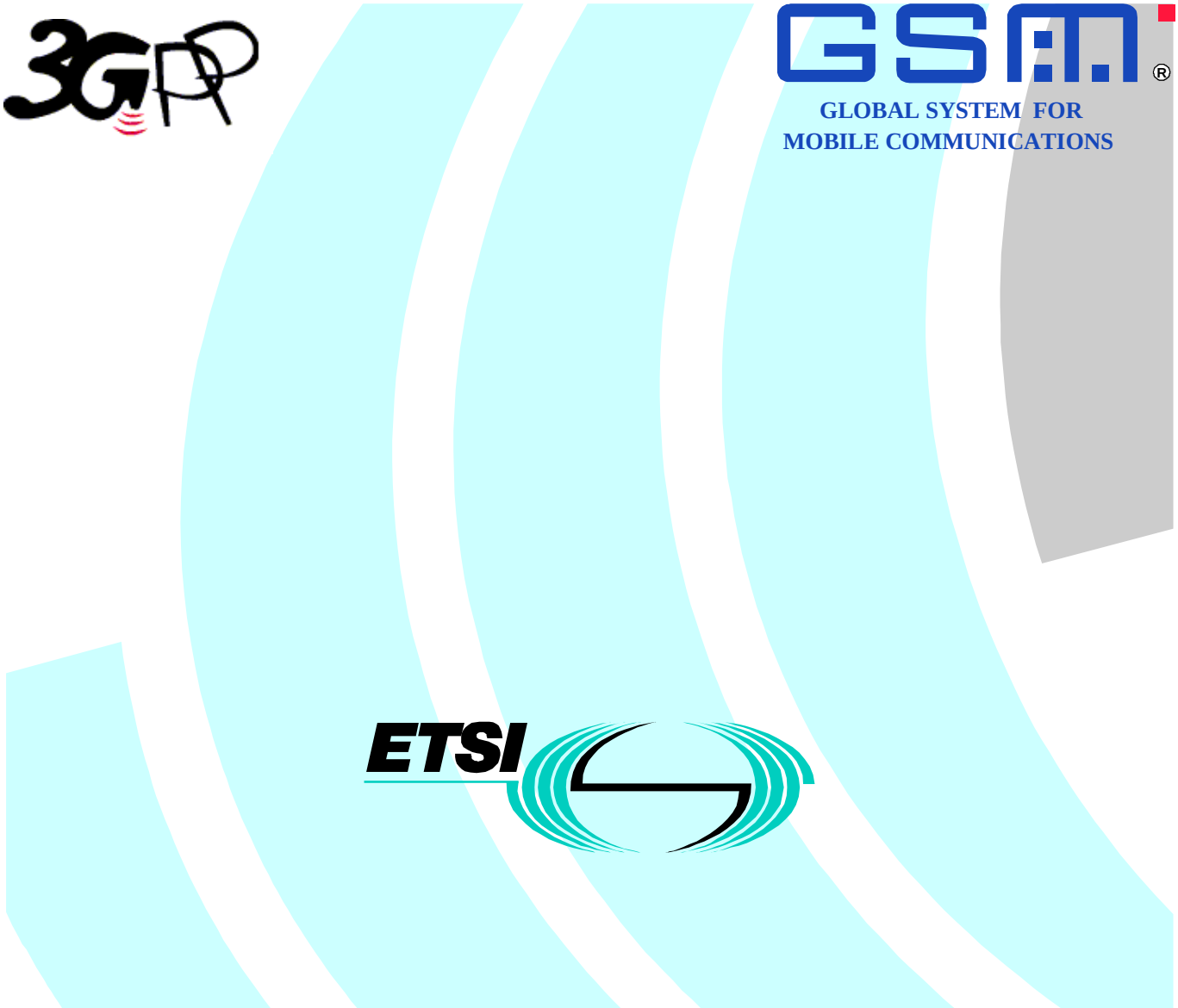
ETSI TS 129 061 V4.0.0 (2001-03)

Technical Specification

**Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
Packet Domain;
Interworking between the Public Land Mobile Network (PLMN)
supporting Packet Based Services
and Packet Data Networks (PDN)
(3GPP TS 29.061 version 4.0.0 Release 4)**



Reference
RTS/TSGN-0329061Uv4

Keywords
GSM, UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.org/ipr).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by the ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under www.etsi.org/key .

Contents

Foreword

This Technical Specification (TS) has been produced by the 3rd Generation Partnership Project (3GPP).

The present document describes the network interworking for the Packet Domain. Interworking to various external networks is defined together with the interworking for data forwarding while subscribers roam within the 3GPP system.

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document defines the requirements for Packet Domain interworking between a:

a) PLMN and PDN;

b) PLMN and PLMN.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

[1] 3GPP TS 01.04: "Digital cellular telecommunication system (Phase 2+); Abbreviations and acronyms".

[2] 3GPP TS 22.060: "3rd Generation Partnership Project: Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS): Stage 1 Service Description".

[3] 3GPP TS 23.060: "3rd Generation Partnership Project: Technical Specification Services and System Aspects; General Packet Radio Service (GPRS); Service Description Stage 2".

[4] 3GPP TS 03.61: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Point to Multipoint Multicast Service Description; Stage 2".

[5] 3GPP TS 03.62: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Point to Multipoint Group Call Service Description; Stage 2".

[6] 3GPP TS 03.64: "Digital cellular telecommunications system (Phase 2+);General Packet Radio Service (GPRS); Overall description of the Radio interface; Stage 2".

[7] 3GPP TS 04.60: "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".

[8] 3GPP TS 04.64: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Logical Link Control (LLC)".

[9] 3GPP TS 24.065: "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)".

[10] 3GPP TS 27.060: "3rd Generation Partnership Project: Technical Specification Group Core Network; Packet Domain; Mobile Station (MS) supporting Packet Switched Services".

[11] ITU-T Recommendation E.164: "Numbering plan for the ISDN era".

[12] <VOID>

[13] <VOID>

[14] <VOID>

[15] IETF RFC 768 (1980): "User Datagram Protocol" (STD 6).

[16] IETF RFC 791 (1981): "Internet Protocol" (STD 5).

[17] IETF RFC 792 (1981): "Internet Control Message Protocol" (STD 5).

[18] IETF RFC 793 (1981): "Transmission Control Protocol" (STD 7).

[19] IETF RFC 1034 (1987): "Domain Names - Concepts and Facilities" (STD 7).

[20] <VOID>

[21] IETF RFC 1661 and 1662 (1994): "The Point-to-Point Protocol (PPP)" (STD 51).

[22] IETF RFC 1700 (1994): "Assigned Numbers" (STD 2).3.

[23] UMTS 24.008: "Mobile radio interface layer 3 specification; Core Network Protocols – Stage 3".

[24] UMTS 29.060: "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface".

[25] IETF RFC2794 (2000), Pat R. Calhoun and Charles E. Perkins: "Mobile IP Network Address Identifier Extension for IPv4", March 2000.

[26] IETF RFC 2131 (1997): "Dynamic Host Configuration Protocol".

[27] IETF RFC 1542 (1993): "Clarification and Extensions for the Bootstrap Protocol".

[28] IETF RFC2373 (1998): "IP version 6 Addressing Architecture".

[29] IETF RFC 2462 (1998): "IPv6 Stateless Address Autoconfiguration".

[30] IETF RFC 2002 (1996), C. Perkins: "IP Mobility Support".

[31] IETF RFC 2486 (1999), B. Aboba and M. Beadles: "The Network Access Identifier".

[32] IETF RFC1112 (1989), S.E. Deering: "Host extensions for IP multicasting".

[33] IETF RFC2236 (1997), W. Fenner: "Internet Group Management Protocol, Version 2".

[34] IETF RFC2362 (1998), D. Estrin and al: "Protocol Independent Multicast-Sparse Mode (PIM-SM)".

[35] IETF RFC1075 (1988), D. Waitzman and al: "Distance Vector Multicast Routing Protocol".

[36] IETF RFC1585 (1994), J. Moy: "MOSPF"..

[37] IETF RFC2290 (1998), J. Solomon, S. Glass: "Mobile-IPv4 Configuration Option for PPP IPCP ".

3 Definitions, abbreviations and symbols

3.1 Definitions

For the purposes of the present document, the following terms and definitions given in UMTS 22.060 and UMTS 23.060 and the following apply:

2G- / 3G-: prefixes 2G- and 3G- refers to functionality that supports only GSM GPRS or UMTS, respectively, e.g., 2G-SGSN refers only to the GSM GPRS functionality of an SGSN. When the prefix is omitted, reference is made independently from the GSM GPRS or UMTS functionality.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

APN	Access Point Name
ATM	Asynchronous Transfer Mode
BG	Border Gateway
CHAP	Challenge Handshake Authentication Protocol
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DVMRP	Distance Vector Multicast Routing Protocol
GGSN	Gateway GPRS Support Node
GTP-U	GPRS Tunnelling Protocol for user plane
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
LAC	L2TP Access Concentrator
LAN	Local Area Network
LNS	L2TP Network Server
MIP	Mobile IP
MOSPF	Multicast Open Shortest Path First
MS	Mobile Station
MT	Mobile Terminal
MTU	Maximum Transfer Unit
NAI	Network Access Identifier
PAP	Password Authentication Protocol
PDCP	Packet Data Convergence Protocol
PDN	Packet Data Network
PDU	Protocol Data Unit
PIM-SM	Protocol Independant Multicast – Sparse Mode
PPP	Point-to-Point Protocol
PS	Packet Switched
RADIUS	Remote Authentication Dial In User Service
SGSN	Serving GPRS Support Node
SMDS	Switched Multimegabit Data Service
TCP	Transmission Control Protocol
TE	Terminal Equipment
TEID	Tunnel End-point Identifier
UDP	User Datagram Protocol

3.3 Symbols

For the purposes of the present document, the following symbols apply:

Gb	Interface between an SGSN and a BSC.
Gi	Reference point between Packet Domain and an external packet data network.
Gn	Interface between two GSNs within the same PLMN.
Gp	Interface between two GSNs in different PLMNs. The Gp interface allows support of Packet Domain network services across areas served by the co-operating PLMNs.
Gs	Interface between an SGSN and MSC.
Iu	Interface between the RNS and the core network. It is also considered as a reference point.
R	The reference point between a non-ISDN compatible TE and MT. Typically this reference point supports a standard serial interface.
Um	The interface between the MS and the GSM fixed network part. The Um interface is the GSM network interface for providing packet data services over the radio to the MS. The MT part of the MS is used to access the GSM services through this interface.

Uu Interface between the mobile station (MS) and the UMTS fixed network part. The Uu interface is the UMTS network interface for providing packet data services over the radio to the MS. The MT part of the MS is used to access the UMTS services through this interface.

4 Network characteristics

4.1 Key characteristics of PLMN

The PLMN is fully defined in the UMTS technical specifications. The Packet Domain related key characteristics are found in 3GPP TS 22.060 and 3GPP TS 23.060.

4.2 Key characteristics of PSDN

<VOID>

4.3 Key characteristics of IP Networks

The Internet is a conglomeration of networks utilising a common set of protocols. IP protocols are defined in the relevant IETF STD specifications and RFCs. The networks topologies may be based on LANs (e.g. ethernet), Point to Point leased lines, PSTN, ISDN, X.25 or WANs using switched technology (e.g. SMDS, ATM).

5 Interworking Classifications

5.1 Service Interworking

Service interworking is required when the Teleservice at the calling and called terminals are different. For Packet Domain, service interworking is not applicable at the Gi reference point.

5.2 Network Interworking

Network interworking is required whenever a PLMN is involved in communications with another network to provide end-to-end communications. The PLMN shall interconnect in a manner consistent with that of a normal Packet Data Network (type defined by the requirements e.g. IP). Interworking appears exactly like that of Packet Data Networks.

5.3 Numbering and Addressing

See 3GPP TS 23.003 and the relevant section for IP addressing below.

6 Access reference configuration

Figure 1 shows the relationship between the MS, its terminal equipment and the UMTS/GSM network in the overall Packet Domain environment.

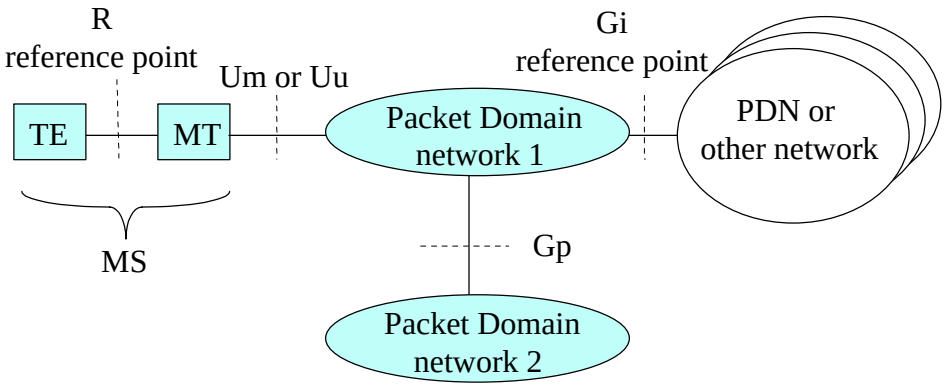


Figure 1: Packet Domain Access Interfaces and Reference Points

7 Interface to Packet Domain Bearer Services

7.1 GSM

The following figure 2a shows the relationship of the GSM Packet Domain Bearer terminating at the SNDCP layer to the rest of the GSM Packet Domain environment. It is shown for reference purposes only and detailed information can be found in 3GPP TS 23.060.

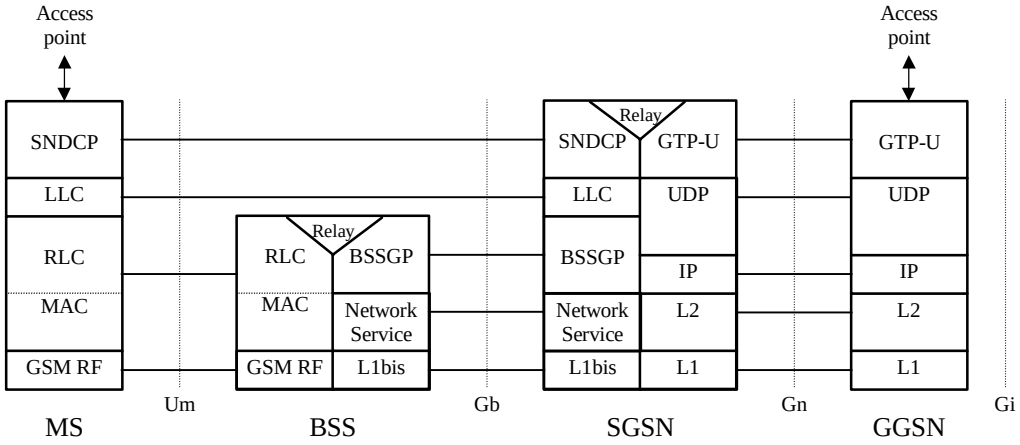


Figure 2a: User Plane for Packet Domain services in GSM

7.2 UMTS

The following figure 2b shows the relationship of the UMTS Packet Domain Bearer, terminating at the PDCP layer, to the rest of the UMTS Packet Domain environment. It is shown for reference purposes only and detailed information can be found in 3GPP TS 23.060.

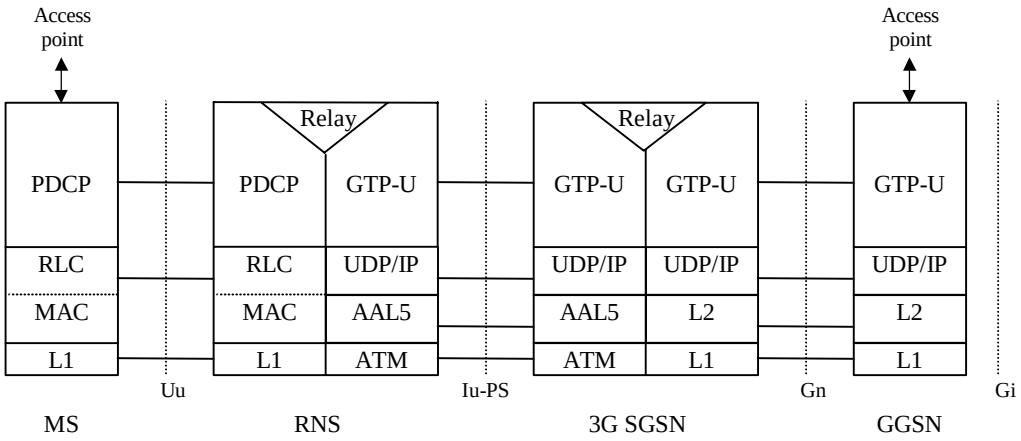


Figure 2b: User Plane for Packet Domain services in UMTS

8 Subscription checking

Subscription is checked during the PS Attach procedure and also during the PDP Context Activation procedure as described in 3GPP TS 23.060. The GGSN implicitly checks its internal context related to the destination address for each mobile terminated packet. If there is a context associated with the PDP address the packet shall be forwarded to the MS, otherwise the packet shall be discarded or rejected depending on the implemented protocol.

9 Message Screening

Screening functions reside within the Packet Domain as described in 3GPP TS 22.060 and 3GPP TS 23.060. Screening may be applicable for only certain protocols. Screening is outside the scope of the present document.

10 Interworking with PSDN (X.75/X.25)

<VOID>

11 Interworking with PDN (IP)

11.1 General

Packet Domain shall support interworking with networks based on the Internet Protocol (IP). These interworked networks may be either intranets or the Internet.

11.2 PDN Interworking Model

When interworking with the IP networks, the Packet Domain can operate IPv4 or Ipv6. The interworking point with IP networks is at the Gi reference point as shown in figure 7.

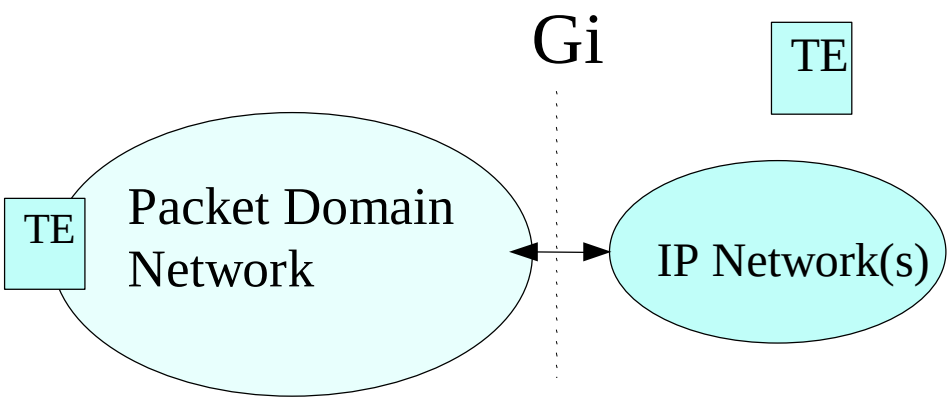


Figure 7: IP network interworking

The GGSN for interworking with the IP network is the access point of the Packet Domain (see figure 8). In this case the Packet Domain network will look like any other IP network or subnetwork.

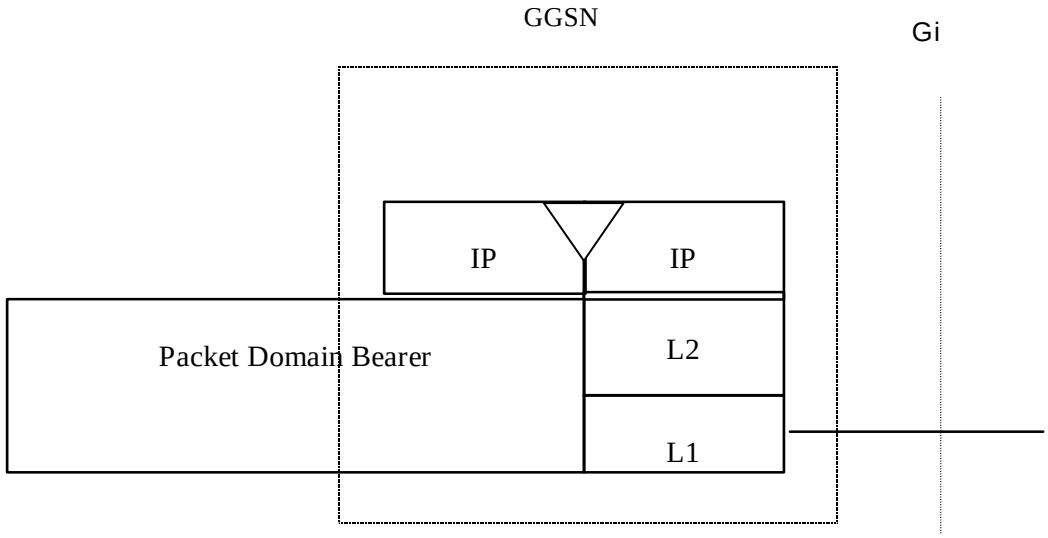


Figure 8: The protocol stacks for the IP / Gi reference point

Typically in the IP networks, the interworking with subnetworks is done via IP routers. The Gi reference point is between the GGSN and the external IP network. From the external IP network's point of view, the GGSN is seen as a normal IP router. The L2 and L1 layers are operator specific.

It is out of the scope of the present document to standardise the router functions and the used protocols in the Gi reference point.

Interworking with user defined ISPs and private/public IP networks is subject to interconnect agreements between the network operators.

No user data or header compression is done in the GGSN.

11.2.1 Access to Internet, Intranet or ISP through Packet Domain

The access to Internet, Intranet or ISP may involve specific functions such as : user authentication, user's authorization, end to end encryption between MS and Intranet/ISP, allocation of a dynamic address belonging to the PLMN/Intranet/ISP addressing space, etc.

For this purpose the Packet Domain may offer:

- either direct transparent access to the Internet; or

- a non transparent access to the Intranet/ISP. In this case the Packet Domain, i.e. the GGSN, takes part in the functions listed above.

11.2.1.1 Transparent access to the Internet

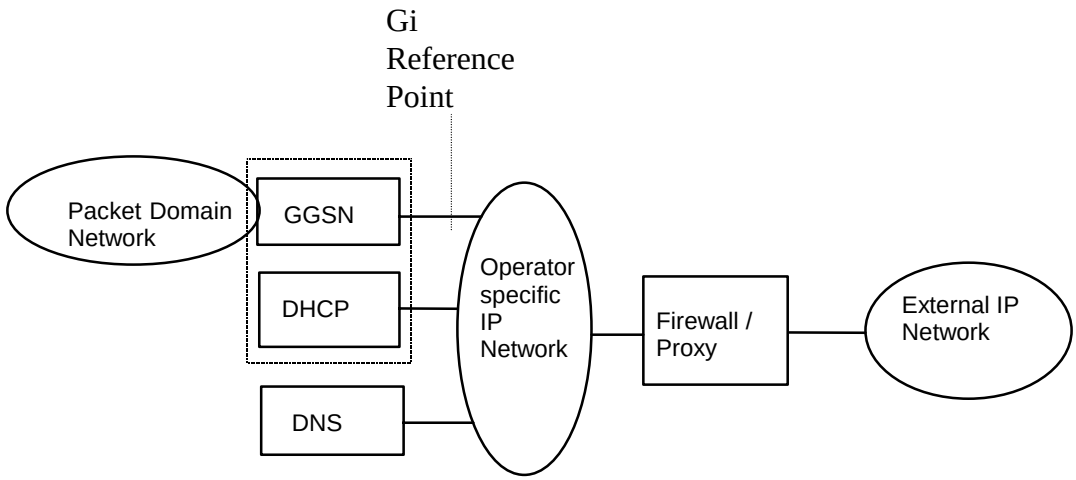


Figure 9: Example of the PDN Interworking Model, transparent case

In this case (see figure 9):

- the MS is given an address belonging to the operator 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 between the Internet and the GGSN and within the GGSN. In IPv6, the address given is the link-local address. Thus, for the IPv6 it is not necessary to use a DHCP implementation for the address allocation, but any unique identifier for the MS in the GGSN is sufficient;

- the MS need not send any authentication request at PDP context activation and the GGSN need not take any part in the user authentication/authorization process.

The transparent case provides at least a basic ISP service. As a consequence of this it may therefore provide a bearer service for a tunnel to a private Intranet.

NB The remainder of this subclause deals with this specific case.

- The user level configuration may be carried out between the TE and the intranet, the Packet Domain network is transparent to this procedure.

The used protocol stack is depicted in figure 10.

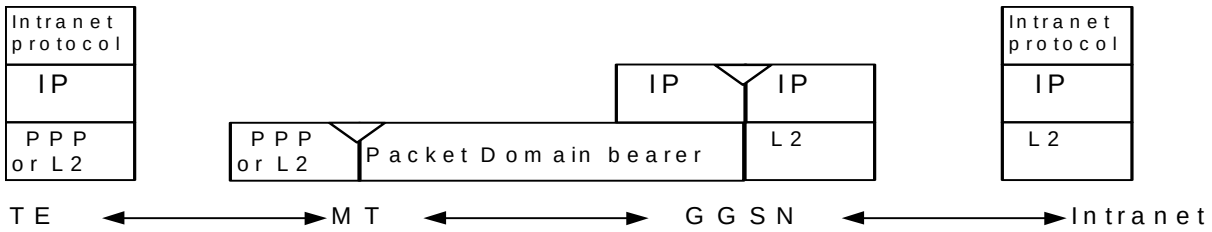


Figure 10: Transparent access to an Intranet

The communication between the PLMN and the Intranet may be performed over any network, even an insecure network e.g. the Internet. There is no specific security protocol between GGSN and the Intranet because security is ensured on an end to end basis between MS and the intranet by the «Intranet protocol».

User authentication and encryption of user data are done within the «Intranet protocol» if either of them is needed. This «Intranet protocol» may also carry private (IP) addresses belonging to the address space of the Intranet.

An example of an «Intranet protocol» is IPsec (see RFC 1825). If IPsec is used for this purpose then IPsec authentication header or security header may be used for user (data) authentication and for the confidentiality of user data (see RFC 1826 and RFC 1827). In this case private IP tunnelling within public IP takes place.

11.2.1.2 Non Transparent access to an Intranet or ISP

In this 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 for packet forwarding on the Intranet/ISP. This requires a link between the GGSN and an address allocation server, like Radius, DHCP, …, belonging to the Intranet/ISP;

- the MS shall send an authentication request at PDP context activation and the GGSN requests user authentication from a server, like Radius, 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 e.g. 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 PLMN operator and Intranet/ISP administrator.

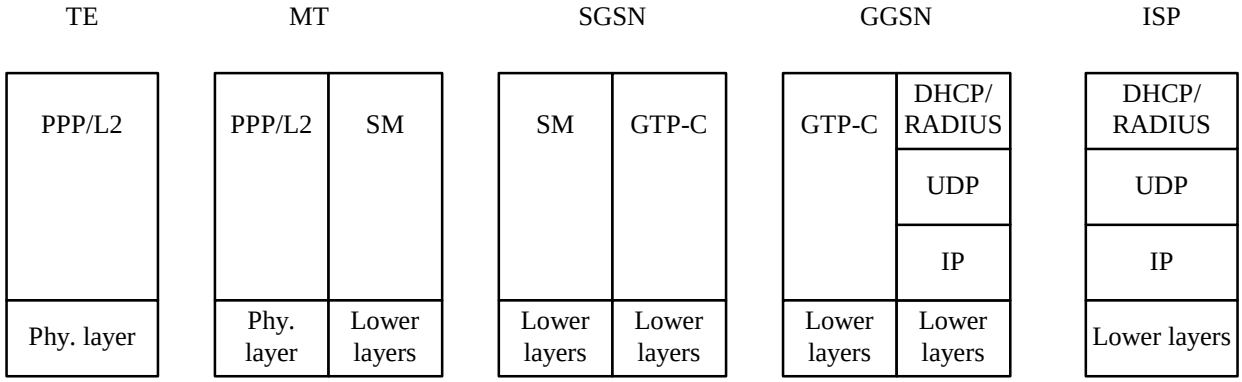


Figure 11a: Signalling plane of non transparent case

The following description bullet items describe the signal flow.

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

2) LCP negotiates Maximum-Receive-Unit and authentication protocol. The negotiated authentication protocol is, either CHAP, PAP or 'none'. The MT shall try to negotiate for CHAP as first priority.

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

4) The TE requests IP configuration by sending the 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. The SGSN sends the Create PDP context req message to the chosen GGSN including the unmodified Protocol Configuration Options.

6) The GGSN deduces from the APN:

   - the server(s) to be used for address allocation, authentication and protocol configuration options retrieval;

   - the protocol like Radius, DHCP, … to be used with this / those server(s);

- the communication and security feature needed to dialogue with this / those server(s) e.g. tunnel, IPSec security association, dial-up 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 an 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.

- If the received Protocol Configurations Options IE contains a PPP IPCP Configure-Request packet, the GGSN shall analyse all the contained IPCP options and their requested values. In accordance with the relevant PPP [20] the GGSN shall respond with the following messages:

  - zero or one PPP IPCP Configure-Reject packet containing options not supported and options which values cannot be returned;

  - zero or one PPP IPCP Configure-Nak packet containing options that are supported but has requested values that are incorrect/unsupported; and

  - zero or one PPP IPCP Configure-Ack packet containing options that are supported and has requested values that are correct/supported.

  Any returned PPP IPCP packets shall be contained in the Protocol Configurations Options IE.

7) The GGSN sends back to the SGSN a Create PDP Context Response message, containing the Protocol Configuration Options 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 Protocol Configurations Options IE. The MS may however later decide to immediately deactivate the activated PDP context due to the information received in the Protocol Configurations Options 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 an Activate PDP Context Reject, to the MS.

   If Protocol Configuration Options are received from the GGSN, the SGSN shall relay those to the MS. The MT sends either the configuration-ack packet (e.g. IPCP Configure Ack in 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 case) back to the TE. In the case where 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) In case 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.

   In case a link terminate request packet was sent to the TE, the TE and MT negotiates 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 (such as LCP Terminate-request in PPP case) causes a PDP context deactivation.

EXAMPLE: In the following example PPP is used as layer 2 protocol over the R reference point.

The MT acts as a PPP server and translates Protocol Configuration Options into SM message IEs. GTP-C carries this information unchanged to the GGSN which uses the information e.g. for DHCP or RADIUS authentication and host configuration. 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.

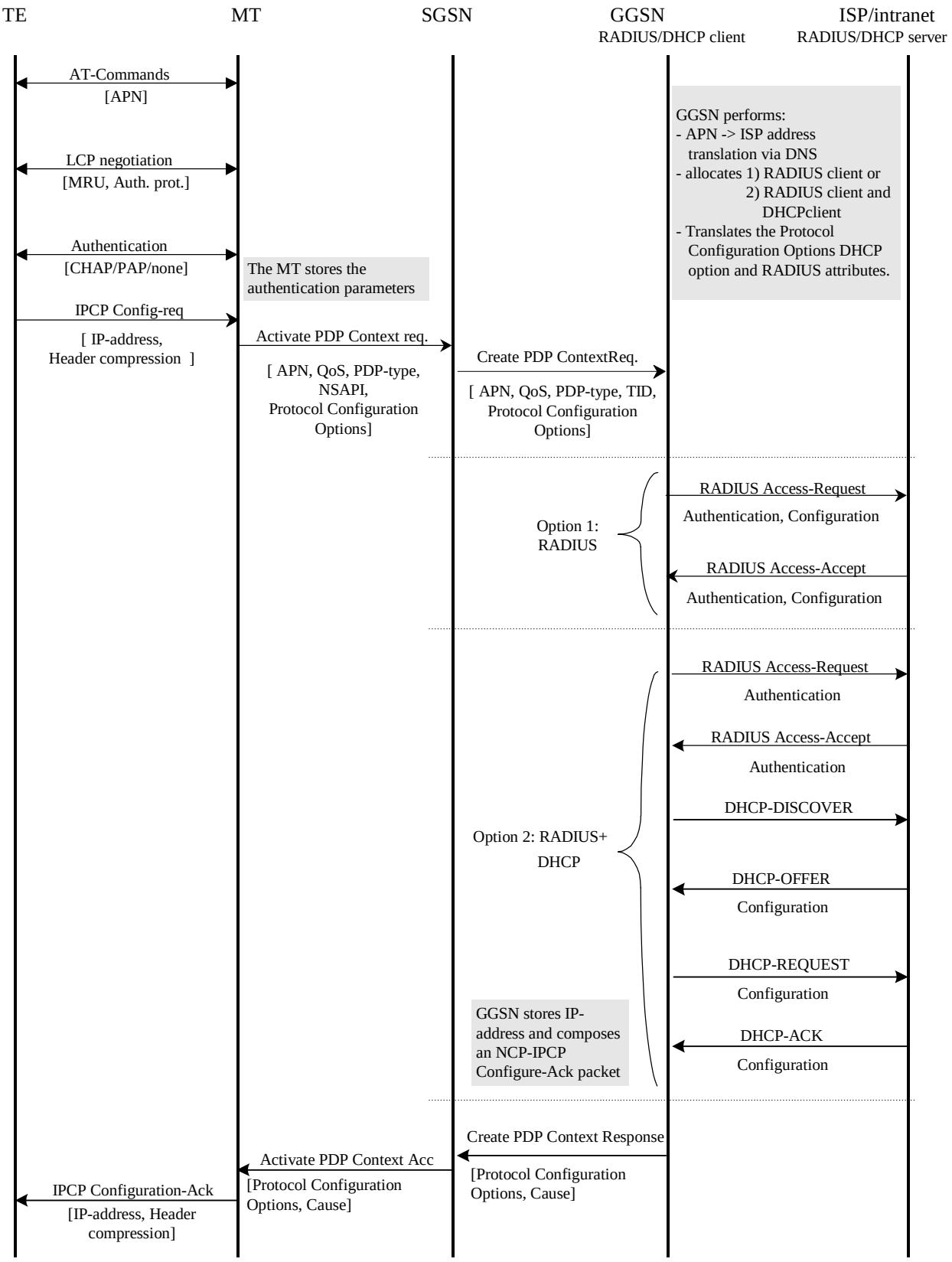


Figure 11b: PDP Context Activation for the Non-transparent IP case

11.2.1.3 Access to Internet, Intranet or ISP with Mobile IPv4

General

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 Mobile IP [30]. Mobile IP (MIP) is a mobility management protocol developed by IETF. The Mobile IP Foreign Agent (FA) [30] is located in the Core Network in the GGSN. MIP also uses a Home Agent (HA) [30] which may or may not be located in a GSM/UMTS network.

Interworking model for MIP

A FA is located in the GGSN. The interface between the GGSN and the FA will probably not be standardised 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 a FA must maintain a list that combines IP addresses with 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 signalling between the MS and the FA is done in the user plane. MIP registration messages [30] are sent with UDP.

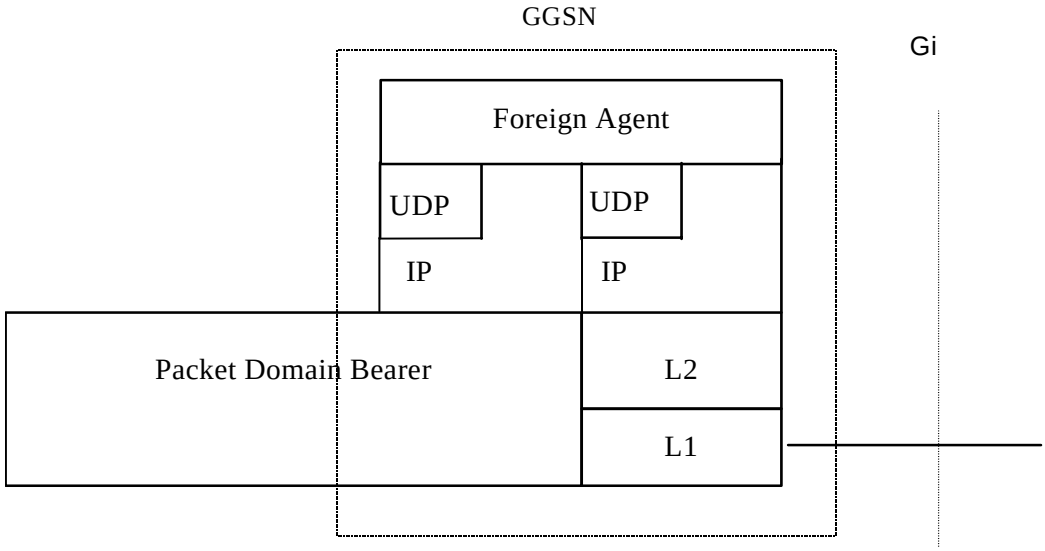


Figure 11c: The protocol stacks for the Gi IP reference point in the MIP signalling plane

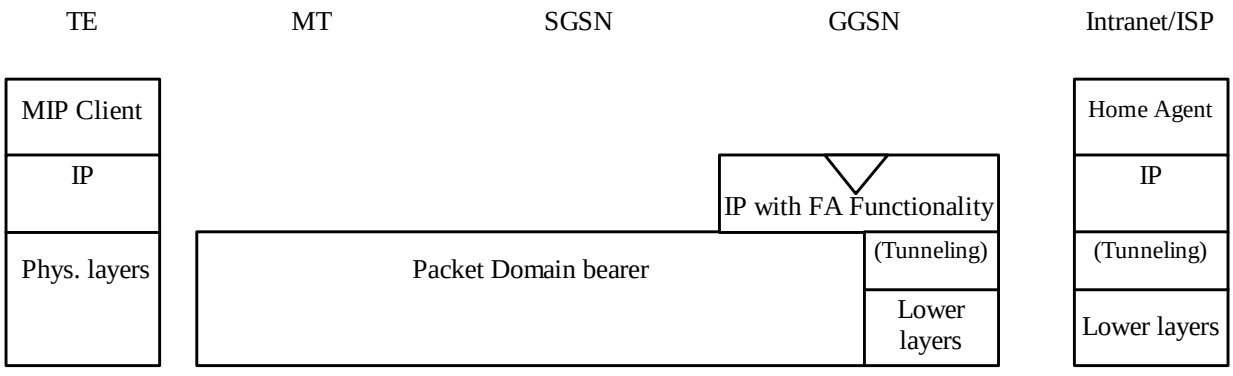


Figure 11d: Protocol stacks for user access with MIP

In figure 11d: "(Tunneling)" is intended to show asymmetric traffic flow. Tunneling (IP-in-IP) is only used in the direction from the ISP towards the MT.

Authentication of the user is supported in Mobile IPv4. This authentication mechanism may involve communication with an authentication server (e.g. RADIUS), although this is not shown in figure 11d.

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 which it could register with the HA, it will acquire a dynamic IP address from the HA [25]. 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.

An example of a signalling scheme, shown in figure 11e, is described below. The PS attach procedures have been omitted for clarity.

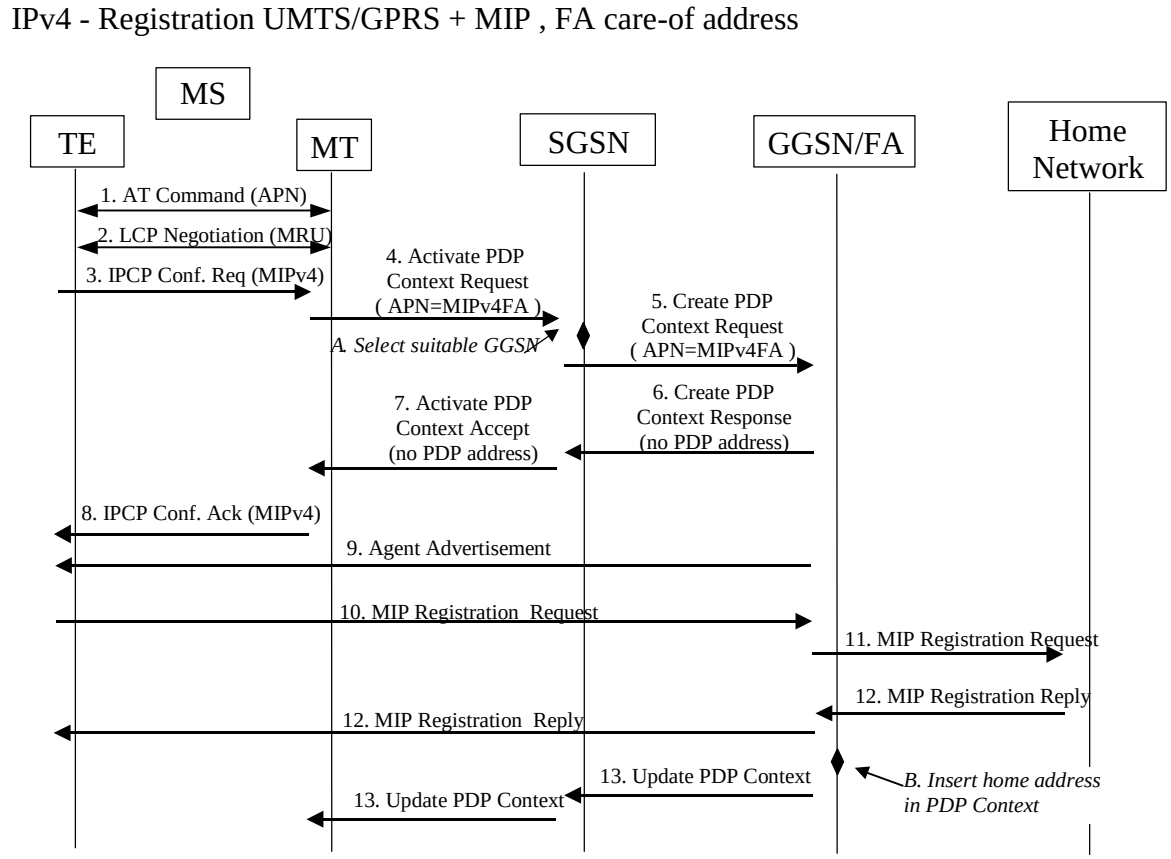


Figure 11e: PDP Context activation with Mobile IP registration (the PS attach procedure not included)

1. The AT command carries parameters that the MT needs to request the PDP Context Activation. The important parameter here, is the APN (Access Point Name), see clause A below. The AT command is followed by a setup of the PPP connection between the MT and the TE.

2. As part of the PPP connection, LCP negotiates Maximum-Receive-Unit between the TE and the MT. No PPP authentication is required when using MIPv4.

3. As part of the PPP connection, the TE sends an IPCP Configure Request using the MIPv4 configuration option (see [37]). The TE sends either its Home Address or a null address (i.e. 0.0.0.0) if the Network Address identifier is used (see [25]).

4. The MT 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 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 to a service that the subscriber wishes to connect to. 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.

A. The SGSN will base the choice of GGSN based on the APN that is given by the MS.

5. 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.

6. 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 a Home Agent after the PDP context activation procedure.

7. The Activate PDP Context Accept message is sent by the SGSN to the MT and contains similar information as the Create PDP Context Response message.

8. The MT sends an IPCP Configure Ack to the TE in order to terminate the PPP connection phase.

9. The Agent Advertisement [30] is an ICMP (Internet Control Message Protocol) 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.

10. 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 [30]. 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 [25], [31].

11. 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 or the NAI and the local link address of the MS, i.e. the TEID (Tunnel Endpoint ID).

12. 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 user plane. As the FA/GGSN knows the TEID and the NAI or home address, it can pass it on to the correct MS.

B. The GGSN/FA extracts the home address from the Mobile IP Registration Reply message and updates its GGSN PDP Context.

13. The GGSN triggers a "GGSN initiated PDP Context modification procedure" in order to update the PDP address in the SGSN and in the MT.

11.3 Numbering and Addressing

In the case of interworking with public IP networks (such as the Internet), the PLMN operator shall use public network addresses. These public addresses can be reserved from the responsible IP numbering body, or from an ISP with which the PLMN operator has an agreement.

In the case of interworking with private IP networks, two scenarios can be identified:

1. the GPRS operator manages internally the subnetwork addresses. Each private network is assigned a unique subnetwork address. Normal routing functions are used to route packets to the appropriate private network;

2. each private network manages its own addressing. In general this will result in different private networks having overlapping address ranges. A logically separate connection (e.g. an IP in IP tunnel or layer 2 virtual circuit) is used between the GGSN and each private network. In this case the IP address alone is not necessarily unique. The pair of values, Access Point Name (APN) and IP address, is unique.

The PLMN operator allocates the IP addresses for the subscribers in either of the following ways.

- The PLMN operator allocates a static IP address when the subscription record is built. The IP address is reserved from a pool of free IP addresses. Each external network has its own pool of addresses.

- The PLMN operator allocates (either on its own or in conjunction with the external network) a dynamic IP address when the MS performs the PDP Context Activation procedure with dynamic address allocation as described in 3GPP TS 23.060.

11.4 Charging

The PLMN operator may define the accuracy of the charging mechanism using one of the following categories:

- every source/destination pair is logged separately;
- source/destination pairs are logged to an accuracy of subnetworks;
- source/destination pairs are logged to an accuracy of connection types (e.g., external data network, corporate network, another mobile).

11.5 Domain Name System Server (DNS Server)

Provision of Domain Name services shall be provided by the PLMN operators in the transparent case and the ISP in the non transparent case. (DNS documentation is provided in RFC 1034 and RFC 1035).

11.6 Screening

The way the PLMN is performing the operator controlled screening and the subscription controlled screening is out of the scope of the present document. These functions may be done, for example, in a firewall.

11.7 IP Multicast access

The Packet Domain could allow access to IP Multicast traffic coming from an external network. The support of IP-Multicast in the Packet Domain is optional.

In order for the Packet Core Network to support Multicast traffic that will allow the MS to subscribe to multicast groups from outside the PLMN, the GGSN shall support IGMP and one or more Inter-Router Multicast protocols, such as DVMRP, MOSPF, or PIM-SM.

IGMP is an integral part of IP. All hosts wishing to receive IP multicasts are required to implement IGMP (or equivalent) and class-D IP addresses. IGMP messages are encapsulated in IP datagrams.

To be able to deliver IP-Multicast packets to the appropriate TEs, the GGSN may have an IP-Multicast proxy functionality.

The IP-Multicast proxy will perform the following tasks:

NOTE: In this example it is assumed that IGMP is used as a Host-Router Multicast protocol.

- maintain a list of mobiles that joined one or more Multicast groups. This list is built/updated each time the GGSN receives an IGMP Join Message from the mobile;
- send, based on this maintained list of mobiles, multicast routing information to the routers attached to the Packet Domain, allowing them to route multicast packets;
- upon reception by the GGSN of multicast packets, make and send a copy as Point-to-Point packets, to each mobile of the group.

IP-Multicast traffic can only be handled after an MS has attached to the Packet Domain, and Activated PDP context(s) (including possibly authentication) to the preferred ISP/external network. The Multicast traffic is handled at the application level from a Packet Domain perspective and is sent over UDP/IP.

The following figure 12 depicts the protocol configuration for handling Multicast traffic (control plane). The Multicast traffic handling affects the GGSN by the introduction of the IP-Multicast proxy and the support for an Inter-Router Multicast protocol and a host-router multicast protocol.

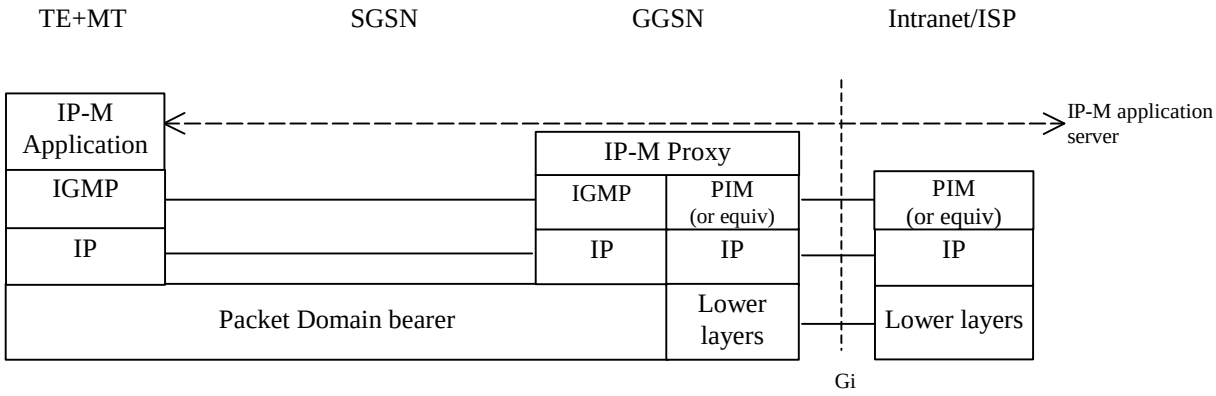


Figure 12: Protocol configuration for IP-Multicast handling (control plane)

12 Interworking with PDN (PPP)

12.1 General

By means of the PDP type 'PPP' Packet Domain may support interworking with networks based on the point-to-point protocol (PPP), as well as with networks based on any protocol supported by PPP through one of its Network Control Protocols (NCPs). All protocols currently supported by PPP NCP's are listed in [21]. It may also support interworking by means of tunnelled PPP, by e.g. the Layer Two Tunnelling Protocol (L2TP).

12.2 PDN Interworking Model

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 (see figure 13). The GGSN will either terminate the PPP connection towards the MS or may further relay PPP frames to the PDN. The PPP frames may be tunnelled in e.g. L2TP.

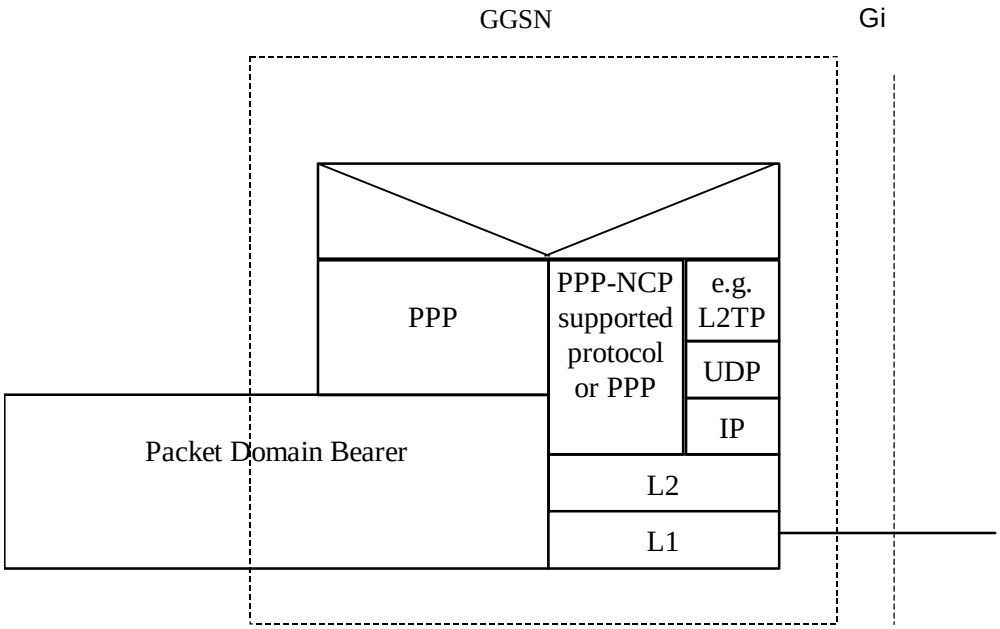


Figure 13: The protocol stacks for the Gi PPP reference point

In case the external PDN is an IP based network and the GGSN terminates PPP the same description applies as specified in subclause 11.2.

In case the GGSN tunnels PPP frames to the PDN, the GGSN may behave like a LAC towards the external network.

12.2.1 Virtual dial-up- and direct Access to PDNs, or ISPs through Packet Domain

The access to PDNs, or ISPs may involve specific functions such as: user authentication, user's authorization, end to end encryption between MS and PDN/ISP, allocation of a dynamic address belonging to the PLMN/PDN/ISP addressing space, etc.

For this purpose the PLMN may offer, based on configuration data:

- direct access to an IP based Intranet/ISP using a protocol configuration as depicted in figure 14. Here DHCP and/or RADIUS are used between the GGSN and Intranet/ISP for performing the specific functions mentioned above. The Packet Domain may also offer access to networks based on any protocol supported by PPP through one of its Network Control Protocols (NCPs);

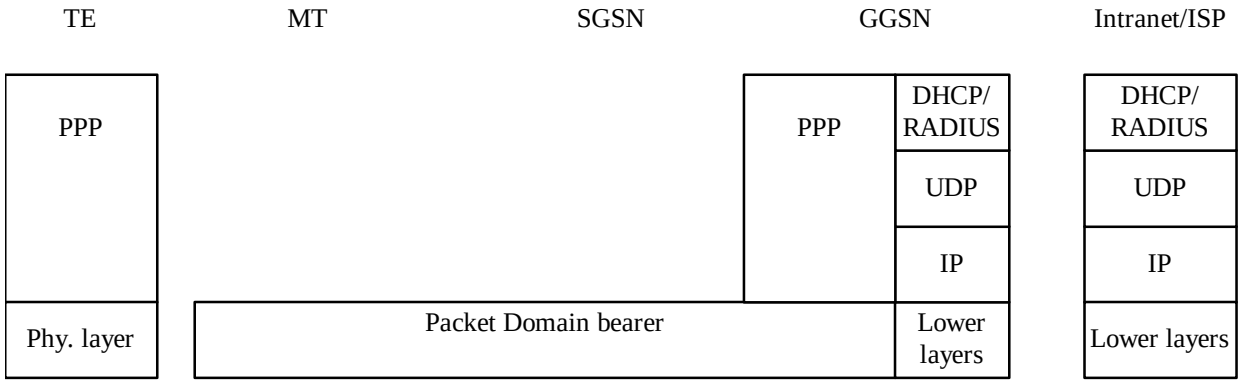


Figure 14: Protocol stack for direct access to IP-based Intranets/ISPs

- virtual dial-up access to a PDN with PPP frame tunnelling as depicted in figure 15.

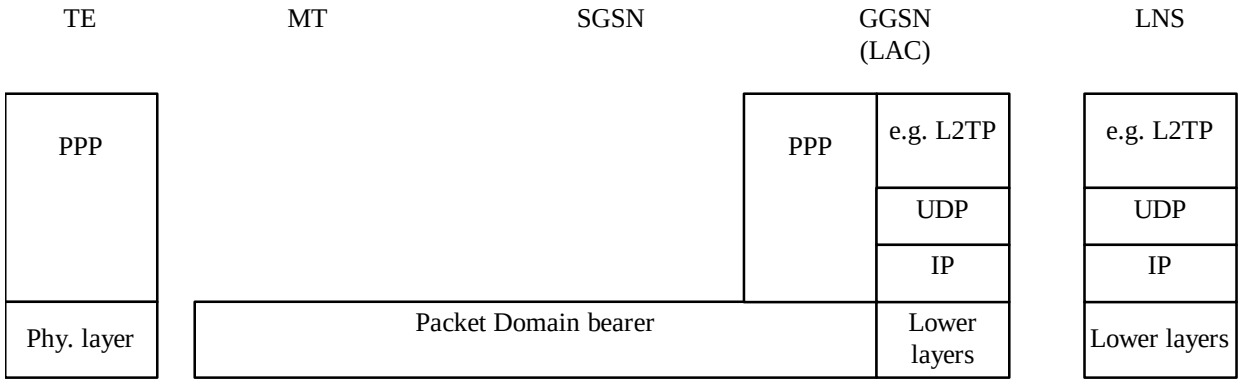


Figure 15: Protocol stack for virtual dial-up access with PPP frame tunnelling

12.2.1.1 Procedural description

In this 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 for packet forwarding 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 e.g. 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 PLMN operator and Intranet/ISP administrator.

The following description bullet items describe 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 which sends the Create PDP context request message to the chosen GGSN.

3) The GGSN deduces from the APN:

   - the server(s) to be used for address allocation and authentication;

   - the protocol such as Radius, DHCP or L2TP to be used with this / those server(s);

   - the communication and security feature needed to dialogue with this / those server(s) e.g. tunnel ,IPSec security association, dial-up 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 an 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 a 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 either send the Activate PDP Context Accept message or send the 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 non-successful 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.

NOTE: With the <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.

EXAMPLE: In the following example the successful PDP context activation is shown.

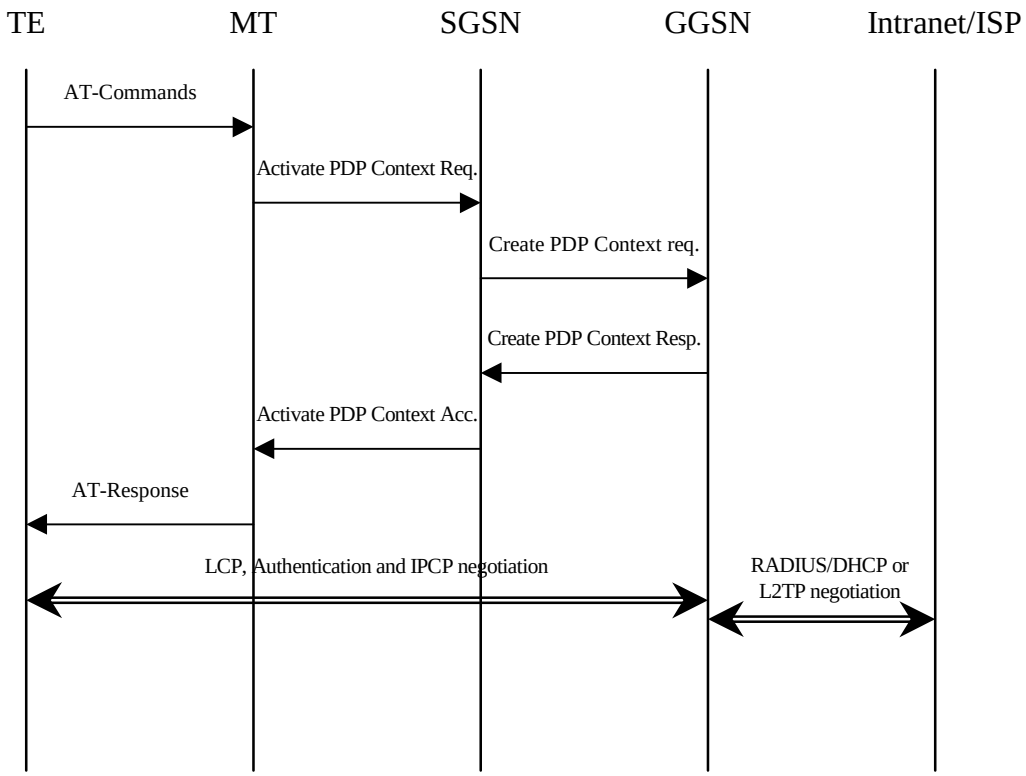


Figure 16a

13 Interworking with PDN (DHCP)

13.1 General

In current LAN environments the most commonly used configuration protocol is DHCP (Dynamic Host Configuration Protocol, [20]). It provides a mechanism for passing a large set of configuration parameters to hosts connected to a TCP/IP network (IP address, sub-net mask, domain name, MTU, etc.) in an automatic manner. Moreover DHCP may assign IP addresses to clients for a finite lease time, allowing for sequential reassignment of addresses to different users.

The lease time is chosen by the administrator of the DHCP server (in the external network), and is therefore out of the scope of this specification.

The Packet Domain offers the end user the possibility to run DHCP end-to-end the same way as he does when connected directly to a LAN (e.g. an enterprise Intranet). No modifications should be required in common implementations of DHCP clients and servers. However a Packet Domain-specific DHCP relay agent [21] is needed in the GGSN so as to allow correct routing of DHCP requests and replies between the TE and the DHCP servers.

At PDP context activation no IP address is allocated, this is done afterwards through DHCP. After the TE's configuration has been completed by DHCP, the PDP context is updated by means of the GGSN-initiated PDP Context Modification Procedure in order to reflect the newly assigned IP address.

In the following cases the corresponding PDP context shall be deactivated and the whole procedure starting with PDP context activation shall be restarted by the MS

- if the DHCP lease expires
- if the DHCP renewal is rejected by the DHCP server
- if the IP address is changed during the renewal process. Usually when the lease is renewed, the IP address remains unchanged. However, if for any reason (e.g. poor configuration of the DHCP server), a different IP address is allocated during the lease renewal process the PDP Context shall be deactivated.

13.2 PDN Interworking Model for DHCP

A DHCP relay agent shall be located in the GGSN used for interworking with the IP network as illustrated in the following figure 16b.

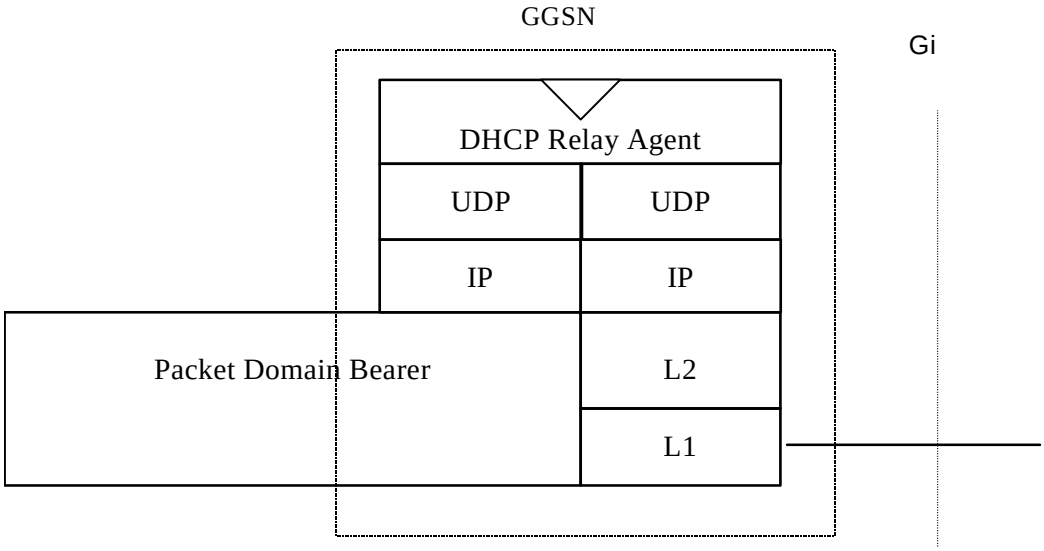


Figure 16b: The protocol stacks for the Gi IP reference point for DHCP

The DHCP relay agent relays the requests received from the DHCP client to the DHCP server(s), and the replies received from the server(s) to the corresponding client. The DHCP relay agent allows for the replies from DHCP servers to be delivered to the correct terminal, as the logical connection from the MT terminates in the GGSN, and consequently only the GGSN holds enough information to locate the DHCP client. How the DHCP relay agent identifies the MT based on the DHCP messages is out of the scope of UMTS standardisation.

DHCP provides mechanisms for user authentication and integrity protection, but does not offer any message confidentiality, therefore additional mechanisms (e.g. IPsec tunnel) may be provided if the link towards the external network is not secure. However this is out of the scope of the present document.

Apart from the particulars mentioned above, this model is basically the same as the one for interworking with IP networks described elsewhere in the present document. Using DHCP corresponds to the transparent access case as the GGSN does not take part in the functions of authentication, authorisation, address allocation, etc.

13.2.1 Address allocation by the Intranet or ISP

The MS is given an address belonging to the Intranet/ISP addressing space. The address is given dynamically immediately after the PDP context activation. This address is used for packet forwarding between the Intranet/ISP and the GGSN and within the GGSN.

The MS may authenticate itself to the Intranet/ISP by means of the relevant DHCP procedures (DHCP authentication is currently described in an Internet Draft).

The protocol configuration options are retrieved from the DHCP server belonging to the Intranet/ISP.

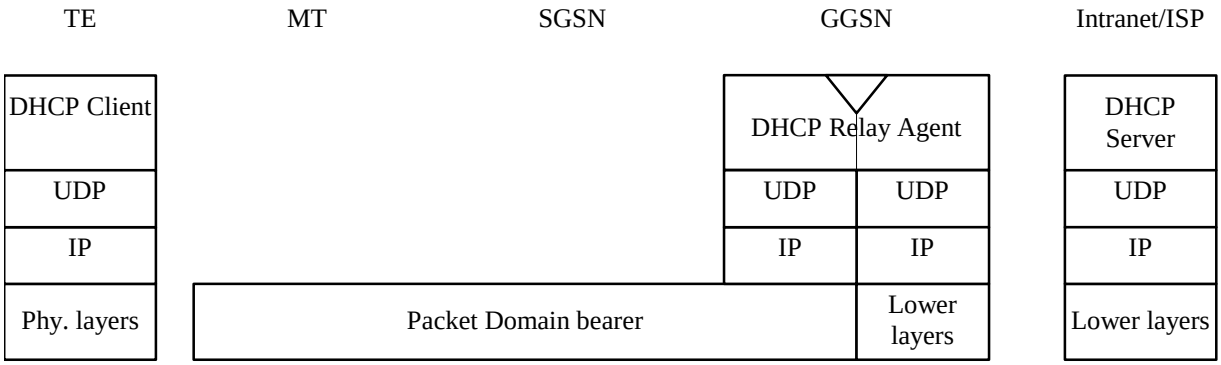


Figure 16c: Protocol stack for access with DHCP end-to-end

The following description bullet items describe the signal flow. For a detailed description of the DHCP messages refer to [26], [27]. The end-to-end protocol configuration is depicted in figure 16c.

1) The TE and MT exchange several AT commands carrying the QoS and other parameters requested by the TE, and requesting the activation of a PDP context of PDP type IP. The TE selects the APN of the configured Intranet/ISP offering a DHCP service, or the APN consisting of the Reserved Service Label for DHCP that the user has subscribed to. In the latter case the TE will be connected to a PLMN operator-configured service provider offering a DHCP service (according to the APN selection rules).

2) The MT sends the Activate PDP Context Request message to the SGSN with an empty PDP address field.

3) The SGSN selects a GGSN based on the APN requested by the MS and sends a Create PDP Context Request message to that GGSN. The GGSN replies with a Create PDP Context Response message. If the GGSN has not been configured by the operator to use external PDN address allocation with DHCP for the requested APN, the cause shall be set to 'Service not supported'. No IP address is assigned at this point; the PDP address returned by the GGSN is set to 0.0.0.0, indicating that the IP address is not yet assigned and shall be negotiated by the TE with the Intranet/ISP after the PDP context activation procedure.

4) Depending on the cause value received in the Create PDP Context Response the SGSN sends either an Activate PDP Context Accept or an Activate PDP Context Reject back to the MT. In case of a successful activation the PDP context is established with the PDP address set to 0.0.0.0.

5) Upon reception of the Activate PDP Context Accept, the MT sends an AT response to the TE that acknowledges the completion of the PDP context activation procedure.

6) The TE sends a DHCPDISCOVER message with the IP destination address set to the limited broadcast address (all 1s). The GGSN will pass the DHCPDISCOVER to the DHCP relay agent which will relay the request to the DHCP server configured for the APN of the PDP context. If more than one DHCP server is configured for a given APN, the request will be sent to all of them. The DHCP relay agent will add enough information to the DHCPDISCOVER message to be able to relay the replies back to the MS. How this is done is out of the scope of UMTS standardisation.

7) DHCP servers receiving the DHCPDISCOVER request reply by sending a DHCPOFFER message including an offered IP address. The DHCP relay agent forwards the replies to the proper MS.

8) The TE chooses one of the possibly several DHCPOFFERs and sends a DHCPREQUEST confirming its choice and requesting additional configuration information. The relay agent relays the DHCPOFFER as explained in step 6.

9) The selected DHCP server receives the DHCPREQUEST and replies with a DHCPACK containing the configuration information requested by the TE. The DHCP relay agent relays the DHCPACK to the TE.

10) The DHCP relay agent passes the allocated IP address to the GGSN which stores it in the corresponding PDP context. The GGSN then initiates a PDP context modification procedure by sending an Update PDP Context Request to the appropriate SGSN with the End User Address information element set to the allocated IP address.

11) The SGSN sends a Modify PDP Context Request to the MT with the allocated IP address in the PDP Address information element. The MT acknowledges by sending a Modify PDP Context Accept to the SGSN.

12) The SGSN sends an Update PDP Context Response to the GGSN. The PDP context has been successfully updated with the allocated IP address.

EXAMPLE: In the following example a successful PDP context activation with use of DHCP from end to end is shown.

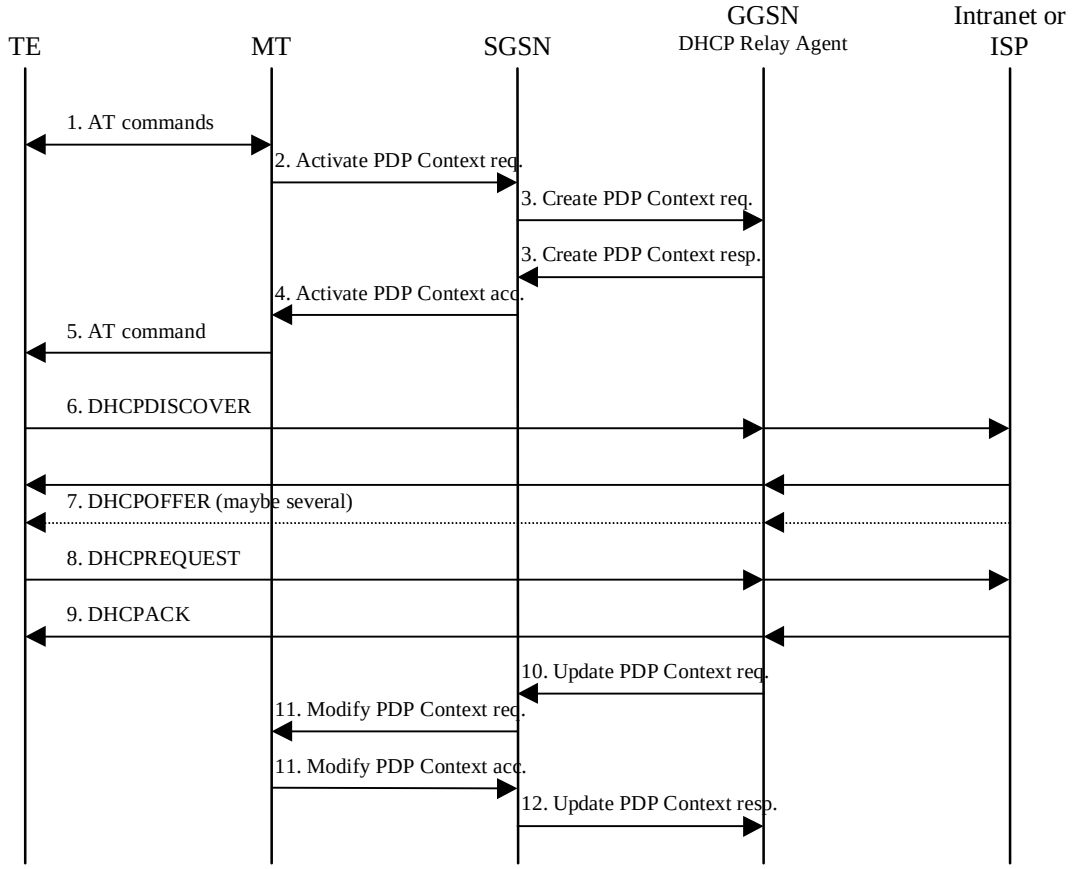


Figure 16d

14 Internet Hosted Octet Stream Service (IHOSS)

Void.

15 Interworking between Packet Domains

The primary reason for the interworking between Packet Domains is to support roaming subscribers as described in TS 23.060. The general model for Packet Domain interworking is shown in figure 21.

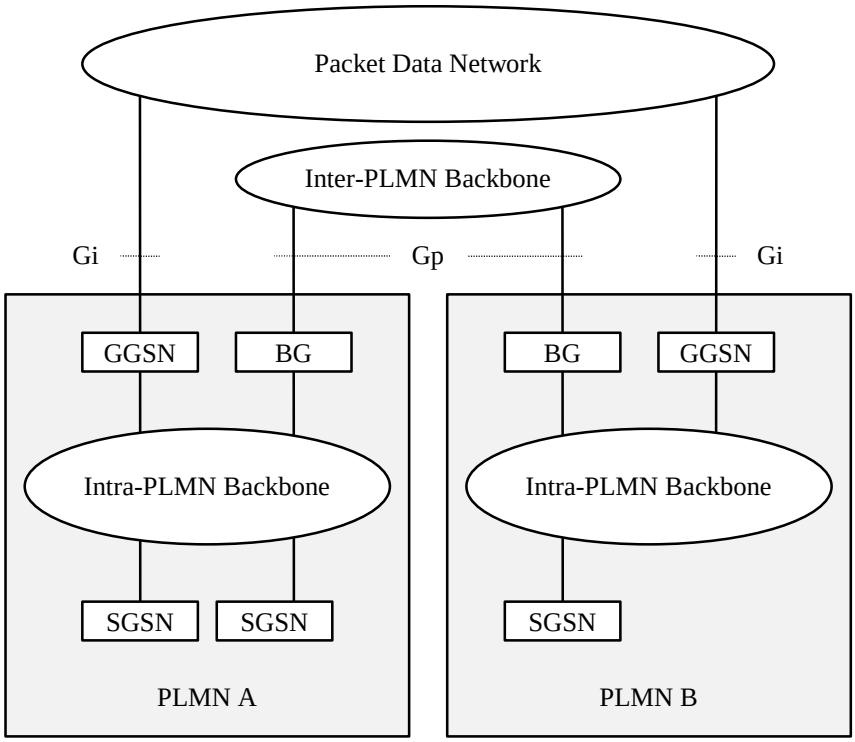


Figure 21: General interworking between Packet Domains to support roaming subscribers.

For roaming subscribers that have a PDP address allocated from the HPLMN a forwarding route between the HPLMN and the VPLMN is created. This route is used for both mobile terminated and mobile originated data traffic. The communication is done via the BGs (Border Gateways) as described in 3GPP TS 23.060.

The procedures to set the link between the SGSN in the VPLMN and the GGSN in the HPLMN are described in 3GPP TS 23.060.

The inter-PLMN link may be any packet data network or dedicated link as described in 3GPP TS 23.060. The PLMN operators may have a dedicated inter-PLMN link to fulfil the QoS requirements of a certain protocol.

15.1 Security Agreements

Each PLMN operator may support IPsec (RFC 1825) and accompanying specifications for authentication (RFC 1826) and encryption (RFC 1827) as a basic set of security functionality in its border gateways. The PLMN operators may decide to use other security protocols based on bilateral agreements.

15.2 Routing protocol agreements

Each PLMN operator may support BGP (RFC 1771) as a basic set of routing functionality in its border gateways. The PLMN operators may decide to use other routing protocols based on bilateral agreements.

15.3 Charging agreements

Sharing the cost of the inter-PLMN link is subject to the agreement between the PLMN operators.

There may be a requirement to collect charging information in the Border Gateway (see figure 21 in clause 15) and this is down to the normal interconnect agreement between PLMN and PDN operators.

Annex A (informative): Interworking PCS1900 with PSDNs

<VOID>

Annex B (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
	Apr 1999				Transferred to 3GPP CN1	7.0.0	
05-1999	TSG#03				Approved at CN#03		3.0.0
06-1999	TSG#04		001		Access to PDNs and ISPs with the PDP-type PPP	3.0.0	3.1.0
06-1999	TSG#04		002		GPRS Internet Hosted Octet Stream Service (IHOSS)	3.0.0	3.1.0
12-1999	TSG#06		003		Clarification on the PPP LCP Negotiation for PDP Type PPP	3.1.0	3.2.0
12-1999	TSG#06		004		Enhancement to Numbering and Addressing to Include the APN	3.1.0	3.2.0
12-1999	TSG#06		005		IPCP Negotiation Interworking at the MT for Non-Transparent IP	3.1.0	3.2.0
12-1999	TSG#06		006		Mobile IP Issues	3.1.0	3.2.0
12-1999	TSG#06		007		Access to an Intranet/ISP with DHCP End to End	3.1.0	3.2.0
12-1999	TSG#06		008		Streamlining	3.1.0	3.2.0
03-2000	TSG#07		009		Specification reference section clean-up	3.2.0	3.3.0
03-2000	TSG#07		010		Support for the IP-Multicast protocol	3.2.0	3.3.0
03-2000	TSG#07		011		Correction for the support of IPv6	3.2.0	3.3.0
03-2000	TSG#07		012		Removal of X.25.	3.2.0	3.3.0
03-2000	TSG#07		013		TSG CN1 Vocabulary Alignment	3.2.0	3.3.0
09-2000	TSG#09		014		Corrections to MobileIP	3.3.0	3.4.0
03-2001	TSG#11	NP-010044	015		DHCP Lease Renewal	3.4.0	3.5.0
03-2001	TSG#11	NP-010044	016		Removal of IHOSS and OSP	3.4.0	3.5.0
03-2001	TSG#11				Upgraded to Release 4	3.5.0	4.0.0

History

Document history		
V4.0.0	March 2001	Publication