responsible for the delivery of data packets from and to the mobile station (MS) within its service area. Its tasks include packet routing and transfer, mobility management (attach/detach and location management), logical link management, and authentication and charging functions. The location register of the SGSN stores location information, e.g., current cell and user profiles, e.g., IMSI, address(es) used in the packet data network of all GPRS users registered with this SGSN.

A gateway GPRS support node (GGSN) acts as an interface between the GPRS backbone network and the external packet data networks. It converts the GPRS packets coming from the SGSN into the appropriate packet data protocol (PDP) format (e.g., IP or X.25) and sends them out on the corresponding packet data network. In the other direction, PDP addresses of incoming data packets are converted to the GSM address of the destination user. The readdressed packets are sent to the responsible SGSN. For this purpose, the GGSN stores the current SGSN address of the user and his or her profile in its location register. The GGSN also performs authentication and charging functions.

Figure 1 also shows the interfaces defined between the network nodes [7].

The Gb interface connects the BSC with the SGSN. Via the Gn and the Gp interfaces, user data and signaling data are transmitted between the GSNs. The Gn interface will be used if SGSN and GGSN are located in the same PLMN, where as the Gp interface will be used if they are in different PLMNs.

All GSNs are connected via an IP-based GPRS backbone network. Within this backbone, the GSNs encapsulate the PDN packets and transmit them using the GPRS Tunneling Protocol GTP. There are two kinds of GPRS backbones:

- Intra-PLMN backbone networks connect GSNs of the same PLMN and are therefore private IP-based networks of the GPRS network provider.
- Inter-PLMN backbone networks connect GSNs of different PLMNs. A roaming agreement between two GPRS network providers is necessary to exploit such a backbone. Inter-PLMN backbone is provided by a number of Global IP connectivity operators and are in the case of GPRS named GRX (GPRS Roaming exchange) providers

The Gn interface is also defined between two SGSNs. This allows the SGSNs to exchange user profiles when a mobile station moves from one SGSN area to another. Across the Gf interface, the SGSN may query the IMEI of a mobile station trying to register with the network. The Gi interface connects the PLMN with external public or private PDNs, such as the Internet or corporate intranets. Interfaces to IP (IPv4 and IPv6) and X.25 networks are supported.

The HLR stores the user profile, the current SGSN address, and the PDP address(es) for each GPRS user in the PLMN. The Gr interface is used to exchange this information between HLR and SGSN. For example, the SGSN informs the HLR about the current location of the MS. When the MS registers with a new SGSN, the HLR will send the user profile to the new SGSN. The signaling path between GGSN and HLR (Gc interface) may be used by the GGSN to query a user's location and profile in order to update its location register.

In addition, the MSC/VLR may be extended with functions and register entries that allow efficient coordination between packet switched (GPRS) and circuit switched (conventional GSM) services. Examples of this are combined GPRS and non-GPRS location updates and combined attachment procedures. Moreover, paging requests of circuit switched GSM calls can be performed via the SGSN. For this purpose, the Gs interface connects the databases of SGSN and MSC/VLR.

2.1.2 Services

Bearer Services and Supplementary Services

The bearer services of GPRS offer end-to-end packet switched data transfer. There are two different kinds: The point-to-point (PTP) service and the point-to-multipoint (PTM) service. The latter will be available in future releases of GPRS.

The PTP service [7] offers transfer of data packets between two users. It is offered in both connectionless mode (PTP connectionless network service (PTP-CLNS), e.g., for IP) and connection-oriented mode (PTP connection-oriented network service (PTP-CONS), e.g., for X.25).

The PTM service offers transfer of data packets from one user to multiple users. There exist two kinds of PTM services:

- Using the multicast service PTM-M, data packets are broadcast in a certain geographical area. A group identifier indicates whether the packets are intended for all users or for a group of users.

- Using the group call service PTM-G, data packets are addressed to a group of users (PTM group) and are sent out in geographical areas where the group members are currently located.

Moreover, a GPRS service provider may offer additional non-standardized services, such as access to data bases, messaging services, and tele-action services (e.g., credit card validations, lottery transactions, and electronic monitoring and surveillance systems) [7].

Quality of Service

The Quality of Service QoS requirements of typical mobile packet data applications are very diverse (e.g., consider real-time multimedia, Web browsing, and e-mail transfer). Support of different QoS classes, which can be specified for each individual session, is therefore an important feature. GPRS allows defining QoS profiles using the parameters service precedence, reliability, delay, and throughput [7].

- The service precedence is the priority of a service in relation to another service. There exist three levels of priority: high, normal, and low.

- The reliability indicates the transmission characteristics required by an application. Three reliability classes are defined, which guarantee certain maximum values for the probability of loss, duplication, mis-sequencing, and corruption (an undetected error) of packets. The table below shows the different reliability classes.

Class	Probability for			
	Lost packet	Duplicate packet	Out of sequence packet	Corrupted packet
1	10^9	10^9	10^9	10^9
2	10^4	10^5	10^5	10^6
3	10^2	10^5	10^5	10^2

Table 2 – Reliability classes [7]

- The delay parameters define maximum values for the mean delay and the 95-percentile delay (see table below). The latter is the maximum delay guaranteed in 95 percent of all transfers. The delay is defined as the end-to-end transfer time between two communicating mobile stations or between a mobile station and the Gi interface to an external packet data network. This includes all delays within the GPRS network, e.g., the delay for request and assignment of radio resources and the transit delay in the GPRS backbone network. Transfer delays outside the GPRS network, e.g., in external transit networks, are not taken into account.

Class	128 byte packet		1024 byre packet	
	Mean delay	95% delay	Mean delay	95% delay
1	< 0,5 s	< 1,5 s	< 2 s	< 7 s
2	< 5 s	< 25 s	< 15 s	< 75 s
3	< 50 s	< 250 s	< 75 s	< 375 s
4	Best effort	Best effort	Best effort	Best effort

Table 3 – Delay classes [7]

- The throughput specifies the maximum/peak bit rate and the mean bit rate.

Using these QoS classes, QoS profiles can be negotiated between the mobile user and the network for each session, depending on the QoS demand and the current available resources. The billing of the service is then based on the transmitted data volume, the type of service, and the chosen QoS profile.

2.1.3 Handover in GPRS

The user movements can produce the need to change the channel or cell, specially when the quality of the communication is decreasing. This procedure of changing the resources is called handover. Four different types of handovers can be distinguished:

- Handover of channels in the same cell.
- Handover of cells controlled by the same BSC.
- Handover of cells belonging to the same SGSN but controlled by different BSCs.
- Handover of cells controlled by different SGSNs.

Handovers are mainly controlled by the SGSN. However in order to avoid unnecessary signaling information, the first two types of handovers are managed by the concerned BSC (in this case, the SGSN is only notified of the handover). The mobile station is the active participant in this procedure. In order to perform the handover, the mobile station controls continuously its own signal strength and the signal strength of the neighboring cells. The list of cells that must be monitored by the mobile station is given by the base station. The power measurements allow deciding which is the best cell in order to maintain the quality of the communication link. Two basic algorithms are used for the handover:

The `minimum acceptable performance' algorithm. When the quality of the transmission decreases (i.e the signal is deteriorated), the power level of the mobile is increased. This is done until the increase of the power level has no effect on the quality of the signal. When this happens, a handover is performed. The `power budget' algorithm. This algorithm performs a handover, instead of continuously increasing the power level, in order to obtain a good communication quality.

2.1.4 Session Management, Mobility Management and Routing

In this section it will be described how a mobile station (MS) registers with the GPRS network and becomes known to an external packet data network (PDN), how packets are routed to or from mobile stations, and how the network keeps track of the current location of the user.

Attachment and Detachment Procedure

Before a mobile station can use GPRS services, it must register with an SGSN of the GPRS network. The network checks if the user is authorized, copies the user profile from the HLR to the SGSN, and assigns a packet temporary mobile subscriber identity (P-TMSI) to the user. This procedure is called GPRS attach. For mobile stations using both circuit switched and packet switched services it is possible to perform combined

GPRS/IMSI attach procedures. The disconnection from the GPRS network is called GPRS detach. It can be initiated by the mobile station or by the network (SGSN or HLR).

Session Management, PDP Context

To exchange data packets with external PDNs after a successful GPRS attach, a mobile station must apply for one or more addresses used in the PDP, in most cases an IP address. This address is called PDP address (Packet Data Protocol address). For each session, a PDP context is created, which describes the characteristics of the session. It contains a PDP type (e.g., IPv4), the PDP address assigned to the mobile station (e.g., 212.17.137.140), the requested QoS, and the address of the GGSN that serves as the access point to the PDN.

This context is stored in the MS, the SGSN, and the GGSN. With an active PDP context, the mobile station is "visible" for the external PDN and is able to send and receive data packets. The mapping between the two addresses, PDP and IMSI, enables the GGSN to transfer data packets between PDN and MS. A user may have several simultaneous PDP contexts active at a given time.

The allocation of the PDP address can be static or dynamic. In the first case, the network operator of the user's home-PLMN permanently assigns a PDP address to the user. In the second case, a PDP address is assigned to the user upon activation of a PDP context. The PDP address can be assigned by the operator of the user's home-PLMN (dynamic home-PLMN PDP address) or by the operator of the visited network (dynamic visited-PLMN PDP address). The home network operator decides which of the possible alternatives may be used. In case of dynamic PDP address assignment, the GGSN is responsible for the allocation and the activation/ deactivation of the PDP addresses.

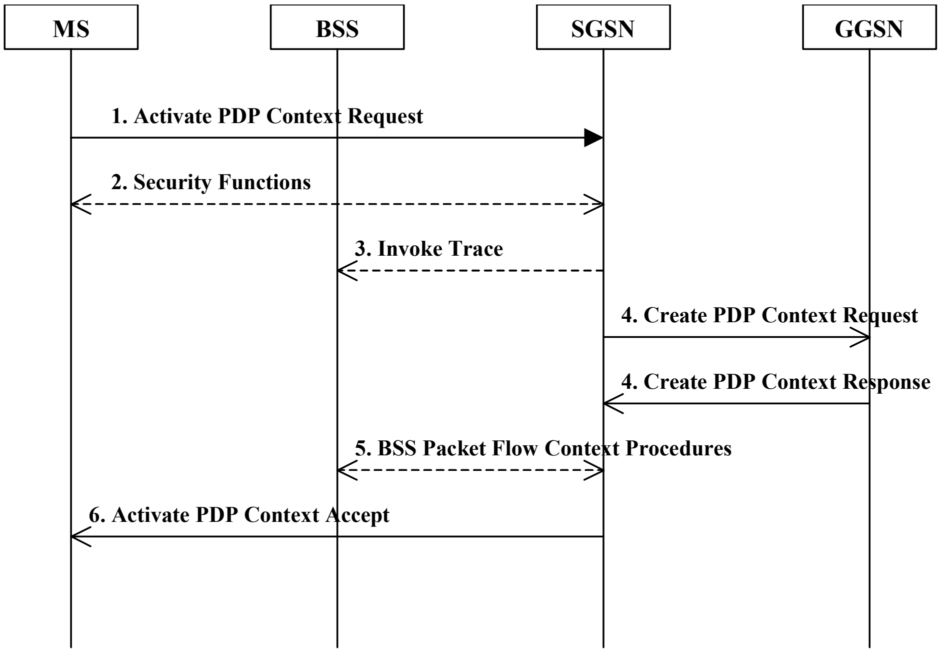

MS
BSS
SGSN
GGSN
1. Activate PDP Context Request
2. Security Functions
3. Invoke Trace
4. Create PDP Context Request
4. Create PDP Context Response
5. BSS Packet Flow Context Procedures
6. Activate PDP Context Accept

Figure 2 - PDP context activation procedure 0

Using the message “activate PDP context request”, the MS informs the SGSN about the requested PDP context. If dynamic PDP address is required, the parameter PDP address will be left empty. Afterwards, usual the security functions Authentication and

Key Agreement (AKA) are performed. If access is granted the SGSN will send a “create PDP context request” to the affected GGSN. The GGSN creates a new entry in its PDP context table, which enables the GGSN to route data between the SGSN and the external PDN. Afterward, the GGSN returns a confirmation message "create PDP context response" to the SGSN, which contains the PDP address. The SGSN updates its PDP context table and confirms the activation of the new PDP context to the MS ("activate PDP context accept").

Routing

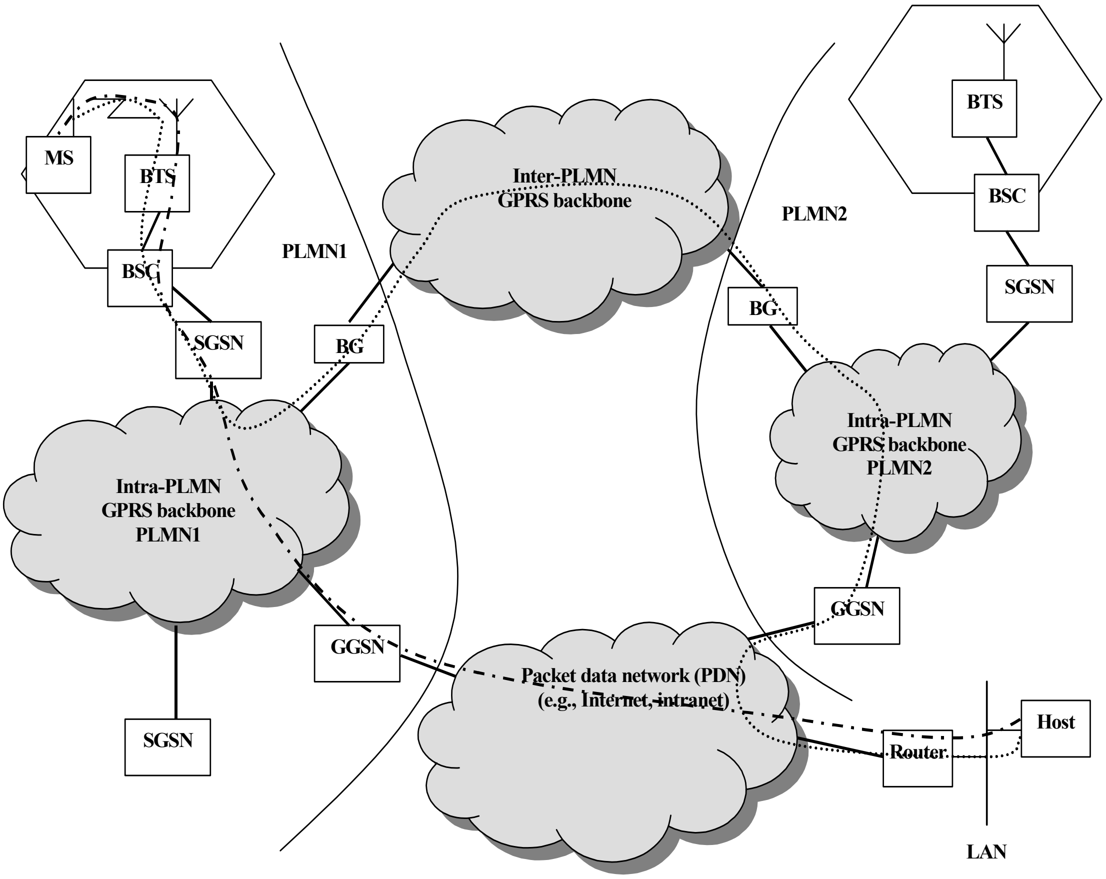


Figure 3 - GPRS routing

Figure 3 gives an example of how packets are routed in GPRS assume that the packet data network is an IP network. A GPRS mobile station located in PLMN1 sends IP packets to a host connected to the IP network, e.g., to a Web server connected to the Internet. The SGSN that the mobile station is registered with encapsulates the IP packets coming from the mobile station, examines the PDP context, and routes them through the intra-PLMN GPRS backbone to the appropriate GGSN. The GGSN decapsulates the packets and sends them out on the IP network, where IP routing mechanisms are used to transfer the packets to the access router of the destination network. The latter delivers the IP packets to the host.

Let us assume the home-PLMN of the mobile station is PLMN2. An IP address has been assigned to the mobile by the GGSN of PLMN2. Thus, the MS's IP address has the same network prefix as the IP address of the GGSN in PLMN2. The correspondent host is now sending IP packets to the MS. The packets are sent out onto the IP network and are routed to the GGSN of PLMN2 (the home-GGSN of the MS). The latter queries the HLR and obtains the information that the MS is currently located in PLMN1. It encapsulates the incoming IP packets and tunnels them through the inter-PLMN GPRS backbone to the appropriate SGSN in PLMN1. The SGSN decapsulates the packets and delivers them to the MS.

Location management

The main task of location management is to keep track of the user's current location, so that incoming packets can be routed to his or her MS. For this purpose, the MS sends location update messages periodic to its current SGSN. If the MS sends updates rather seldom, its location (e.g., its current cell) is not known exactly and paging is necessary for each downlink packet, resulting in a significant delivery delay. On the other hand, if location updates happen very often, the MS's location is well known to the network, and the data packets can be delivered without any additional paging delay. A state model has been defined for location management in GPRS [7]. A MS can be in one of three states depending on its current traffic amount; the location update frequency is dependent on the state of the MS.

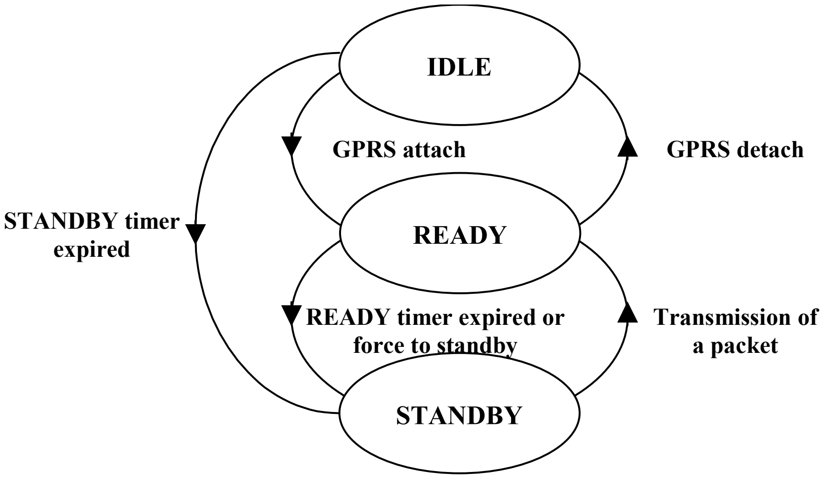


Figure 4 - State model of a GPRS mobile station [7]

In IDLE state the MS is not reachable. Performing a GPRS attach, the MS gets into READY state. With a GPRS detach it may disconnect from the network and fall back to IDLE state. All PDP contexts will be deleted. The STANDBY state will be reached when an MS does not send any packets for a longer period of time, and therefore the READY timer (which was started at GPRS attach) expires.

In IDLE state, no location updating is performed, i.e., the current location of the MS is unknown to the network. An MS in READY state informs its SGSN of every movement to a new cell. For the location management of an MS in STANDBY state, a GSM location area (LA) is divided into several routing areas (RA). In general, an RA consists of several cells. The SGSN will only be informed when an MS moves to a new RA and not when it changes cell. To locate the coverage providing cell of an MS in STANDBY state, paging of the MS within a certain RA must be. For MSs in READY state, no paging is necessary.

Whenever an MS moves to a new RA, it sends a "routing area update request" to its assigned SGSN. The message contains the routing area identity (RAI) of its old RA. The base station subsystem (BSS) adds the cell identifier (CI) of the new cell, from which the SGSN can derive the new RAI. Two different scenarios are possible:

- Intra-SGSN routing area update: The MS has moved to an RA that is assigned to the same SGSN as the old RA. In this case, the SGSN has already stored the necessary user profile and can assign a new packet temporary mobile subscriber identity (P-TMSI) to the user ("routing area update accept"). Since the routing context does not change, there is no need to inform other network elements, such as GGSN or HLR.

- Inter-SGSN routing area update: The new RA is administered by a different SGSN than the old RA. The new SGSN realizes that the MS has changed to its area and requests the old SGSN to send the PDP contexts of the user. Afterward, the new SGSN informs the involved GGSNs about the user's new routing context. In addition, the HLR and the MSC/VLR are informed about the user's new SGSN.

2.1.5 Protocol Architecture

Transmission plane

Figure 5 illustrates the protocol architecture of the GPRS transmission plane [7], providing transmission of user data and its associated signaling such as flow control, error detection and error correction.

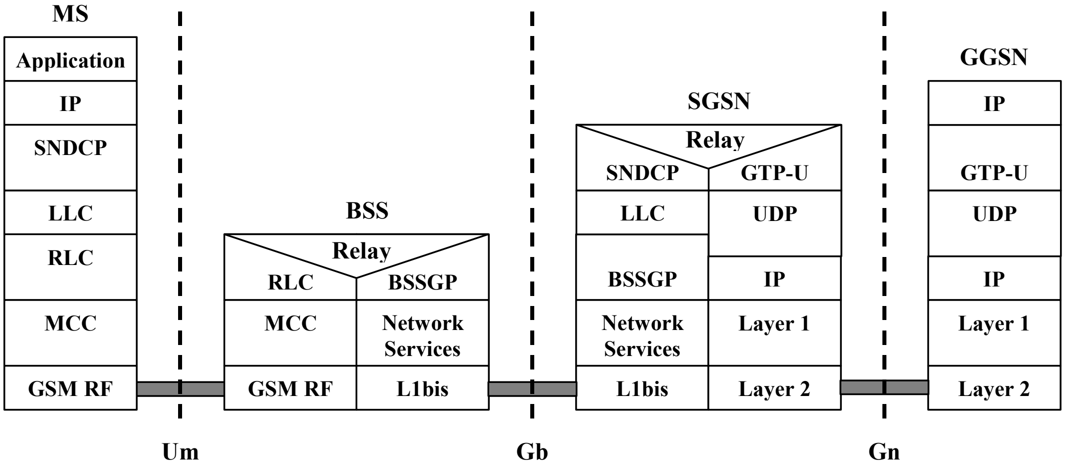


Figure 5 - Transmission plane [7]

GPRS Backbone: SGSN – GGSN: User data packages are encapsulated within the GPRS backbone network. The GPRS Tunneling Protocol (GTP) [7] tunnels the user data packets and related signaling information between the GPRS support nodes (GSNs). The protocol is defined both between GSNs within one PLMN (Gn interface) and between GSNs of different PLMNs (Gp interface). In the transmission plane, GTP employs a tunnel mechanism to transfer user data packets. In the signaling plane, GTP specifies a tunnel control and management protocol. The signaling is used to create, modify, and delete tunnels.

Subnetwork Dependent Convergence Protocol: The Subnetwork Dependent Convergence Protocol (SNDCP) [8] is used to transfer data packets between SGSN and MS. Its functionality includes:

- Multiplexing of several connections of the network layer onto one virtual logical connection of the underlying LLC layer.
- Compression and decompression of user data and redundant header information.

Data link layer: The data link layer between the MS and the network is divided into two sublayers, the LLC layer between the MS and the SGSN, and the RLC/MAC layer between the MS and the BSS.

The logical link control (LLC) layer [9] provides a highly reliable logical link between an MS and its assigned SGSN. Its functionality is based on the well-known HDLC protocol and includes sequence control, in-order delivery, flow control, detection of transmission errors, and retransmission (automatic repeat request (ARQ)). Ciphering functions ensures the data confidentiality. Variable frame lengths are possible. Both acknowledged and unacknowledged data transmission modes are supported. The protocol is mainly an adapted version of the LAPDm protocol used in GSM.

The RLC/MAC layer [10] at the air interface includes two functions. The main purpose of the radio link control (RLC) layer is to establish a reliable link between the MS and the BSS. This includes the segmentation and reassembly of LLC frames into RLC data blocks and ARQ of uncorrectable codewords. The medium access control (MAC) layer controls the access attempts of an MS on the radio channel shared by several MSs. It employs algorithms for contention resolution, multiuser multiplexing on a PDTCH, and scheduling and prioritizing based on the negotiated QoS. The GPRS MAC protocol is based on the principle of slotted Aloha. In the RLC/MAC layer, both the acknowledged and unacknowledged modes of operation are supported.

Physical Layer: The physical layer between MS and BSS is divided into the two sublayers, the physical link layer (PLL) and the physical RF Layer (RFL)

The PLL provides a physical channel between the MS and the BSS. Its tasks include channel coding (detection of transmission errors, forward error correction (FEC), indication of uncorrectable codewords), interleaving, and detection of physical link congestion.
The RFL operates below the PLL. Among other things, it includes modulation and demodulation.

The BSS – SGSN interface: The BSS GPRS Application Protocol (BSSGP) [11] delivers routing and QoS-related information between BSS and SGSN. The underlying Network Service (NS) protocol is based on the Frame Relay protocol.

Signaling plane

The protocol architecture of the signaling plane [7] comprises protocols for control and support of the functions of the transmission plane as GPRS attach and detach, PDP context activation, control of routing paths, and allocation of network resources.

Between MS and SGSN the GPRS Mobility Management and Session Management (GMM/SM) protocol supports mobility and session management when performing functions such as GPRS attach/detach, security functions, PDP context activation, and routing area updates.

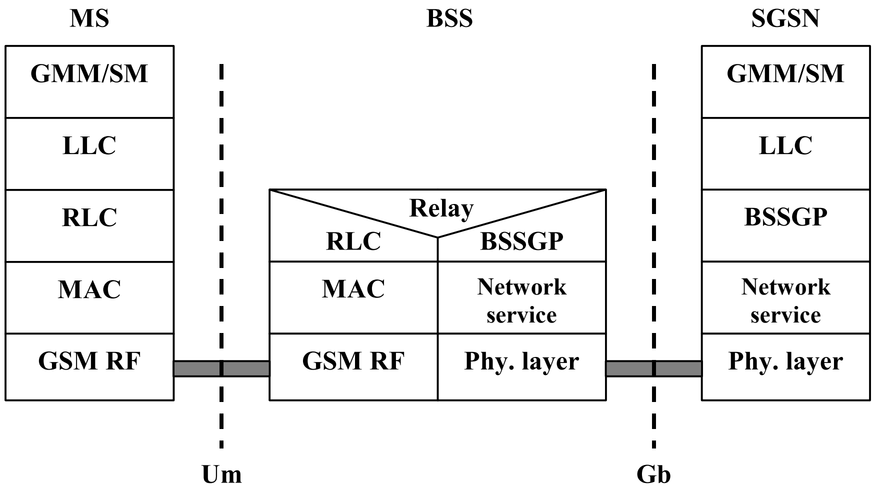
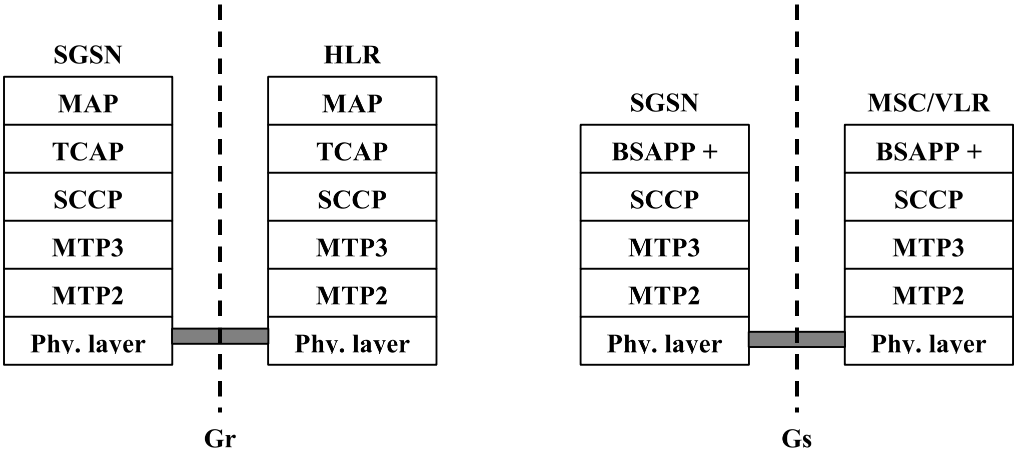


Figure 6 - Signaling plane: MS-SGSN [7]

The signaling architecture between SGSN and the registers HLR, VLR, and EIR uses the same protocols as conventional GSM and extends them with GPRS-specific functionality.



MAP: Mobile application part
TCAP: Transaction capabilities application part
SCCP: Signaling connection control part
MTP: Message transfer part
BSSAP +: BSS application part +

Figure 7 - Signaling plane SGSN – HLR and SGSN VLR/MSC 23.060

Between SGSN and HLR as well as between SGSN and EIR, an enhanced Mobile Application Part (MAP) is employed. The MAP is a mobile network-specific extension of the Signaling System SS#7. It transports the signaling information related to location updates, routing information, user profiles, and handovers. The exchange of MAP messages is accomplished over the transaction capabilities application part (TCAP) and the signaling connection control part (SCCP). The base station system application part (BSSAP+) includes functions of GSM's BSSAP. It is applied to transfer signaling information between the SGSN and the VLR (Gs interface). This includes signaling of the mobility management when coordination of GPRS and conventional GSM functions is necessary (e.g., combined GPRS and non-GPRS location update, combined GPRS/IMSI attach, or paging of an MS via GPRS for an incoming GSM call).

Interworking with IP Networks

Finally it is show how a GPRS network can be interconnected with an IP-based packet data network, such as the Internet or intranets. GPRS supports both IPv4 and IPv6The Gi interface is the interworking point with IP networks. From outside, i.e., from an external IP network's point of view, the GPRS network looks like any other IP subnetwork, and the GGSN looks like a usual IP router. Figure 1 shows the protocol stacks at the GGSN [12].

Each registered user who wants to exchange data packets with the IP network gets an IP address, as explained earlier. The IP address is taken from the address space of the GPRS operator. In order to support a large number of mobile users, it is essential to use dynamic IP address allocation (in IPv4). Thus, a DHCP server (Dynamic Host Configuration Protocol) is installed. The address resolution between IP address and GSM address is performed by the GGSN, using the appropriate PDP context. The routing of IP packets and the tunneling through the intra-PLMN backbone (using the GPRS Tunneling Protocol GTP) has been explained in prior sections.

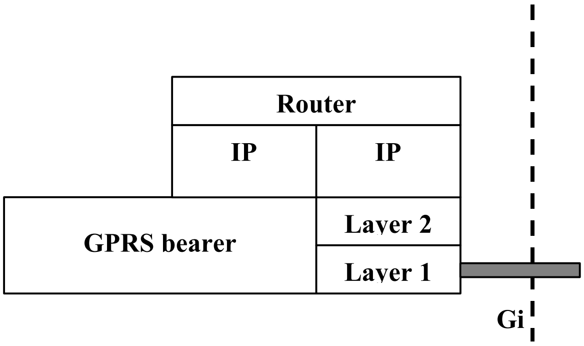


Figure 8 - Protocols at the Gi IP interface [12]

Each registered user who wants to exchange data packets with the IP network gets an IP address, as explained earlier. The IP address is taken from the address space of the GPRS operator. In order to support a large number of mobile users, it is essential to use dynamic IP address allocation (in IPv4). Thus, a DHCP server (Dynamic Host Configuration Protocol) is installed. The address resolution between IP address and GSM address is performed by the GGSN, using the appropriate PDP context. The routing of IP packets and the tunneling through the intra-PLMN backbone (using the GPRS Tunneling Protocol GTP) has been explained in prior sections.

2.2 Mobile IP

Mobile IP is a mechanism for maintaining transparent network connectivity to mobile hosts. Mobile IP allows a mobile host to be addressed by the IP address it uses in its home network (home IP address), regardless of the network to which it is currently physically attached. Mobil IP is a standard designed by an IETF workgroup to solve these problems [13].

IP routs datagrams to the destination point out from IP-addresses associated to a fixed network connection. These IP addresses are associated with a fixed network location. When the packet's destination is a mobile node, this means that each new point of attachment made by the node is associated with a new network number and, hence, a new IP address. Changing the IP-address solves the routing problem, but creates a problem for connection-oriented protocols such as TCP. Changing the IP-address of a TCP connection causes the connection to fall down.

2.2.1 Mobile IP in essence

Mobile IP takes use of two new nodes to the network, the home agent (HA) and the foreign agent (FA). A mobile node (MN) situated away from its home network is associated with a care-of address. That address provides information about its current point of attachment. The MN registers the care-of address with its HA, so that the HA always now where its belonging MN's are situated. Mobile nodes use two IP addresses, a fixed home address and a care-of address that changes at each new point of attachment.

Mobile IP is best understood as the cooperation of three separate mechanisms:

- The discovering the care-of address
- The registering the care-of address
- The tunneling to the care-of address

2.2.2 Discovering the care-of address

The mobile IP discovery process has been built on top of the existing Routing Advertisement protocol [14]. Mobile IP discovery does not modify the original fields of existing router advertisements but simply extends them to associate mobility functions. Thus, a router advertisement can carry information about default routers, just as before, and in addition carry further information about one or more care-of addresses. When the router advertisements are extended to also contain the needed care-of address, they are known as agent advertisements. Router advertisements extended to also contain the needed care-of address are known as agent advertisements. Home agents and foreign agents typically broadcast agent advertisements at periodic intervals.

Agent advertisement perform the following functions:

- Allows the detection of mobility agents
- Lists one or more available care-of address
- Informs the mobile node about special features provided by foreign agents (e.g., alternative encapsulation techniques).
- Lets the mobile nodes determine the network number and the status of their link to the Internet.
- Lets the mobile node know whether the agent is a home agent, a foreign agent or both.

If a mobile node needs to get a care-of address and does not wish to wait for the periodic advertisement, the mobile node can broadcast or multicast a solicitation that will be answered by any foreign agent or home agent that receives it. Mobile nodes use router solicitation [14] to detect any change in the set of mobility agents available at the current point of attachment. If advertisements are no longer detectable from a foreign agent that previously had offered a care-of address to the mobile node, the mobile node should presume that foreign agent is no longer within range of the mobile node's network interface. In this situation, the mobile node should begin to hunt for a new care-of address, or possibly use a care-of address known from advertisements it is still receiving. The mobile node may choose to wait for another advertisement if it has not received any recently advertised care-of addresses, or it may send an agent solicitation.

2.2.3 Registering the care-of address

Once a mobile node has a care-of address, its home agent must be updated. Figure 9 shows the registration process defined by Mobile IP for this purpose. The process begins when the mobile node, possibly with the assistance of a foreign agent, sends a registration request with the care-of address information. When the home agent receives this request, it adds the necessary information to its routing table, approves the request, and sends a registration reply back to the mobile node.

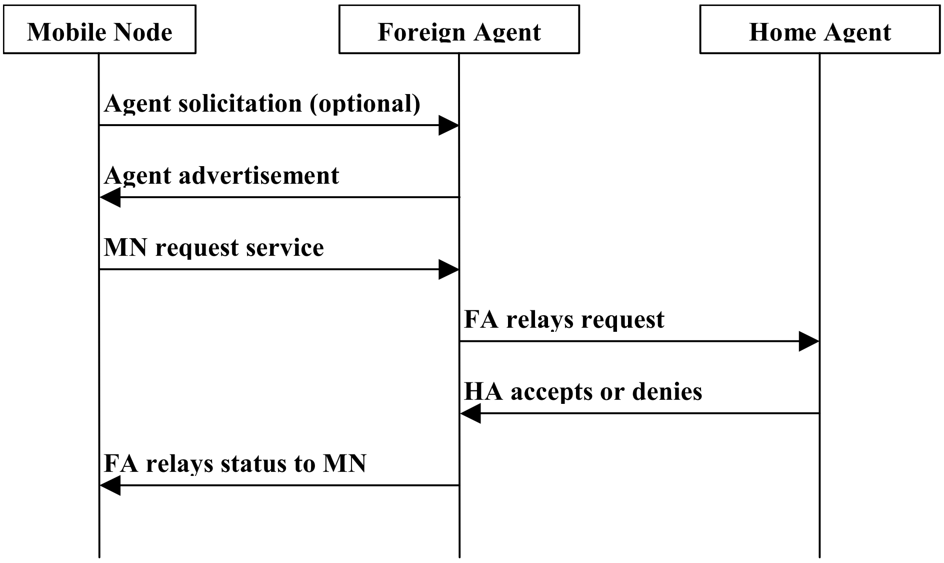


Figure 9- Care-of address registration procedure

2.2.4 Tunneling to the Care-of address

Figure 10 shows the tunneling operations in Mobile IP. The default encapsulation mechanism that must be supported by all mobility agents using Mobile IP is IP-within-IP [15]

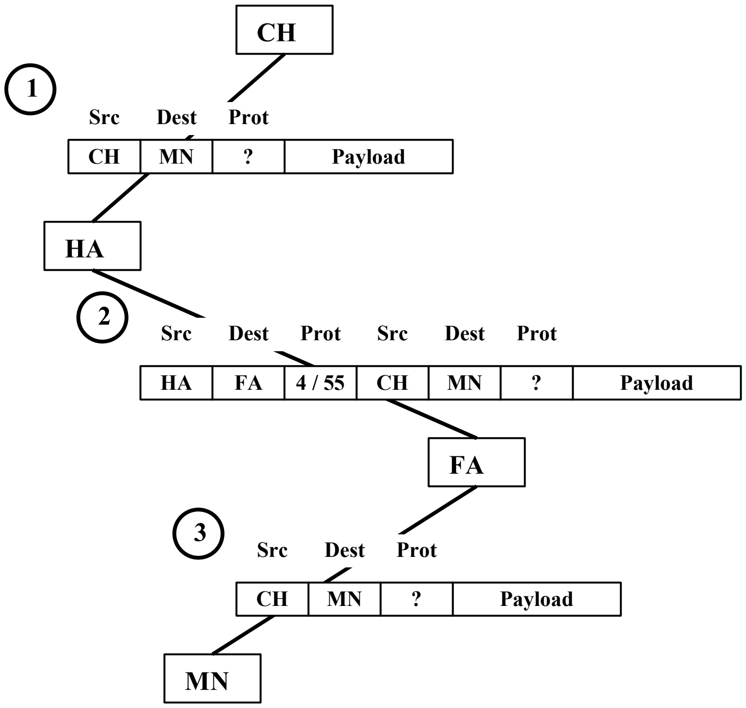


Figure 10 - Tunneling operations in mobile IP

Using IP-within-IP, the home agent, the tunnel source, inserts a new IP header, or tunnel header, in front of the IP header of any datagrams addressed to the mobile node's home address.

1) The CH sends the IP datagram with the IP address of the MN as destination address.

2) The new tunnel header inserted by the HA uses the mobile node's care-of address as the destination IP address, or tunnel destination. The tunnel source IP address is the home agent, and the tunnel header uses 4 as the higher-level protocol number, indicating that the next protocol header is again an IP header.

3) In IP-within-IP the entire original IP header is preserved as the first part of the payload of the tunnel header. Therefore, to recover the original packet, the foreign agent has to eliminate the tunnel header and deliver the rest to the mobile node.

Figure 10 shows that sometimes the tunnel header uses protocol number 55 as the inner header. This happens when the home agent uses minimal encapsulation [16] instead of IP-within-IP. Processing for the minimal encapsulation header is slightly more complicated than that for IP-within-IP, because some of the information from the tunnel header is combined with the information in the inner minimal encapsulation header to reconstitute the original IP header. On the other hand, header overhead is reduced.

2.2.5 Care-of address

The mobile nodes care of address can be either the IP address of the FA or an IP address obtained by the mobile node. In the first case the HA encapsulate datagrams and forwards them to the FA, which decapsulates them and sends them to the MN. FA uses link-level protocols to forward packets to the mobile nodes, which results in demand of just one IP address for all visiting hosts. The MN normally uses its home address as source address and sends datagrams directly to the corresponding hosts. This results in a triangle routing shown with the figure below.

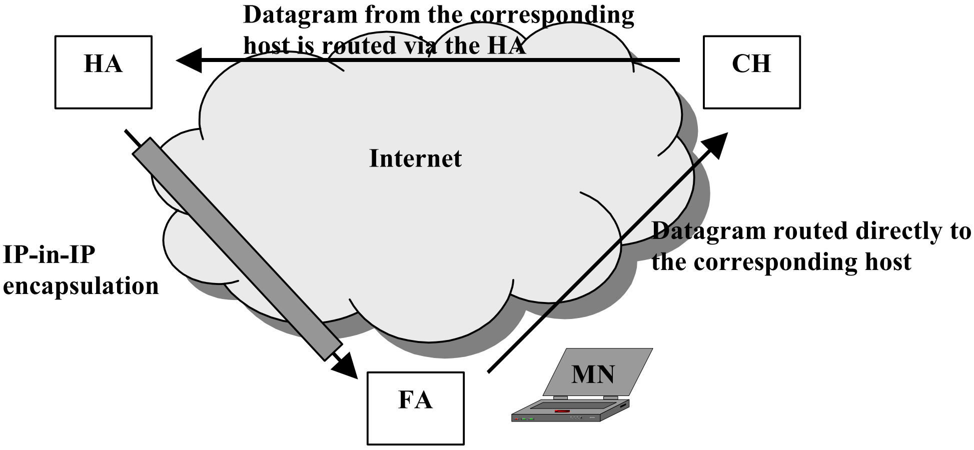

Datagram from the corresponding host is routed via the HA
HA
CH
Internet
IP-in-IP encapsulation
Datagram routed directly to the corresponding host
MN
FA

Figure 11 - Triangle routing with mobile IP

Co-located care-of address

The mobile node can register an IP address obtained from the foreign network as a care-of address, called a co-located care-of address. In this scenario, the mobile host receives an IP-address to use while it visits the network, via DHCP or some other protocol or policy. It registers this address with its home agent, which tunnels packets directly to the mobile host at this address.

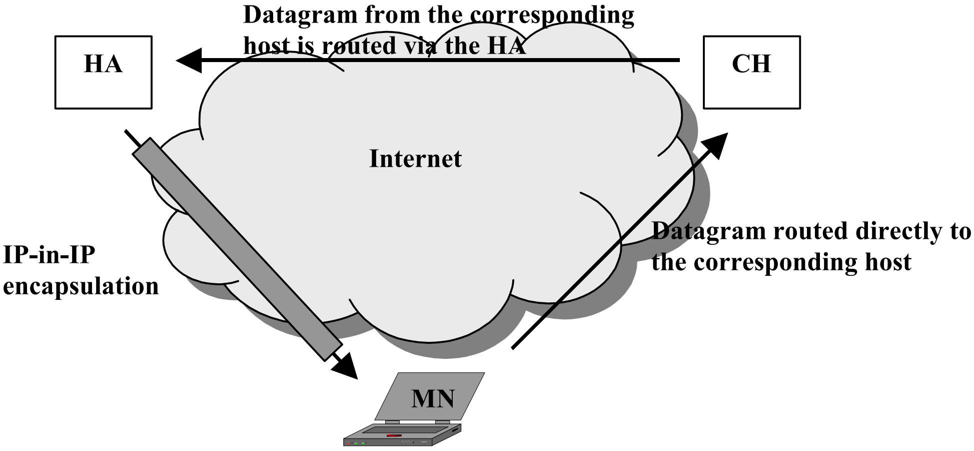

Datagram from the corresponding host is routed via the HA
HA
CH
Internet
IP-in-IP encapsulation
Datagram routed directly to the corresponding host
MN

Figure 12 - Co-located care-of address

The difference between FA located care-of and co-located care-of is that the mobile node has to decapsulate packets when co-located care-of address. Each visiting node need also its own IP address at the foreign network..

2.2.6 Ingress filtering

Some networks accomplish “ingress filtering”, which means that the networks routers will reject datagrams with a source address that not belongs in the current network. If the foreign network accomplish ingress filtering the MN has to use its care-off address as source address. This problem is solved by tunneling the datagrams to the HA, that forwards the datagrams to the corresponding host.

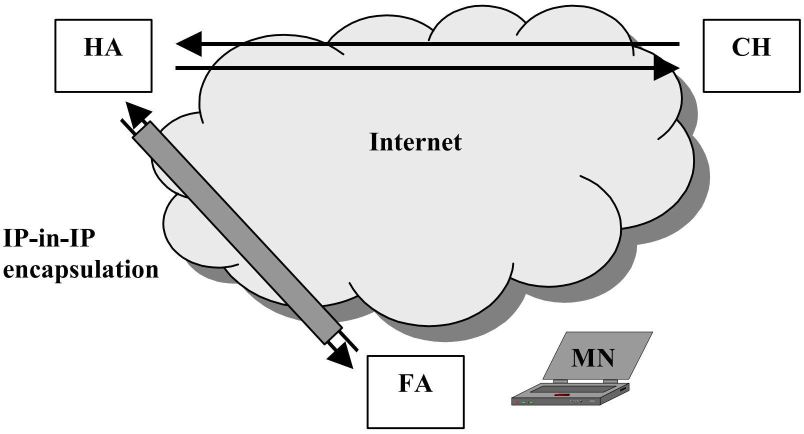


Figure 13 - Routing with ingress filtering

2.2.7 Authentication

Registration requests contain parameters and flags that characterize the tunnel through which the home agent will deliver packets to the care-of address. When a home agent accepts the request, it begins to associate the home address of the mobile node with the care-of address, and maintains this association until the registration lifetime expires. The triplet that contains the home address, care-of address, and registration lifetime is called a binding for the mobile node. A registration request can be considered a binding update sent by the mobile node.

A binding update is an example of a remote redirect, because it is sent remotely to the home agent to affect the home agent’s routing table. This view of registration makes the need for authentication clear. The home agent must be certain registration was originated by the mobile node and not by some other malicious node pretending to be the mobile node. A malicious node could cause the home agent to update its routing table with a false care-of address.

The binding update is signed with a one-way hash algorithm over all the data within the registration message header and the extensions that precede the signature. To secure the registration request, each request must contain unique data so that two different registrations will in practical terms never have the same MD5 hash. If the same MN5 hash is used for all binding updates a malicious node can perform a replay attack. Creating different MD5 hashes is done by the use of timestamps or random number.

The identification field is also used by the foreign agent to match pending registration requests to registration replies when they arrive at the home agent and to subsequently be able to relay the reply to the mobile node. The foreign agent also stores other information for pending registrations, including the mobile node's home address, the mobile node's Media Access Layer (MAC) address, the source port number for the registration request from the mobile node, the registration lifetime proposed by the mobile node, and the home agent's address. The foreign agent can limit registration lifetimes to a configurable value that it puts into its agent advertisements. The home agent can reduce the registration lifetime, which it includes as part of the registration reply, but it can never increase it.

Discovering the care-of address Discovering the care-of address Discovering the care-of address Discovering the care-of address Discovering the care-of address Discovering the care-of address

2.3 WLAN

A wireless LAN (WLAN) is typically an extension of a wired LAN. WLAN components convert data packets into radio waves or infrared (IR) light pulses and sends them to other wireless devices or to an access point that serves as a gateway to the wired LAN.

2.3.1 IEEE 802.11

802.11b

Most WLANs today are based on the IEEE 802.11b standard for wireless communication between devices and a LAN. This standard permits data transmissions at 5 to 11 Mbps. Most 802.11 access point works as a bridge between Ethernet 802.3 and 802.11.

802.11e MAC Enhancement

The purpose of 802.11e is to enhance the current 802.11 MAC to improve and manage Quality of Service (QoS) requirements and support multimedia. Improvements in security and authentication mechanisms are also in the scope of 802.11e. The 802.11e standard is not published yet.

802.11f Inter-Access Point protocol

The 802.11f Inter-Access Point protocol specifies the MAC and PHY layers of a WLAN system and includes the basic architecture of Access Points and Distribution Systems. The main purpose of the protocol is to specify at protocol for Interworking between Access Points to avoid equipment from different vendors to interfere with each other.

802.11g Higher data rates for 802.11b

The 802.11g specifies higher data rate by enhancement of the physical layer specified in 802.11b. The 802.11e standard is not published yet.

802.11a

The 802.11a specification applies to wireless ATM systems and operates at radio frequencies between 5 GHz and 6 GHz. A modulation scheme known as OFDM Orthogonal Frequency-Division Multiplexing (OFDM) makes possible data speeds as high as 54 Mbps, but most commonly, communications takes place at 6 Mbps, 12 Mbps, or 24 Mbps.

2.3.2 HIPERLAN2

High Performance Radio LAN 2 (HIPERLAN 2) specifications are developed by ETSI and the first specifications was published May 2000. The general features of the HiperLAN2 technology are high-speed transmission, connection-oriented, Quality-of-Service support, automatic frequency allocation, security support, mobility support, network & application independent and power save. The transmission rate at the physical layer extends up to 54 Mbit/s. At layer 3 the transmission speed is up to 25 Mbit/s

In a HiperLAN/2 network, data is transmitted on connections between the MT and the AP that have been established prior to the transmission using signalling functions of the HiperLAN/2 control plane. Connections are time-division-multiplexed over the air interface. There are two types of connections, point-to-point and point-to-multipoint. Point-to-point connections are bi-directional whereas point-to-multipoint are unidirectional in the direction towards the Mobile Terminal. In addition, there is also a dedicated broadcast channel through which traffic reaches all terminals transmitted from one AP.

The connection-oriented nature of HiperLAN/2 makes it straightforward to implement support for QoS. Each connection can be assigned a specific QoS, for instance in terms of bandwidth, delay, jitter, bit error rate, etc. It is also possible to use a more simplistic approach, where each connection can be assigned a priority level relative to other connections.

2.3.3 IEEE 802.15 WPAN

The IEEE 802.15 Wireless Personal-Area Network (WPAN) is divided into three projects, Bluetooth, Coexistence and WPAN High Rate. The 802.15 standard is not published yet.

2.4 Mobility issues

Mobile wireless networks and fixed networks behave different because of the radio interface. The radio interface involves a higher bit error rate and different distribution of bit errors than fixed networks. The delay in mobile systems is often longer and varies more than in fixed networks. The bandwidth is natural limited in wireless networks, and will generally be lower than in fixed networks.

The Internet and Internet services known today are not designed for the issues linked to wireless access. The behavior of Internet protocols can also increase the effect of the problems related to the radio interface. For instance the TCP protocol takes no regard to the variation in data rate and delay or the bit error rate. The radio canal changes characteristic frequently. Packet losses caused by fading on the radio canal can lead TCP to reduce the congestion window [17]. In the moment just after the packet loss the characteristic of the radio canal can be good, but will not be made the most of because of reduced congestion window.

The mobility requirements must be seen in accordance with the limitations wireless access brings.

3 Technical solutions

This chapter will look at different possible solutions for handover between WLAN 802.11b and GPRS. The solutions are based on different levels of integration, telecom integrated and IP level integration.

3.1 Telecom integrated solution

When considering possibilities of doing a handover between GPRS and WLAN on a telecom level, a WLAN segment must be integrated into the GPRS network. The thought behind this solution was to integrate “bridge” between the GPRS network and a WLAN network segment.

The transmission plane in GPRS is defined through nodes and interfaces as shown in the figure below.

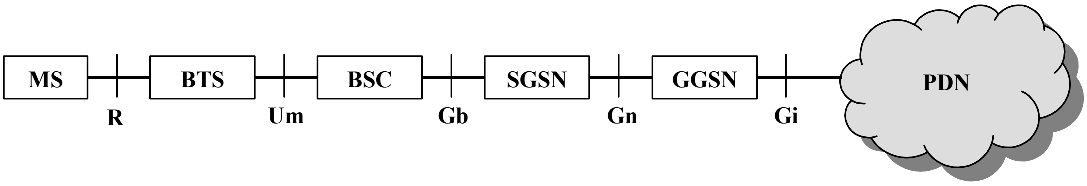


Figure 14 - GPRS transmission plane

The communication protocols defined for each of the GPRS network nodes are shown in Figure 5. It is preferred to avoid forcing modifications to existing GPRS nodes. A bridge between GPRS and a WLAN segment should therefore satisfy one of the interfaces defined between the GPRS network nodes.

Possible solutions are to integrate the WLAN bridge into the Gb or Gn interface. When choosing the solution with the Gn interface the signaling interfaces Gr between SGSN and HLR and Gs between SGSN and MSC/VLR must be taken care of. Predicting that the MS operates in class-C mode, which means the MS is exclusively attached to GPRS services, gives the opportunity to exclude the Gs interface [7]

3.1.1 Gb – Integration

The protocols in towards the Gb interface shown in Figure 5 must be implemented into the WLAN-bridge. The figure below shows possible protocol architecture for the user plane.

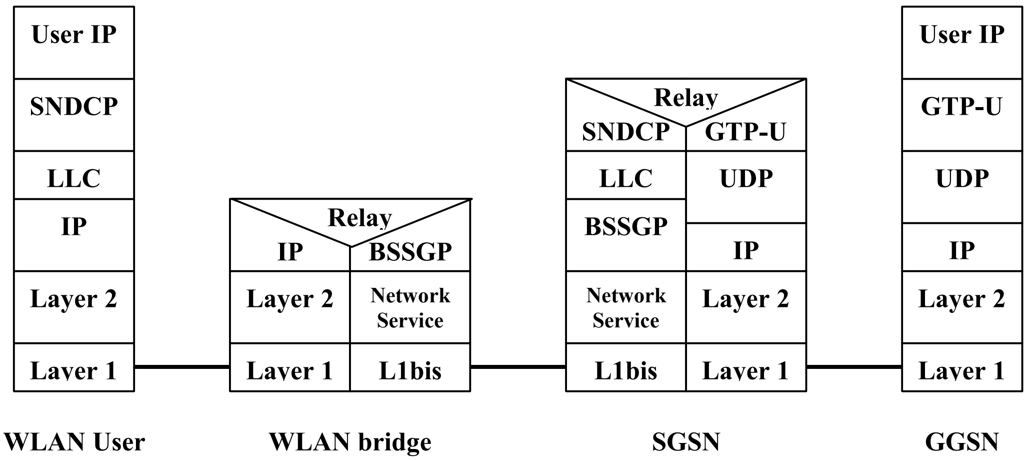


Figure 15 – User plane protocols

The physical layer L1bis [18], Network Service [19] and BSS GPRS Protocol (BSSGP) [11] are protocols that can be implemented into a WLAN bridge. The addressing of the MS from the BSS is handled by the radio Link Control (RLC) and medium access control (MAC).

In the figure above the relay function in the WLAN Bridge must link between BSSGP and IP. The IP address must be assigned when the TE connects to the WLAN. This process can be avoided by integrating the logical link control (LLC) layer and subnetwork dependent convergence protocol (SNDCP) into the WLAN Bridge. This results in the architecture shown in the figure below.

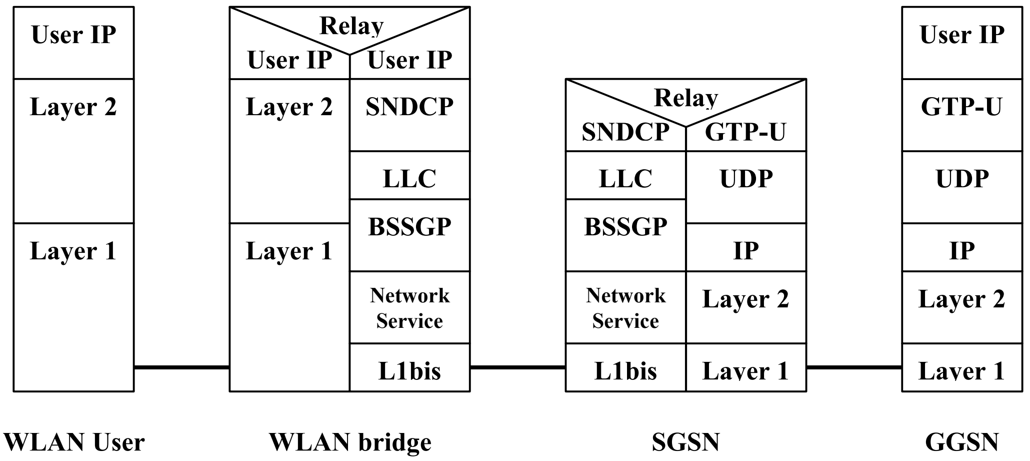


Figure 16 – transmission plane for the WLAN bridge

The LLC layer is designed to provide a highly reliable logical link between the MS and the SGSN. LLC also provides user data confidentiality by means of ciphering function and user identity confidentiality [9].

The SNDCP's main functionality is multiplexing of PDPs, compression and decompression of user data, compression and decompression of protocol control information and segmentation of a network protocol data unit (N-PDU) into Logical Link Control Protocol Data Units (LL-PDUs) and re-assembly of LL-PDUs into a N-PDU [8].

Integration of the LLC layer and SNDCP into the WLAN Bridge makes the implementation of the bridge more complex and simplifies the implementation on the TE.

For user confidentiality the user data between SGSN and the MS is ciphered. Keys used for ciphering is generated by an algorithm on the SIM. Including the LLC and SNDCP into the WLAN Bridge makes it possible to avoid the need of these algorithms on the TE when connecting to the WLAN.

Another reason for integrating the LLC and SNDCP into the WLAN Bridge is to open for using the user IP address for addressing from the WLAN Bridge to the TE. The BBSGP layer can not directly link to the PDP address without the LLC and SNDCP layer.

This is a suggestion for the transmission plane for user data when using WLAN as access technology. For GPRS Mobility Management (GMM) and Session Management (SM) the signaling protocol GMM/SM is used. This protocol must be integrated to the architecture described above.

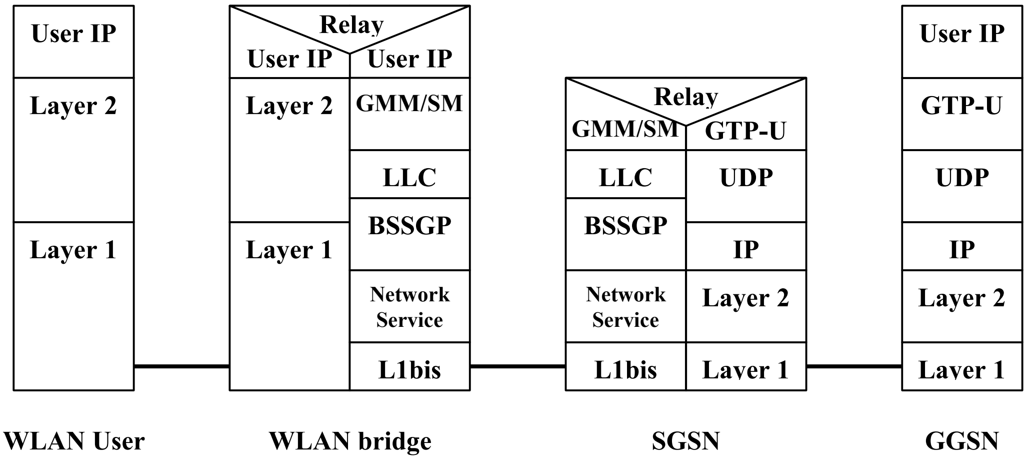


Figure 17- signaling plane for the WLAN Bridge

The main functionality in GMM/SM is as described earlier GPRS attach, GPRS detach, security functions, routing area update, location update, PDP context activation, and PDP context deactivation. These functions require information (i.e., the International Mobile Subscriber Identity (IMSI)) from the Service Identity Module (SIM). This brings out a problem when the TE is attached to WLAN because the only MS can access the SIM.

A possible solution to the problem to access SIM can be to store SIM information of all subscribers in a database connected to the WLAN Bridge.

The MS measure signal strength on neighbour cell in the free time between the assigned TDMA timeslots. The handover procedure is initiated by the network, but is based on these signal strength measurement deliveries from the MS.

The WLAN segment has to look like a cell to the rest of the GPRS network to make it possible to do a handover from GPRS to WLAN and reverse. When the TE discovers sufficient signal strength on the WLAN card the handover process should be started.

The handover between WLAN to and from the WLAN segment will be inter BSC handovers since the WLAN Bridge operates like a BSC seen from the SGSN.

The TE must communicate with lover layer protocols on the MS to inform about the WLAN coverage. The TE must identify the WLAN segment and force the MS to report high signal strength on the WLAN "cell". The WLAN segment must be assigned an own Base transceiver Station Identity Code (BSIC), which the TE reports to the MS. The MS must report god signal strength on the BSCI to force the system to initiate a handover.

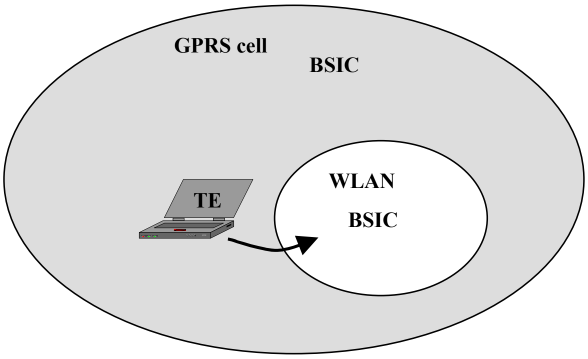


Figure 18 – BSIC for WLAN segment and GPRS cell

When the TE moves out of the WLAN coverage a new problem shows up. The ME must retrieve information from the MS about which cells the signal strength is god and force the WLAN bridge to report this back to the network and in that way force a handover. A simplification can be to configure the WLAN bridge with a standard cell to report with good coverage when the TE reports low signal strength on the WLAN interface. The WLAN coverage is much smaller than the coverage area of a GSM cell. It would therefore be possible to plan the cell structure in a way that the same cell covers the whole WLAN coverage area. This is shown in Figure 18.

The routing area (RA) update is a little less complex than the handover procedure. RA update is done periodic or when the MS is moving between RAs. The MS and not the network initiate these updates. As shown in Figure 17 is the GMM/SM protocol implemented into the WLAN bridge, which in this case means that the WLAN bridge can initiate a RA update when the TE connects to the WLAN segment. The MS will perform RA updates periodic, and must therefore be noticed to not do so when the TE is attached to WLAN segment. When the TE moves out from the WLAN coverage area the MS must be forced to do a RA update, and then the TE will be attached to the GPRS radio interface.

Evaluation

The solution sketched out above may be possible, but it requires a lot of effort in implementation. The transmission plane shown in Figure 16 seems to be relatively straightforward to implement. The TE sees a standard GPRS connection when attached to the GPRS radio interface and standard IP when attached to the WLAN segment. It requires some software modification on the TE to be able to use both the MS and the WLAN interface with the same IP address.

The main problems with this solution seem to be the need for SIM information on the TE and in the WLAN Bridge. The SIM information can only be read by the MS and will therefore demand an interface for communication with lover level protocols on the MS.

The signalling plane with GMM and SM can also be problematic. Each BTS broadcast information about them selves which contain RA and BSCI The MS must be award of the BSCI belonging to the WLAN segment to be able to force a handover based on signal strength measurement.

A complete implementation of the solution should give the user full mobility, but the data rate can be limited because of the capacity on the physical layer in the Gb interface. The use of Frame Relay in the Gb interface limits the data rate to 2Mbps, which can be scanty when the WLAN offers up to 11Mbps.

The security is not elaborated here, but must be considered. The need of SIM information on the TE and in the WLAN bridge can be security problem. The integrate of GMM/SM and LLC into the WLAN bridge reduces the security problem since it then will be less use of sending SIM information over the WLAN radio interface.

If a large amount of user are attached to the WLAN segments will the load in the GPRS backbone increase a lot because of the data rate difference between GPRS and WLAN. The load problem will be greatest in the Gb interface because of the limitations on the physical layer. The load in the Gn should be less of a problem since it can be an optional IP network that should be possible to scale up.

3.1.2 Gn / Gr – Integration

The solution described above leads to several implementation problems. The following section will be an elaboration of a solution where the WLAN bridge is moved to the Gn interface located between GGSN and SGSN.

The GTP protocol at the Gn interface is the only non-standard Internet protocol in the interface. At first glance this seems to be relatively straightforward implementation, but the signalling interface Gr towards HLR must also be supported.

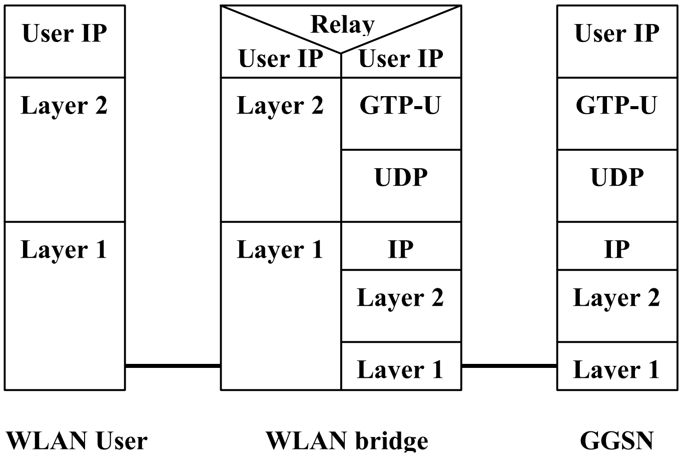


Figure 19 – transmission plane

The figure above shows the transmission plane from the GGSN to the WLAN interface on the TE. The GTP-U is the user plain of GTP, which provide a service for carrying user data packets [20]. GTP also specifies a tunnel control and management protocol

(GTP-C) which allows the SGSN to provide packet data network access for an MS. Control Plane signaling is used to create, modify and delete tunnels, which are one of the most essential features in the creation of connectivity to GPRS services.

The GTP-U message contains a tunnel end point identifier (TEID) field in the header. On the SGSN the TEID is linked with Network Service Access Point Identifier (NSAPI) in the SNDCP [8]. The NSAPI is an index to the PDP context of the PDP that is using the services provided by SNDCP [7].

The TEID can be ignored at the WLAN Bridge as long as further addressing can be done by the user IP (PDP address), but the TEID is required in the PDP context activation procedure. The GGSN includes this TEID in the GTP header of all subsequent downlink G-PDUs that are related to the requested PDP context.

Signalling interfaces Gr and Gs

As shown in Figure 7 the signaling plane between SGSN and HLR is built on MAP. This signaling between HLR and SGSN includes information related to location updates, routing information, user profiles, and handovers [21]. The protocols at the Gr interface must be integrated into the WLAN Bridge.

A signaling interface between SGSN and MSC/VLR is defined over the Gs interface. It should be possible to ignore this interface at the WLAN bridge as long as the MS operates in class-c mode, which means the MS is exclusively attached to GPRS services.

The handling of routing area updates and handover procedures will be the main challenge. The routing area updates requires the MS to inform the GPRS network about its current location. The WLAN segment must have its own RA that can be reported as a location of an MS. The handover procedure requires the WLAN segment to be assigned to an own BSIC. The GPRS network will initiate the handover process when the MS reports strong signal strength on WLAN BSIC .

Evaluation

This solution causes some major implications on the user equipment. Information and algorithms stored on the SIM card must be accessible for the TE also when connected to WLAN. The handling of the SIM information needed for identification of the user when he is attached to WLAN segment can cause a degradation of the security.

The implementation of the WLAN Bridge is complex due to the requirement of satisfying both the Gn and the Gr interface. Implementation of the MAP signalling over the Gr interface is likely to be the most complicated part of the bridge implementation, but it should be feasible to do without affecting the existing network nodes.

A complete implementation of this solution will give the user full mobility. The GPRS network will not limit the data when the user is attached to the WLAN segment. The backbone in the Gn interface is not specified on lower level an will there fore be possible to scale up.

3.2 IP level integrated solution

As described earlier is Mobile IP a mechanism to handle mobility on the IP level. Mobile IP is designed to be transparent for routers and servers in the Internet. When looking at the GPRS from outside through the Gi interface the GGSN is seen as a normal IP router shown in Figure 8 [12]. It should therefore be possible to integrate Mobile IP also when using GPRS as one access technology.

The mobile IP specification is designed for handover between different access technologies, but not when their coverage areas are overlapping. In most cases the WLAN coverage are also is covered by GPRS. The Mobile IP software on the mobile node must therefore be implemented for the possibility to use one access technology as preferred.

The WLAN signal level should be measured periodic once a second or so. If the signal strength is at an acceptable level the mobile node should try to find a care-of address from the WLAN network and register it with its home agent.

It is various solutions for handover between GPRS and WLAN using mobile IP. The location of home agent and foreign agents can be done in different ways.

When using Mobile IP for linking WLAN and GPRS the placement of home agent and foreign agents can be done in different ways. The following part will sketch some possible solutions and take a look at advantages and disadvantages with each solution.

3.2.1 Home solution

The first solution considered with mobile IP was to locate a home agent at a home network any place in the Internet. The location could, e.g., be on a company network or it could belong to an ISP.

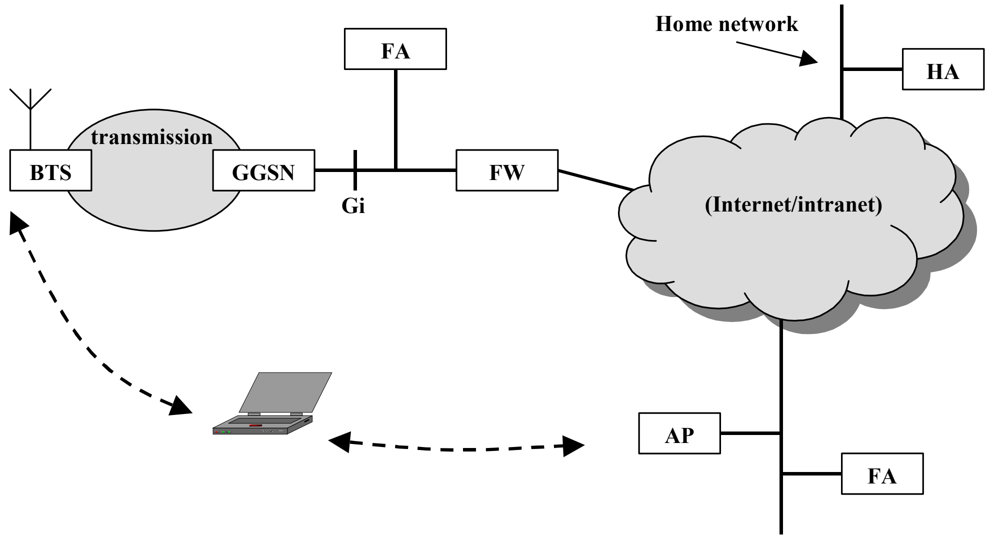


Figure 20 – Home solution

Foreign agents must be located at all veritable networks both the GPRS network and WLAN networks. As described earlier is the WLAN AP a bridge between Ethernet 802.3 and WLAN 802.11(b). The FAs located at the WLAN segment can therefore use standard implementation as specified for mobile IP [13].

The location of a FA in the Gi interface outside the GGSN cases some problem according to the mobile IP specification. The MN's care-of address in this case would be an IP address belonging to the FA. The home agent forwards packets addressed to the foreign agent which dencapsulate the datagrams and forwards them to the mobile node. The mobile IP standard specifies the foreign agent to use link-layer protocols to forward messages to the mobile nodes. For a FA located in the Gi interface the mobile node can be addressed only by its IP address, which requires some modification according to the mobile IP standard.

Modifications of the FA software on the FA located in the Gi interface should not affect other mobile nodes. The FA in the Gi interface must be modified to link the mobile nodes home addresses to the IP address they are assigned from the GGSN instead of using link-layer addressing.

Evaluation

From the users point of view the location of the home agent at a arbitrary point of attachment to the internet seems to be obvious. This solution opens for placement of HA at a corporate network or an ISP dependent of what is best for the current user. A mobile node located at the home network operates as a fixed node. Location of the home agent at the network where the mobile node is situated most of the time will decrease the load on the network and the mobility nodes.

From the operators point of view this solution require small changes in the network architecture. The placement of a FA in the Gi interface will not affect other nodes in the network.

Implementation of the FA located at the Gi interface require some modifications of standard FA implementations because of the impossibilities of physical addressing of mobile nodes situated connected to the GPRS network.

3.2.2 Operator dependent solution

To avoid the modification of the FA software in the Gi interface a solution with the home agent located at the Gi interface considered. When the home agent is located in the Gi interface the telecom operator must offer a static IP address as home agent for all mobile nodes.

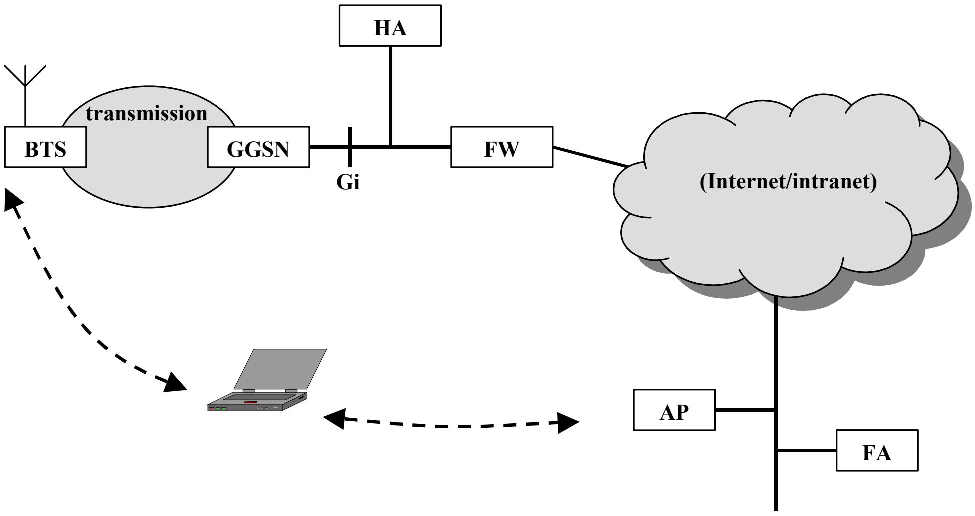


Figure 21 – Operator dependent solution

Both home agent and foreign agents could with this architecture operate at specified in the mobile IP standard. The home agent is able to se all data packets addressed to a mobile node, and can forward the packets to the care-of address when the mobile node is away from its home network.

Evaluation

From the users point of view it could be a disadvantage with a home agent belonging to the telecom operator. It could be desirable not to be dependent of the operator of one access technology. If the same operator delivers a packet with both WLAN and GPRS would it be out of consequence where the home agent is located.

From the telecom operators point of view it seems to be a solution with possibilities create dependence among customers. The greatest disadvantage will be the load on the network in the Gi interface. This network must be dimensioned for a much higher rate of data because of the extra traffic routed through the HA. A user situated at a WLAN spot will create a lot more traffic in the Gi interface than when he is situated at the GPRS home network. Today the WLAN data rate can be more than a hundred times the GPRS data rate.

The implementation of this solution requires no modification of the Mobile IP standard.

3.2.3 Independent solution

A solution independent of both telecom operator and WLAN operator is possible if the mobile uses co-located care-of addresses when it is away from its home network.

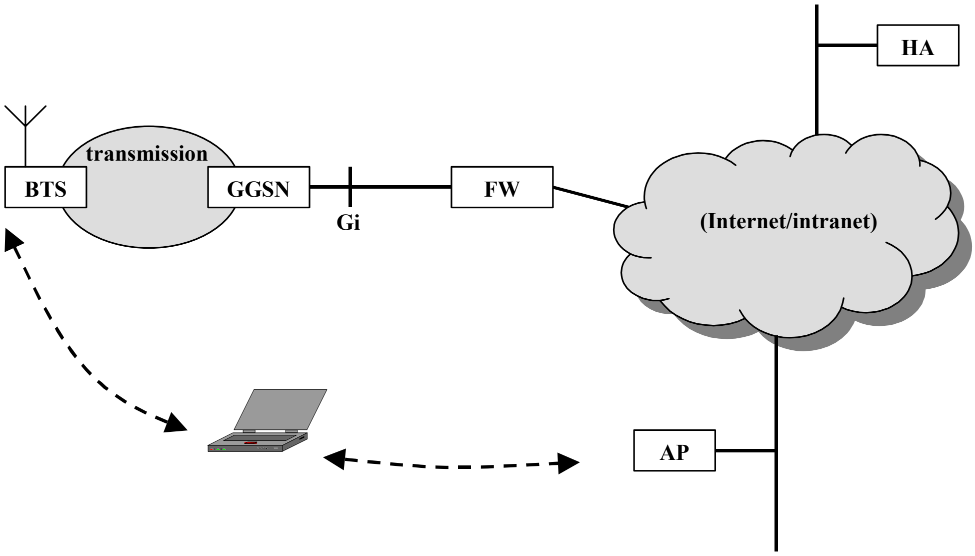


Figure 22 – Independent solution

Co-located care-of address demands that each mobile node obtain its own IP address belonging to the foreign network. This IP address will be used as the endpoint of the tunnel between the HA and the MN. The home agent can be situated at any network, either at a company network or an ISP.

Evaluation

From the user point of view this solution seems to flexible and should not be problematic fore any services. The double IP header is a small disadvantage because of the small bandwidth with GPRS. The IP header usually is 20 octets and the IP packet size is from 500 octets to 1500 octets the extra header is from 0,5 % to 1,5 % [17]. The use of a co-located care-of address gives opportunities to implement more flexibility on the mobile node. Transparent mobility support of mobile IP is important to long-lived connection-oriented traffic and for traffic initiated by correspondent hosts. For applications generating this kind of traffic the mobile node's home address will be used, and mobility is supported.

For more short-lived connections as web browsing traffic the mobile node can use the mobile node's care-of and work as a fixed node. This will reduce the load on home agents and foreign agents.

Both WLAN and telecom operators should not be affected of the use of mobile IP with this solution as long as the mobile node require an own IP address while it operates without support of mobility. From the WLAN operator the use of a co-located care-of address require that all mobile nodes get their own IP-address while visiting the network. (må finne ut om eventuelle problemer med bruk av private IP-adresser).

Implementation of this solution requires no changes to the mobile IP standard.

3.2.4 Prospective solution

The 3GPP has in release 1999 specified that a foreign agent can be integrated into the GGSN.

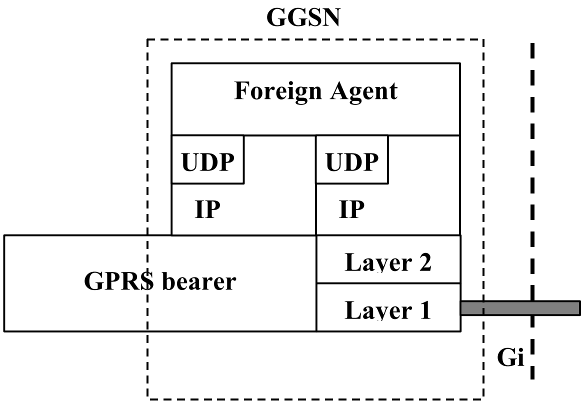


Figure 23 - FA integrated to the GGSN [12]

The FA in the GGSN will be configured with at least one care-of address. In addition a FA must maintain a list that combines IP addresses with Tunnel End-point Identifiers (TEIDs) of all the visiting MSs that have registered with the FA. IP packets destined for the MS are intercepted by the HA and tunneled to the MS's care-of address, i.e. the FA. The FA de-tunnels the packets and forwards the packets to the MS. Mobile IP related signaling between the MS and the FA is done in the user plane. MIP registration messages are sent with UDP.

The figure below shows the PDP context activation and Mobile IP registration process when the MS take use of the foreign agent in the GGSN.

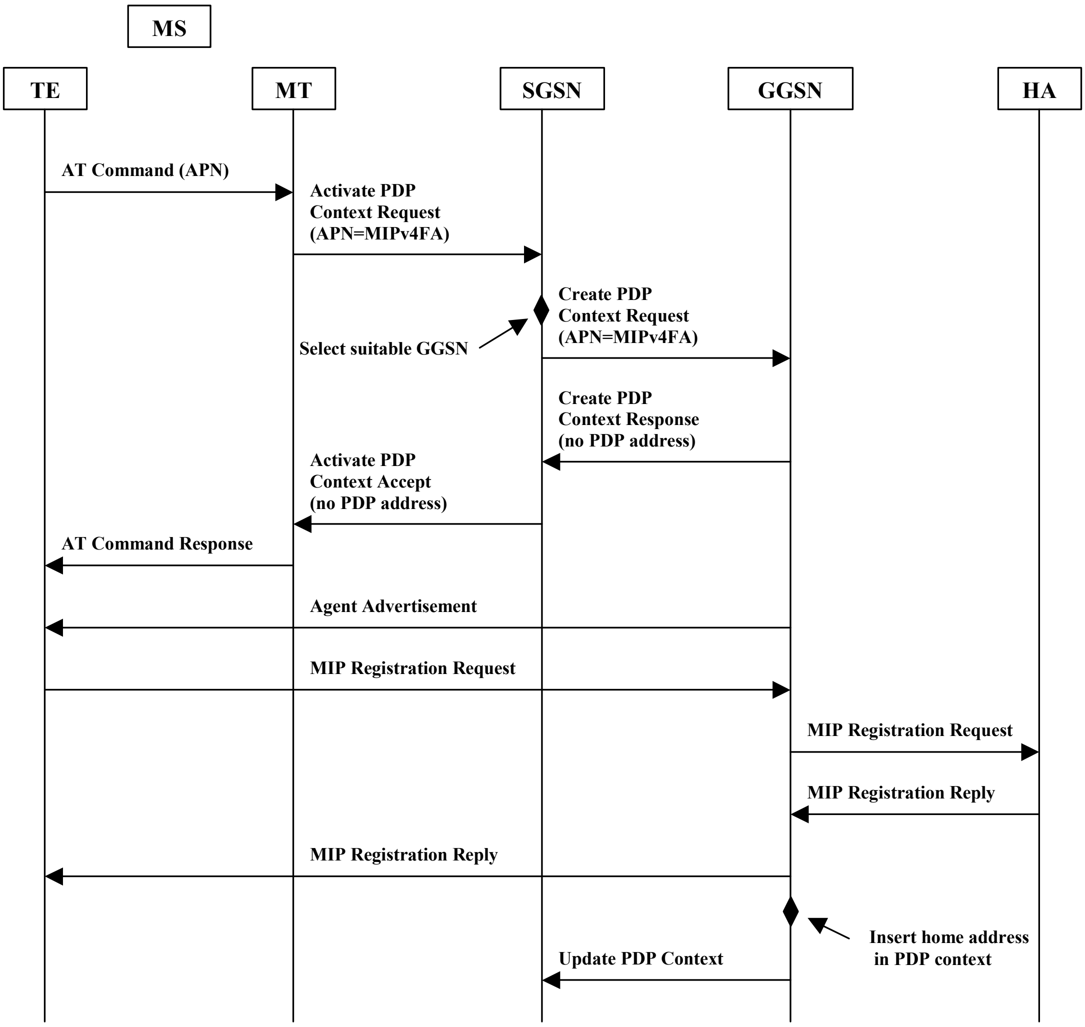

MS
TE
MT
SGSN
GGSN
HA
AT Command (APN)
Activate PDP Context Request (APN=MIPv4FA)
Select suitable GGSN
Create PDP Context Request (APN=MIPv4FA)
Create PDP Context Response (no PDP address)
Activate PDP Context Accept (no PDP address)
AT Command Response
Agent Advertisement
MIP Registration Request
MIP Registration Request
MIP Registration Reply
MIP Registration Reply
Insert home address in PDP context
Update PDP Context

Figure 24 - PDP context activation with Mobile IP [12]

The TE sends the "Activate PDP Context Request" to the SGSN. The message includes various parameters of which the "APN" (Access Point Name) and the "Requested PDP Address" are of interest here. The "Requested PDP Address" should be omitted for all MS's using Mobile IP. This is done irrespective of if the TE has a permanently assigned Mobile IP address from its Mobile IP home network, a previously assigned dynamic home address from its Mobile IP home network or if it wishes the Mobile IP home network to allocate a "new" dynamic home address [12].

A Create PDP Context Response is sent from the GGSN/FA to the SGSN. If the GGSN has been configured, by the operator, to use a Foreign Agent for the requested APN, the PDP address returned by the GGSN shall be set to 0.0.0.0. indicating that the PDP address shall be reset by the MS with a Home Agent after the PDP context activation procedure.

The FA forwards the Mobile IP Registration Request to the home network of the mobile node, where a home agent (HA) processes it. Meanwhile, the GGSN/FA needs to store the home address of the mobile node and the local link address of the MS, i.e. the TEID (Tunnel Endpoint ID).
Foreign agent integrated to the GGSN gives eh opportunity to the architecture shown below.

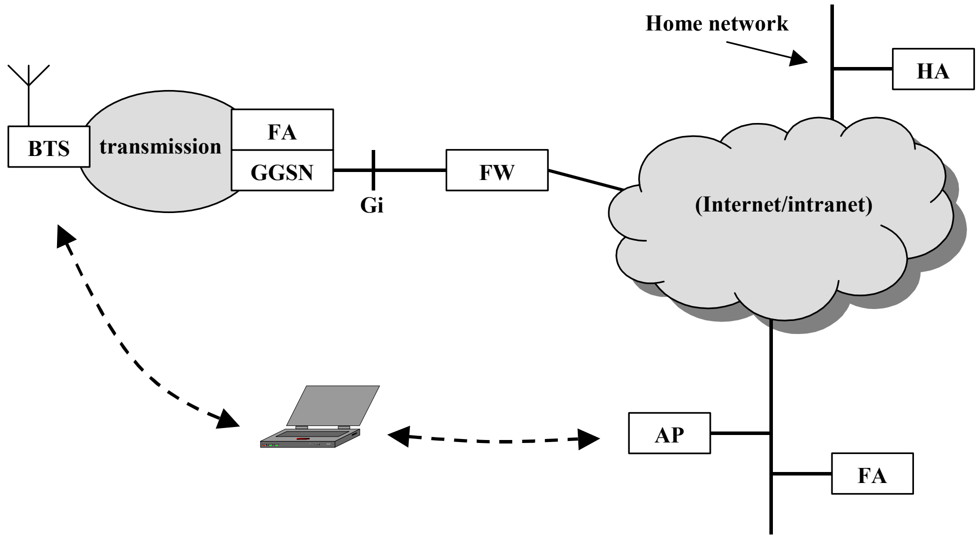


Figure 25 - Foreign Agent integrated to GGSN

This architecture is almost like the first one considered, with FA in the Gi interface. The main difference with this architecture is that the FA uses the TEID to address the mobile node.

Evaluation

From the users point of view will this solution look much like the solution with foreign agent located in the Gi interface.

The telecom operator will with this solution be able to offer access to foreign agent without locating new nodes in the Gi interface. The demand for IP addresses will also be reduced because of the TEID addressing between the FA and the MN cases no need for the mobile node to obtain an IP address belonging to the GGSN.

Implementation of this solution is depending on the suppliers of GPRS nodes. The HA and FAs with different point of attachment to the Internet can us software implementations that follows the mobile IP standard.

4 Discussion

The various solutions for handover between GPRS and WLAN described in the previous chapter should be valuated from criteria like user functionality, complexity of implementation and flexibility. The telecom-integrated solutions described in section 3.1 require implementation of new nodes into the existing GSM/GPRS network and a considerable amount of new functionality must be developed to the user equipment. The IP level integration solutions described in section 3.2 affects protocols on a higher level than the telecom integration solutions.

The implementation of the user equipment for both the telecom-integrated solutions described in section 3.1.1 and 3.1.2 will be exactly the same. This solution requires some integration between the WLAN card and the GPRS MS. The MS identifies itself through transmitting IMSI or TMSI on the signaling plane to the GSM/GPRS network. The IMSI/TMSI must be used for identification when the TE is attached to the network through the WLAN interface if the connection of a WLAN segment towards the GPRS network shall be transparent for existing network nodes. Authentication and Key Agreement (AKA) procedure requires SIM information.

Implementation of a WLAN bridge attached to the Gb or Gn interface seems to be relatively simple for the transmission plane, but somewhat more complex for the signaling plane. The Gb integration solution described in section 3.1.1 has only the Gb interface to satisfy. The specified a interface towards the MSC/VLR can be left out assuming the MS works in class-c mode.

The integration at the Gn interface described in section 3.1.2 requires a WLAN bridge that contains the signaling interface Gr. The Gr interface makes the implementation of the WLAN Bridge complex because of the MAP signaling part that must be implemented.

The main challenge with both of the proposed telecom-integrated solutions is the integration of mobility management with Routing Area and Base transceiver Station Identity Code.

The described IP-level integrated solutions in section 3.2 are all based on Mobile IPv4. Mobile IP mobility management operates on the IP protocol. Solutions based on Mobile IP will therefore be possible to make transparent for the GPRS network and will therefore be relatively easy to implement.

All suggested IP level solutions could with some small modifications be implemented as specified in the Mobile IP standard. The use of different access technologies requires some logic for the selection of interface to use. This should be based on the signal strength measured at the WLAN interface and should be fairly easy to implement.

The home solution described in section 3.2.1, with the home agent at the home network, may at first time look as the obvious way to locate the agents whether it is a company network or an ISP. The implementation of the FA located at the GPRS network requires some changes within the mobile IP standard.

The operator dependent solution described in chapter 3.2.2 requires that the users home address belong to the telecom operator. This may look adequate from a telecom operator's point of view, but it can result in unnecessary load on the home agent and in the home network. This solution will also induce increased operator control of the WLAN users.

The independent solution described in section 3.2.3 will not affect the foreign network as long as they provide an IP address for each user. The disadvantage with this solution is the use of IP addresses on the foreign network. The need for more IP addresses can be a problem when a large number of users are visiting the same network.

The prospective solution that is proposed in section 3.2.4 fits fully with all the functionality in the mobile IPv4 standard. The insecurity related to the time aspect for implementation of FA in GGSN speaks against this solution.

5 Conclusion

Different solution with different level of integration has been evaluated. The first solutions described how to integrate WLAN with the GPRS network through the Gm or the Gb interface. Both of these solutions require some extensive challenges to be met for realization. The largest problem seems to be related to the user equipment, which require possibilities to communicate with lower level protocols on the MS for accessing SIM information. A complete implementation of these solutions should have the functionality to handle the mobility requirements efficiently, but in relation to the foreseen implementation complexity will these solutions not be recommended. The efficient mobility management carries less of weight because of the mobility limitations caused by the round trip time in the GPRS network.

The IP level solutions is of less effort to implement. Implementation of the home agent and foreign agents require no modification related to the mobile IP standard in most of these solutions. The user equipment requires some added algorithm for the selection of either to use GPRS or the WLAN network interface.

The various solutions of home agent and foreign agent placement have different qualities. Most of these qualities can be added into one solution by combining them.

The proposed (operator dependent) solution where HA is located at the Gi causes user traffic to be routed through the network segment outside the Gi interface. With a large number of users located at foreign networks, the extra load on the home network will be considerable. A location of Home Agents that is independent of the operator networks will spread the load to more than a single home network and a single home agent.

Use of foreign agent reduces the need for IP addresses and will therefore be preferred at WLAN segments. From the WLAN operators' point of view it is advantageous to use foreign agents for better controlling the traffic on the network. A foreign agent located at the Gi interface must use the mobile node IP address when forwarding messages, and will therefore not reduce the use of IP addresses.

The recommended solution will be to locate the home agent independently of both WLAN operator and telecom operator. This suggests a location of the home agent either at a corporate network or an ISP. Foreign agents are preferred to use at WLAN networks, but the mobile node should be enabled for use of co-located care-of address if no foreign agent is present. Co-located care-of address should also be used when connected to the GPRS network if no foreign agent is implemented into the GGSN.

6 References

[1] UNINETT (2001, may 23) [online]. - URL: http://www.uninett.no/prosjekt/trondlost/

[2] Telenor R&D *"I-CELL"*. Kjeller, Telenor Research & Development, 2000. (FoU R 21/2000)

[3] WAP Forum (2001, may 23) [online]. URL: http://www.wapforum.org/

[4] IEEE, *"Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications"* 1999 (ANSI/IEEE Std 802.11)

[5] IEEE, *"Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications"* 1999 (ANSI/IEEE Std 802.11b)

[6] IT Avisen, (2001, may 23) [online]. URL: http://www.itavisen.no/art/1296202.html

[7] 3GPP, *"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description; Stage 2 (Release 1999)"*. (3G TS 23.060 v3.4.0)

[8] 3GPP, *"3rd Generation Partnership Project; Technical Specification Group Core Network; General Packet Radio Service (GPRS); Mobile Station (MS) - Serving GPRS Support Node (SGSN); Subnetwork Dependent Convergence Protocol (SNDCP) (Release 1999)"*. (3G TS 24.065 V3.1.0)

[9] 3GPP, *"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)"* (3G TS 04.64 version 8.6.0)

[10] 3GPP, *"Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Mobile Station (MS) - Base Station System (BSS) interface; Radio Link Control/Medium Access Control (RLC/MAC) protocol (Release 1997)"*. (3G TS 04.60 version 6.10.0)

[11] 3GPP, *"Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Base Station System (BSS) - Serving GPRS Support Node (SGSN); BSS GPRS Protocol (BSSGP) (Release 1999)"*. (3G TS 08.18 version 6.1.0)

[12] 3GPP, "Packet Domain; Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN)". (3G TS 29.061 V3.3.0 - Release 1999)

[13] Charles E. Perkins, *"IP Mobility Support"*, (RFC 2002 – 1996)

[14] S. Deering, *"ICMP Router Discovery Messages"*, RFC 1256 – 1991

[15] Charles E. Perkins, *"IP Encapsulation within IP"*, RFC 2003 – 1996

[16] Charles E. Perkins, *"Minimal Encapsulation within IP"*, RFC 2004 – 1996

[17] Larry L. Peterson & Bruce S. Davie, *"Computer Networks: A System Approach"*, Morgan Kaufmann 2nd ed. 2000, ISBN: 1-55860-577-0

[18] 3GPP, *"Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Base Station System (BSS) - Serving GPRS Support Node (SGSN) interface; Gb interface Layer 1 (Release 1999)"*. (GSM 08.14 version 8.0.0)

[19] 3GPP, *“Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Base Station System (BSS) - Serving GPRS Support Node (SGSN) interface; Network Service (Release 1999)”*. (GSM 08.16 version 8.0.0)

[20] 3GPP, *“3rd Generation Partnership Project; Technical Specification Group Core Network; General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface (Release 1999)”*. (3G TS 29.060 V3.5.0)

[21] 3GPP, *“Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Mobile Application Part (MAP) specification (Release 1999)”*. (3G TS 29.002 V3.5.1)

[22] http://www.etsi.org/bran/

Appendix A

This appendix will describe an attempt to implement a solution for handover between GPRS and WLAN using Mobile IPv4.

Software

The software chosen for implementation was Sum Microsystems Mobile IPv4 software. In this implementation the source code for both Solaris and Linux is available through a license agreement. The license agreement grants an unlimited access to modifications and use of the code as long as it is not used for commercial purposes. The software implementation of Mobile IP consists of two components:

- The mobility agent software incorporates home agent and foreign agent functionality. Each network on which mobility support is desired should have at least one static (non-mobile) host running this software.

- The mobile node software incorporates Mobile IP client functionality. The software should typically run on a laptop.

ReadHat Linux 7.0 was chosen for operative system (OS). Other software used is Microsoft Network Monitor 2.0 v5.00.943.

Hardware

The hardware used for implementation are listed in the table below.

Equipment	**Manufacture**	**Designation of type**
Portable PC	Fujitsu Siemens	Lifebook E-Series
PC	Cinet	Cinet PPI-600
Ethernet Hub	UNEX	HA080
GPRS phone	Motorola	Timeport 260
WLAN Access point [1)]	Ericsson	AP-10D PRO.11
WLAN Card [2)]	Ericsson	SA-PCR PRO.11

[1),2)] The WLAN Access point and WLAN Card are manufactured by BreezeCOM and marked with Ericsson product name.

Desired architecture

The following network architecture was desired to use. The location of home agent and foreign agent is not in accordance with the recommended solution. The reason for the chosen solution is based on the functionality supported by the SUN Mobile IP software.

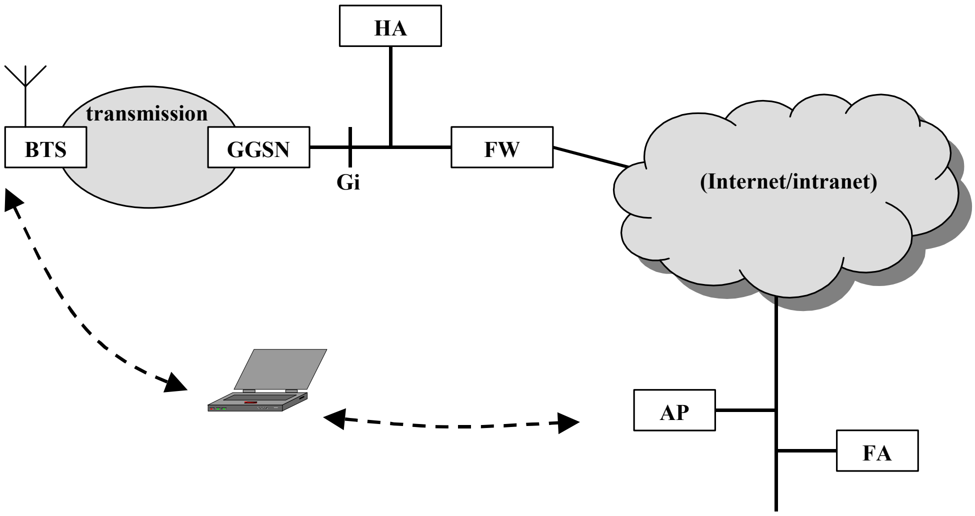


Figure A1 -Chosen architecture

The Mobile IP software does not support the use of co-located care-of address. This results in some problems when connected to the GPRS network. Locating the HA in the Gi interface is the only possible solution that require no modification of the mobility node software. As described earlier must a FA located in the Gi interface use the mobile nodes IP address for datagram delivery.

Mobility agent configuration

RedHat Linux 7.0 was installed on the Cinet P-600. The original kernel distributed with RedHat 7.0 is 2.2.16-22. Some unidentified problems appeared with this kernel version and the Mobile IP software. To avoid these problems the kernel was changed to the older version 2.2.5. With this kernel the software can be configured as described in the documentation delivered with the Mobile IP software [A1].

After installing the software both home agent and foreign agent functionality was tested. Agent advertisements was periodically broadcasted from both HA and FA. The agent advertisements were monitored with Network Monitor and seem to be correct.

Mobile node configuration

The Fujitsu Siemens portable PC was used fore mobile node. RedHat Linux 7.0 was installed and the kernel was changed to version 2.2.5. The original PCMCIA packet delivered with RedHat 7.0 did not work together with kernel 2.2.5 and was therefore changed with the pcmcia-cs-3.0.9.

The PCMCIA WLAN Card was installed using BreezeCOM Linux Driver version 1.0 [A2]. This driver works with the pcmcia-cs-3.0.9 packet with some small modifications. The installation description delivered with the driver was followed almost through the whole installation. The only change done was to change the line
module "xbrzcom_cs" opts "ess_id=ESSID1 irq_list=10,11 verbose=0 to
module "xbrzcom_cs" opts "-f ess_id=ESSID1 irq_list=10,11 verbose=0

The mobile phone was configured with the standard modem configuration script delivered with RedHat 7.0. This is one opportunity of many for configuration modems on Linux systems. The AT command used was: at+cgdcount = 1, "IP", "internet", “0.0.0.0”, 0, 0 Different data rates was tested and 56kbps seems to be the only stable data rate.

The mobile node software was implemented and tested. When linking only the WLAN interface (eth1) to the configuration file the software seems act well.

The mobile node software must be modified to selectively choose the network interace to use. The chose of interface to use should be based on the signal strength measurements. The signal strength can be read from the file ‘/proc/net/BreezeCOM’.

The signal strength levels chosen for handover are based on some simple tests and should probably be optimized on a later stage. The signal strength lower than –74dB initiate lead to handover to GPRS. The handover limit to GPRS was chosen to be –70dB. These values make a hysteresis that avoids the mobile node to do constantly change make handovers when the signal strength is at a certain level.

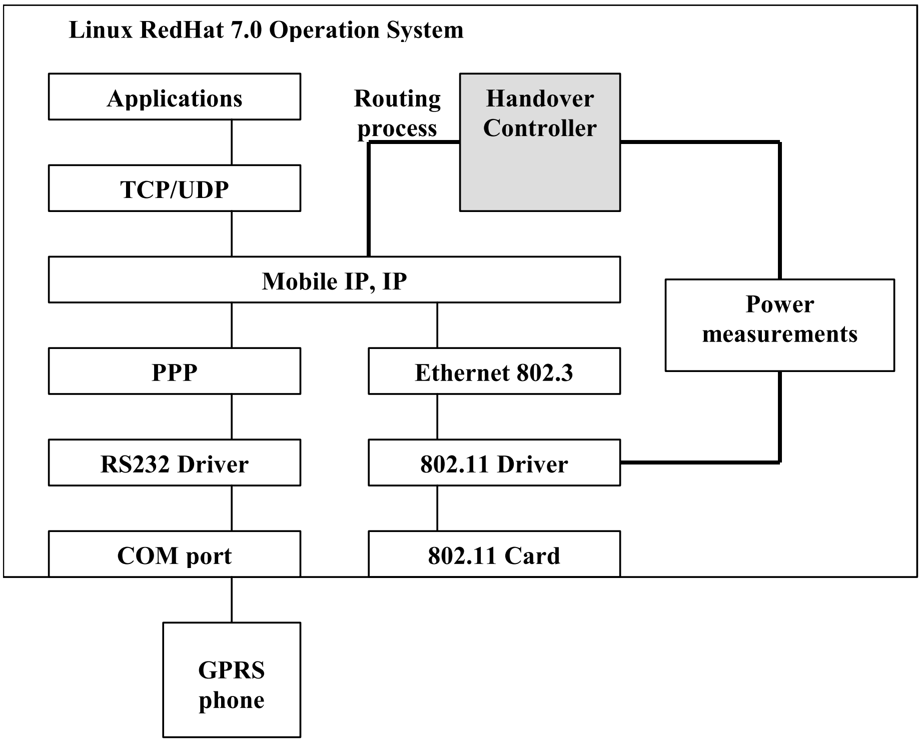


Figure A2 - Handover architecture and protocol stack

The implementation of the architecture shown above was not fulfilled because of the time limitations of the project.

[A1] SUN Microsystems, *“Solaris Mobile IP: Design and Implementation”*, 1998

[A2] BreezeCOM, *“BreezeNet SA-PCR PRO.11 Linux Driver README”*, 1999