ETSI TS 129 061 V3.2.0 (2000-01)

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)
(3G TS 29.061 version 3.2.0 Release 1999)

Reference
DTS/TSGN-0329061U

Keywords
GSM, UMTS

ETSI

Postal address
F-06921 Sophia Antipolis Cedex - FRANCE

Office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - 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

Internet
secretariat@etsi.fr
Individual copies of this ETSI deliverable
can be downloaded from
http://www.etsi.org
If you find errors in the present document, send your
comment to: editor@etsi.fr

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 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 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 or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables. The mapping of document identities is as follows:

For 3GPP documents:

3G TS | TR nn.nnn "<title>" (with or without the prefix 3G)

is equivalent to

ETSI TS | TR 1nn nnn "[Digital cellular telecommunications system (Phase 2+) (GSM);] Universal Mobile Telecommunications System; <title>

For GSM document identities of type "GSM xx.yy", e.g. GSM 01.04, the corresponding ETSI document identity may be found in the Cross Reference List on www.etsi.org/key

Contents

Foreword 5

1 Scope 6

2 References 6

3 Definitions, abbreviations and Symbols 8
3.1 Definitions 8
3.2 Abbreviations 8
3.3 Symbols 9

4 Network characteristics 9
4.1 Key characteristics of PLMN 9
4.2 Key characteristics of PSDN 9
4.3 Key characteristics of IP Networks 9

5 Interworking Classifications 10
5.1 Service Interworking 10
5.2 Network Interworking 10
5.3 Numbering and Addressing 10

6 Access reference configuration 10

7 Interface to Packet Domain Bearer Services 10
7.1 GPRS 10
7.2 UMTS 11

8 Subscription checking 11

9 Message Screening 11

10 Interworking with PSDN (X.75/X.25) 12
10.1 General 12
10.2 PSDN Interworking Models 12
10.2.1 X.75 Interworking at the Gi Reference Point 12
10.2.1.1 Numbering and Addressing 13
10.2.1.2 Charging 13
10.2.2 X.25 Interworking at the Gi Reference Point 14
10.2.2.1 Numbering and Addressing 15
10.2.2.2 Charging 15
10.3 User Facilities 15
10.4 The Packet Domain Interworking to PSDN Characteristics 16

11 Interworking with PDN (IP) 16
11.1 General 16
11.2 PDN Interworking Model 16
11.2.1 Access to Internet, Intranet or ISP through Packet Domain 18
11.2.1.1 Transparent access to the Internet 18
11.2.1.2 Non Transparent access to an Intranet or ISP 19
11.2.1.3 Access to Internet, Intranet or ISP with Mobile IPv4 23
11.3 Numbering and Addressing 25
11.4 Charging 26
11.5 Domain Name System Server (DNS Server) 26
11.6 Screening 26

12 Interworking with PDN (PPP) 26
12.1 General 26
12.2 PDN Interworking Model 27
12.2.1 Virtual dial-up- and direct Access to PDNs, or ISPs through Packet Domain 27
12.2.1.2 Procedural description 28

13 Interworking with PDN (DHCP) 30
13.1 General 30
13.2 PDN Interworking Model for DHCP 30
13.2.1 Address allocation by the Intranet or ISP 31

14 Internet Hosted Octet Stream Service (IHOSS) 33
14.1 Introduction 33
14.2 Protocol stacks at the GGSN 34
14.3 IHOSS connection control and OSP PDP context management 34
14.3.1 Connection establishment and PDP context activation 34
14.3.2 Connection release and PDP context deactivation 35
14.4 OSP:IHOSS - TCP (UDP) relay 35
14.4.1 Required feature 35
14.4.1.1 Flow control 35
14.4.2 Optional features 36
14.4.2.1 Break handling 36
14.4.2.2 GGSN maximum buffer size 36

15 Interworking between Packet Domains 36
15.1 Security Agreements 37
15.2 Routing protocol agreements 37
15.3 Charging agreements 37

Annex A (normative): Interworking PCS1900 with PSDNs 37

A.1 Key characteristics of interworking PCS1900 with PSDNs 37
A.1.1 PSPDNs which are outside the BOC's LATA 38
A.1.2 PSPDNs which are inside the BOC's LATA 38

A.2 Subscription checking 38

A.3 Interworking PCS1900 with PSDN using X.75' 38
A.3.1 General 38
A.3.2 PSDN Interworking Model using X.75' Interworking at the Gi Reference Point 39
A.3.3 Numbering and Addressing 39
A.3.4 Charging 40
A.3.5 User Facilities 40
A.3.6 The Packet Domain Interworking to PSDN Characteristics 40

Annex B: Change history 41

Foreword

This Technical Specification has been produced by the 3GPP.

This TS 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 this TS, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version 3.y.z

where:

3 the first digit:

3 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

This document defines the requirements for Packet Domain interworking between a:

a) PLMN and PSDN

b) PLMN and IP Networks

c) PLMN and PLMN

In addition, annex X describes the special requirements for interworking between a PCS1900 PLMN and a PSDN within a BOC's LATA.

2 References

(References to be cleaned up when release 99 is stable).

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.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

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

[2] 3G TS 22.060: "Digital cellular telecommunication system (Phase 2+); General Packet Radio Service (GPRS): Stage 1 Service Description".

[3] 3G TS 23.060: "Digital cellular telecommunication system (Phase 2+); General Packet Radio Service (GPRS); Stage 2 Service Description ".

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

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

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

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

[9] GSM 04.65: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Subnetwork Dependent Convergence Protocol (SNDCP)".

[10] 3G TS 27.060: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Mobile Station (MS) supporting GPRS".

[11] CCITT Recommendation E.164: "Numbering plan for the ISDN era".

[12] CCITT Recommendation X.25: "Interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit".

[13] CCITT Recommendation X.75: "Packet-switched signalling system between public networks providing data transmission services".

[14] CCITT Recommendation X.121: "International Numbering Plan for Public Data Networks".

[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] Bellcore GR-000301 Issue 2 December 1997; “Public Packet Switched Network Generic Requirements (PPSNGR)”.

[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] Pat R. Calhoun and Charles E. Perkins, “Mobile IP Network Address Identifier Extension”, October 1999. Work in progress (http://www.ietf.org/internet-drafts/draft-ietf-mobileip-mn-nai-05.txt).

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

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

[RFC2002] IETF RFC 2002 (1996), C. Perkins: “IP Mobility Support”

[RFC2486] IETF RFC 2486 (1999), B. Aboba and M. Beadles: “The Network Access Identifier”,

January 1999

3 Definitions, abbreviations and Symbols

3.1 Definitions

Refer to UMTS 22.060 and UMTS 23.060.

2G- / 3G- The 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
BOC Bell Operating Company
CHAP Challenge Handshake Authentication Protocol
DHCP Dynamic Host Configuration Protocol
DNS Domain Name System
DNIC Data Network Identification Code
DSE Data Switch Exchange
GGSN Gateway GPRS Support Node
GTP-U GPRS Tunnelling Protocol for user plane
IC Interexchange Carrier
ICMP Internet Control Message Protocol
IETF Internet Engineering Task Force
IHOSS Internet Hosted Octet Stream Service
IP Internet Protocol
IPv4 Internet Protocol version 4
IPv6 Internet Protocol version 6
ISDN Integrated Services Digital Network
ISP Internet Service Provider
LATA Local Access and Transport Area
LAPB Link Access Protocol Balanced
LAC L2TP Access Concentrator
LAN Local Area Network
LNS L2TP Network Server
MIP Mobile IP
MS Mobile Station
MT Mobile Terminal
MTU Maximum Transfer Unit
NAI Network Access Identifier

OSP Octet Stream Protocol
OSP:IHOSS Octet Stream Protocol for Internet Hosted Octet Stream Service
PAP Password Authentication Protocol
PDCP Packet Data Convergence Protocol
PDN Packet Data Network
PDU Protocol Data Unit
PHF Packet Handler Function
PNIC Pseudo Network Identification Code
PPP Point-to-Point Protocol

PS	Packet Switched
PPSN	Public Packet Switched Network
PSDN	Packet Switched Data Network
PSPDN	Packet Switched Public Data Network
RADIUS	Remote Authentication Dial In User Service
SGSN	Serving GPRS Support Node
SMDS	Switched Multimegabit Data Service
TE	Terminal Equipment
TEID	Tunnel End-point Identifier
TCP	Transmission Control Protocol
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.
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 GPRS fixed network part. The Um interface is the GPRS network interface for providing packet data services over the radio to the MS. The MT part of the MS is used to access the GPRS 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 3G TS 22.060 and 3G TS 23.060.

4.2 Key characteristics of PSDN

Packet Switched Data Networks (PSDNs) are defined in the relevant CCITT/ITU-T X series.

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, PSDN X.75). Interworking appears exactly like that of Packet Data Networks.

5.3 Numbering and Addressing

See 3G TS 23.003 and the relevant sections for X.25 and 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.

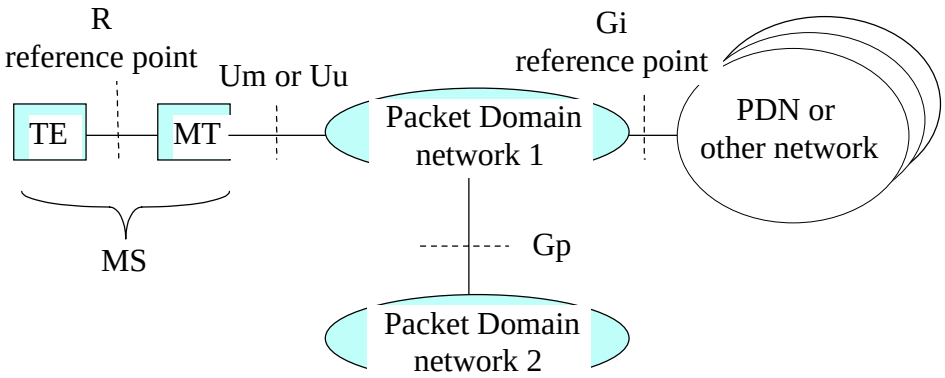
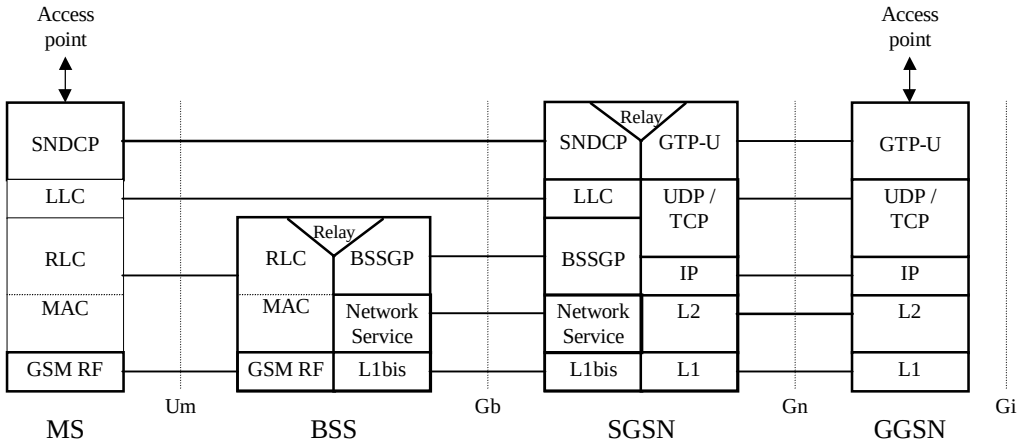


Figure 1: Packet Domain Access Interfaces and Reference Points

7 Interface to Packet Domain Bearer Services

7.1 GPRS

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



NOTE: In the SGSN and GGSN UDP is mandatory. TCP is optional but recommended for X.25 services.

Figure 2a: GPRS Transmission Plane

7.2 UMTS

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

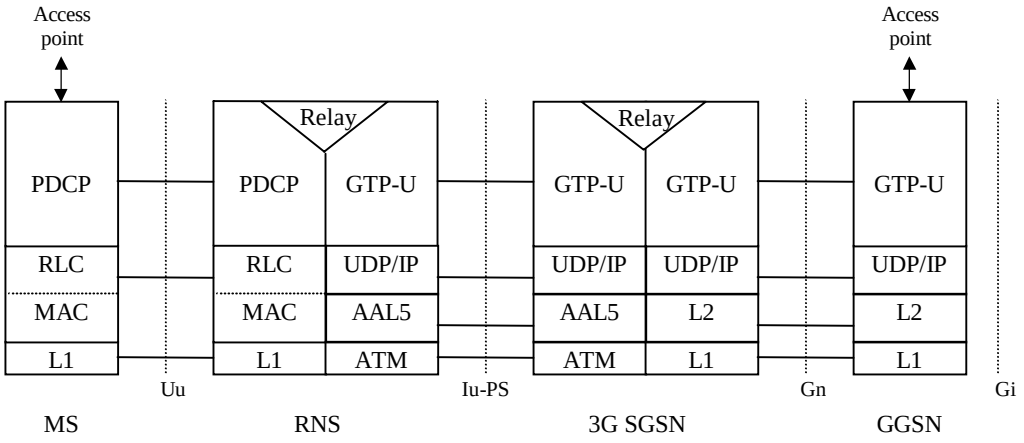


Figure 2b: UMTS User Plane

8 Subscription checking

Subscription is checked during the PS Attach procedure and also during the PDP Context Activation procedure as described in 3G 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 3G TS 22.060 and 3G TS 23.060. Screening may be applicable for only certain protocols. Screening is outside the scope of this specification .

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

10.1 General

The Packet Domain shall support interworking with PSDN networks. The interworking may be either direct or through a transit network.

Packet Domain shall support both CCITT/ITU-T X.121 and CCITT/ITU-T E.164 addressing.

Packet Domain shall provide support for CCITT/ITU-T X.25 and CCITT/ITU-T X.75.

The Packet Domain TE's shall have addresses provided , and controlled, by their PLMN operator. The PSDN TE sends data to the Packet Domain TE by use of that TE's Packet Domain DNIC (Data Network Identification Code) or equivalent which uniquely identifies that Packet Domain network worldwide.

The GGSN for interworking with PSDNs is the access point of the Packet Domain network.

There are two models for PSDN interworking.

- X.75 over the Gi reference point.
- X.25 over the Gi reference point with the DCE located within the PSDN and the DTE located within the TE of the PLMN.

Both X.75 and X.25 access methods are supported when mobile users are resident on HPLMN or VPLMN. A roaming user may be allocated a dynamic address from the VPLMN.

10.2 PSDN Interworking Models

The two models of X.75 and X.25 represent the different scenarios for PSDN interworking with the Packet Domain network.

The model differences lie in the interconnection protocol over the Gi reference point.

10.2.1 X.75 Interworking at the Gi Reference Point

Figure 3 represents the case where X.75 is used as the interworking protocol, as used between interconnect X.25 PSDNs currently. The Packet Domain network will look like any other PSDN in all respects and uses X.75 addressing. Figure 4 shows the interconnecting protocol stacks to the Packet Domain bearer. The Packet Domain bearer is described in 3G TS 27.060, which uses the protocols described in 3G TS 23.060.

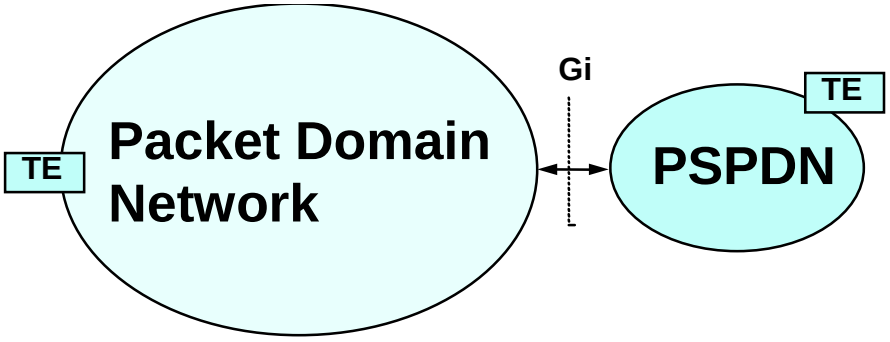


Figure 3: PSPDN Interworking with X.75 at Gi Reference Point

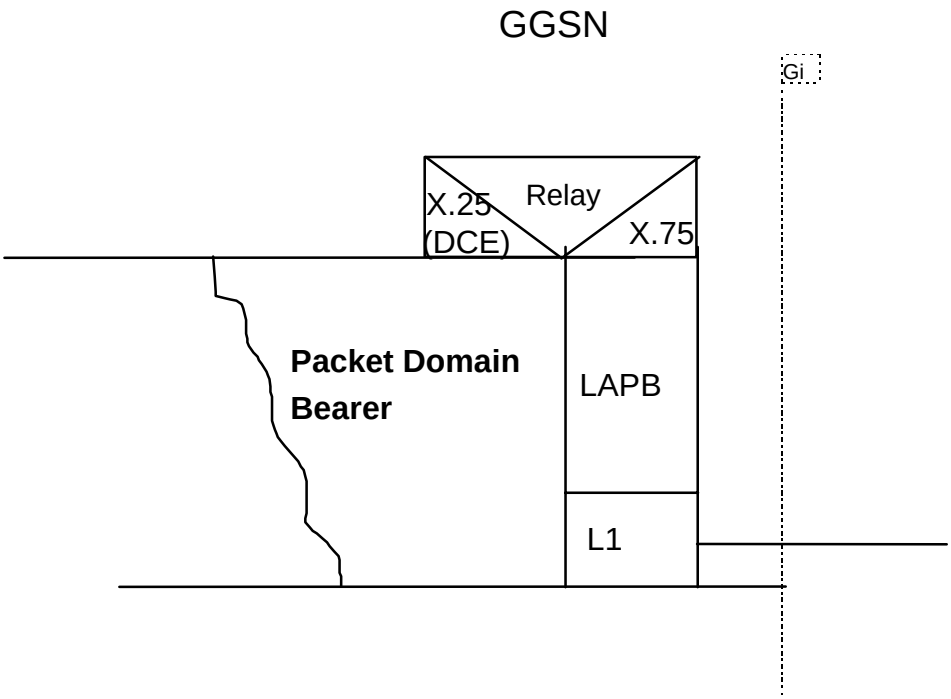


Figure 4: The Protocol Stack for the X.75 Gi Reference Point

10.2.1.1 Numbering and Addressing

A PLMN interworking with PSPDN requires a DNIC or PNIC.

X.121 addresses allocated to subscribers belong to the PLMN operator.

10.2.1.2 Charging

Charging of X.25 packets is done at the GGSN.

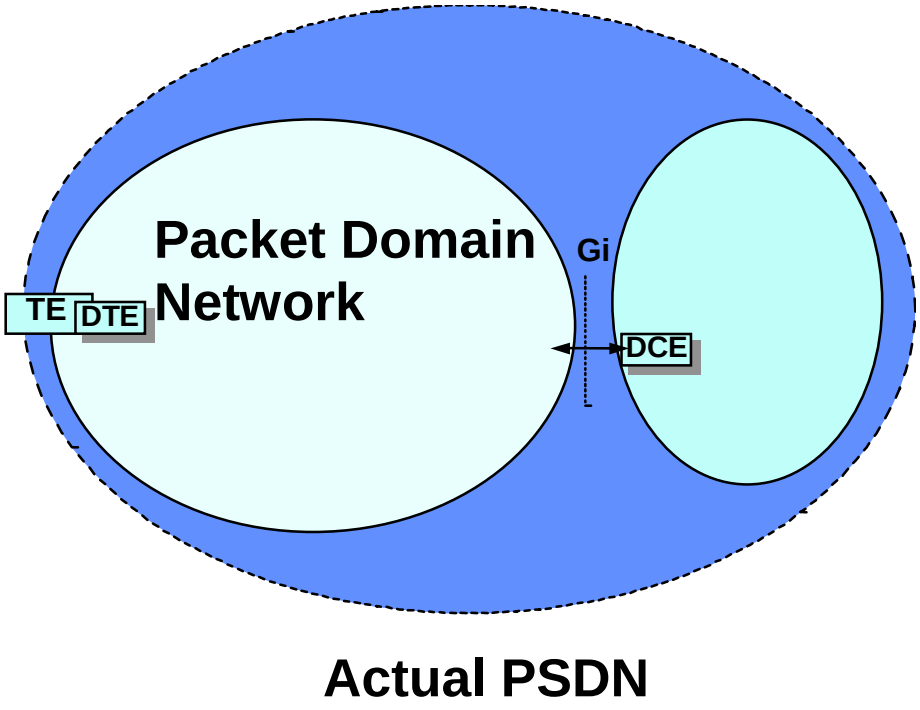
10.2.2 X.25 Interworking at the Gi Reference Point

Figure 5 represents the case where X.25 is used as the interconnect protocol between a DCE and a DTE.

The DTE resides within the Packet Domain network. The DCE resides within the PSDN.

The Packet Domain Network is seen as part of the PSDN, as the Gi reference point is the interconnect point between the DCE and the DTE.

The protocol stack for this model is shown in Figure 6.



NOTE: The PSDN can interwork at X.75 to other PSDN's

Figure 5: PSDN Interworking with X.25 over Gi Interface

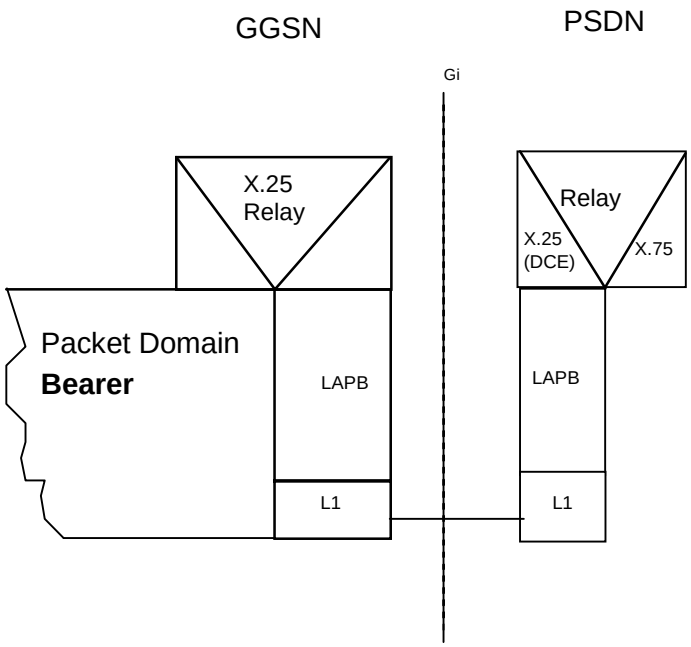


Figure 6: The Protocol Stack for the X.25 / Gi Reference point

Figure 6 shows the transmission plane only. In this case the GGSN shall resolve the association between thePacket Domain bearer and the X.25 DCE. L1 is left to operators to determine connection to other networks.

The X.25 Relay performs the following:

- mapping of logical channel numbers.

10.2.2.1 Numbering and Addressing

A fixed X.121 address for the MS maybe allocated by the PSDN operator, and is integral to the PSDN numbering plan. A dynamic X.121 address can also be used which is assigned by the Packet Domain network at PDP context activation.

10.2.2.2 Charging

The charging information may be collected in the X.25 network, depending upon the agreement between the PLMN operator and the PSDN operator. The charging may also be collected in the Packet Domain network. If the VPLMN assigns the dynamic address, the charging of the Packet Domain and the external network shall be gathered and sent to the HPLMN.

10.3 User Facilities

The set of user facilities as defined in CCITT/ITU-T X.25 may be supported.

As a minimum the following shall be supported:

- reverse charging;
- reverse charging acceptance;

- fast select restricted;
- fast select unrestricted;
- fast select acceptance.

10.4 The Packet Domain Interworking to PSDN Characteristics

The following table describes the differences in addressing, and user profile for each interconnect type. The static X.121 address in the following table indicates an address which is permanently allocated to the subscriber by the network operator. The dynamic X.121 address is assigned automatically on the PDP Context Activation procedure. The dynamic address is allocated from a free pool held in the GGSN. This is described in 3G TS 23.060.

Table 1: PSPDN Packet Domain Interconnection Characteristics

Metric	X.75 – Stand Alone PSPDN X.25 – PSPDN Sub Network	
	Static X.121 address	Dynamic X.121 address
X.25 profile	User determined in X.25 DCE	Only Default Profiles allowed in X.25 DCE- Selected upon PDP context activation
X.28/X.29 PAD	Address in GGSN	Address in GGSN after PDP Context Activation

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.

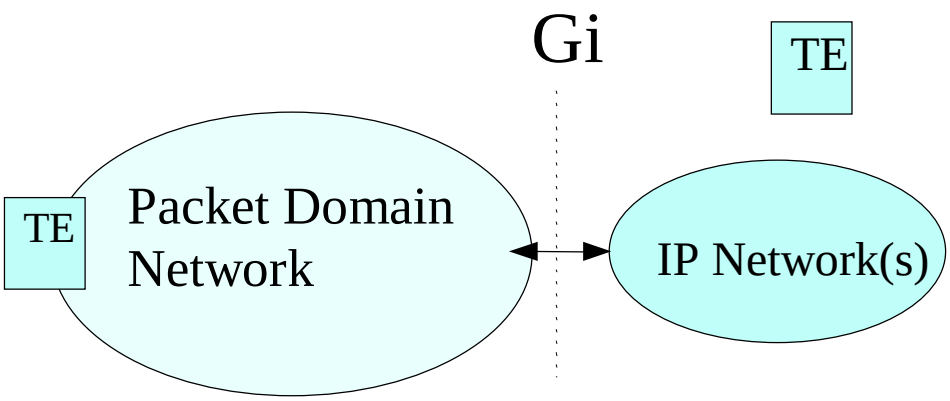


Figure 7: IP network interworking

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.

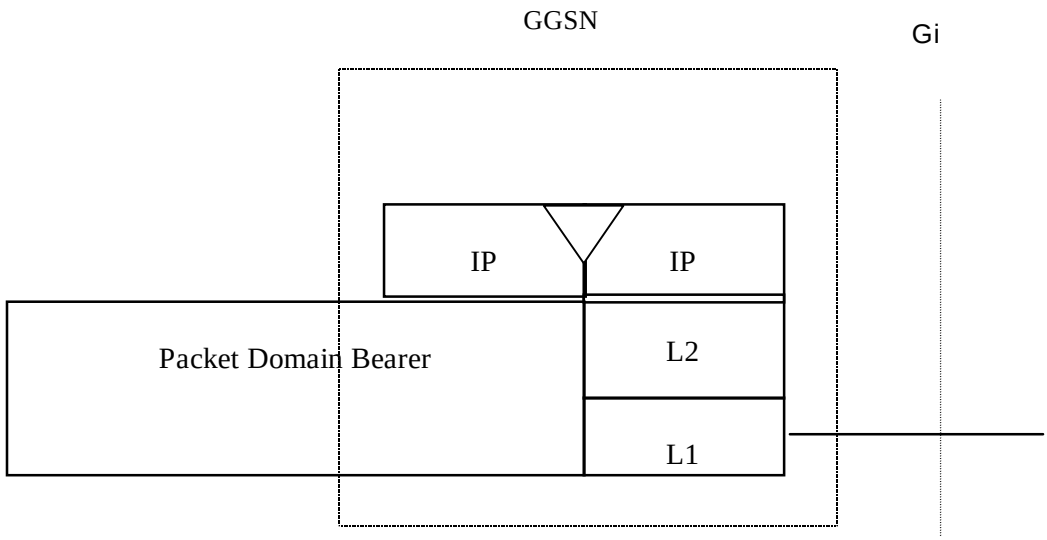


Figure 8: The protocol stacks for the IP / Gi reference point

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 this specification 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

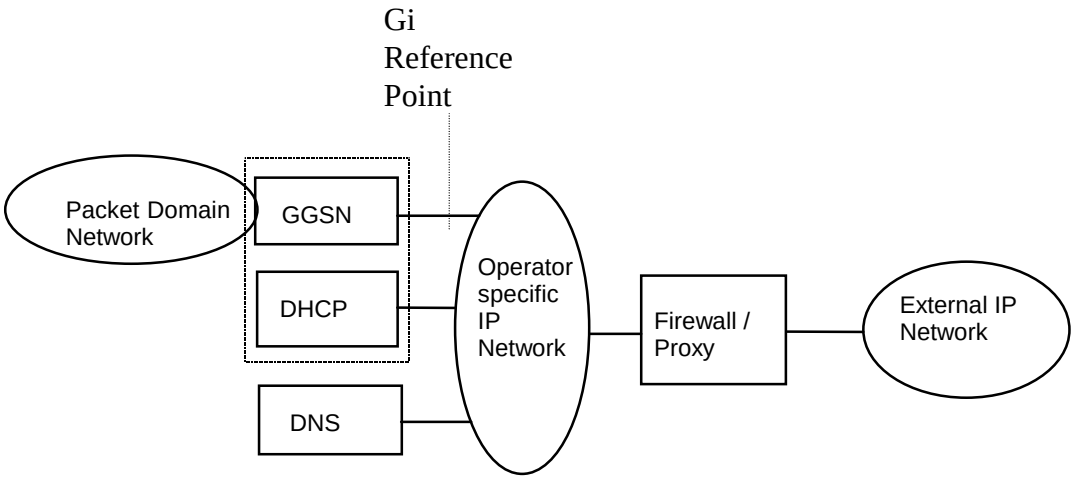


Figure 9: Example of the PDN Interworking Model, transparent case

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.
- 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 section 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.

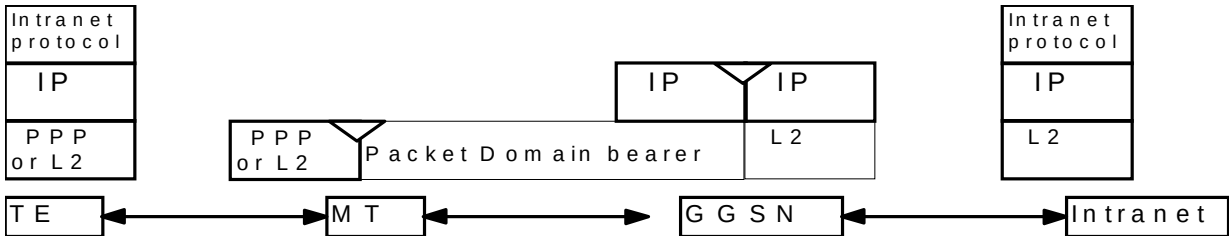


Figure 10: Transparent access to an Intranet

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.

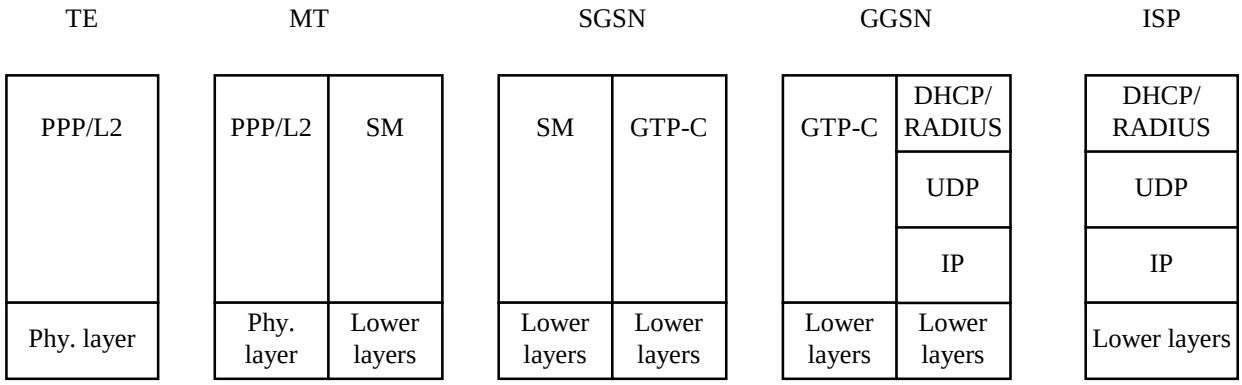


Figure 11a: Signalling plane of non transparent case

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 RFC[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.

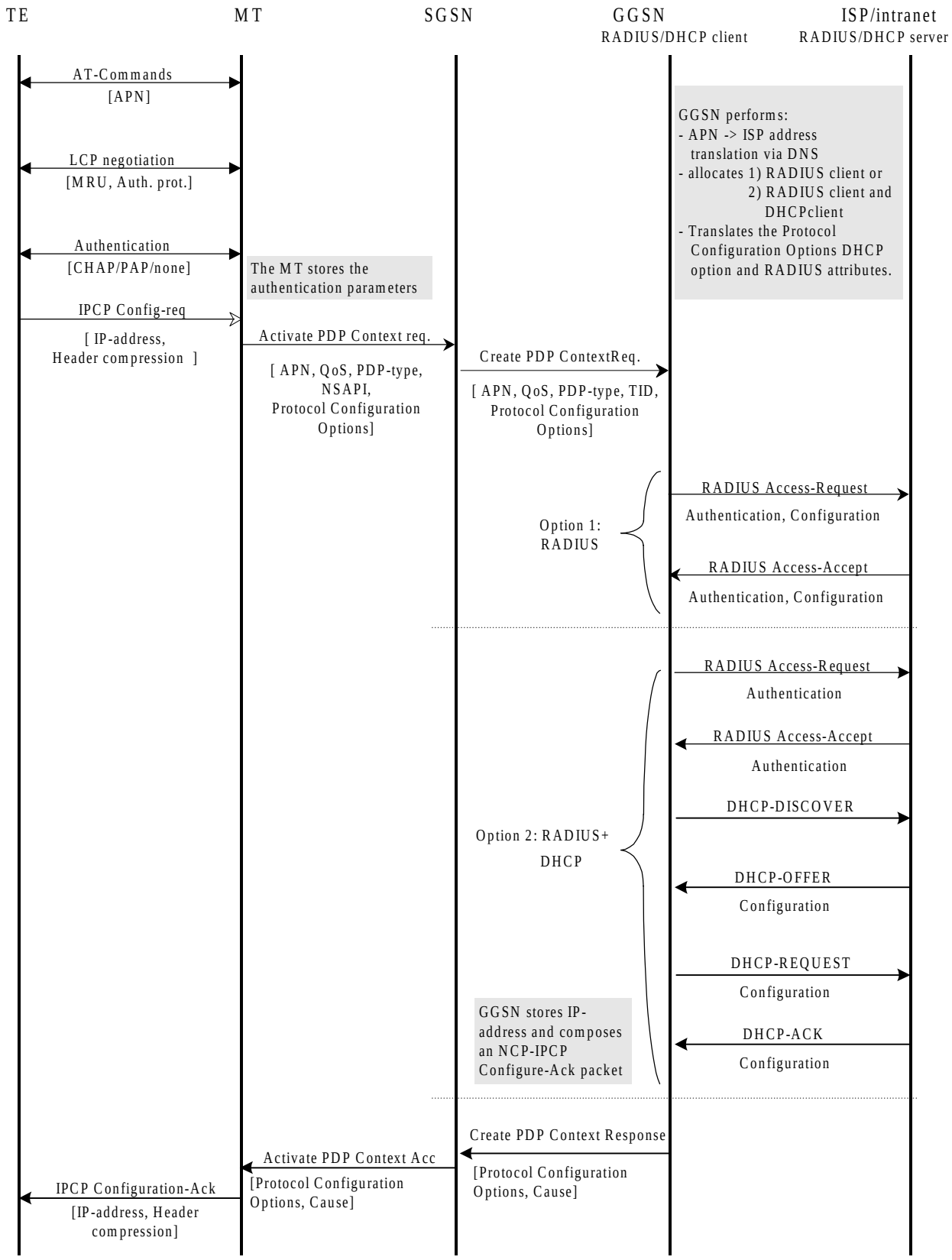


Figure 11b: PDP Context Activation for the Non-transparent IP case

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 [RFC2002]. Mobile IP (MIP) is a mobility management protocol developed by IETF. The Mobile IP Foreign Agent (FA) [RFC2002] is located in the Core Network in the GGSN. MIP also uses a Home Agent (HA) [RFC2002] which may or may not be located in a GPRS/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 [RFC2002] are sent with UDP.

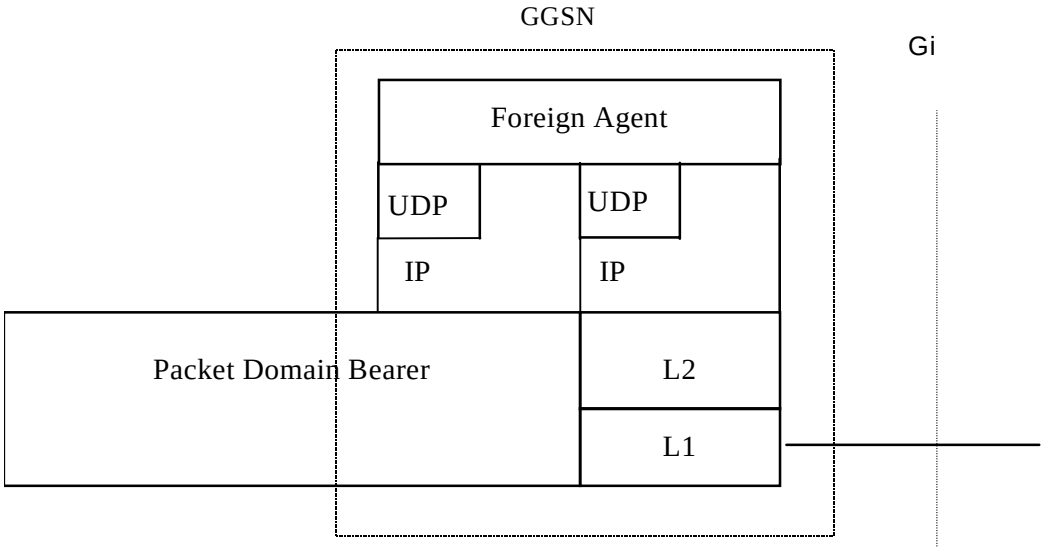


Figure 11c: The protocol stacks for the Gi IP reference point in the MIP signalling plane

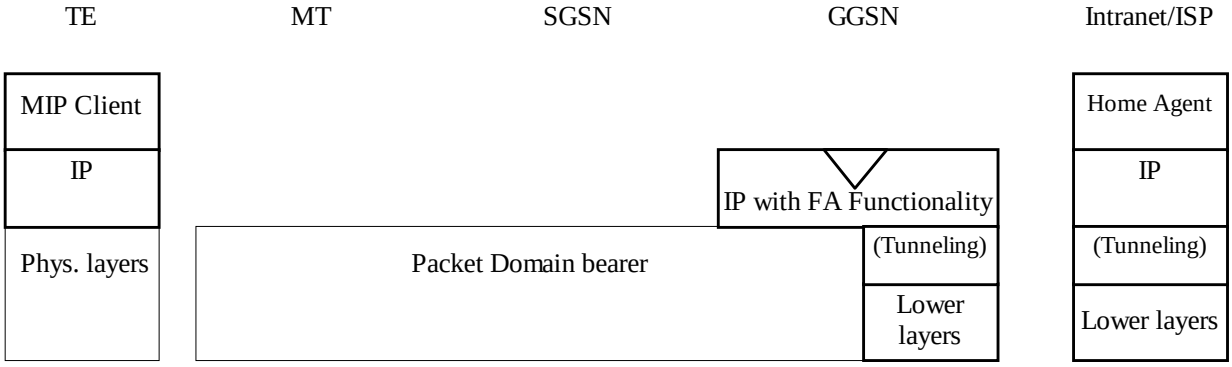


Figure 11d: Protocol stacks for user access with MIP

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.

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

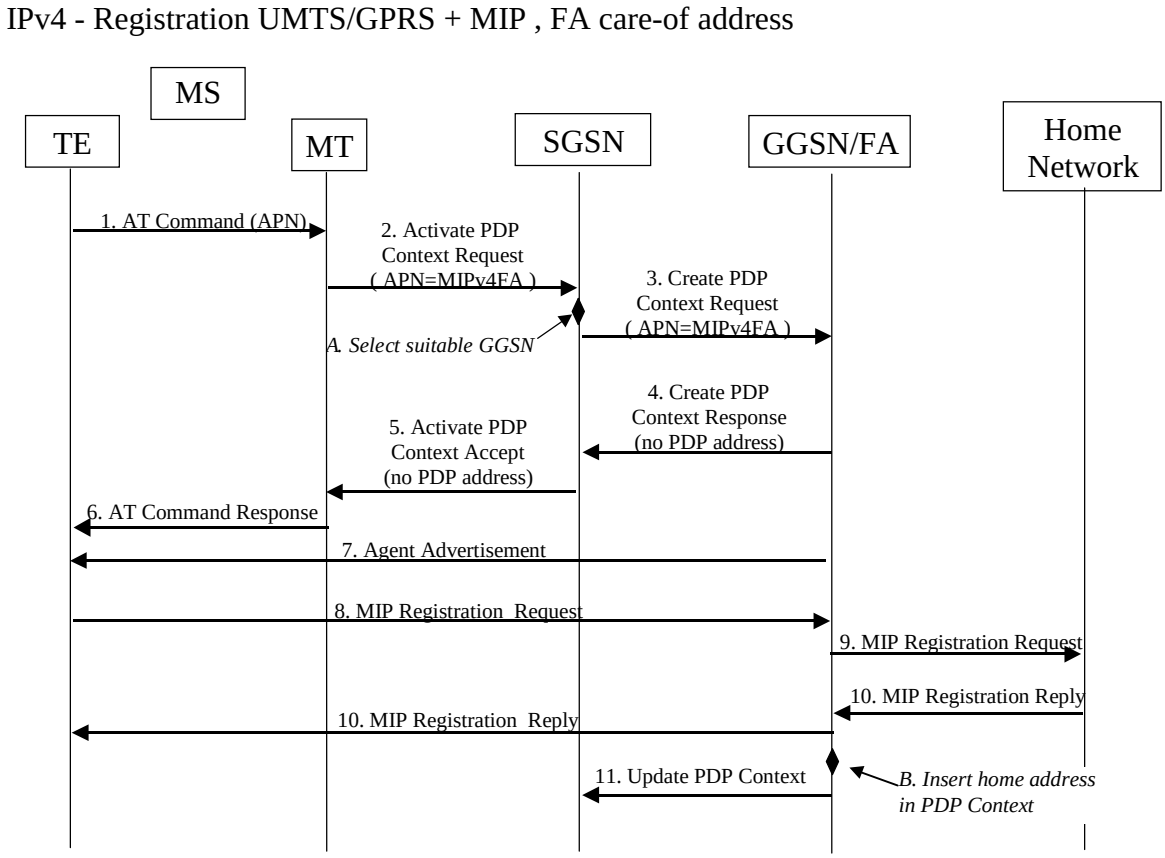


Figure 11e: PDP Context activation with Mobile IP registration (the PS attach procedure not included)

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 section A below. The AT command is followed by a setup of the PPP connection between the MT and the TE, which are not included in the figure.

2. 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 MT 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.

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 a Home Agent 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 [RFC2002] 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 UMTS/GPRS 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 GPRS/UMTS backbone as user traffic. The mobile node includes its (permanent) home address as a parameter [RFC2002]. 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 [23][RFC2486].

9. 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).

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 UMTS/GPRS 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.

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

11.3 Numbering and Addressing

In the case of interworking with public IP networks (such as the Internet), the GPRS 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 GPRS 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 GPRS operator allocates the IP addresses for the subscribers in either of the following ways.

- The GPRS 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 GPRS 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 3G 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 this specification. These functions may be done, for example, in a firewall.

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.

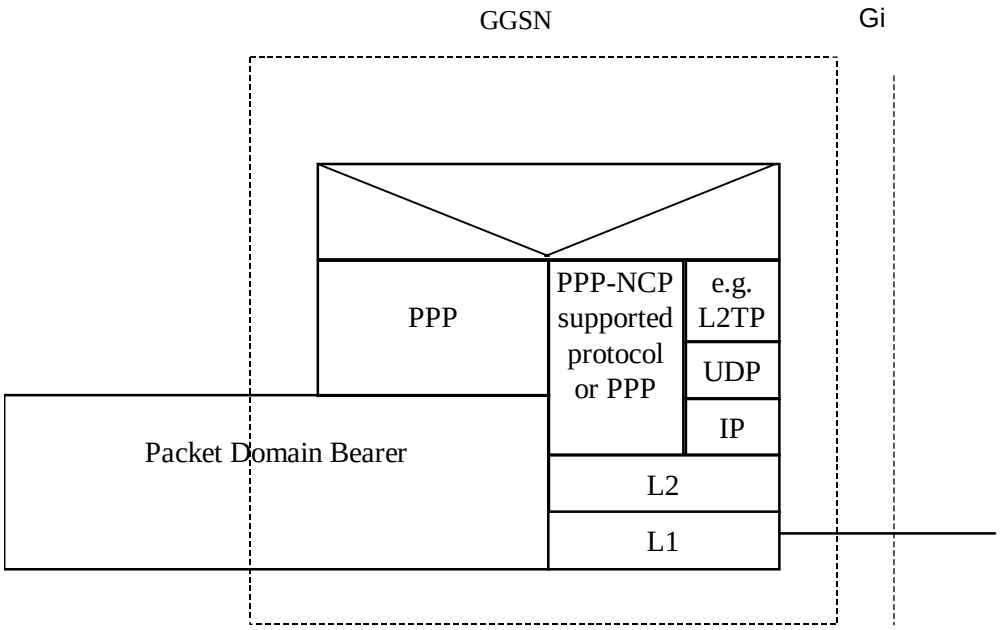


Figure 13: The protocol stacks for the Gi PPP reference point

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

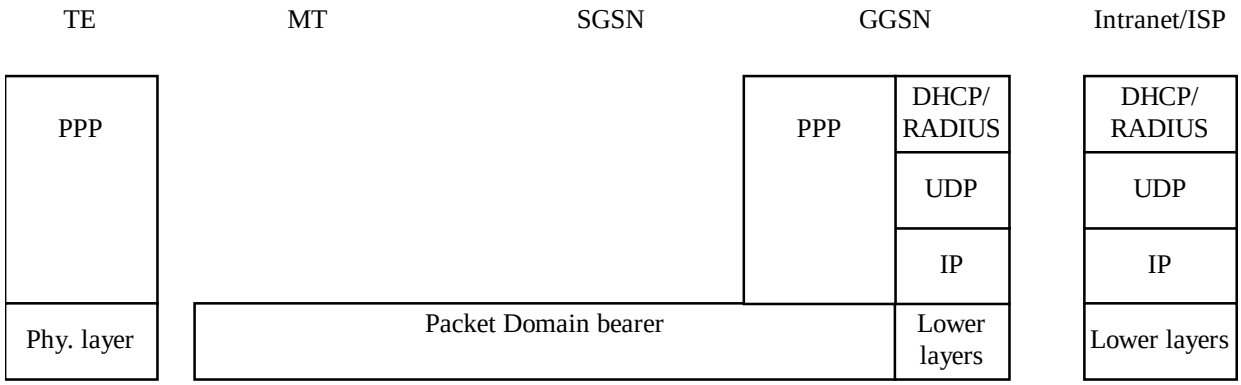


Figure 14: Protocol stack for direct access to IP-based Intranets/ISPs

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

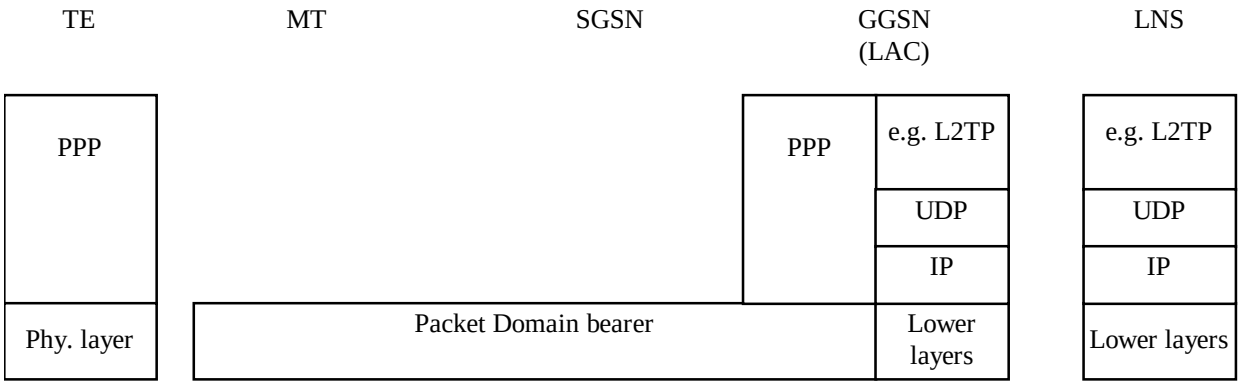


Figure 15: Protocol stack for virtual dial-up access with PPP frame tunnelling

12.2.1.2 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.

7) 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.

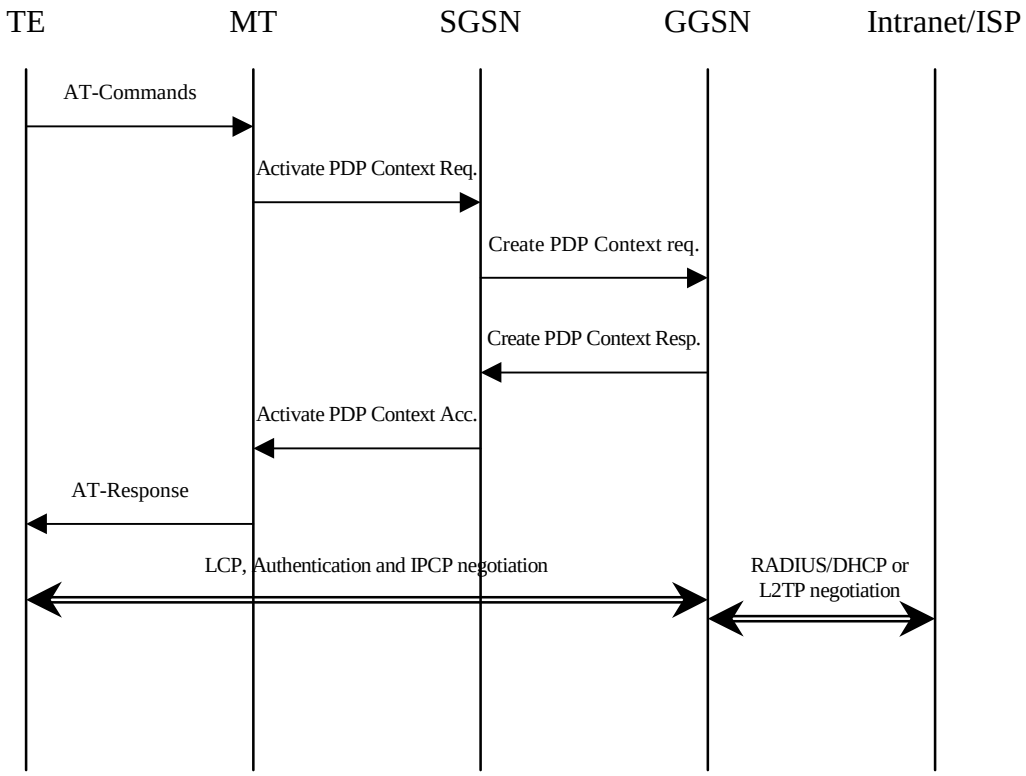


Figure 16a

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 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 update by means of the GGSN-initiated PDP Context Modification Procedure in order to reflect the newly assigned IP address.

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.

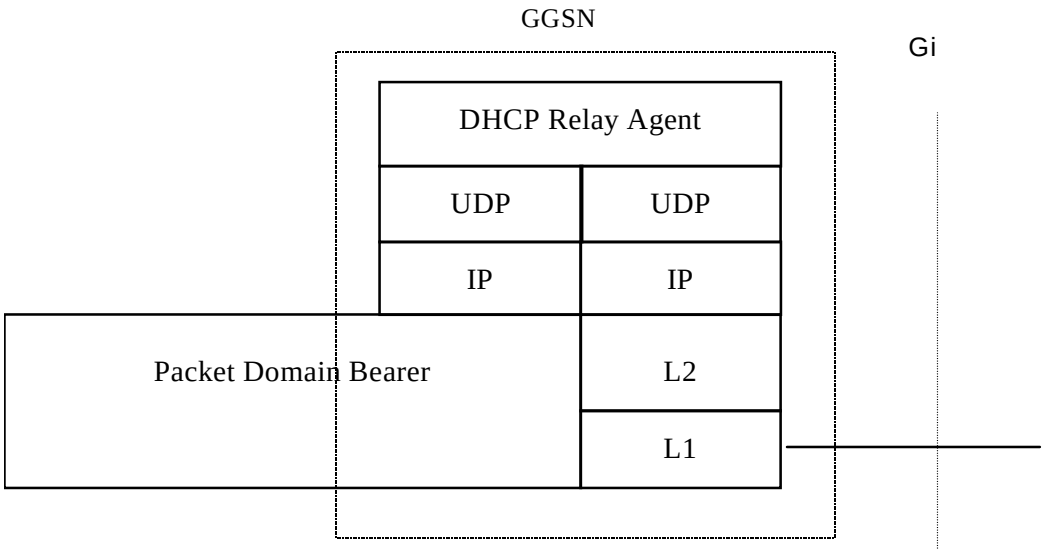


Figure 16b: The protocol stacks for the Gi IP reference point for DHCP

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 GPRS 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 this specification.

Apart from the particulars mentioned above, this model is basically the same as the one for interworking with IP networks described elsewhere in this Specification. 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.

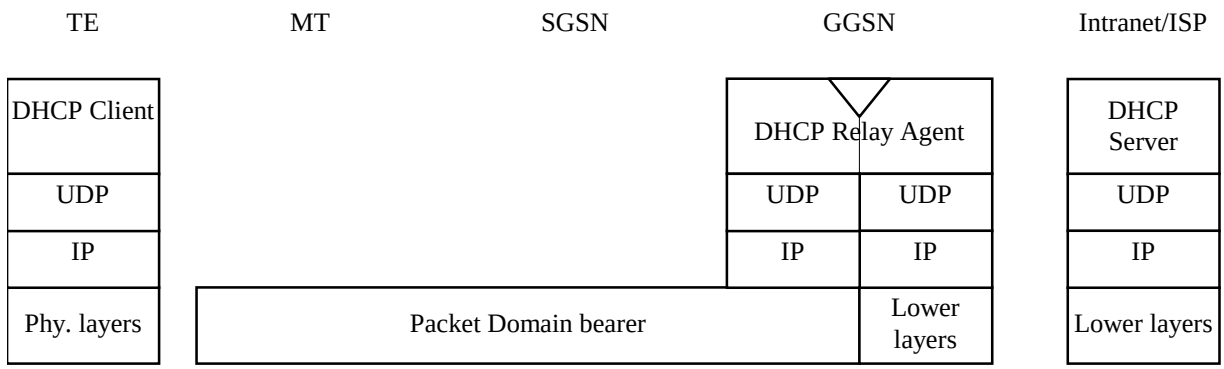


Figure 16c: Protocol stack for access with DHCP end-to-end

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.

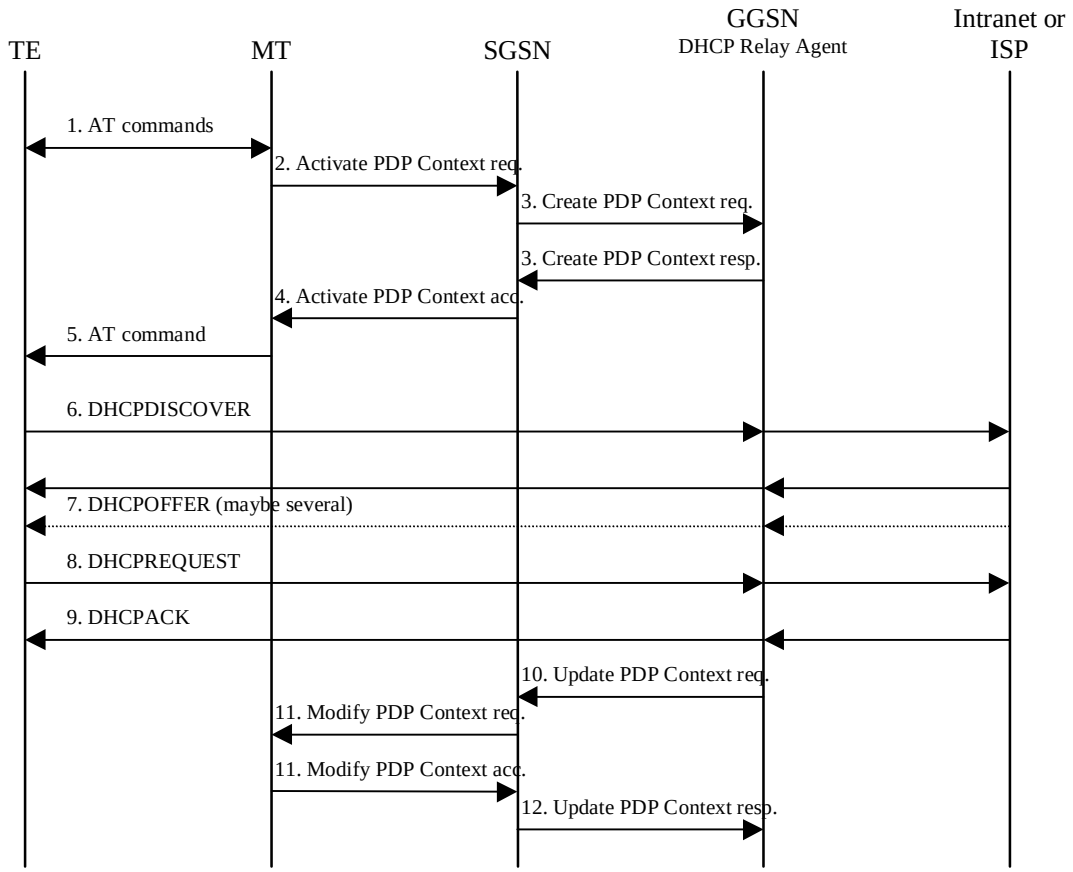
9) The selected DHCP server receives the DHCPREQUEST and replies with a DHCPACK containing the configuration information requested by the TE. The DHCP relay agent relays the DHCPACK to the TE.

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.



14 Internet Hosted Octet Stream Service (IHOSS)

14.1 Introduction

This section describes the GGSN aspects of the Packet Domain Internet Hosted Octet Stream Service (IHOSS). This is a MO-only, connection-oriented service that carries an unstructured octet (character) stream between a Packet Domain MS and an Internet Host.

IHOSS uses OSP:IHOSS which is a subset of the Octet Stream Protocol (OSP) PDP type to provide a 'character pipe' between the MS and the GGSN. In the GGSN there is a relay function between the OSP and the Internet Host protocol (usually TCP). An annex to 3G TS 27.060 contains the generic description of OSP. The subset of features of OSP that are used by OSP:IHOSS is also described in 3G TS 27.060.

Figure 17 shows the scope of IHOSS and OSP:IHOSS.

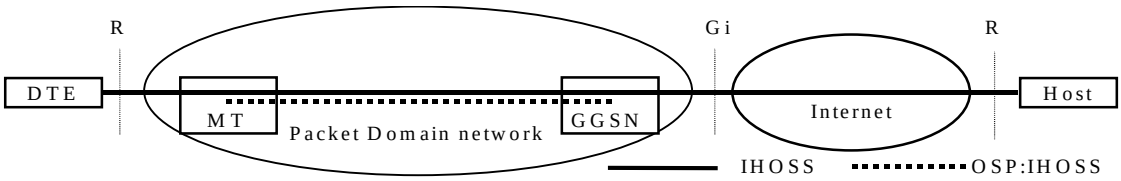


Figure 17: Scope of the Internet Hosted Octet Stream Service and Octet Stream Protocol

14.2 Protocol stacks at the GGSN

Figure 18 shows the protocol stacks at the GGSN. The GGSN contains a relay function between OSP and and the protocol used on the Internet (usually TCP, alternatively UDP).

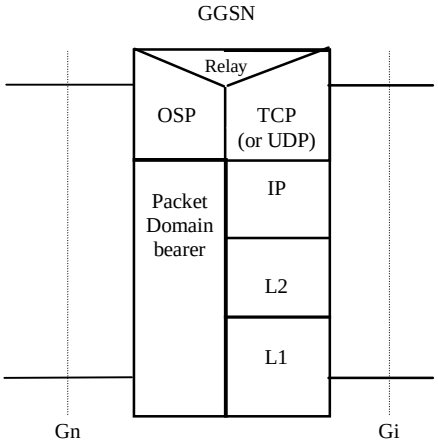


Figure 18: Protocol stacks at the GGSN

14.3 IHOSS connection control and OSP PDP context management

Establishing an IHOSS connection involves setting up two segments, the PLMN segment (using the OSP) between the MS and GGSN, and the Internet segment between the GGSN and the Internet Host. There is a one-to-one mapping between the PLMN segment of an IHOSS connection and an OSP:IHOSS context. When the IHOSS connection is established, an OSP PDP context is activated. When the connection is released, the context is deactivated. Each context supports only one IHOSS connection.

14.3.1 Connection establishment and PDP context activation

Establishing the PLMN segment of an IHOSS connection follows the normal procedures for PDP context activation described in 3G TS 23.060 using messages described in 3G TS 24.008 [23] (MS-SGSN) and 3G TS 29.060 [24] (SGSN-GGSN).

A request to establish an IHOSS connection is signalled to the GGSN by the receipt of a Create PDP context Request message from an SGSN with the PDP type set to OSP:IHOSS. The PDP configuration options may provide information to enable the GGSN to set up a connection to the Internet host. (The contents and format of the PDP configuration options are described in 3G TS 27.060.) Alternatively this information may be derived from subscription information in the HLR and configuration information within the GGSN.

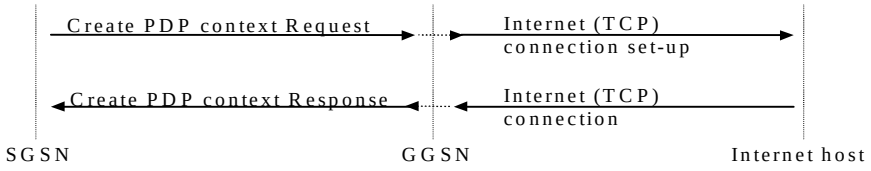


Figure 19: IHOSS connection establishment (TCP over the Internet)

In the case where TCP is used over the Internet (figure 19), the response creating the context activation request is returned to the SGSN only when the TCP connection to the Internet host has been established. If the TCP connection attempt fails, the request to create a context is rejected.

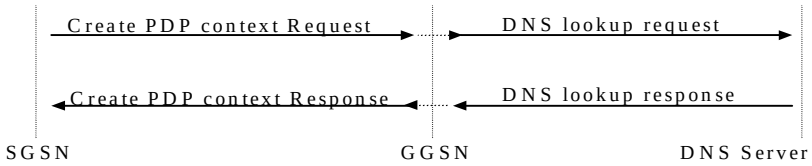


Figure 20: IHOSS connection establishment (UDP over the Internet)

In the case where UDP is used over the Internet (figure 20), the response accepting the context activation request is returned to the SGSN only when a successful DNS lookup of the Internet host name has been completed. If the lookup fails, the request to create a context is rejected. (The GGSN may perform additional checks before responding to the context activation request but these are not specified here.)

14.3.2 Connection release and PDP context deactivation

When the IHOSS connection is released the OSP:IHOSS context is deactivated. The disconnection can be originated either by the MS or the Internet host (TCP only), or exceptionally by the SGSN under fault conditions. A MS-initiated or SGSN-initiated disconnection is signalled to the GGSN by the receipt of a Delete PDP context request from an SGSN.

In the case where TCP is used over the Internet, the GGSN first clears the TCP connection and then sends a Delete PDP context response to the SGSN.

In the case where UDP is used over the Internet, the GGSN sends a Delete PDP context response to the SGSN immediately, there being no actual Internet connection to clear.

The GGSN signals an Internet host-initiated disconnection to the SGSN by sending a Delete PDP context request.

14.4 OSP:IHOSS - TCP (UDP) relay

14.4.1 Required feature

14.4.1.1 Flow control

The OSP flow control procedures shall map on to the TCP flow control procedures. There is no flow control mapping in the case of UDP.

14.4.2 Optional features

14.4.2.1 Break handling

The OSP break procedure may map on to the TCP break procedure. There is no break mapping in the case of UDP.

14.4.2.2 GGSN maximum buffer size

Although the OSP entity in the GGSN does not have a PAD, it still requires buffers to hold the relayed packets. The GGSN PAD maximum buffer size parameters (in the Protocol Configuration Options) may be used to specify the maximum buffer sizes for the two directions of data transfer. Details are given in 3G TS 27.060.

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.

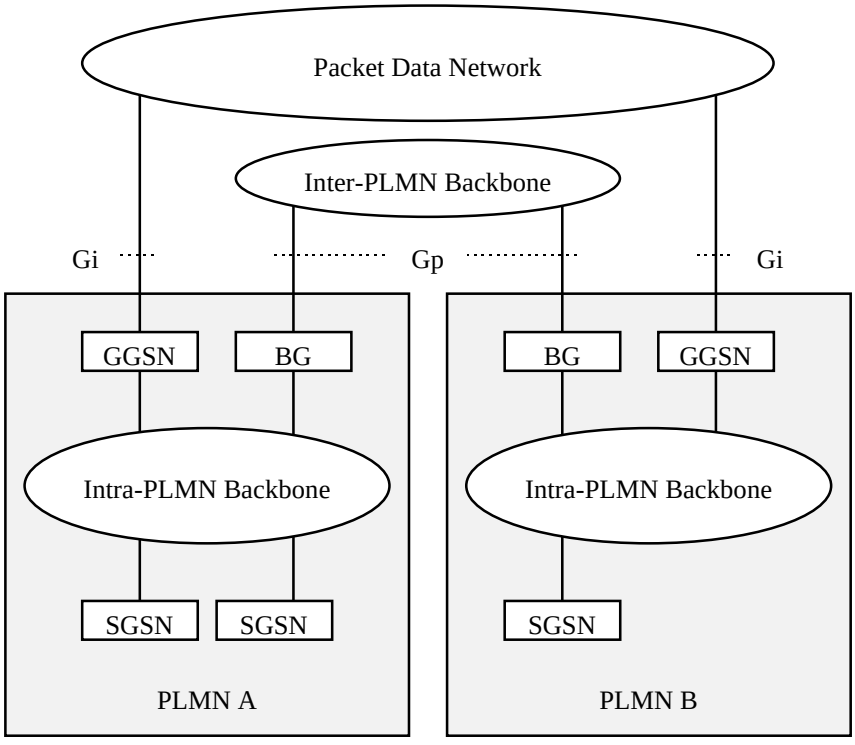


Figure 21: General interworking between Packet Domains to support roaming subscribers.

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 3G TS 23.060.

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

The inter-PLMN link may be any packet data network or dedicated link as described in 3G 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 section 15) and this is down to the normal interconnect agreement between PLMN and PDN operators.

Annex A (normative): Interworking PCS1900 with PSDNs

A.1 Key characteristics of interworking PCS1900 with PSDNs

Bell Operating Company’s (BOC’s) Public Packet Switching Networks provide data transport services within it’s LATA and support data transport as follows:

- between Terminal Equipment (TE) and host computers,
- between TE to TE, between host computer to host computer,
  - and interface to Private Networks within LATA.
  -

The interface to other Packet Switched Public Data Networks (PSPDNs) outside the LATA is via Interexchange Carriers (ICs).

For PCS1900, two types of PSDN may exist - those outside a BOC's LATA and those inside.

A.1.1 PSPDNs which are outside the BOC's LATA

PSPDNs which are outside the BOCs LATA are connected via X.75 interface. Interworking is the same as described in section 10.2.1, X.75 Interworking at the Gi Reference Point.

A.1.2 PSPDNs which are inside the BOC's LATA

BOCs PPSN consists of Data Switching Exchanges (DSE) and ISDN Packet Handler Functions (PHFs).

The Bellcore defined X.75' protocol is used on intranetwork DSE to DSE, DSE to ISDN Packet Handler Function (PHF), and ISDN PHF to ISDN PHF within BOC administered networks, and is used for intra-LATA packet data calls.

X.75 interface is used on ICs connected to other PSPDNs outside the LATA.

Therefore, in order to support packet data services within BOC's LATA for PCS 1900 subscribers, support of Bellcore defined X.75' interface is required at the Gi interface.

Bellcore defined X.75' protocol is an extension of X.75 protocol. The extension consists primarily of additional utilities some of which are analogous to X.25 facilities The extension is necessary to maintain service transparency when interconnection equipment supplied by different manufacturers within a single network.

The rest of this annex describes X.75' interworking.

A.2 Subscription checking

Subscriptions checking for Bellcore defined X.75' interface is outside the scope of this specification.

A.3 Interworking PCS1900 with PSDN using X.75'

A.3.1 General

The Packet Domain shall support interworking with PSDN networks. The interworking may be either direct or through a transit network (e.g. ISDN).

The Packet Domain shall support both ITU-T X.121 and ITU-T E.164 addressing.

The Packet Domain shall provide support for interworking using Bellcore specified X.75' protocol for data transport within BOC's LATA.

The Packet Domain TE's shall have addresses provided, and controlled, by their Packet Domain operator. The PSDN TE sends data to the Packet Domain TE by use of that TE's Packet Domain DNIC (Data Network Identification Code) or equivalent which uniquely identifies that GPRS network worldwide.

The GGSN for interworking with PSDNs is the access point of the Packet Domain data network.

The X.75' access method is supported when mobile users are resident on HPLMN or VPLMN. A roaming user may be allocated a dynamic address from the VPLMN.

A.3.2 PSDN Interworking Model using X.75' Interworking at the Gi Reference Point

Figure A.1 represents the case where X.75' is used as the interworking protocol, as used between interconnect X.25 PSDNs within the BOC's LATA. The GPRS network will look like any other PSDN in the BOC's LATA and will use X.75' addressing. Figure 4 shows the interconnecting protocol stacks to the Packet Domain bearer. The Packet Domain bearer is described in 3G TS 27.060, which uses the protocols described in 3G TS 23.060.

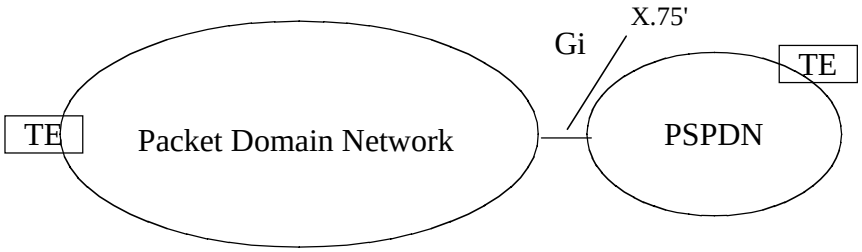


Figure A.1: PSPDN Interworking with X.75' at Gi Reference Point

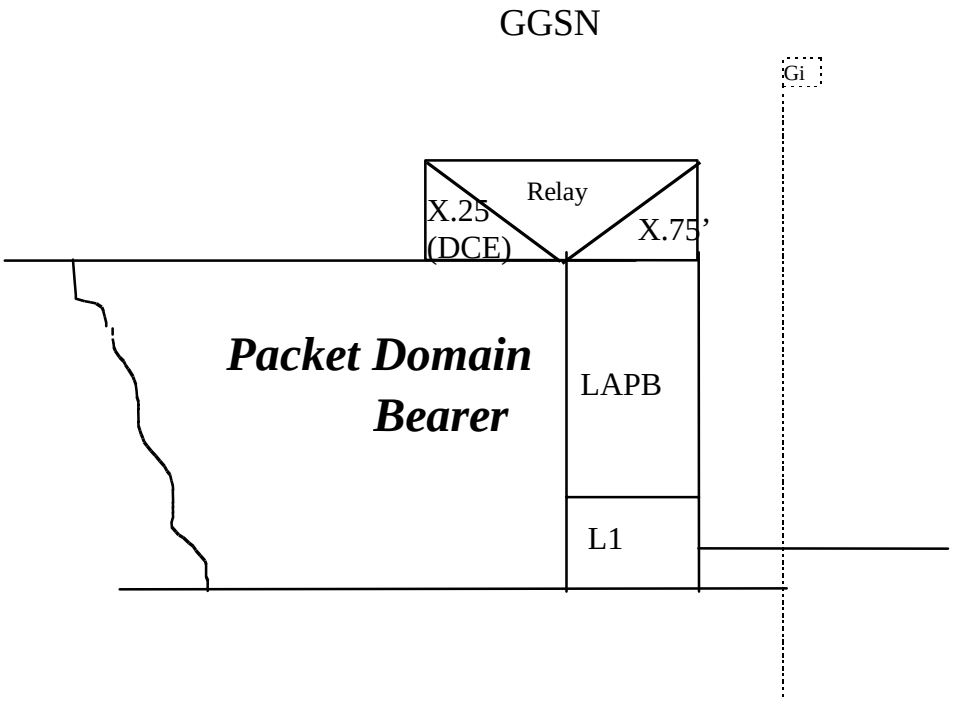


Figure A.2: The Protocol Stack for the X.75' Gi Reference Point

A.3.3 Numbering and Addressing

A PLMN interworking with a PSPDN requires a DNIC or PNIC.

X.121 addresses allocated to subscribers belong to the PLMN operator.

A.3.4 Charging

Charging of X.25 packets is done at the GGSN.

A.3.5 User Facilities

These are the same as in section 10.3 in the main part of this specification.

A.3.6 The Packet Domain Interworking to PSDN Characteristics

These are the same as in section 10.4 in the main part of this specification.

Annex B:
Change history

Change history						
TSG CN#	**Spec**	**Version**	**CR**	**<Phase>**	**New Version**	**Subject/Comment**
Apr 1999	GSM 09.61	7.0.0				Transferred to 3GPP CN1
CN#03	29.061				3.0.0	Approved at CN#03
CN#04	29.061	3.0.0	001		3.1.0	Access to PDNs and ISPs with the PDP-type PPP
CN#04	29.061	3.0.0	002		3.1.0	GPRS Internet Hosted Octet Stream Service (IHOSS)
CN#06	29.061	3.1.0	003		3.2.0	Clarification on the PPP LCP Negotiation for PDP Type PPP
CN#06	29.061	3.1.0	004		3.2.0	Enhancement to Numbering and Addressing to Include the APN
CN#06	29.061	3.1.0	005		3.2.0	IPCP Negotiation Interworking at the MT for Non-Transparent IP
CN#06	29.061	3.1.0	006		3.2.0	Mobile IP Issues
CN#06	29.061	3.1.0	007		3.2.0	Access to an Intranet/ISP with DHCP End to End
CN#06	29.061	3.1.0	008		3.2.0	Streamlining

History

Document history		
V3.2.0	January 2000	Publication