Wireless Internet Access for Mobile Subscribers Based on the GPRS/UMTS Network

Jeong-Hyun Park, ETRI

ABSTRACT

With the advent of IP technologies and the tremendous growth in data traffic, the wireless industry is evolving its core networks toward IP technology. Enabling wireless Internet access is one of the upcoming challenges for mobile radio network operators. General Packet Radio Service is the packet-switched extension of GSM and was developed to facilitate access to IP-based services better than existing circuit-switched services provided by GSM. In this article we illustrate how a visited mobile subscriber on a GPRS/UMTS network can access his/her home network via the gateway GPRS support node (GGSN). We also propose some implementation ideas on wireless Internet access for a remote mobile subscriber based on a GPRS/UMTS network.

INTRODUCTION

In recent years, Internet technology has emerged as the major driving force behind new developments in the area of telecommunications networks. The volume of packet data traffic has increased at extreme rates. In order to meet these changing traffic patterns, more and more network operators adapt their strategies and plan to migrate to IP-based backbone networks. Clearly, the Internet will dominate our daily life in the future much more than today.

Meanwhile, mobile networks face a similar trend of exponential traffic increase and growing importance to users. In some countries, such as Korea, the number of mobile subscriptions has recently exceeded the number of fixed lines. This tremendous success was not expected in the 1980s, when today's second-generation mobile communication systems were designed.

The combination of both developments, the growth of the Internet and the success of mobile networks, suggests that the next trend will be an increasing demand for mobile access to Internet applications. It is therefore increasingly important that mobile radio networks support these applications in an efficient manner. Thus, mobile radio systems currently under development include support for packet data services. The most widely deployed standard for second-generation mobile radio networks is the Global System for Mobile Communications (GSM) [1]. Networks based on this standard will be extended in the near future with the General Packet Radio Service (GPRS)/Universal Mobile Telecommunications Systems (UMTS) [2, 3], which provides data rates up to 384 kb/s (2 Mb/s). The Enhanced Data Rate for GSM Evolution (EDGE)-based version of GPRS that uses 8-phase shift keying (PSK) can deliver 384 kb/s.

When discussions about GPRS started in the early 1990s, applications such as road transport telemetrics and financial services drove the demand. The high costs for circuit-switched GSM connections prevented widespread use of mobile data transmission for such services. In recent years, however, end-user applications such as Web browsing and email have become increasingly popular; therefore, the Internet has dominated the standardization of GPRS. Internet applications are predicted to contribute the largest share of the expected traffic volume.

In brief, GPRS can be described as a service providing optimized access to the Internet, while reusing to a large degree existing GSM infrastructure. Advanced mobile terminals using multiple slots will offer more convenient and faster Internet access than today's technology. The GPRS concept allows volume-oriented charging, which permits users to have cheap, permanent connections to the Internet.

We have designed a GPRS/UMTS prototype system with mobile IP (MIP) as a third-generation wireless Internet access packet service system. We implemented a serving GPRS support node (SGSN) and a gateway GPRS support

0163-6804/02/$17.00 © 2002 IEEE

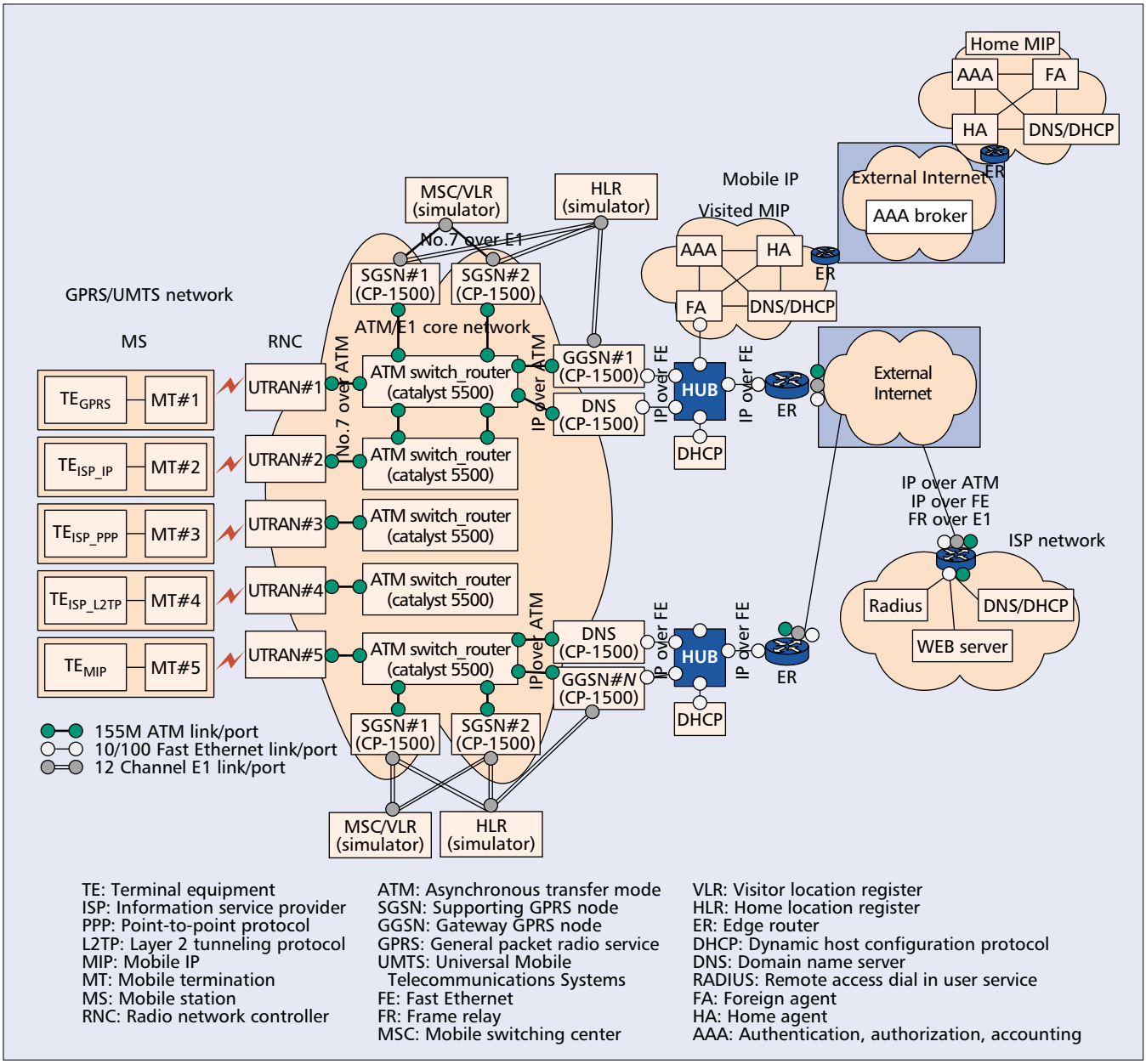

Figure 1. *The network architecture of a development system for wireless Internet.*

node (GGSN) for interworking with Internet as core network testbed. There are some implementation hints for wireless Internet access of a mobile Internet service provider (ISP) subscriber based on GPRS/UMTS.

This article describes in detail the network architecture, protocol stack and operation scenarios for wireless Internet access for a mobile ISP subscriber based on a GPRS/UMTS network. We then describe the core network testbed with wireless Internet access cases based on GPRS /UMTS, and define messages and parameters between the GGSN and the ISP, and the GGSN and mobile IP. There are overall simulation results of packets with IP-in-IP and without IP-in-IP between the GGSN and the foreign agent (FA), and the GGSN and the ISP Web server on our core network testbed in a later section, and finally, conclusions are drawn.

The Architecture and Protocol Stack of a Development System for Wireless Internet Service

The Network Architecture of a Development System for Wireless Internet Service

GPRS is being defined by the European Telecommunications Standards Institute (ETSI) to provide packet data service using Global System for Mobile Communications (GSM) cellular networks. As impressively demonstrated by the Internet, packet-switched networks make more efficient use of the resources for bursty data applications and provide more flexibility in general. We designed a third-generation system based on GPRS/UMTS for wireless Internet

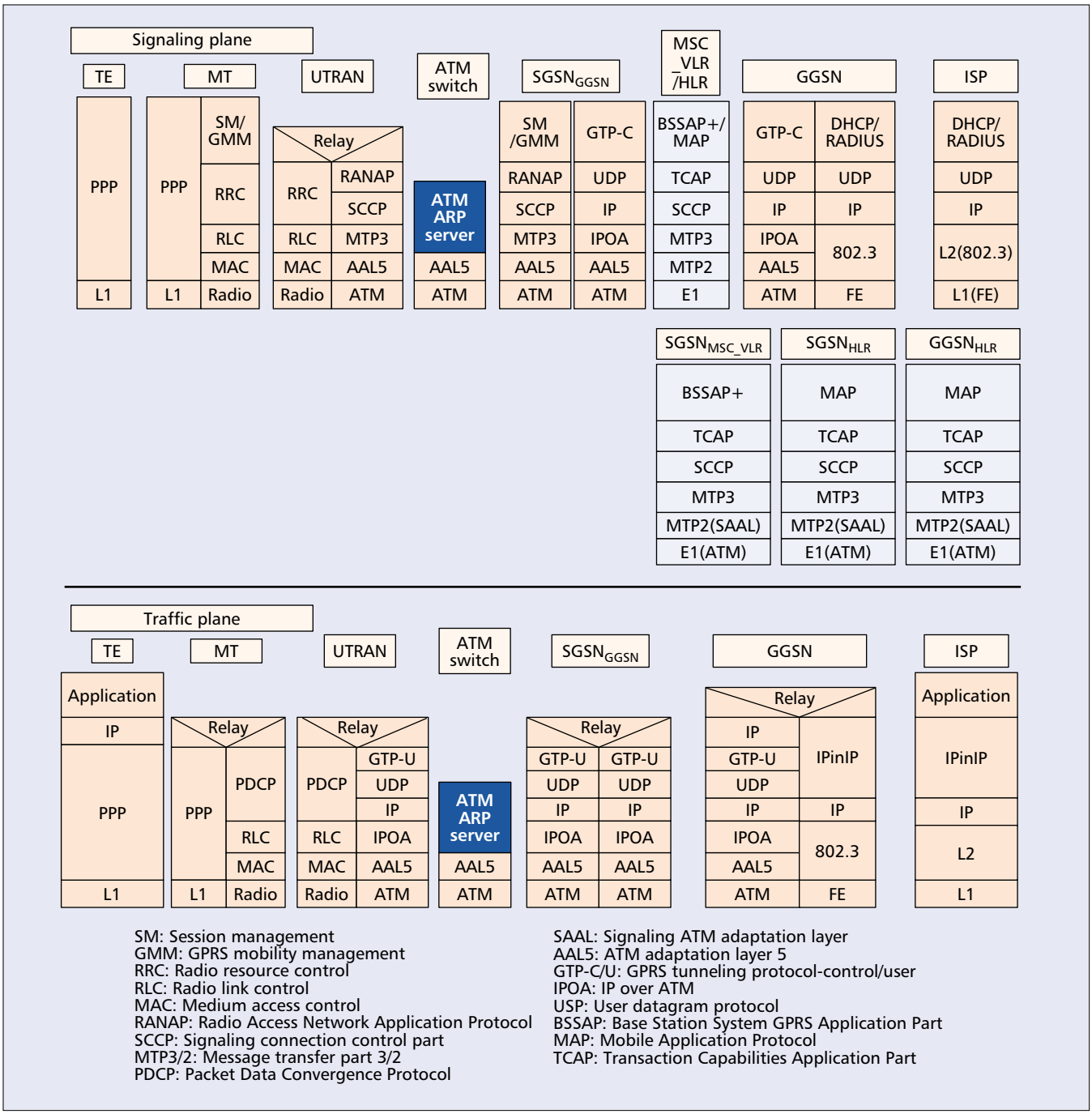

Figure 2. *Protocol stack of 3rd generation GPRS/UMTS development system.*

access and mobile packet data service. Figure 1 depicts our development system architecture for wireless Internet. We have Catalyst 5500 for an asynchronous transfer mode (ATM) network, and use the CP1500 (Solaris2.7) Model for SGSN and GGSN platforms.

The GGSN is the gateway node between GPRS and an external packet data network (IP) or a packet-switched data network (X.25/X.75) and the GPRS core networks. In the case of an external IP network, the GGSN is seen as an ordinary IP router serving all IP addresses of mobile stations (MSs). This node may include firewall and packet-filtering mechanisms. Additionally, its task is to assign the correct SGSN for a mobile station depending on the location of the MS.

The SGSN interfaces between the GPRS backbone and the radio access network, and switches the packets to the correct UMTS terrestrial radio access network (UTRAN). Its task includes ciphering and authentication, session management, mobility management, and logical link management to the MS. It also provides a connection to databases, such as the home location register (HLR) in the mobile switching center (MSC).

The UTRAN, including the packet control unit (PCU), supports all relevant GPRS protocols for communication over the air interface. The PCU's function is to set up, supervise, and

disconnect packet-switched calls, including support for cell change, radio resource configuration, and channel assignment.

The MSC/visitor location register (VLR), HLR, and short message service (SMS) center are functional entities of the initial circuit-switched GSM. These nodes are enhanced by additional interfaces for interworking with GPRS. The MS is equipped with the GPRS protocol stack and is the means of connecting the user to the GPRS network. The GPRS standard foresees MSs that can connect to either circuit-or packet-switched services, or both simultaneously [1–3].

Protocol Stack

On the network level, the development system supports IP and Point-to-Point Protocol (PPP) use by an end-to-end application. A peculiarity of the development system is that, independent of the packets transported, IP is used as the network layer protocol for the GPRS backbone (e.g., to connect the SGSN and GGSN). Also, in the backbone network, GPRS defines a new tunneling protocol built on top of an IP network, called the GPRS Tunneling Protocol (GTP), to handle MS mobility, and support registration and authentication procedures. The GTP enables tunneling multiprotocol data packet through the GPRS backbone between GPRS support nodes. Application data flowing through the tunnel are encapsulated with an outer GTP/UDP/IP header. This adds 48 bytes of header overhead to each data packet, which is substantial for voice-over-IP applications that transmit data packet with small payload.

Figure 2 shows protocol stacks of the third-generation development system. There are two planes, the user and signal planes, in Fig. 2.

The user plane consists of a layered protocol structure providing user information transfer, along with associated information transfer control procedures (e.g., flow control, error detection, error correction, and error recovery).

Packet Data Convergence Protocol (PDCP): The main task of PDCP is to carry network-layer protocol data units (IP) transparently between the MS and UTRAN. This transmission functionality maps higher-level characteristics onto the characteristics of the underlying radio interface protocols. PDCP provides protocol transparency for higher-layer protocols. PDCP supports, for example, IPv4, PPP, and IPv6. Introduction of new higher-layer protocols shall be possible without any changes to the radio interface protocols. PDCP provides protocol control information compression.

GPRS Tunneling Protocol for the user plane (GTP-U): This protocol tunnels user data between SGSNs and GGSNs, and between SGSNs, in the backbone network. All PDP PDUs shall be encapsulated by GTP.

UDP/IP: These are the backbone network protocols used for routing user data and control signaling.

ATM: The information to be transmitted is divided into fixed-size cells (53 octets), multiplexed, and transmitted.

ATM adaptation layer 5 (AAL5): This adaptation layer protocol provides support for variable-bit-rate connection-oriented or connectionless data services.

Radio link control (RLC): The RLC protocol provides logical link control over the radio interface. There may be several simultaneous RLC links per MS. Each link is identified by a bearer ID.

Medium access control (MAC): The MAC protocol controls the access signaling (request and grant) procedures for the radio channel.

The control plane consists of protocols for control and support of the user plane functions:

- Controlling the packet domain network access connections, such as attaching to and detaching from the packet domain network
- Controlling the attributes of an established network access connection, such as activation of a PDP address
- Controlling the routing path of an established network connection in order to support user mobility
- Controlling the assignment of network resources to meet changing user demands

The following are examples of protocol functions in the control plane.

GPRS Mobility Management and Session Management (GMM/SM): This protocol supports mobility management functionality such as GPRS attach, GPRS detach, security, routing area update, location update, PDP context activation, and PDP context deactivation, as described in "Mobility Management Functionality" and "PDP Context Activation, Modification, Deactivation, and Preservation Functions."

Radio Access Network Application Protocol (RANAP): This protocol encapsulates and carries higher-layer signaling, handles signaling between the SGSN and UTRAN, and manages the GTP connections on the Iu interface.

Base Station System Application Part + (BSSAP+): A subset of BSSAP procedures supports signaling between the SGSN and MSC/VLR.

Mobile Application Part (MAP): This protocol supports signaling exchange with the HLR.

The development system also defines a quality of service (QoS) profile for each user with attributes for precedence, delay, reliability, and peak and mean throughput classes. However, the drawback of defining GPRS-specific QoS support mechanisms is that advances in IP QoS support such as integrated and differentiated services may not be directly applicable.

On the network level, the development system supports IP and Point-to-Point Protocol use by an end-to-end application. A peculiarity of the development system is that, independent of the packets transported, IP is used as the network layer protocol for the GPRS backbone.

Wireless Internet Access of Remote Mobile Subscriber Based on GPRS/UMTS Network

Core Network Testbed

To gain experience and iterate on our design, we have been implementing wireless Internet access model in a testbed. This currently consists of a GGSN, SGSN, mobile IP included FA and HA, and ISP network included RADIUS, DHCP/DHCP relay, PPP, L2TP, and Web server. We have RAN simulator which can be supported UTRAN with multimedia mobile terminal. Figure 3 depicts the core network testbed which is implemented. We verify the roaming service of remote mobile subscriber through SGSN and GGSN using mobile IP and L2TP [4]. There is ATM network to connect

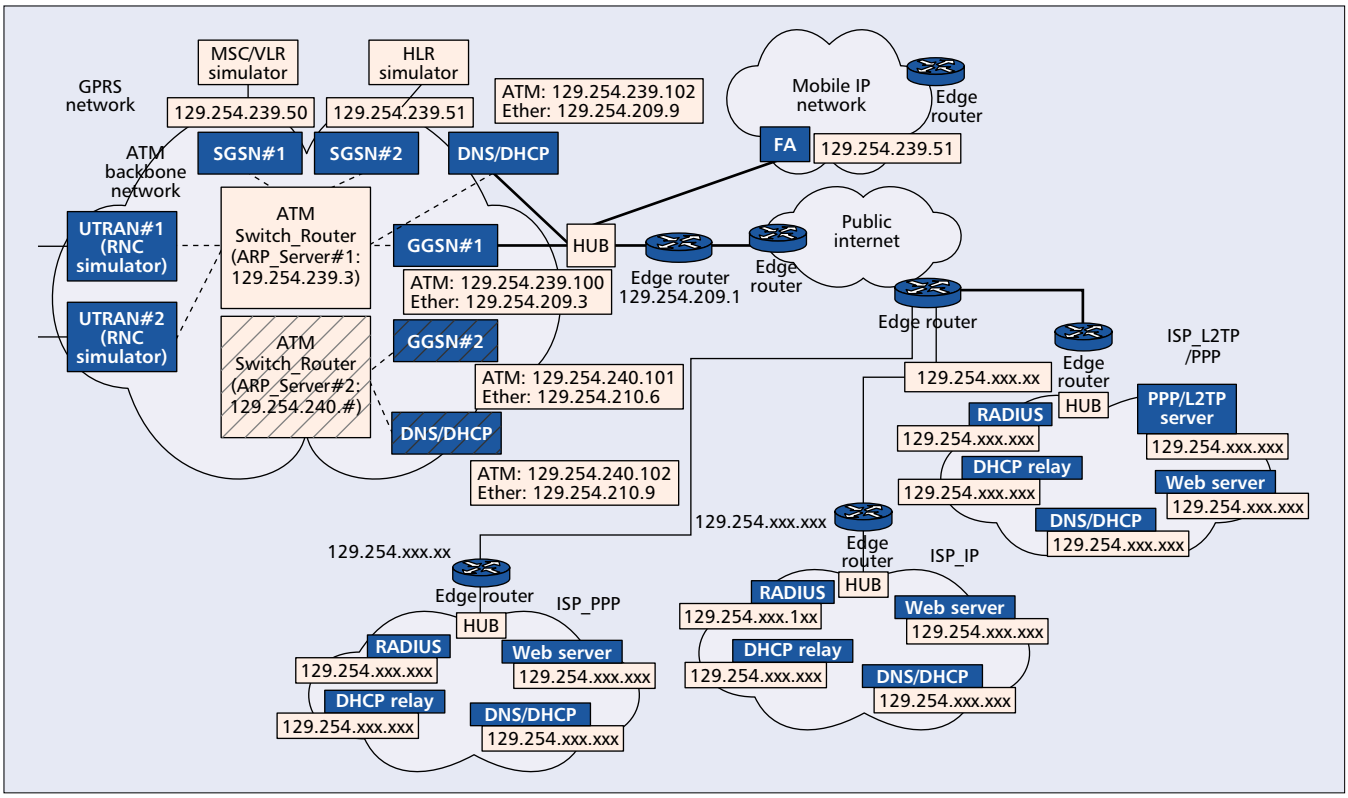

Figure 3. *The core network testbed with RNC simulator.*

UTRAN, SGSN, and GGSN via ATM using IPOA. We also connected between MSC/VLR and SGSN via Signaling System No.7 (SS7) over E1, and HLR and GGSN via SS7 over E1. We have Catalyst 5500 for an ATM network, and use a CP1500 (Solaris2.7) Model for the SGSN and GGSN platform.

IP based access network: For an IP access network such as an ISP network based on IP, we have several servers such as RADIUS [5], DHCP [6], and Web. This Web server (129.254.xxx.xxx) has a telnet, ftp, and mail server for users. We use RADIUS in another IP (129.254.xxx.xxx) as an IP based ISP network access authentication server, and DHCP for dynamic address allocation of roaming ISP subscriber who is in another wireless packet network such as GPRS. Tunneling is intended to show asymmetric traffic flow. Tunneling (IP-in-IP) [7] is only used between the GGSN and the ISP Web server.

PPP [8] via an L2TP-based access network: For PPP via an L2TP access network as ISP-network-based PPP via L2TP, we also have several servers such as RADIUS, DHCP, and a Web sever separately. This Web server (129.254.xxx.xxx) also has a telnet, ftp, and mail server for users. We also use RADIUS in another IP (129.254.xxx.xxx) as a PPP via L2TP ISP network access authentication server, and DHCP for dynamic address allocation of a roaming ISP subscriber who is in another wireless packet network such as GPRS. We use UDP/IP for traffic and signal packet forwarding between the GGSN and the ISP Web server via PPP L2TP.

Mobile IP (MIP) [1, 9] based access network: For the MIP-based access network, we also have several servers such as authentication, authorization, and accounting (AAA), DHCP, domain name server (DNS), and Web sever, separately. This Web server (129.254.xxx.xxx) also has a telnet, ftp, and mail server for users. We also use AAA in another IP (129.254.xxx.xxx) as the authentication server in the FA area, the MIP network, and DHCP for dynamic address allocation of a roaming mobile IP network subscriber who is in another wireless packet network such as GPRS. There is DNS for interpretation of IP from domain name. We use UDP/IP for signal packet forwarding between the GGSN and the FA [9], and IP-in-IP for traffic forwarding between the GGSN and the FA.

Operation

We now describe operation scenarios of three cases: IP-based access, L2TP-based access, and MIP-based access to wireless Internet for a remote mobile subscriber based on GPRS.

IP-Based Access to Wireless Internet — Figure 4 shows the signaling flow for wireless Internet access case of a remote mobile ISP subscriber based on GPRS using IP.

For wireless Internet access of mobile an ISP subscriber based on IP (PDP-type IP):

The mobile station (MS) is given an address belonging to the intranet/ISP addressing space. The address is given at either subscription, in which case it is static, or PDP context activation, in which case it is dynamic. This address is used for packet forwarding within the GGSN and for packet forwarding on the intranet/ISP. This requires a link between the GGSN and an address allocation server, like RADIUS and DHCP, belonging to the intranet/ISP.

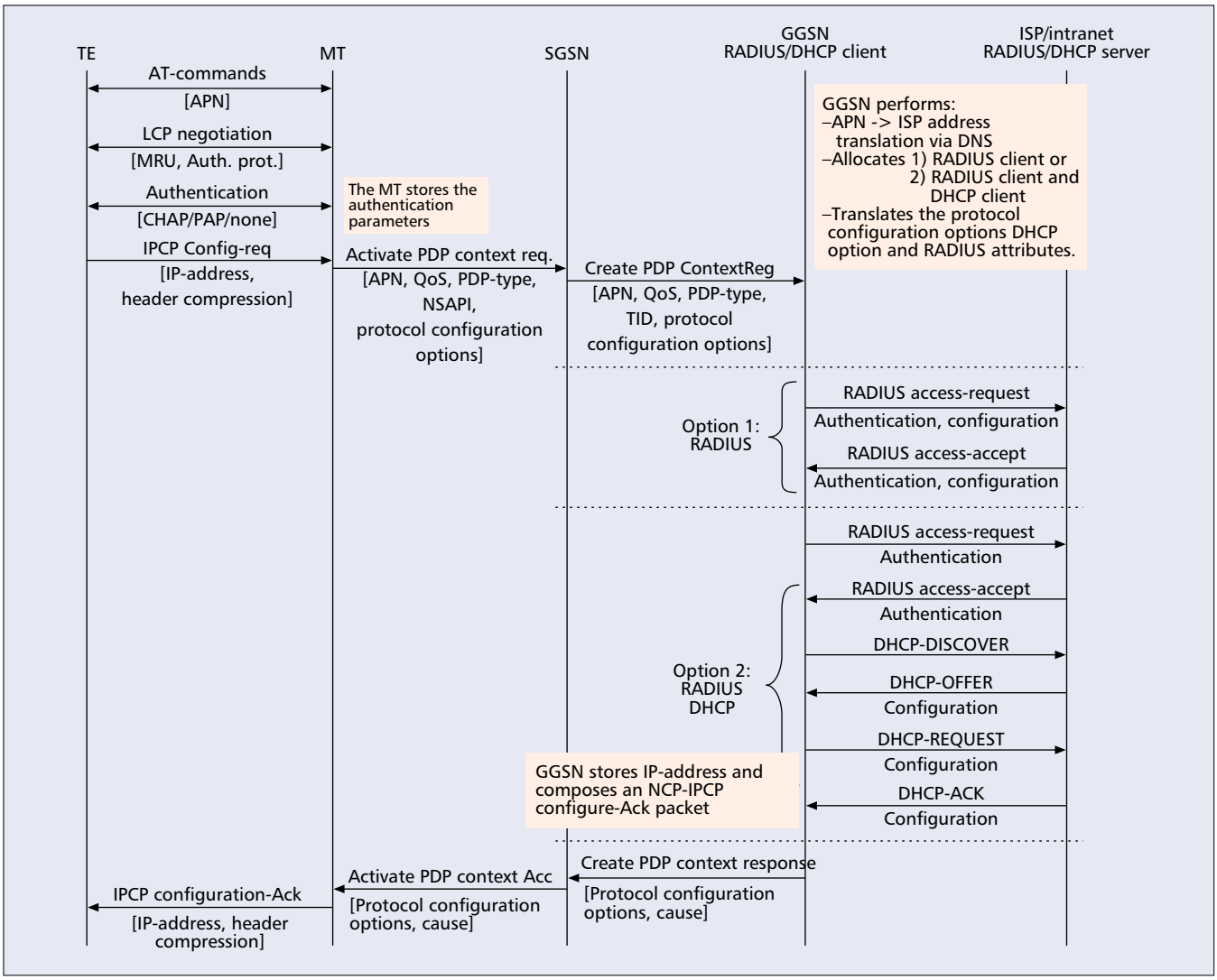

Figure 4. *Signaling flow for IP-based access.*

The MS shall send an authentication request at PDP context activation; the GGSN requests user authentication from a server, like RADIUS and DHCP, belonging to the intranet/ISP.

The protocol configuration options are retrieved (if requested by the MS at PDP context activation) from some server (RADIUS or DHCP) belonging to the intranet/ISP.

The communication between the packet domain and the intranet/ISP may be performed over any network, even an insecure one such as the Internet. For an insecure connection between the GGSN and the intranet/ISP there may be a specific security protocol in between. This security protocol is defined by mutual agreement between the public land mobile network (PLMN) operator and the intranet/ISP administrator.

The following describes the signal flow:

(1) The terminal equipment (TE) sends an AT command to the mobile terminal (MT) to set up parameters and enter PPP mode. The MT responds with an AT response.

(2) Link control protocol (LCP) negotiates Maximum-Receive-Unit and authentication protocol. The negotiated authentication protocol is either a challenge handshake authentication protocol (CHAP), password authentication protocol (PAP), or none. The MT shall try to negotiate for CHAP as first priority.

(3) If the negotiated authentication protocol is either CHAP or PAP, the TE authenticates itself to the MT by means of that protocol. The MT stores the necessary authentication data and sends a forced positive acknowledgment of the authentication to the TE.

(4) The TE requests IP configuration by sending the IP configuration packet (IPCP) Configure-Request message to the MT indicating either the static IP address that shall be used or that an IP address shall be dynamically allocated.

(5) The MT sends the Activate PDP context request message to the SGSN, including the protocol configuration options (PCOs). The SGSN sends the Create PDP context request message to the chosen GGSN, including the unmodified PCOs.

(6) The GGSN deduces from the APN:

- The server(s) to be used for address allocation, authentication, and PCO retrieval
- The protocol (e.g., RADIUS and DHCP) to be used with server(s)
- The communication and security feature needed to dialog with server(s), such as

The development system defines a QoS profile for each user with attributes for precedence, delay, reliability, and peak and mean throughput classes. However, the drawback of defining GPRS-specific QoS support mechanisms is that advances in IP QoS support may not be directly applicable.

tunnel, IPsec security association, or dialup connection (possibly using PPP)

As an example, the GGSN may use one of the following options:

- RADIUS for authentication and IP address allocation. The RADIUS server responds with either an Access-Accept or Access-Reject to the RADIUS client in the GGSN.
- RADIUS for authentication and DHCP for host configuration and address allocation. The RADIUS server responds with either an Access-Accept or Access-Reject to the RADIUS client in the GGSN. After a successful authentication, the DHCP client discovers the DHCP server(s) in the ISP/intranet and receives host configuration data.
- If the received PCOs information element (IE) contains a PPP IPCP Configure-Request packet, the GGSN shall analyze all the contained IPCP options and their requested values. In accordance with the relevant PPP the GGSN shall respond with the following messages:
- Zero or one PPP IPCP Configure-Reject packet containing options not supported and options whose values cannot be returned
- Zero or one PPP IPCP Configure-Nak packet containing options that are supported but requested values that are incorrect/unsupported
- Zero or one PPP IPCP Configure-Ack packet containing options that are supported and requested values that are correct/supported
- Any returned PPP IPCP packets to be contained in the PCO IE

(7) The GGSN sends back to the SGSN a Create PDP Context Response message, containing the PCOs IE. The cause value shall be set according to the outcome of the host authentication and configuration. A PDP context activation shall not be rejected solely due to the presence of unsupported or incorrect PPP IPCP options or option values received from the MS in the PCOs IE. The MS may, however, later decide to immediately deactivate the activated PDP context due to the information received in the PCOs IE received from the network.

(8) Depending on the cause value received in the Create PDP Context Response, the SGSN sends either an Activate PDP Context Accept or Activate PDP Context Reject to the MS.

If PCOs are received from the GGSN, the SGSN shall relay them to the MS. The MT sends either the configuration-Ack packet (e.g., IPCP Configure Ack in the PPP case), the configure-Nack packet in case of dynamic address allocation (e.g., IPCP Configure Nack. in PPP case), or a link Terminate request (LCP Terminate-Request in PPP) back to the TE. If a configure-Nack packet was sent by the MT, a local negotiation may take place at the R reference point (i.e., the TE proposes the new value to the MT), after which a configuration-Ack packet is sent to the TE.

(9) If a configuration-Ack. packet was sent to the TE, the link from the TE to the external ISP/Intranet is established and IP packets may be exchanged. If a link terminate request packet was sent to the TE, the TE and MT negotiate for link termination. The MT may then send a final AT response to inform the TE about the rejected PDP Context activation. A link terminate request packet (e.g., LCP Terminate-request in PPP) causes a PDP context deactivation. In the following example PPP is used as the layer 2 protocol between the TE and MT. The MT acts as a PPP server and translates PCOs into session management (SM) message IEs. GTP-C (control) carries this information unchanged to the GGSN, which uses the information for DHCP or RADIUS authentication and host configuration, for example. The result of the host authentication and configuration is carried via GTP-C to the SGSN, which relays the information to the MT. The MT sends an IPCP Configure-Ack to the TE with the appropriate options included.

L2TP_PPP-Based Access — Figure 5 shows the signaling flow in wireless Internet access for a remote mobile ISP subscriber based on GPRS using PPP via L2TP. By means of the PDP type, PPP packet domain may support interworking with networks based on PPP, as well as with networks based on any protocol supported by PPP through one of its network control protocols (NCPs). It may also support interworking by means of tunneled PPP, such as by the layer two tunneling protocol (L2TP). With <PDP Type>PPP the MT may provide a PPP relay (or proxy) function between the TE and GGSN. This gives the opportunity for the MT to intercept the L2 framing end-to-end negotiations. In Fig. 6 successful PDP context activation is shown. The interworking point is at the Gi reference point. The GGSN for interworking with the ISP/PDN is the access point of the packet domain. The GGSN will either terminate the PPP connection toward the MS or further relay PPP frames to the PDN. The PPP frames may be tunneled in, say, L2TP. If the GGSN tunnels PPP frames to the PDN, the GGSN may behave like an L2TP access concentrator (LAC) toward the external network.

In the PDP type PPP case:

The MS is given an address belonging to the intranet/ISP addressing space. The address is given either at subscription in which case it is a static address or at PDP context activation in which case it is a dynamic address. This address is used for packet forwarding within the GGSN and on the intranet/ISP. This requires a link between the GGSN and an address allocation server, such as RADIUS or DHCP, belonging to the intranet/ISP.

The communication between the packet domain and the intranet/ISP may be performed over any network, even an insecure one such as the Internet. In case of an insecure connection between the GGSN and the intranet/ISP, there may be a specific security protocol in between. This security protocol is defined by mutual agreement between the PLMN operator and the intranet/ISP administrator.

The following describes the signal flow:

(1) The TE sends an AT command to the MT to set up parameters.

(2) The MT sends the Activate PDP context request message to the SGSN that sends the Create PDP context request message to the chosen GGSN.

(3) The GGSN deduces from the APN:

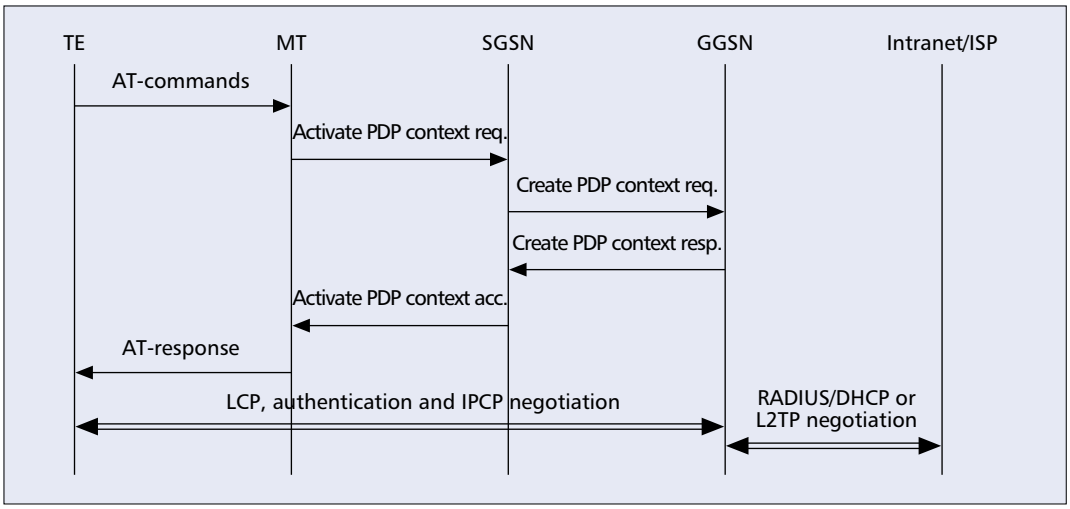

Figure 5. *Signaling flow for PPP-L2TP-based access.*

In case of an insecure connection between the GGSN and the Intranet/ISP, there may be a specific security protocol in between. This security protocol is defined by mutual agreement between the PLMN operator and the Intranet/ISP administrator.

- The server(s) to be used for address allocation and authentication
- The protocol such as RADIUS, DHCP or L2TP to be used with server(s)
- The communication and security feature needed to dialog with server(s) for tunnel, IPSec security association, and dialup connection (using possibly PPP)

As an example the GGSN may use one of the following options:

- RADIUS for authentication and IP address allocation. The RADIUS server responds with either an Access-Accept or Access-Reject to the RADIUS client in the GGSN.
- RADIUS for authentication and DHCP for host configuration and address allocation. The RADIUS server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the GGSN. After a successful authentication, the DHCP client discovers the DHCP server(s) in the ISP/intranet and receives host configuration data.
- L2TP for forwarding PPP frames to an L2TP network server

(4) The GGSN sends back to the SGSN a Create PDP Context Response message.

(5) Depending on the cause value received in the Create PDP Context Response the SGSN may send either the Activate PDP Context Accept message or Activate PDP Context Reject message to the MS.

(6)The MT responds with an AT response that may indicate whether the context activation was successful or not. In the case of a nonsuccessful context activation the response may also indicate the cause. In case of a successful context activation, the TE will start its PPP protocol after the LLC link has been established. The LCP, Authentication and IPCP (in case of IP) negotiations are then carried out. During these negotiations the GGSN may acknowledge values, for any LCP options related to L2 framing (e.g., ACCM, ACFC, and FCS-Alternatives), as proposed by the MT, which itself is forwarding these negotiations from the TE.

MIP-Based Access — Figure 6 shows the signaling flow in wireless Internet access for a remote mobile ISP subscriber based on GPRS using MIP. A way to allow users to roam from one environment to another, between fixed and mobile, between public and private as well as between different public systems is to use MIP. MIP is a mobility management protocol developed by IETF. The MIP FA is located in the core network in the GGSN. MIP also uses an HA [9], which may or may not be located in a GSM/UMTS network. The interface between the GGSN and the FA will probably not be standardized as the GGSN/FA is considered being one integrated node. The mapping between these two is a matter of implementation. Each FA must be configured with at least one care-of address. In addition, an FA must maintain a list that combines IP addresses with tunnel endpoint identifications (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 detunnels the packets and forwards the packets to the MS. MIP-related signaling between the MS and the FA is done in the user plane. MIP registration messages are sent with UDP. Address allocation: at PDP context activation no IP address is allocated to the MS indicated by 0.0.0.0. in the Requested PDP Address field. If the MS does not have a static IP address that it could register with the HA, it will acquire a dynamic IP address from the HA. After completion of the PDP activation the SGSN is informed of the assigned IP address by means of the GGSN-initiated PDP Context Modification Procedure. A signaling scheme is described below. The PS attach procedures have been omitted for clarity in Fig. 6.

In case of MIP-based access:

(1) The AT command carries parameters that the MT needs to request the PDP Context Activation. The important parameter here is th access point namee (APN). The AT command is followed by a setup of the PPP connection between the MT and the TE, which are not included in Fig. 6.

(2) The MT sends the Activate PDP Context Request to the SGSN. The message includes various parameters of which the APN and the

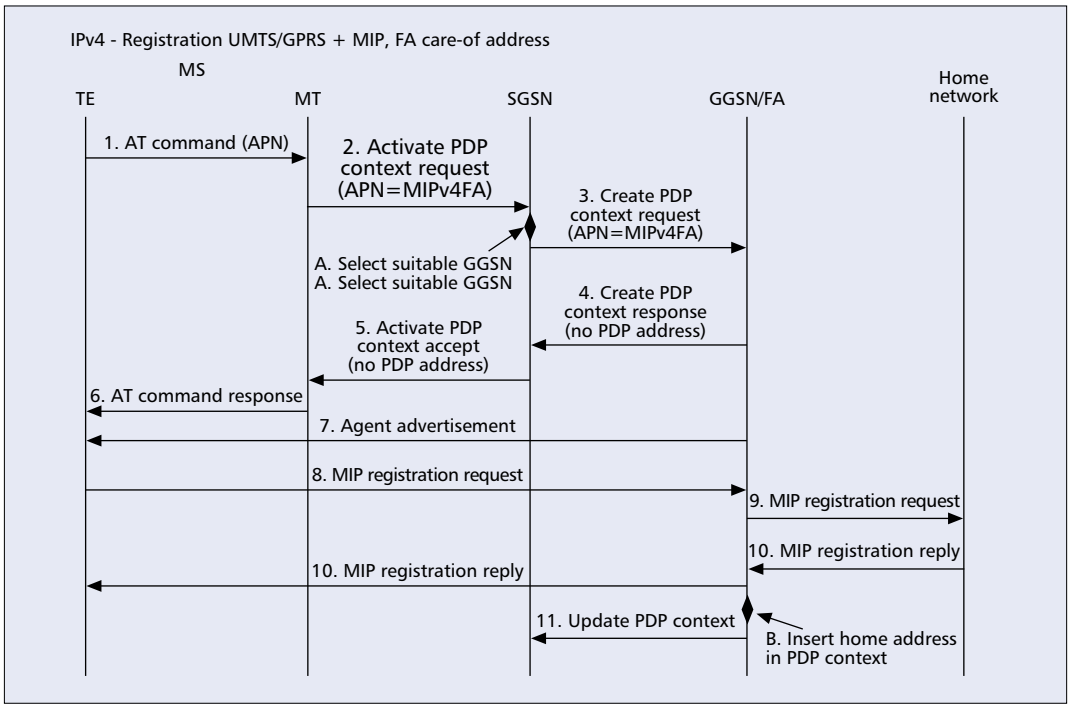

Figure 6. *Signaling flow for MIP-based access.*

	Without IP in IP	With IP in IP	Remark
Delay	20 ms	30 ms	Increasing packet size: $Delay_{with\ IP\text{-}in\text{-}IP} > Delay_{without\ IP\text{-}in\text{-}IP}$
Loss	Same rate		
Throughput	Same (78 Mb/s with 8 packets lost)		Reliability level 95 % with significant level ±5

Table 1. *Performance test results.*

Requested PDP Address are of interest here. The TE/MT may use APN to select a reference point to a certain external network or to select a service. APN is a logical name referring to the external packet data network or a service to which the subscriber wishes to connect. The Requested PDP Address should be omitted for all MS's using Mobile IP. This is done irrespective of whether the MT has a permanently assigned Mobile IP address from its Mobile IP home network or a previously assigned dynamic home address from its Mobile IP home network, or it wishes the Mobile IP home network to allocate a "new" dynamic home address. The SGSN will base the choice of GGSN on the APN given by the MS.

(3) The SGSN requests the selected GGSN to set up a PDP Context for the MS. The PDP address and APN fields are the same as in the Activate PDP Context Request message.

(4) A Create PDP Context Response is sent from the GGSN/FA to the SGSN. If the creation of PDP Context was successful, some parameters will be returned to the SGSN, if not, an error code will be returned. 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 an HA after the PDP context activation procedure.

(5) The Activate PDP Context Accept message is sent by the SGSN to the MS and contains similar information as the Create PDP Context Response message.

(6) The MT sends an AT response back to the TE to confirm that the PDP context activation has been done.

(7) The Agent Advertisement [8] is an Internet Control Message Protocol (ICMP) Router Advertisement message with a mobility agent advertisement extension. The latter part contains parameters of the FA that the mobile node needs, among those are one or more care-of addresses that the FA offers. This message should be sent, in the Packet Domain user plane, as an IP limited broadcast message (i.e., destination address 255.255.255.255); however, only on the TEID for the requesting MS to avoid broadcast over the radio interface.

(8) The Mobile IP Registration Request is sent from the mobile node to the GGSN/FA across the packet domain backbone as user traffic. The mobile node includes its (permanent) home address as a parameter. Alternatively, it can request a temporary address assigned by the home network by sending 0.0.0.0 as its home address, and include the network access identifier (NAI) in a mobile-node-NAI extension.

(9) The FA forwards the Mobile IP Registration Request to the home network of the mobile node, where an HA processes it. Meanwhile, the GGSN/FA needs to store the home address of the mobile node or NAI and the local link address of the MS (i.e., the TEID).

(10) The Registration Reply is sent from the home network to the FA, which extracts the information it needs and forwards the message to the mobile node in the packet domain

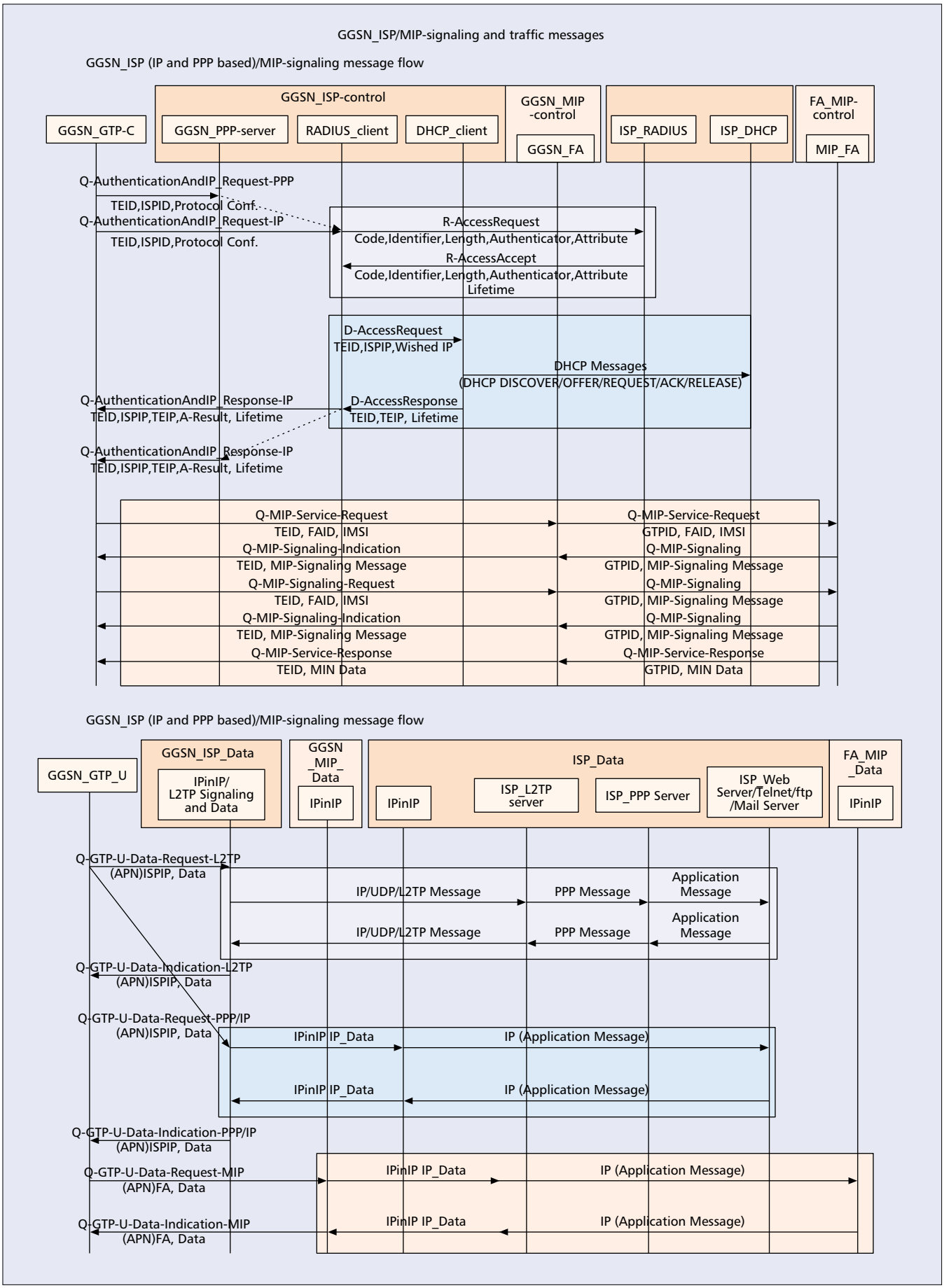

Figure 7. *Messages between GGSN and ISP Web server, and FA in an MIP network for interworking.*

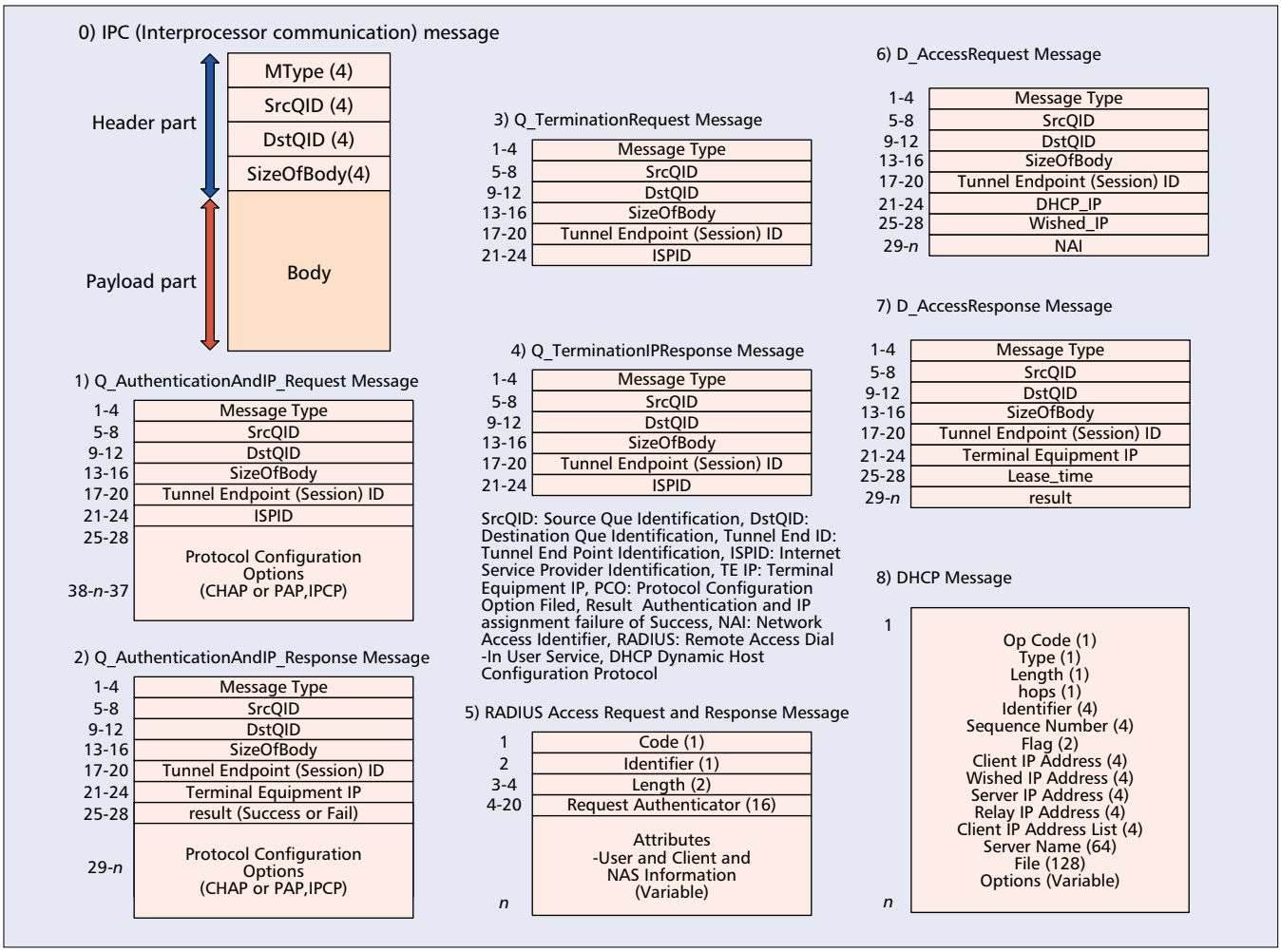

Figure 8. *Messages format for interworking between GGSN and ISP servers.*

user plane. Since the FA/GGSN knows the TEID and the NAI or home address, it can pass it on to the correct MS. The GGSN/FA extracts the home address from the Mobile IP Registration Reply message and updates its GGSN PDP Context.

(11) The GGSN triggers a GGSN initiated PDP Context modification procedure in order to update the PDP address in the SGSN.

Implementation

Messages for Interworking

Figure 7 shows messages between GGSN and ISP Web server, and the FA in an MIP network for interworking.

IP-based access network: There are four messages for signal plane called Authentication_IP_Assignment_Request and Authentication_IP_Assignment_Response, Termination_Extension_Request, and Termination_Extension_Response between GTP and GGSN_ISP. There are also RADIUS and DHCP messages already defined in IETF as RFCs. For data forwarding between GGSN_ISP and ISP Web server, we use an IP-in-IP tunnel scheme.

PPP via L2TP-based access network: There are two messages for signal and traffic planes called L2TP_Access_Request and L2TP_Access_Response between GTP and GGSN_ ISP. On both signal and traffic planes we use UDP/IP between GGSN_ISP and ISP web server in ISP network. There are also PPP and L2TP messages which already defined in IETF as RFC.

Mobile-IP-based access network: There are several messages for signal plane called MIP_Service_Request and MIP_Service_Response, MIP_Signaling_Indicator, and MIP_Signaling_Response between GTP and GGSN_MIP. These messages also forward to foreign agent on signal plane. There are also MIP signaling messages between GGSN_MIP and FA which already defined in IETF as RFCs. For data forwarding between GGSN_MIP and FA, we use IP-in-IP tunnel scheme.

Message Format for Interworking between GGSN and ISP

Figure 8 shows messages format for interworking between GGSN and ISP Web server. Each message structure is:

A. Basic interprocessor communication (IPC) message structure
B. Message structure of Q-AuthenticationAndIP_Request
C. Message structure of Q-AuthenticationAndIP_Response

D. Message structure of Q-TerminationIP_Request
E. Message structure of Q-TerminationIP_Response
F. Message structure of RADIUS message
G. Message structure of D-AccessRequest
H. Message structure of D-AccessResponse
I. Message structure of DHCP message

PERFORMANCE

As mentioned in the previous section, we implemented GGSN and SGSN on Solaris, FA, HA, and AAA on Linux, and ISP servers on Solaris and Linux. We also implemented a performance tool called loadbox that can generate packets with some options such as packet length and interval, and measure delay, packet loss, and throughput at IP layer. For synchronization between GGSN and ISP, and GGSN and FA, we prepared network time protocol server. We observed the performance of IP-in-IP of test packet between GGSN and ISP web server, and GGSN and FA. For simulation, we stimulated test packets with varying length (1054 Byte x 10, 100, 1000) and varying interval (10 ms, 100 ms, 1000 ms). The following are simulation results of delay, packet loss, and throughput with IP-in-IP and without IP-in-IP on the testbed:

Delay: For a packet with IP-in-IP, delay time is about 30 ms, and in case of packet without IP-in-IP, it's about 20 ms. If test packet size increase with fast interval, we can see that time delay of packets with IP-in-IP is more than the time delay of packets without IP-in-IP. But the increased interval of time delay is minor. Also the time delay of the packets is almost the same situations between GGSN and FA, and GGSN and ISP Web server.

Lost Packet: For both packets with IP-in-IP and packets without IP-in-IP, lost packets rate is the same.

Throughput: With both packets with IP-in-IP and packets without IP-in-IP at reliability level 95 percent with significant level ±5, throughput is the same. Normally, we can see that throughput is about 78 Mb/s with 8 packets lost on our core network testbed (Table 1).

CONCLUSION

If the advent of the commercial Internet is the engine behind the new post-industrial revolution, "wireless Internet" will surely accelerate innovation in this economy. These days many people use the term wireless Internet to indicate wireless access to Web services and content. However, the architecture, protocols, services, and wireless technologies that constitute wireless Internet are still under consideration and subjects of great debate. There are a number of companies, standards bodies, and industry fora vying to define future wireless Internet technology. The end result is that operators are faced with a large and confusing array of choices on how best to build next-generation mobile networks. Each technology has it pros and cons. For example, the IETF Mobile IP protocol represents a simple and scalable global mobility solution but lacks support for fast handoff control, real-time location tracking, authentication, and distributed policy management found in the cellular network today. In contrast, the International Mobile Telecommunications 2000 (IMT-2000) mobile network system offers support for seamless mobility, paging, and service quality but is built on complex and costly connection-oriented networking infrastructure that lacks the flexibility, scalability, and cost effectiveness found in IP networks. Wireless Internet should be capable of combining the strengths of both approaches without inheriting their weaknesses.

Actually, we have studied how to apply the GPRS/UMTS network model to the Internet as a next-generation wireless packet network model. This article showed a wireless Internet access model for a remote mobile subscriber based on a GPRS/UMTS network using IP, L2TP, and mobile IP. In this article we discuss a wireless Internet access network architecture and protocol stack, and operation scenarios for mobile packet data and Internet service for a roaming subscriber based on a GPRS/UMTS network. For a wireless Internet access model of a remote mobile subscriber based on a GPRS/UMTS network, we defined messages and parameters between GGSN and mobile IP, and GGSN and ISP network. We also implemented SGSN, GGSN, FA, and HA for simulation. We simulated GPRS functions, Internet services, and performance of IP-in-IP between GGSN and FA, and GGSN and ISP Web server using our core network testbed including GPRS and MIP components, and a RAN simulator.

ACKNOWLEDGMENTS

The author would like to thank the anonymous referees for their review and excellent comments, which helped us improve the quality of the article.

REFERENCES

[1] 3GPP, "Combined GSM and Mobile IP Mobility Handling in UMTS IP CN," 3G TR23.923 version 3.0.0, May 2000.
[2] 3GPP, "GPRS Service Description, Stage 2," 3G TS 23.060 v. 3.3.0, Mar. 2000.
[3] 3GPP, "GPRS Service Description, Stage 1," 3G TS 22.060 v. 3.3.0, Mar. 2000.
[4] W. Townsley *et al.*, "Layer Two Tunneling Protocol (L2TP)," RFC 2661, Aug. 1999.
[5] C. Rigney *et al.*, "Remote Authentication Dial In User Service (RADIUS)," RFC 2865, June 2000.
[6] R. Droms, " Dynamic Host Configuration Protocol (DHCP)," RFC 2131, Mar. 1997.
[7] C. Perkins, "IP Encapsulation within IP," RFC2003, Oct. 1996.
[8] William Allen Simpson, "The Point-to-Point Protocol (PPP)," RFC1661, July 1994.
[9] C. Perkins, "IP Mobility Support," RFC2002, Oct. 1996.

ADDITIONAL READING

[1] R. Stevens, "UNIX Network Programming; Networking APIs: Sockets and XTI Volume 1," 1997.

BIOGRAPHY

JEONG-HYUN PARK (jh-park@etri.re.kr) received his B.S. and M.S. degrees in electronics engineering from Soongsil University, Seoul, Korea, in 1982 and 1985, his Ph.D degree in computer science from Chungbuk National University, Korea, in 1997. He joined the Electronics and Telecommunication Research Institute in March 1982, and was a junior member of research staff in the Communications Systems Research Division. From February 1994 to September 1995 he was a senior member of the Transmitter Team for DBS Joint Project in SATCOM DIVISION, at MPR Teltech, Canada. Now he is involved in the IMT-2000 System Development Task. He is currently a principal member of research staff in the Global Wireless LAN Research Team, Local Area Mobile Communication Researche Department, Mobile Telecommunication Research Laboratory, ETRI. His current interests include security for mobile and satellite communication, communication protocols, and wireless mobile network architecture.