3GPP TSG CN Plenary Meeting #19 **NP-030074**
12th - 14th March 2003. Birmingham, U.K.

Source: TSG CN WG3

Title: CRs on pre-Rel-4 Work Item TEI.

Agenda item: 7.1.1

Document for: APPROVAL

Introduction:

This document contains **6** CRs on **pre-Rel-4 WI TEI,** including the corresponding mirror CRs (as required).

These CRs have been agreed by TSG CN WG3 and are forwarded to TSG CN Plenary meeting #19 for approval.

WG_tdoc	Title	Spec	CR	Rev	Cat	Rel	C_Ver
N3-030120	Correction of references and specification corrections	09.61	A047	1	F	R97	6.9.0
N3-030121	Correction of references and specification corrections	09.61	A048	1	A	R98	7.8.0
N3-030122	Correction of references and specification corrections	29.061	081	1	A	R99	3.11.0
N3-030123	Correction of references and specification corrections	29.061	082	1	A	Rel-4	4.6.0
N3-030124	Correction of references and specification corrections	29.061	083	1	A	Rel-5	5.4.0
N3-030125	Correction of References and specification Corrections	24.022	008	1	F	Rel-5	5.1.0

3GPP TSG-CN WG3 Meeting #27
Dublin, Ireland, 10th - 14th February 2003.

Tdoc ⌘N3-030120

CR-Form-v7

CHANGE REQUEST

⌘ **09.61** **CR** **A047** ⌘ **rev** **1** ⌘ Current version: **6.9.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Correction of References and specification Corrections
Source:	⌘	TSG_CN WG3 *[Siemens AG, MCC]*
Work item code:	⌘	TEI
Date:	⌘	11/02/2003
Category:	⌘	**F**
Release:	⌘	R97

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Inconsistencies in the specification, Missing and incorrect references
Summary of change:	⌘	Correction of incorrect and missing reference and general specification clean-up
Consequences if not approved:	⌘	Inconsistencies and errors in the referencing. Possible misunderstanding when reading specification.

Clauses affected:	⌘	Most of the specification

	Y	N		
Other specs affected: ⌘		X	Other core specifications	⌘
		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

3GPP TS 09.61 V6.9.0 (2002-12)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Core Network; General Packet Radio Service (GPRS); Interworking between the Public Land Mobile Network (PLMN) supporting GPRS and Packet Data Networks (PDN) (Release 1997)

Keywords

GSM, network, GPRS, interworking, PLMN, PDN, PLMN, packet mode

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Contents

Foreword

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

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 General Packet Radio Service (GPRS) interworking between a:

a) PLMN and PSDN;

b) PLMN and IP Networks;

c) 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. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TR 01.04: "Abbreviations and acronyms".

[2] 3GPP TS 02.60: "General Packet Radio Service (GPRS); Service Description; Stage 1 Service Description".

[3] 3GPP TS 03.60: "General Packet Radio Service (GPRS); Service Description; Stage 2 Service Description ".

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

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

[6] 3GPP TS 03.64: "General Packet Radio Service (GPRS); Overall description of the GPRS Rradio interface; Stage 2".

[7] 3GPP TS 04.60: "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: "General Packet Radio Service (GPRS); Mobile Station - Serving GPRS Support Node (MS-SGSN) Logical Link Control (LLC) layer specificationLogical Link Control (LLC)".

[9] 3GPP TS 04.65: "General Packet Radio Service (GPRS); Mobile Station (MS) - Serving GPRS Support Node (SGSN); Subnetwork Dependent Convergence Protocol (SNDCP)".

[10] 3GPP TS 07.60: "General Packet Radio Service (GPRS); Mobile Station (MS) supporting GPRS".

[11] ITU-T Recommendation E.164: "The international public telecommunication numbering planNumbering plan for the ISDN era".

[12] ITU-T Recommendation X.25: "Interface between data Data tTerminal eEquipment (DTE) and Ddata eCircuit-terminating eEquipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit".

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

[14] ITU-T Recommendation X.121: "International ~~Numbering~~ numbering ~~Plan~~ plan for ~~Public~~ public ~~Data~~ data ~~Networks~~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 ~~N~~names ~~–~~ ~~Concepts~~ concepts and ~~Facilities~~facilities" (STD 7).

[20] IETF RFC 1661 (1994): "~~-~~The Point-to-Point Protocol (PPP)" (STD 51).

[21] IETF RFC 2865 (2000)~~, C. Rigney, S. Willens, A. Rubens, W. Simpson~~: "Remote Authentication Dial In User Service (RADIUS)", C. Rigney, S. Willens, A. Rubens, W. Simpson.

[22] IETF RFC 2866 (2000)~~, C. Rigney, Livingston~~: "~~-~~RADIUS Accounting~~-~~", C. Rigney.

[23] 3GPP TS 03.03: "Numbering, addressing and identification".

[24] IETF RFC 2882 (2000):~~, D. Mitton:~~ "Network Access Servers Requirements: Extended RADIUS Practices", D. Mitton.

[25] IETF RFC 1035 (1987): "Domain names - implementation and specification".

[26] IETF RFC 1771 (1995): "A Border Gateway Protocol 4 (BGP-4)".

[27] IETF RFC 1825 (1995): "Security Architecture for the Internet Protocol".

[28] IETF RFC 1826 (1995): "IP Authentication Header".

[29] IETF RFC 1827 (1995): "IP Encapsulating Security Payload (ESP)".

[30] 3GPP TS 04.08: " Mobile radio interface layer 3 specification ".

[31] 3GPP TS 09.60: "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface ".

3 Definitions, abbreviations and symbols

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ~~See~~ 3GPP TS 02.60 [2] apply.

~~In 3GPP TS 02.02 the bearer services are described. The general network configuration is described in 3GPP TS 03.02 and the GSM PLMN access reference configuration is defined in 3GPP TS 04.02. The various connection types used in the GSM PLMN are presented in 3GPP TS 03.10.~~ Terminology used in ~~this Specification~~the present document is presented in 3GPP ~~-~~TS ~~-~~01.04 [1]. For support of data services between GSM PLMN and other networks see 3GPP TS 09-series of ~~Specifications~~specifications.

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
DNIC	Data Network Identification Code
DNS	Domain Name Server
GGSN	Gateway GPRS Support Node
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
LAPB	Link Access Protocol Balanced
MS	Mobile Station
MT	Mobile Terminal
PDN	Packet Data Network
PDU	Protocol Data Unit
PNIC	Pseudo Network Identification Code
PSDN	Packet Switched Data Network
RADIUS	Remote Authentication Dial In User Service
SGSN	Serving GPRS Support Node
SMDS	Switched Multimegabit Data Service
TCP	Transmission Control Protocol
TE	Terminal Equipment
UDP	User Datagram Protocol

3.3 Symbols

For the purposes of th~~is specification~~e present document, the following ~~Symbols~~ symbols apply:

Gb	Interface between an SGSN and a BSC.
Gi	Reference point between GPRS 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 GPRS network services across areas served by the co-operating GPRS 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.

4 Network characteristics

4.1 Key characteristics of PLMN

The GSM PLMN is fully defined in the GSM technical specifications. The GPRS related key characteristics are found in 3GPP TS 02.60 [2] and 3GPP TS 03.60 [3].

4.2 Key characteristics of PSDN

Packet Switched Data Networks (PSDNs) are defined in the relevant ~~CCITT/~~ITU-T Recommendation 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~~ 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 GPRS, 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 3GPP TS 03.03 [23] 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 GSM network in the overall GPRS environment.

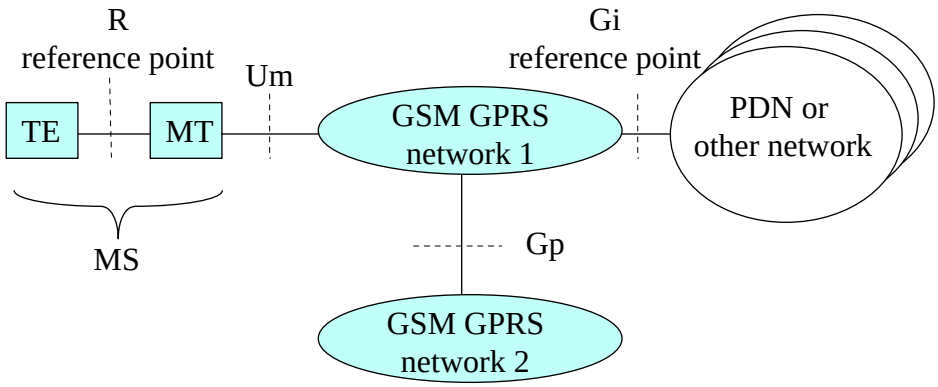
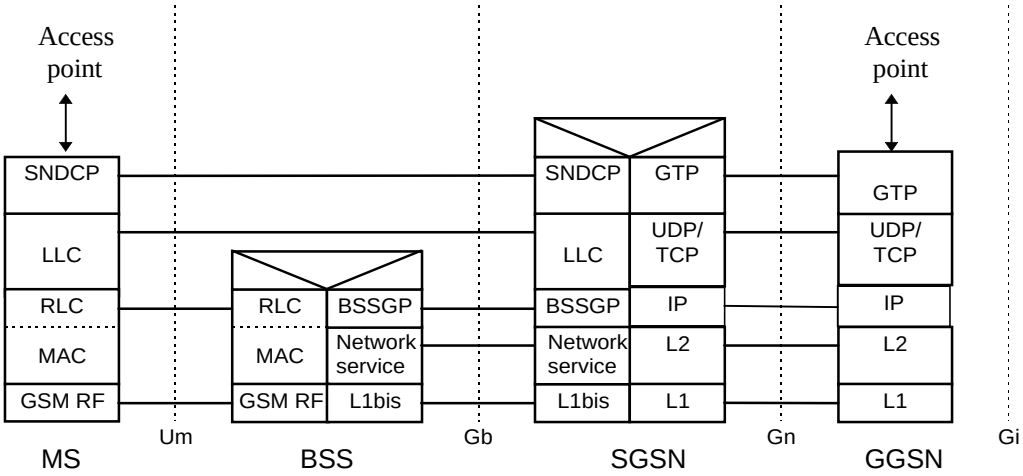


Figure 1: GPRS Access Interfaces and Reference Points

7 Interface to GPRS Bearer Services

~~The following~~ Figure 2: Transmission Plane 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 3GPP ~~-~~TS~~-~~ 03.60, 3GPP TS 04.64 [8]~~,~~ and 3GPP TS 04.65 [9].



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

Figure 2: GPRS Transmission Plane

8 Subscription checking

Subscription is checked during the GPRS Attach procedure and also during the PDP Context Activation procedure as described in 3GPP TS 03.60 [3]. 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 Screening

Screening function''s reside within the GPRS network and has three levels as described in 3GPP TS 02.60 [2] and 3GPP TS 03.60 [3]. Screening may be applicable for only certain protocols. Screening is outside the scope of GPRS standardisation, however, the following types of screening shall be supported.

9.1 Network controlled screening

The PLMN administration and/or the GPRS service provider shall set basic screening functionality, if applicable, (e.g. firewall) to reduce the risk of fraud and misuse. This is to ensure the integrity of the network and to protect subscribers.

9.2 Subscription controlled screening

This will not be in GPRS phase 1.

9.3 User controlled screening

This will not be in GPRS phase 1.

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

10.1 General

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

GPRS shall support both ~~CCITT/~~ITU-T Recommendation X.121 [14] and ~~CCITT/~~ITU-T Recommendation E.~~164~~ 164 [11] addressing.

GPRS shall provide support for ~~CCITT/~~ITU-T Recommendation X.25 and ~~CCITT/~~ITU-T Recommendation X.75.

The GPRS TE~~'~~'s shall have addresses provided , and controlled, by their GPRS operator. The PSDN TE sends data to the GPRS TE by use of that TE~~'~~'s GPRS 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 GSM GPRS data 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 GPRS 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 GPRS network.

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

10.2.1 X75 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 GPRS network will look like any other PSDN in all respects and uses X.75 addressing. Figure 4 shows the interconnecting protocol stacks to the GPRS bearer. The GPRS bearer is described in 3GPP TS 07.60 [10], which uses the protocols described in 3GPP TS 03.60 [3].

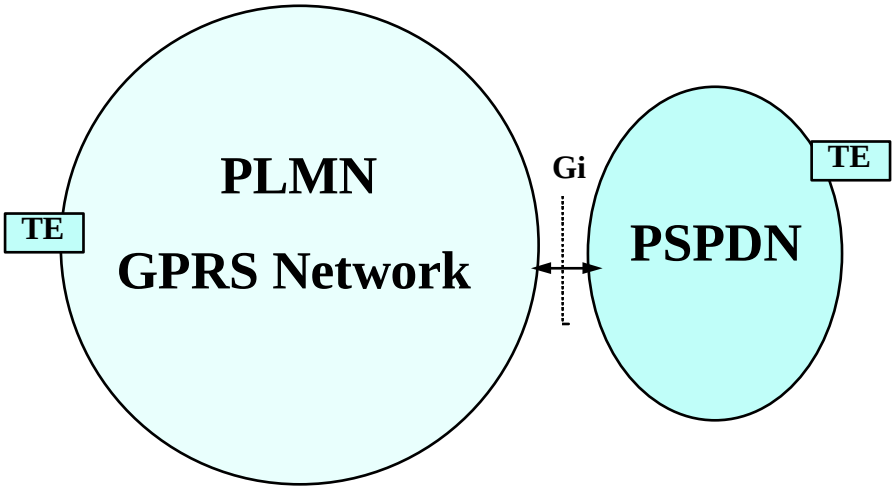


Figure 3: PSPDN Interworking with X.75 at Gi Reference Point

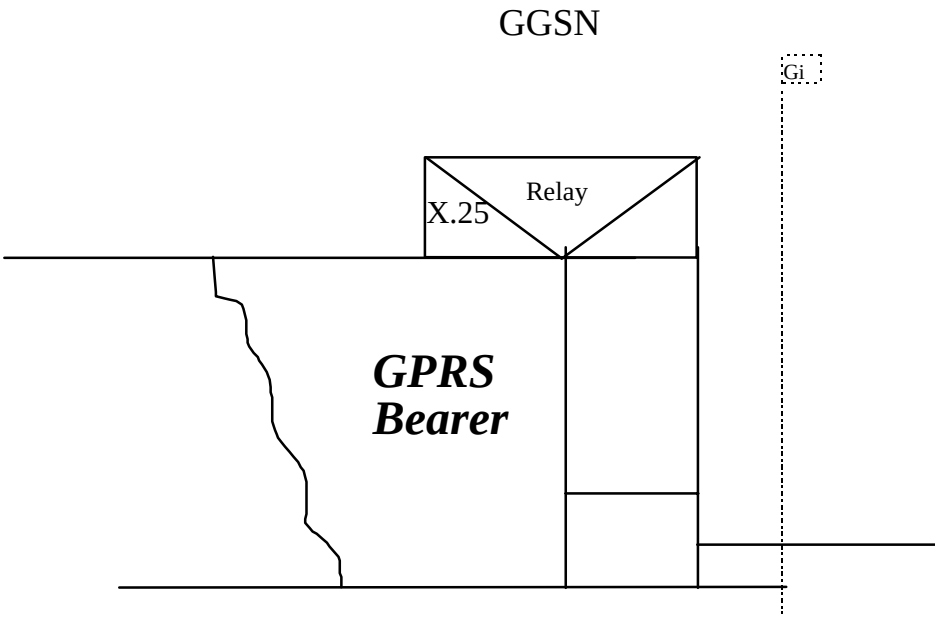


Figure 4: The Protocol Stack for the X.75 Gi Reference Point

10.2.1.1 Numbering and Addressing

A PLMN GPRS network 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.

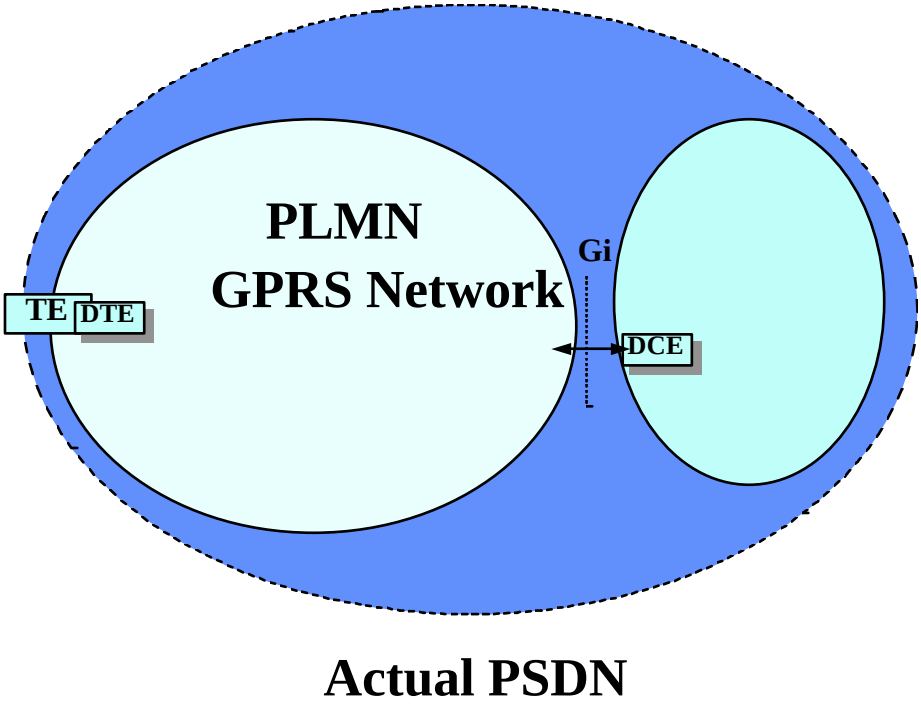
10.2.2 X25 Interworking at the Gi Reference Point

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 GPRS network. The DCE resides within the PSDN.

The GPRS 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~~ figure 6.



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

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

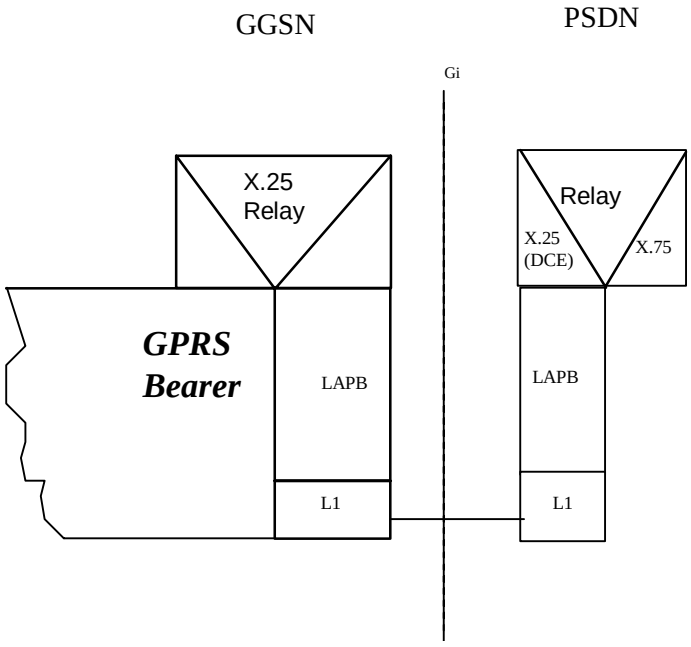


Figure 6: The Protocol Stack for the X.25 / Gi Reference point

Figure 6 shows the transmission plane only. In this case the GGSN shall resolve the association between the MS GPRS 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 GPRS 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 GPRS operator and the PSDN operator. The charging may also be collected in the GPRS network. If the VPLMN assigns the dynamic address, the charging of the GPRS 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 Recommendation X.25 [12] 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 GPRS Interworking to PSDN Characteristics

~~The following t~~Table 0 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 GPRS 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 3GPP TS 03.60 [3].

Table ~~1~~0: PSPDN GPRS 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

GPRS 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, GPRS can operate IPv4 or ~~Ipv6~~IPv6. The interworking point with IP networks is at the Gi reference point as shown in ~~Figure~~ figure 7.

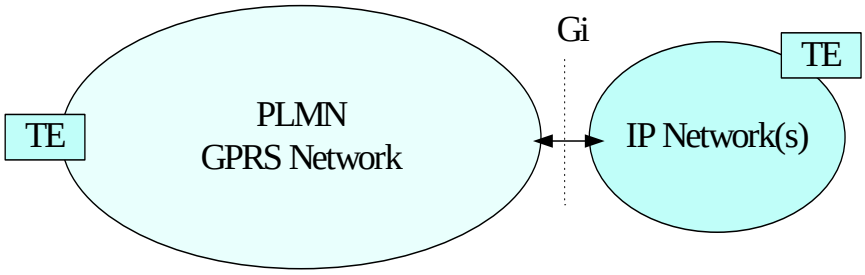


Figure 7: IP network interworking

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

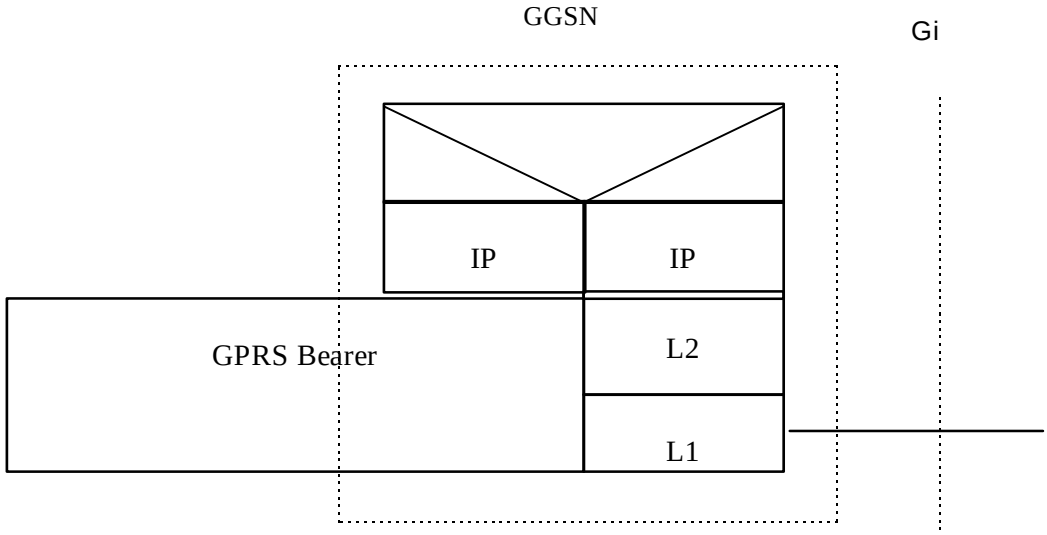


Figure 8: The protocol stacks for the GiIP reference point

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~~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.

The following working assumptions are valid in the generic case:

- A firewall is configured by the GPRS operator. In general, all applications that are using IP as the underlying protocol are supported, but the GPRS operator may restrict their usage.
- A Domain Name Server is managed by the GPRS operator. Alternatively, the Domain Name Server can be managed by the external IP network operator.
- From the GPRS network~~'~~'s point of view, the allocation of a dynamic IP address is done by the GGSN as described in 3GPP TS 03.60 [3]. The GGSN may allocate these addresses by itself or use an external device such as an DHCP server. This external device may be operated by an external organisation such as an ISP or Intranet operator.

11.2.1 Access to Internet, Intranet or ISP through GPRS

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 GPRS PLMN may offer:

- either direct transparent access to the Internet; or~~.~~
- ~~or~~ a non transparent access to the Intranet/ISP. In this case the GPRS PLMN, i.e. the GGSN, takes part in the functions listed above.

11.2.1.1 Transparent access to the Internet

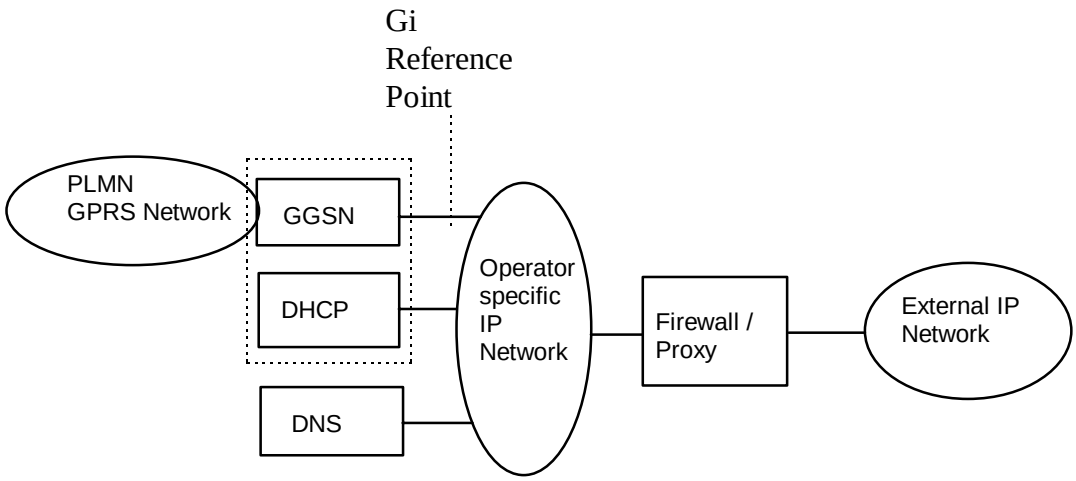


Figure 9: Example of the PDN Interworking Model, transparent case

In this case (see ~~Figure~~ 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~~subclause deals with this specific case.

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

The used protocol stack is depicted in ~~Figure~~ figure 10.

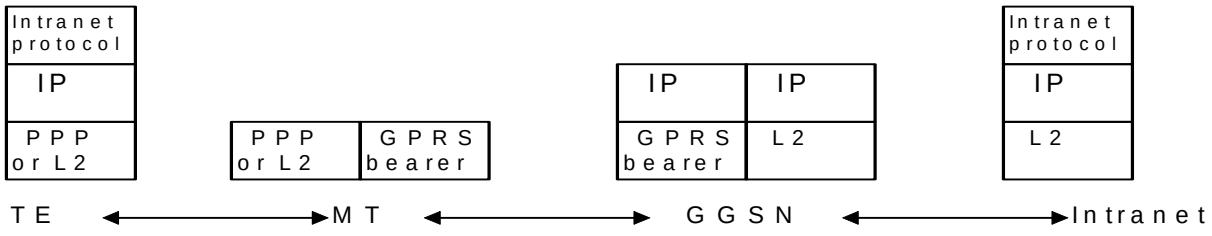


Figure 10: Transparent access to an Intranet

The communication between the GPRS 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 Pprotocol»".

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

An example of an «"Intranet protocolProtocol»" is IPsec (see RFC 1825 [27]). 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 [28] and RFC 1827 [28]). 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 GPRS PLMN 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 GPRS PLMN operator and Intranet/ISP administrator.

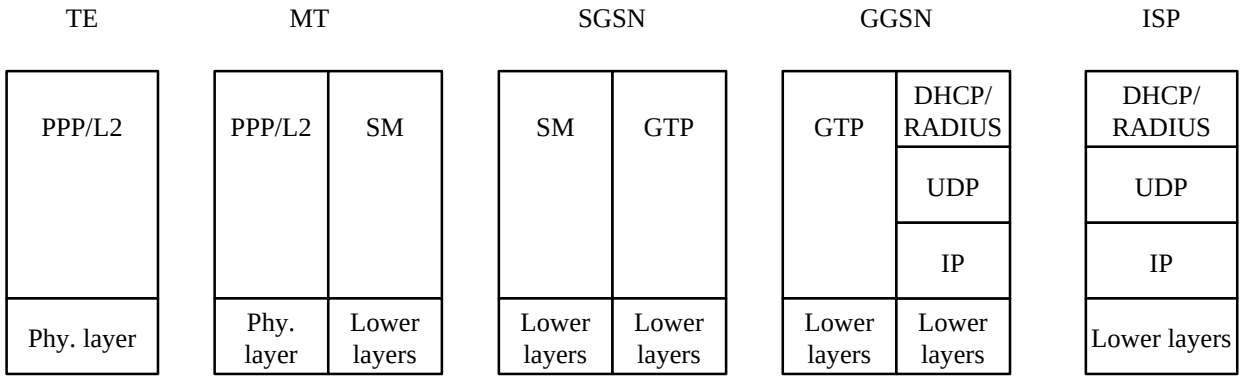


Figure 11: Signalling plane of non transparent case

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 1661[20] the GGSN shall respond with the following messages:

   - ~~Z~~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-nak packet in case of dynamic address allocation (e.g. IPCP Configure Nak in PPP case), or a link Terminate request (LCP Terminate-Request in PPP case) back to the TE. In the case where a configure-nak 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: ~~**Example:**~~ In the following example PPP is used as layer 2 protocol over the R reference point (figure 11a).

The MT acts as a PPP server and translates Protocol Configuration Options into SM message IEs. GTP 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 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.

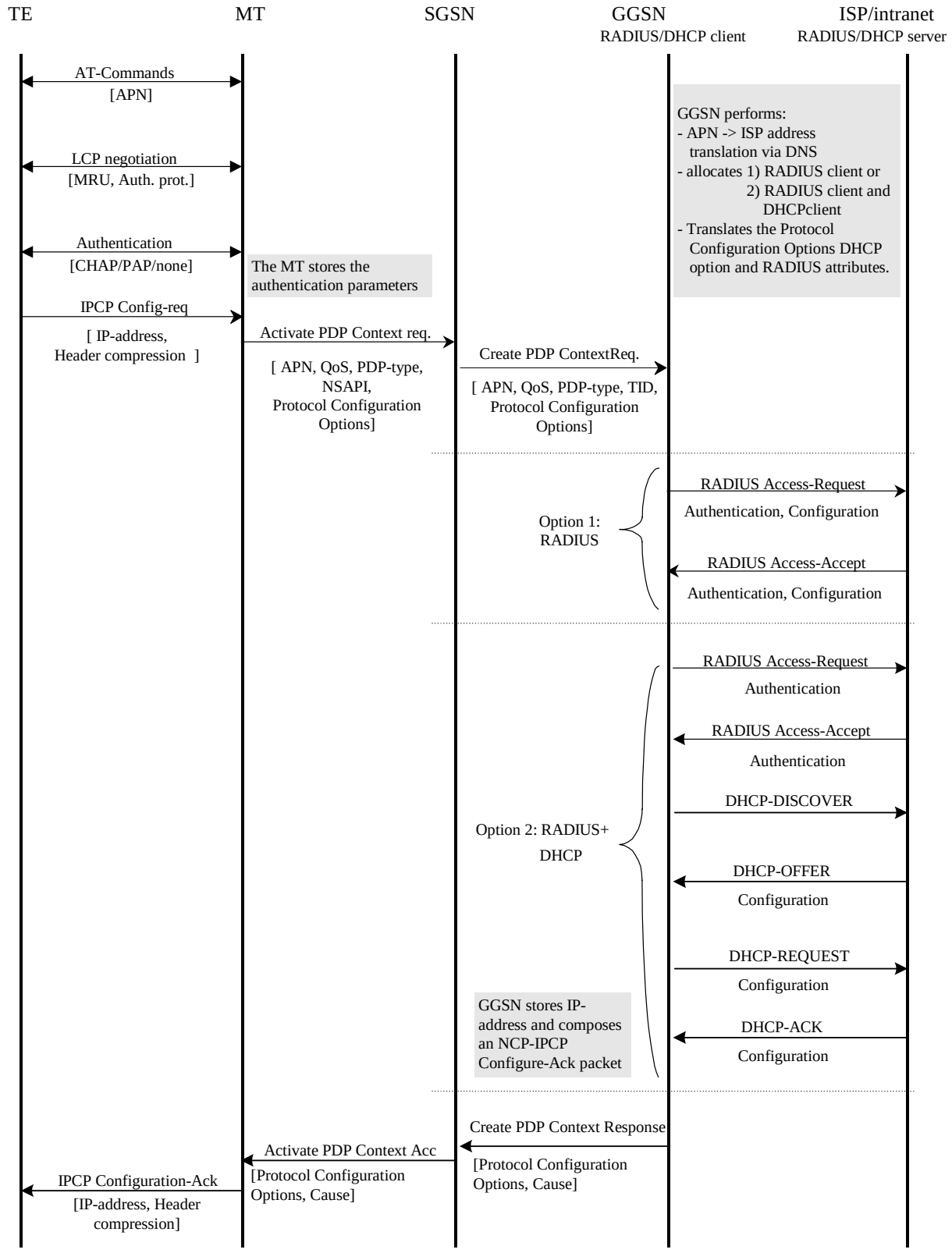


Figure 11a: Example where PPP is used as layer 2 protocol over the R reference point

11.3 Numbering and Addressing

In the case of interworking with the 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 the private IP networks, the GPRS operator manages internally the subnetwork addresses.

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.
- The GPRS operator allocates (either on its own or in conjunction with an ISP) a dynamic IP address when the MS performs the PDP Context Activation procedure with dynamic address allocation as described in 3GPP -TS 03.60 [3].

11.4 Charging

The GPRS 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 Server (DNS)

Provision of Domain Name services shall be provided by the GPRS operators in the transparent case and the ISP in the non transparent case. Domain name registration is handled by RIPE (Réseaux IP Européens) in Europe (DNS documentation is provided in RFC 1034 [19] and RFC 1035 [25]).

11.6 Screening

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

12 Interworking between GPRS networks

The primary reason for the interworking between the GPRS networks is to support roaming GPRS subscribers as described in 3GPP TS 03.60 [3]. The general model for GPRS network interworking is shown in ~~F~~figure 12.

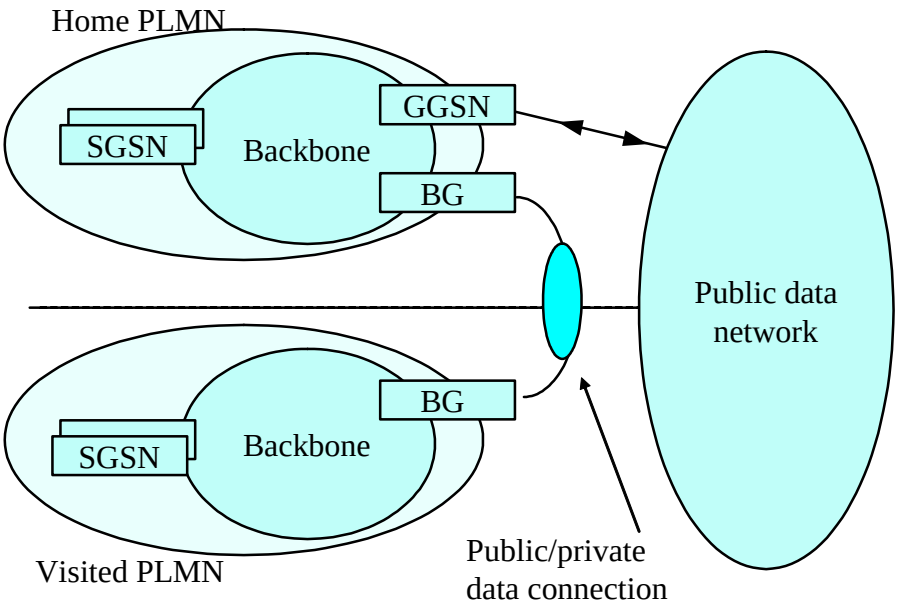


Figure 12: General interworking between GPRS networks to support roaming subscribers

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 03.60 [3].

The procedures to set the link between the SGSN in the VPLMN and the GGSN in the HPLMN is described in 3GPP TS 03.60 [3].

The inter-PLMN link may be any packet data network or dedicated link as described in 3GPP TS 03.60 [3]. The GPRS operators may have a dedicated inter-PLMN link to fulfil the QoS requirements of a certain protocol.

12.1 Security Agreements

Each GPRS operator may support IPsec (RFC 1825 [27]) and accompanying specifications for authentication (RFC 1826 [28]) and encryption (RFC 1827 [29]) as a basic set of security functionality in its border gateways. The GPRS operators may decide to use other security protocols based on bilateral agreements.

12.2 Routing protocol agreements

Each GPRS operator may support BGP (RFC 1771 [26]) as a basic set of routing functionality in its border gateways. The GPRS operators may decide to use other routing protocols based on bilateral agreements.

12.3 Charging agreements

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

There may be a requirement to collect charging information in the Border Gateway (see ~~F~~figure 12) and this is down to the normal interconnect agreement between PLMN and PDN operators.

13 Void

Figure 12: Void

Figure 13: Void

Figure 14: Void

Figure 15: Void

14 Void

Figure 16: Void

Figure 17: Void

Figure 18: Void

Figure 19: Void

Figure 20: Void

15 Void

Figure 21: Void

16 Usage of RADIUS on Gi interface

A GGSN may, on a per APN basis, use RADIUS authentication to authenticate a user and RADIUS accounting to provide information to an AAA (Authentication, Authorization and Accounting) server.

16.1 RADIUS Authentication

RADIUS Authentication shall be used according to RFC2865 [21].

The RADIUS client function may reside in a GGSN. When the GGSN receives a Create PDP Context request message the RADIUS client function may send the authentication information to an authentication server, which is identified during the APN provisioning.

The authentication server checks that the user can be accepted. The response (when positive) may contain network information, such as an IP address for the user.

The information delivered during the Radius authentication can be used to automatically correlate the users identity (the MSISDN or IMSI) to the IP-address, assigned/confirmed by the GGSN or the authentication server respectively. The same procedure applies, in case of sending the authentication to a 'proxy' authentication server.

RADIUS Authentication is only applicable to the primary PDP context. When the GGSN receives an Access-Accept message from the authentication server it shall complete the PDP context activation procedure. If Access-Reject or no response is received, the GGSN shall reject the PDP Context Activation attempt with a suitable cause code, e.g. User Authentication failed.

16.2 RADIUS Accounting

RADIUS Accounting shall be used according to RFC 2866 [22].

The RADIUS accounting client function may reside in a GGSN. The RADIUS accounting client may send information to an accounting server, which is identified during the APN provisioning. The accounting server may store this information and use it to automatically identify the user. This information can be trusted because the GPRS network has authenticated the subscriber (i.e. SIM card and possibly other authentication methods).

RADIUS Accounting-Request Start and Stop messages may be used during both primary and secondary PDP context activation and deactivation procedures respectively.

The use of Accounting-Request STOP and in addition the Accounting ON and Accounting OFF messages may be used to ensure that information stored in the accounting server is synchronised with the GGSN information.

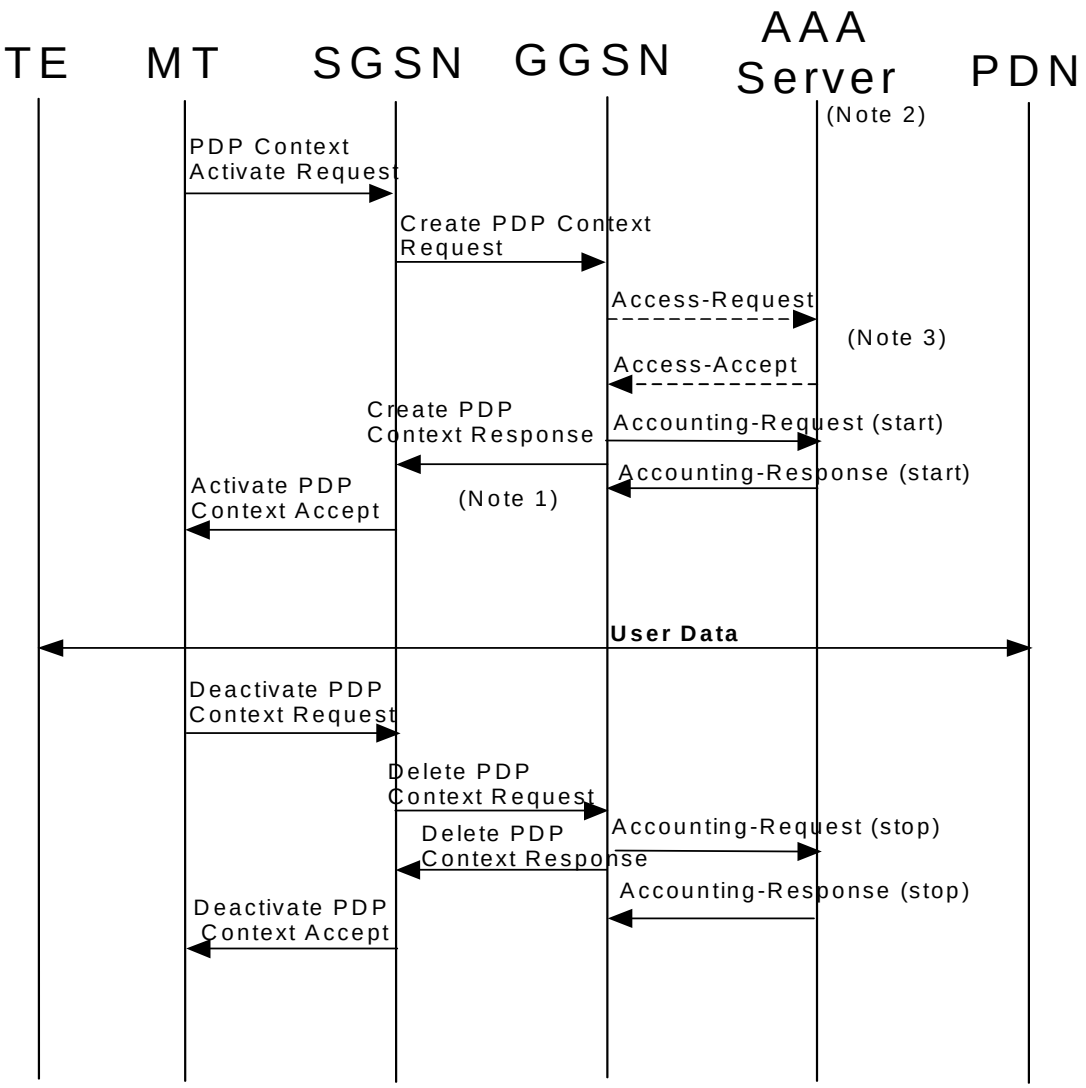
If the AAA server is used for IP address assignment, then, upon reception of a RADIUS Accounting-Request STOP message for all PDP contexts associated to a session defined by APN and IMSI or MSISDN, the AAA server may make the associated IP address available for assignment.

In order to avoid race conditions, the GGSN shall include a 3GPP Vendor-Specific sub-attribute "Session Stop indicator" when it sends the Accounting-Request STOP for the last PDP context of a PDP session and the PDP session is terminated ~~.~~(i.e. the IP address and all GTP tunnels can be released). The AAA server shall not assume the PDP session terminated until an Accounting-Request STOP with the Session Stop indicator is received.

16.3 Authentication and accounting message flows

16.3.1 IP PDP type

~~The f~~Figure 22 represents the RADIUS message flows between a GGSN and an Authentication, Authorization and Accounting (AAA) server.



NOTE 1: If some external applications require RADIUS Accounting request (Start) information before they can process user packets, then the selected APN (GGSN) may be configured in such a way that the GGSN drops user data until the Accounting Response (START) is received from the AAA server. The GGSN may wait for the Accounting Response (START) before sending the CreatePDPContextResponse. The GGSN may reject the PDP context if the Accounting Response (START) is not received.
NOTE 2: Separate accounting and authentication servers may be used.
NOTE 3: The Access-Request message shall be used for primary PDP context only.

Figure 22: RADIUS message flow for PDP type IP (successful user authentication case)

When a GGSN receives a Create PDP Context Request message for a given APN, the GGSN may (depending on the configuration for this APN) send a RADIUS Access-Request to an AAA server. The AAA server authenticates and authorizes the user. If RADIUS is also responsible for IP address allocation the AAA server shall return the allocated IP address in the Access-Accept message.

Even if the GGSN was not involved in user authentication (e.g. transparent network access mode), it may send a RADIUS Accounting-Request START message to an AAA server. This message contains parameters, e.g. the tuple which includes the user-id and IP address, to be used by application servers (e.g. WAP gateway) in order to identify the user. This message also indicates to the AAA server that the user session has started.

If some external applications require RADIUS Accounting request (Start) information before they can process user packets, then the selected APN (GGSN) may be configured in such a way that the GGSN drops user data until the Accounting Response (START) is received from the AAA server. The GGSN may wait for the Accounting Response (START) before sending the CreatePDPContextResponse. The GGSN may reject the PDP context if the Accounting

Response (START) is not received. The authentication and accounting servers may be separately configured for each APN.

When the GGSN receives a Delete PDP Context Request message and providing a RADIUS Accounting-Request START message was sent previously, the GGSN shall send a RADIUS Accounting-Request STOP message to the AAA server, which indicates the termination of this particular user session. The GGSN shall immediately send a Delete PDP context response, without waiting for an Accounting-Response STOP message from the AAA server.

The AAA server shall deallocate the IP address (if any) initially allocated to the subscriber, if there is no session for the subscriber.

Accounting-Request ON and Accounting-Request OFF messages may be sent from the GGSN to the AAA server to ensure the correct synchronization of the session information in the GGSN and the AAA server.

The GGSN may send an Accounting-Request ON message to the AAA server to indicate that a restart has occurred. The AAA server may then release the associated resources.

Prior to a scheduled restart, the GGSN may send Accounting-Request OFF message to the AAA server. The AAA server may then release the associated resources.

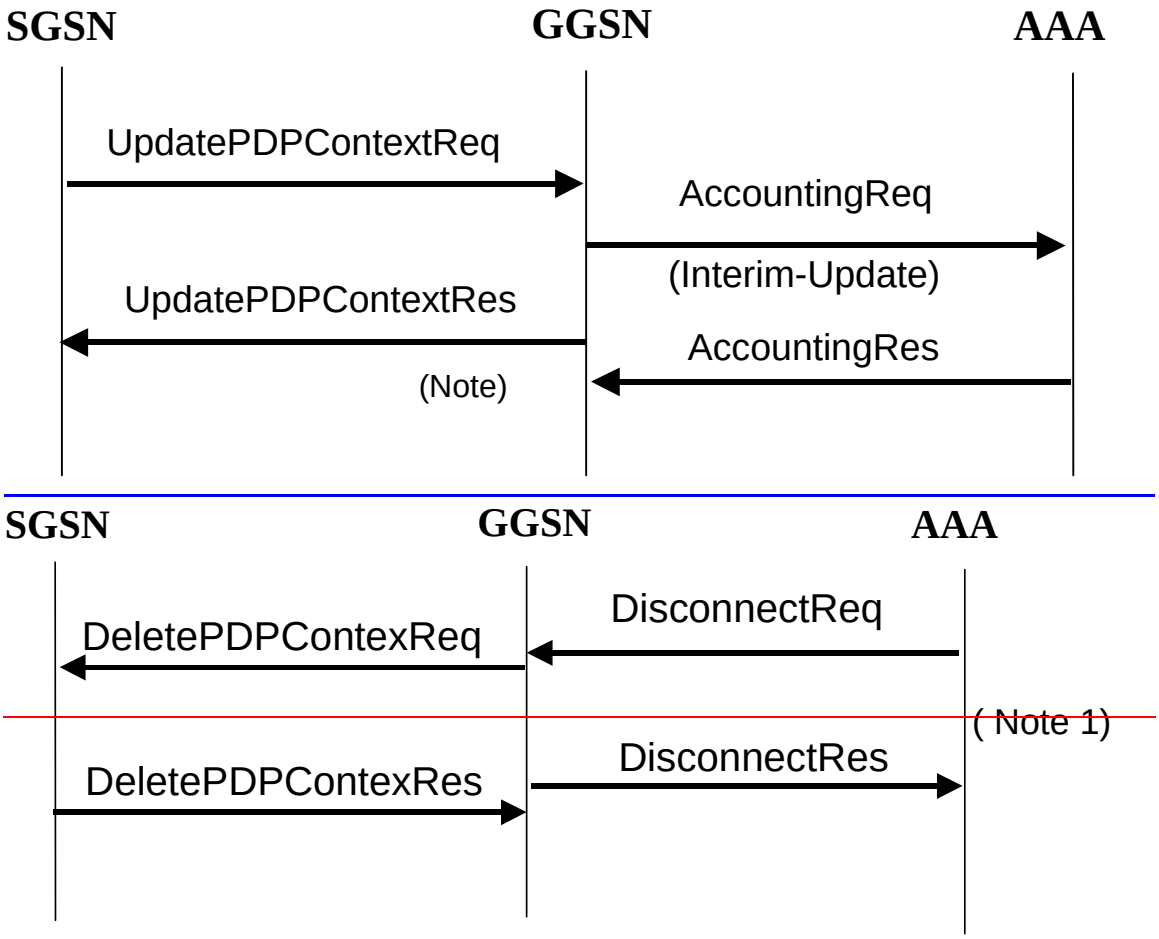
If an Access-Challenge is sent to the GGSN when an Access-Request message is pending and when IP PDP type is used, the GGSN shall silently discard the Access-Challenge message and it shall treat an Access-Challenge as though it had received an Access-Reject instead RFC 2865 [21].

16.3.2 Void

Figure 23: Void

16.3.3 Accounting Update

During the life of a PDP context some information related to this PDP context may change (i.e. SGSN address if a Inter-SGSN RA update occurs). Upon reception of an UpdatePDPContextRequest from the SGSN, the GGSN may send an Accounting Request Interim-Update to the AAA server to update the necessary information related to this PDP context (See figure 24). In such a case, the GGSN need not wait for the RADIUS AccountingResponse from the AAA server message before sending the UpdatePDPContextResponse to the SGSN. The GGSN may delete the PDP context if the AccountingResponse is not received from the AAA.



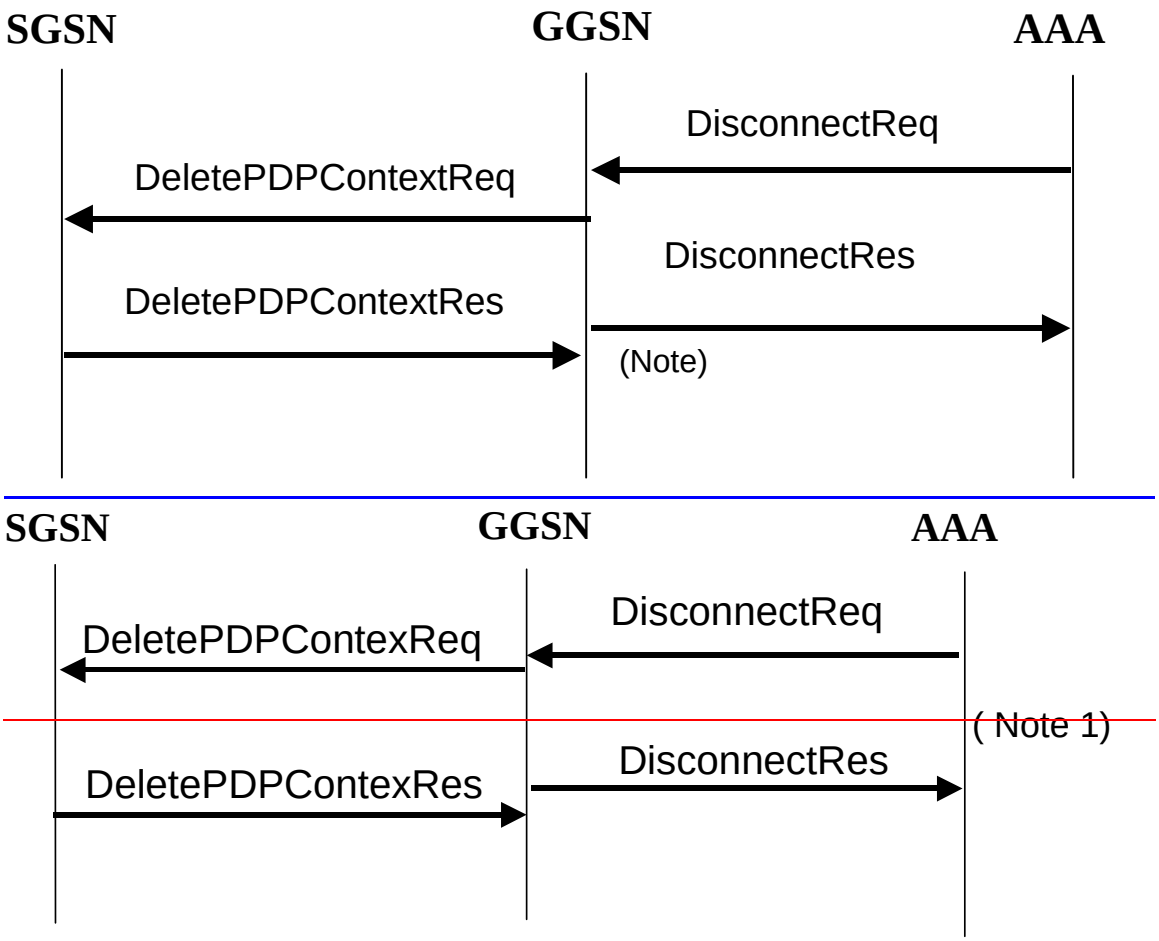
NOTE 1: As shown the GGSN need not wait for the RADIUS AccountingResponse from the AAA server message to send the UpdatePDPContextResponse to the SGSN. The GGSN may delete the PDP context if the AccountingResponse is not received from the AAA.

Figure 24: RADIUS for PDP context Update

16.3.4 AAA-Initiated PDP context termination

RADIUS is used as the protocol between the GGSN and a AAA server or proxy for applications (e.g. MMS) to deliver information related to GPRS user session. However some IP applications could need to interwork with the GGSN to terminate a particular PDP context. For this purpose, the AAA server or proxy may send a RADIUS Disconnect Request to the GGSN. As depicted in figure 25, the GGSN may react by deleting the corresponding PDP context or silently discard the Disconnect Request message. For more information on RADIUS Disconnect, see RFC 2882 [24].

If the GGSN deletes the corresponding PDP context, it need not wait for the DeletePDPContextResponse from the SGSN before sending the RADIUS DisconnectResponse to the AAA server.



N~~ote 1~~OTE:- As showed on ~~F~~figure 25, the GGSN need not wait for the DeletePDPContextResponse from the SGSN to send the RADIUS DisconnectResponse to the AAA server.

Figure 25: PDP Context deletion with RADIUS

16.4 List of RADIUS attributes

The following tables describe the actual content of the RADIUS messages exchanged between the GGSN and the AAA server. Other RADIUS attributes may be used as defined in RADIUS RFC(s). Unless otherwise stated, when the encoding scheme of an attribute is specified as UTF-8 encoding, this shall be interpreted as UTF-8 hexadecimal encoding.

16.4.1 Access-Request message (sent from the GGSN to AAA server)

The table 1 describes the attributes of the Access-Request message.

Table 1: The attributes of the Access-Request message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username is provided by the user (extracted from the Protocol Configuration Options (PCO) field of the Create PDP Context Request message). If no username is available a generic username, configurable on a per APN basis, shall be present.	String	Mandatory
2	User-Password	User password provided by the user if PAP is used (extracted from the PCO field of the Create PDP Context Request message). If no password is available a generic password, configurable on a per APN basis, shall be present.	String	Conditional Note 1
3	CHAP-Password	User password provided by the user if CHAP is used (extracted from the PCO field of the Create PDP Context Request message).	String	Conditional Note 2
4	NAS-IP-Address	IP address of the GGSN for communication with the AAA server.	IPv4	Conditional Note 3
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 3
6	Service-Type	Indicates the type of service for this user	Framed	Optional
7	Framed-Protocol	Indicates the type of protocol for this user	7 (GPRS PDP Context)	Optional
8	Framed-IP-Address	IP address allocated for this user	IPv4	Conditional
9	Framed-IP-Netmask	Netmask for the user IP address	IPv4	Conditional
30	Called-Station-Id	Identifier for the target network	APN (UTF-8 encoded)	Mandatory
31	Calling-Station-Id	This attribute is the identifier for the MS, and it shall be configurable on a per APN basis.	MSISDN in international format according to 3GPP TS ~~23.003~~03.03 [23], UTF-8 encoded decimal. Note that there are no leading characters in front of the country code.	Optional
60	CHAP-Challenge	Challenge if CHAP is used (extracted from the PCO field of the Create PDP Context Request message).	String	Conditional Note 2
61	NAS-Port-Type	Port type for the GGSN	As per RFC 2865 [21]	Optional
26/10415	3GPP Vendor-Specific	Sub-attributes according sub-clause 16.4.7	See sub-clause 16.4.7	Optional except sub-attribute 3 which is conditional
NOTE 1: Shall be present if PAP is used. NOTE 2: Shall be present if CHAP is used. NOTE 3: Either NAS-IP-Address or NAS-Identifier shall be present.				

16.4.2 Access-Accept (sent from AAA server to GGSN)

~~The t~~Table 2 describes the attributes of the Access-Accept message.

Table 2: The attributes of the Access-Accept message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username received in the Access-Request message or a substitute username provided by the AAA server. If the User-Name has been received in the Access-Accept message, this user-name shall be used in preference to the above	String	Optional
6	Service-Type	Indicates the type of service for this user	Framed	Optional
7	Framed-Protocol	Indicates the type of protocol for this user	7 (GPRS PDP Context)	Optional
8	Framed-IP-Address	IP address allocated for this user, if the AAA server is used to allocate IP address.	IPv4	Conditional
9	Framed-IP-Netmask	Netmask for the user IP address, if the AAA server is used to allocate IP netmask.	IPv4	Conditional
12	Framed-IP-MTU	MTU for the user towards this particular APN, MTU shall be less or equal to 1500	String	Optional
25	Class	Identifier to be used in all subsequent accounting messages.	String	Optional (~~NOTE 4~~Note)
27	Session-Timeout	Indicates the timeout value (in seconds) for the user session	32 bit unsigned Integer	Optional
28	Idle-Timeout	Indicates the timeout value (in seconds) for idle user session	32 bit unsigned Integer	Optional
26/311	MS- primary-DNS-server	Contains the primary DNS server address for this APN	Ipv4	Optional
26/311	MS-Secondary-DNS-Server	Contains the secondary DNS server address for this APN	IPv4	Optional
26/311	MS-Primary-NBNS-Server	Contains the primary NetBios name server address for this APN	IPv4	Optional
26/311	MS-Secondary-NBNS-Server	Contains the secondary NetBios server address for this APN	IPv4	Optional
NOTE ~~4~~: The presence of this attribute is conditional upon this attribute being received in the Access-Accept message.				

16.4.3 Accounting-Request START (sent from GGSN to AAA server)

~~The t~~Table 3 describes the attributes of the Accounting-Request START message.

Table 3: The attributes of the Accounting-Request START message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username provided by the user (extracted from the PCO field of the Create PDP Context Request message). If no username is available a generic username, configurable on a per APN basis, shall be present. If the User-Name has been received in the Access-Accept message, this user-name shall be used in preference to the above	String	Optional
4	NAS-IP-Address	GGSN IP address for communication with the AAA server.	IPv4	Conditional Note 1~~3~~
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 1~~3~~
6	Service-Type	Indicates the type of service for this user	Framed	Optional
7	Framed Protocol	Indicates the type of protocol for this user	7 (GPRS PDP Context)	Optional
8	Framed-IP-Address	User IP address	IPv4	Mandatory
25	Class	Received in the access accept	String	Conditional (~~NOTE 4~~Note 2)
30	Called-Station-Id	Identifier for the target network	APN (UTF-8 encoded)	Mandatory
31	Calling-Station-Id	This attribute is the identifier for the MS, and it shall be configurable on a per APN basis.	MSISDN in international format according to 3GPP TS ~~23.003~~03.03 [23], UTF-8 encoded decimal.~~—~~ Note that there are no leading characters in front of the country code.	Optional
40	Acct-Status-Type	Type of accounting message	START	Mandatory
41	Acct-Delay-Time	Indicates how many seconds the GGSN has been trying to send this record for, and can be subtracted from the time of arrival on the AAA server to find the approximate time (in seconds) of the event generating this Accounting-Request.	32 unsigned integer	Optional
44	Acct-Session-Id	User session identifier.	GGSN IP address and Charging-ID concatenated in a UTF-8 encoded hexadecimal. ~~NOTE: The GGSN IP address is the same as that used in the GCDRs.~~(Note 3)	Mandatory
45	Acct-Authentic	Authentication method	RADIUS or LOCAL	Optional

Attr #	Attribute Name	Description	Content	Presence Requirement
61	NAS-Port-Type	Port type for the GGSN	As per RFC 2865 [21]	Optional
26/10415	3GPP Vendor-Specific	Sub-attributes according ~~sub-clause~~subclause 16.4.7.	See ~~sub-clause~~subclause 16.4.7	Optional except sub-attribute 3 which is conditional
NOTE ~~3~~1: Either NAS-IP-Address or NAS-Identifier shall be present. NOTE 2~~4~~: The presence of this attribute is conditional upon this attribute being received in the Access-Accept message. NOTE 3: The GGSN IP address is the same as that used in the GCDRs.				

16.4.4 Accounting Request STOP (sent from GGSN to AAA server)

~~The t~~Table 4 describes the attributes of the Accounting-Request STOP message.

Table 4: The attributes of the Accounting-Request STOP message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username provided by the user (extracted from the PCO field of the Create PDP Context Request message). If no username is available a generic username, configurable on a per APN basis, shall be present. If the User-Name has been received in the Access-Accept message, this user-name shall be used in preference to the above	String	Optional
4	NAS-IP-Address	IP address of the GGSN for communication with the AAA server.	IPv4	Conditional Note 1~~3~~
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note ~~3~~1
6	Service-Type	Indicates the type of service for this user	Framed	Optional
7	Framed Protocol	Indicates the type of protocol for this user	7 (GPRS PDP Context)	Optional
8	Framed-IP-Address	User IP address	IPv4	Mandatory
25	Class	Received in the access accept	String	Optional (~~NOTE 4~~Note 2)
30	Called-Station-Id	Identifier for the target network	APN (UTF-8 encoded)	Mandatory
31	Calling-Station-Id	This attribute is the identifier for the MS, and it shall be configurable on a per APN basis.	MSISDN in international format according to 3GPP TS ~~23.003~~03.03 [23], UTF-8 encoded. Note that there are no leading characters in front of the country code.	Optional
40	Acct-Status-Type	Indicates the type of accounting request	STOP	Mandatory
41	Acct-Delay-Time	Indicates how many seconds the GGSN has been trying to send this record for, and can be subtracted from the time of arrival on the AAA server to find the approximate time of the event generating this Accounting-Request	Second	Optional
42	Acct-Input-Octets	GGSN counted number of octets sent by the user for the PDP context	32 bit unsigned integer	Optional
43	Acct-Output-Octets	GGSN counted number of octets received by the user for the PDP context	32 bit unsigned integer	Optional

Attr #	Attribute Name	Description	Content	Presence Requirement
44	Acct-Session-Id	User session identifier.	GGSN IP address and Charging-ID concatenated in a UTF-8 encoded hexadecimal. (Note 3)~~NOTE: The GGSN IP address is the same as that used in the GCDRs.~~	Mandatory
45	Acct-Authentic	Authentication method	RADIUS or LOCAL	Optional
46	Acct-Session-Time	Duration of the session	Second	Optional
47	Acct-Input-Packets	GGSN counted number of packets sent by the user	Packet	Optional
48	Acct-Output-Packets	GGSN counted number of packets received by the user	Packet	Optional
49	Acct-Terminate-Cause	Indicate how the session was terminated	See RFC 2866 [22]	Optional
61	NAS-Port-Type	Port type for the GGSN	As per RFC 2865 [21]	Optional
26/10415	3GPP Vendor-Specific	Sub-attributes according to ~~sub-clause~~subclause 16.4.7.	See ~~sub-clause~~subclause 16.4.7	Optional except sub-attribute 3 which is conditional
NOTE 1~~3~~: Either NAS-IP-Address or NAS-Identifier shall be present. NOTE 2~~4~~: The presence of this attribute is conditional upon this attribute being received in the Access-Accept message. NOTE 3: The GGSN IP address is the same as that used in the GCDRs.				

16.4.5 Accounting Request ON (optionally sent from GGSN to AAA server)

T~~he t~~able 5 describes the attributes of the Accounting-Request ON message.

Table 5: The attributes of the Accounting-Request ON message

Attr #	Attribute Name	Description	Content	Presence Requirement
4	NAS-IP-Address	IP address of the GGSN for communication with the AAA server.	IPv4	Conditional Note~~3~~
30	Called-Station-ID	Identifier for the target network.	APN (UTF-8 encoded)	Optional
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note~~3~~
NOTE~~3~~: Either NAS-IP-Address or NAS-Identifier shall be present.				

16.4.6 Accounting Request OFF (optionally sent from GGSN to AAA server)

T~~he t~~able 6 describes the attributes of the Accounting-Request OFF message.

Table 6: The attributes of the Accounting-Request OFF message

Attr #	Attribute Name	Description	Content	Presence Requirement
4	NAS-IP-Address	IP address of the GGSN for communication with the AAA server.	IPv4	Conditional Note ~~3~~
30	Called-Station-ID	Identifier for the target network.	APN (UTF-8 encoded)	Optional
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note ~~3~~
NOTE ~~3~~: Either NAS-IP-Address or NAS-Identifier shall be present.				

16.4.7 Sub-attributes of the 3GPP Vendor-Specific attribute

T~~he t~~able 7 describes the sub-attributes of the 3GPP Vendor-Specific attribute of the Access-Request, Accounting-Request START, Accounting-Request STOP and Accounting-Request Interim-Update messages.

Table 7: The sub-attributes of the 3GPP Vendor-Specific attribute of the Access-Request, Accounting-Request START, Accounting-Request STOP and ~~-~~Accounting-Request Interim-Update messages

Sub-attr #	Sub-attribute Name	Description	Presence Requirement	Associated attribute (Location of Sub-attr)
1	3GPP-IMSI	IMSI for this user	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
2	3GPP-Charging-Id	Charging ID for this PDP Context (this together with the GGSN-Address constitutes a unique identifier for the PDP context).	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
3	3GPP-PDP Type	Type of PDP context, i.e. IP	Conditional (mandatory if attribute 7 is present)	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
4	3GPP-CG-Address	Charging Gateway IP address	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
5	3GPP-GPRS-Negotiated-QoS-Profile	QoS profile applied by GGSN	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
6	3GPP-SGSN-Address	SGSN IP address that is used by the GTP control plane for the handling of control messages.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request

Sub-attr #	Sub-attribute Name	Description	Presence Requirement	Associated attribute (Location of Sub-attr)
		It may be used to identify the PLMN to which the user is attached.		Interim-Update
7	3GPP-GGSN-Address	GGSN IP address that is used by the GTP control plane for the context establishment. It is the same as the GGSN IP address used in the GCDRs.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
8	3GPP-IMSI-MCC-MNC	MCC and MNC extracted from the user-''s IMSI (first 5 or 6 digits, as applicable from the presented IMSI).	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
9	3GPP-GGSN- MCC-MNC	MCC-MNC of the network the GGSN belongs to.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
10	3GPP-NSAPI	Identifies a particular PDP context for the associated PDN and MSISDN/IMSI from creation to deletion.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP Accounting-Request Interim-Update
11	3GPP- Session-Stop-Indicator	Indicates to the AAA server that the last PDP context of a session is released and that the PDP session has been terminated.	Optional	Accounting Request STOP
12	3GPP- Selection-Mode	Contains the Selection mode for this PDP Context received in the Create PDP Context Request Message	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
18	3GPP-SGSN-MCC-MNC	MCC and MNC extracted from the RAI within the Create PDP Context Request or Update PDP Context Request message.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update

The RADIUS vendor Attribute is encoded as follows (as per RFC 2865 [21])

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1	Type = 26							
2	Length = n							
3	Vendor id octet 1							
4	Vendor id octet 2							
5	Vendor id octet 3							
6	Vendor id octet 4							
7-n	String							

n ≥ ~~>=~~7

3GPP Vendor Id = 10415

The string part is encoded as follows:

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1	3GPP type =							
2	3GPP Length = m							
3 –m	3GPP value							

m ≥ ~~>=~~2 and m ≤ ~~<=~~ 248

The 3GPP specific attributes encoding is clarified below.

1 -- 3GPP-***IMSI***

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1	3GPP type = 1							
2	3GPP Length= m							
3-m	IMSI digits 1-n (UTF-8 encoded)							

3GPP Type: 1

n ≤ ~~<=~~15

Length: m ≤ ~~<=~~17

IMSI value: Text:

This is the UTF-8 encoded IMSI; The definition of IMSI shall be in accordance with 3GPP TS 03.03 [23] and 3GPP TS 09.60 [31]~~[24]~~. There shall be no padding characters between the MCC and MNC, and between the MNC and MSIN. If the IMSI is less than 15 digits, the padding in the GTP information element shall be removed by the GGSN and not encoded in this sub-attribute.

2 - 3GPP-***Charging ID***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 2							
2	3GPP Length= 6							
3	Charging ID value Octet 1							
4	Charging ID value Octet 2							
5	Charging ID value Octet 3							
6	Charging ID value Octet 4							

3GPP Type: 2

Length: 6

Charging ID value: 32 bits unsigned integer

3 - 3GPP-***PDP type***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 3							
2	3GPP Length= 6							
3	PDP type octet 1							
4	PDP type octet 2							
5	PDP type octet 3							
6	PDP type octet 4							

3GPP Type: 3

Length: 6

PDP type value: Unsigned 32 bits integer

PDP type octet possible values:

0 = IP

4 - 3GPP-***Charging Gateway address***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 4							
2	3GPP Length= 6							
3	Charging GW addr Octet 1							
4	Charging GW addr Octet 2							
5	Charging GW addr Octet 3							
6	Charging GW addr Octet 4							

3GPP Type: 4

Length: 6

Charging GW address value:- Address

5 - 3GPP-***GPRS Negotiated QoS profile***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 5							
2	3GPP Length= L							
3 -L	UTF-8 encoded QoS profile							

3GPP Type: 5

Length: -27 (release 99) or 11 (release 98)

QoS profile value: -Text

UTF-8 encoded QoS profile syntax:

"<Release indicator> – <release specific QoS IE UTF-8 encoding>"

<Release indicator> = UTF-8 encoded number :

"98" = Release 98

"99"= Release 99

<release specific QoS profile UTF-8 encoding> = UTF-8 encoded QoS profile for the release indicated by the release indicator.

The UTF-8 encoding of a QoS IE is defined as follows: each octet is described by 2 UTF-8 encoded digits, defining its hexadecimal representation. The QoS profile definition is in 3GPP TS ~~24.008~~04.08 [30].

The release 98 QoS profile data is 3 octets long, which then results in a 6 octets UTF-8 encoded string,

The release 99 QoS profile data is 11 octets long, which results in a 22 octets UTF-8 encoded string.

6 - 3GPP-***SGSN address***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 6							
2	3GPP Length= 6							
3	SGSN addr Octet 1							
4	SGSN addr Octet 2							
5	SGSN addr Octet 3							
6	SGSN addr Octet 4							

3GPP Type: 6

Length: 6

SGSN address value: -Address

7 - 3GPP-***GGSN address***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 7							
2	3GPP Length= 6							
3	GGSN addr Octet 1							
4	GGSN addr Octet 2							
5	GGSN addr Octet 3							
6	GGSN addr Octet 4							

3GPP Type: 7

Length: 6

GGSN address value: -Address

8 - 3GPP-***IMSI MCC-MNC***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 8							
2	3GPP Length= n							
3	MCC digit1 (UTF-8 encoded)							
4	MCC digit2 (UTF-8 encoded)							
5	MCC digit3 (UTF-8 encoded)							
6	MNC digit1 (UTF-8 encoded)							
7	MNC digit2 (UTF-8 encoded)							
8	MNC digit3 if present (UTF-8 encoded)							

3GPP Type: 8

Length: n shall be 7 or 8 octets depending on the presence of MNC digit 3

MS address value: -text

This is the UTF-8 encoding of the MS MCC-MNC values. In accordance with 3GPP TS 03.03 [23] and 3GPP TS 09.60 [31][24] the MCC shall be 3 digits and the MNC shall be either 2 or 3 digits. There shall be no padding characters between the MCC and MNC.

9 - 3GPP-***GGSN MCC-MNC***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 9							
2	3GPP Length= n							
3	MCC digit1 (UTF-8 encoded)							
4	MCC digit2 (UTF-8 encoded)							
5	MCC digit3 (UTF-8 encoded)							
6	MNC digit1 (UTF-8 encoded)							
7	MNC digit2 (UTF-8 encoded)							
8	MNC digit3 if present (UTF-8 encoded)							

3GPP Type: 9

Length: n shall be 7 or 8 octets depending on the presence of MNC digit 3

GGSN address value: -text

This is the UTF-8 encoding of the GGSN MCC-MNC values. In accordance with 3GPP TS 03.03 [23] and 3GPP TS 09.60 [31][24] the MCC shall be 3 digits and the MNC shall be either 2 or 3 digits. There shall be no padding characters between the MCC and MNC.

10 - 3GPP-***NSAPI***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 10							
2	3GPP Length= 3							
3	NSAPI							

3GPP Type: 10

Length: 3

NSAPI value: text

It is the value of the NSAPI of the PDP context the RADIUS message is related to. It is encoded as its hexadecimal representation, using 1UTF-8 encoded digit.

11 - 3GPP-***Session Stop Indicator***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 11							
2	3GPP Length= 3							
3	1	1	1	1	1	1	1	1

3GPP Type: 11

Length: ~~-~~3

Value is set to all 1.

12 - 3GPP-***Selection-Mode***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 12							
2	3GPP Length= 1							
3	UTF-8 encoded Selection mode string							

3GPP Type: 12

Length: ~~-~~3

Selection mode value: Text

The format of this attribute shall be a character string consisting of a single digit, mapping from the binary value of the selection mode in the Create PDP Context message (3GPP TS 09.60 [31])~~[22]~~. Where 3GPP TS ~~29.060~~09.60 ~~-~~[31] provides for interpretation of the value, e.g. map ~~"~~'3'~~"~~ to ~~"~~'2'~~"~~, this shall be done by the GGSN.

18 - 3GPP-***SGSN MCC-MNC***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 18							
2	3GPP Length= n							
3	MCC digit1 (UTF-8 encoded)							
4	MCC digit2 (UTF-8 encoded)							
5	MCC digit3 (UTF-8 encoded)							
6	MNC digit1 (UTF-8 encoded)							
7	MNC digit2 (UTF-8 encoded)							
8	MNC digit3 if present (UTF-8 encoded)							

3GPP Type: 18

Length: n shall be 7 or 8 octets depending on the presence of MNC digit 3

SGSN address value:~~-~~ text

This is the UTF-8 encoding of the RAI MCC-MNC values. In accordance with 3GPP TS 03.03 [23] and 3GPP TS 09.60 [31]~~[24] and [41]~~ the MCC shall be 3 digits and the MNC shall be either 2 or 3 digits. There shall be no padding characters between the MCC and MNC.

16.4.8 Accounting Request Interim-Update (sent from GGSN to AAA server)

T~~he t~~able 8 describes the attributes of the Accounting-Request Interim-Update message.

Table 8: The attributes of the Accounting-Request Interim-Update message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username provided by the user (extracted from the PCO field of the Create PDP Context Request message). If no username is available a generic username, configurable on a per APN basis, shall be present. If the User-Name has been received in the Access-Accept message, this user-name shall be used in preference to the above	String	Optional
4	NAS-IP-Address	IP address of the GGSN for communication with the AAA server.	IPv4	Conditional Note 1~~3~~
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 1~~3~~
6	Service-Type	Indicates the type of service for this user	Framed	Optional
7	Framed Protocol	Indicates the type of protocol for this user	7 (GPRS PDP Context)	Optional
8	Framed-IP-Address	User IP address	IPv4	Mandatory
25	Class	Received in the access accept	String	Optional (N~~OTE 4~~ote 2)
30	Called-Station-Id	Identifier for the target network	APN (UTF-8 encoded)	Mandatory
31	Calling-Station-Id	This attribute is the identifier for the MS, and it shall be configurable on a per APN basis.	MSISDN in international format according to 3GPP TS ~~23.003~~03.03 [23], UTF-8 encoded. Note that there are no leading characters in front of the country code.	Optional
40	Acct-Status-Type	Indicates the type of accounting request	Interim-Update	Mandatory
41	Acct-Delay-Time	Indicates how many seconds the GGSN has been trying to send this record for, and can be subtracted from the time of arrival on the AAA server to find the approximate time of the event generating this Accounting-Request	Second	Optional
42	Acct-Input-Octets	GGSN counted number of octets sent by the user for the PDP context	32 bit unsigned integer	Optional
43	Acct-Output-Octets	GGSN counted number of octets received by the user for the PDP context	32 bit unsigned integer	Optional
44	Acct-Session-Id	User session identifier.	GGSN IP address and Charging-ID concatenated in a UTF-8 encoded hexadecimal.	Mandatory

Attr #	Attribute Name	Description	Content	Presence Requirement
			(Note 3)~~NOTE: The GGSN IP address is the same as that used in the GCDRs.~~	
45	Acct-Authentic	Authentication method	RADIUS or LOCAL	Optional
46	Acct-Session-Time	Duration of the session	Second	Optional
47	Acct-Input-Packets	GGSN counted number of packets sent by the user	Packet	Optional
48	Acct-Output-Packets	GGSN counted number of packets received by the user	Packet	Optional
61	NAS-Port-Type	Port type for the GGSN	As per RFC 2865 [21]	Optional
26/10415	3GPP Vendor-Specific	Sub-attributes according to ~~sub-clause~~subclause 16.4.7.	See ~~sub-clause~~subclause 16.4.7	Optional except sub-attribute 3 which is conditional
NOTE 3: Either NAS-IP-Address or NAS-Identifier shall be present. NOTE 4: The presence of this attribute is conditional upon this attribute being received in the Access-Accept message. NOTE 3: The GGSN IP address is the same as that used in the GCDRs.				

16.4.9 Disconnect Request (optionally sent from AAA server to GGSN)

T~~he t~~able 9 describes the attributes of the Disconnect-Request message.

Table 9: The attributes of the Disconnect-Request message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username provided by the user (extracted from the PCO field of the Create PDP Context Request message). If no username is available a generic username, configurable on a per APN basis, shall be present. If the User-Name has been sent in the Access-Accept message, this user-name shall be used in preference to the above	String	Optional
8	Framed-IP-Address	User IP address	IPv4	Mandatory
44	Acct-Session-Id	User session identifier.	GGSN IP address and Charging-ID concatenated in a UTF-8 encoded hexadecimal. NOTE: The GGSN IP address is the same as that used in the GCDRs.	Mandatory

Annex A (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
	s25	98-0101	A001		Access to an Intranet or ISP through GPRS	5.0.0	6.0.0
	s26	98-0292	A002		Authentication protocol when accessing an intranet or ISP through GPRS	6.0.0	6.1.0
	s26	98-0292	A003		Clarifications to Intranet/ISP Interworking section	6.0.0	6.1.0
	s26	98-0292	A004		Architecture Diagrams	6.0.0	6.1.0
	s26	98-0292	A005		Editorial review of 09.61	6.0.0	6.1.0
	s26				Correction of Word 95/97 problem (incomplete incorporation of CR A003 into V6.1.0)	6.1.0	6.2.0
	s27	98-0735	A006		Protocol Configuration Options at PDP context activation failure	6.2.0	6.3.0
	TSG#06	NP-99431	A015		Approved CR from TSG#6 incorporated:A012 IPCP negotiation at the GGSN for non-transparent IP	6.3.0	6.4.0
09-2001					Conversion to 3GPP layout and number	6.4.0	6.5.0
09-2001	TSG#13	NP-010530	A017	2	Standard method for information delivery (MSISDN; IP address…) between GPRS and external PDN using RADIUS	6.4.0	6.5.0
12-2001	TSG#14	NP-010572	A021	1	Correction to calling station id	6.5.0	6.6.0
12-2001	TSG#14	NP-010572	A023	1	Correction to 3GPP Vendor specify attribute 3GPP-IMSI	6.5.0	6.6.0
12-2001	TSG#14	NP-010572	A025		Correction to 3GPP vendor specific attributes containing MCC-MNC	6.5.0	6.6.0
12-2001	TSG#14	NP-010672	A027		Standard method for information update between GPRS and external PDN using RADIUS	6.5.0	6.6.0
12-2001	TSG#14	NP-010672	A030		Standard method for interworking between GPRS and external PDN using RADIUS	6.5.0	6.6.0
03-2002	TSG#15	NP-020080	A031		Change of associated attribute for 3GPP-NSAPI	6.6.0	6.7.0
06-2002	TSG#16	NP-020295	A035		Corrections to the 3GPP RADIUS attributes	6.7.0	6.8.0
06-2002	TSG#16	NP-020295	A037	1	Clarification on the Radius Flows	6.7.0	6.8.0
12-2002	TSG#18	NP-020613	A039	1	RADIUS enhancement for identification of VPLMN	6.8.0	6.9.0

3GPP TSG-CN WG3 Meeting #27
Dublin, Ireland, 10th - 14th February 2003.

Tdoc ⌘N3-030121

CR-Form-v7

CHANGE REQUEST

⌘ **09.61** **CR** **A048** ⌘**rev** **1** ⌘ Current version: **7.8.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Correction of References and specification Corrections
Source:	⌘	TSG_CN WG3 *[Siemens AG, MCC]*
Work item code:	⌘	TEI
Date:	⌘	11/02/2003
Category:	⌘	**A**
Release:	⌘	R98

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Inconsistencies in the specification, Missing and incorrect references
Summary of change:	⌘	Correction of incorrect and missing reference and general specification clean-up
Consequences if not approved:	⌘	Inconsitencies and errors in the referencing. Possible misunderstanding when reading specification.

Clauses affected:	⌘	Most of the specification			
Other specs affected:	⌘	**Y**	**N**		
			X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

3GPP TS 09.61 V7.8.0 (2002-12)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Core Network; General Packet Radio Service (GPRS); Interworking between the Public Land Mobile Network (PLMN) supporting GPRS and Packet Data Networks (PDN) (Release 1998)

Keywords

GSM, network, GPRS, interworking, PLMN, PDN, PLMN, packet mode

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Contents

Foreword

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

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 General Packet Radio Service (GPRS) interworking between a:

a) PLMN and PSDN;

b) PLMN and IP Networks;

c) PLMN and PLMN.

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

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. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TR 01.04: "Abbreviations and acronyms".

[2] 3GPP TS 02.60: "General Packet Radio Service (GPRS)~~:~~; Service Description; Stage 1~~ Service Description~~".

[3] 3GPP TS 03.60: "General Packet Radio Service (GPRS); Service Description; Stage 2~~ Service Description~~ ".

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

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

[6] 3GPP TS 03.64: "General Packet Radio Service (GPRS); Overall description of the GPRS ~~R~~radio interface; Stage 2".

[7] 3GPP TS 04.60: "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: "General Packet Radio Service (GPRS); Mobile Station - Serving GPRS Support Node (MS-SGSN) Logical Link Control (LLC) layer specification~~Logical Link Control (LLC)~~".

[9] 3GPP TS 04.65: "General Packet Radio Service (GPRS); Mobile Station (MS) - Serving GPRS Support Node (SGSN); Subnetwork Dependent Convergence Protocol (SNDCP)".

[10] 3GPP TS 07.60: "General Packet Radio Service (GPRS); Mobile Station (MS) supporting GPRS".

[11] ITU-T Recommendation E.164: "The international public telecommunication numbering plan~~Numbering plan for the ISDN era~~".

[12] ITU-T Recommendation X.25: "Interface between D~~d~~ata ~~t~~Terminal ~~e~~Equipment (DTE) and ~~d~~Data ~~c~~Circuit-terminating ~~e~~Equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit".

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

[14] ITU-T Recommendation X.121: "International nNumbering Pplan for Ppublic Ddata Nnetworks".

[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 nNames – Cconcepts and Ffacilities" (STD 7).

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

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

[21b] IETF RFC 1662 (1994): "PPP in HDLC-like Framing".

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

[23] IETF RFC 2865 (2000), C. Rigney, S. Willens, A. Rubens, W. Simpson:: "Remote Authentication Dial In User Service (RADIUS), C. Rigney, S. Willens, A. Rubens, W. Simpson".

[24] IETF RFC 2866 (2000), C. Rigney, Livingston: "-RADIUS Accounting-", C. Rigney, Livingston.

[25] 3GPP TS 03.03: "Numbering, addressing and identification".

[26] IETF RFC 2882 (2000), D. Mitton: "Network Access Servers Requirements: Extended RADIUS Practices", D. Mitton.

[27] IETF RFC 1035 (1987): "Domain names - implementation and specification".

[28] IETF RFC 1771 (1995): "A Border Gateway Protocol 4 (BGP-4)".

[29] IETF RFC 1825 (1995): "Security Architecture for the Internet Protocol".

[30] IETF RFC 1826 (1995): "IP Authentication Header".

[31] IETF RFC 1827 (1995): "IP Encapsulating Security Payload (ESP)".

[32] 3GPP TS 04.08: " Mobile radio interface layer 3 specification".

[33] 3GPP TS 09.60: "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface ".

3 Definitions, abbreviations and symbols

3.1 Definitions

For the purposes of the present document, the terms and definitions given in See 3GPP TS 02.60 [2] apply.

In 3GPP TS 02.02 the bearer services are described. The general network configuration is described in 3GPP TS 03.02 and the GSM PLMN access reference configuration is defined in 3GPP TS 04.02. The various connection types used in the GSM PLMN are presented in 3GPP TS 03.10. Terminology used in this Specificatione present document is presented in 3GPP -TS -01.04 [1]. For support of data services between GSM PLMN and other networks see 3GPP TS 09-series of Specifications.

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
DNIC	Data Network Identification Code
DNS	Domain Name Server
DSE	Data Switch Exchange
GGSN	Gateway GPRS Support Node
IC	Interexchange Carrier
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
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
LAPB	Link Access Protocol Balanced
LATA	Local Access and Transport Area
LNS	L2TP Network Server
MS	Mobile Station
MT	Mobile Terminal
PDN	Packet Data Network
PDU	Protocol Data Unit
PHF	Packet Handler Function
PNIC	Pseudo Network Identification Code
PPP	Point-to-Point Protocol
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
TCP	Transmission Control Protocol
TE	Terminal Equipment
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 GPRS 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 GPRS network services across areas served by the co-operating GPRS 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.

4 Network characteristics

4.1 Key characteristics of PLMN

The GSM PLMN is fully defined in the GSM technical specifications. The GPRS related key characteristics are found in 3GPP TS 02.60 [2] and 3GPP TS 03.60 [3].

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 GPRS, 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 3GPP TS 03.03 [25] 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 GSM network in the overall GPRS environment.

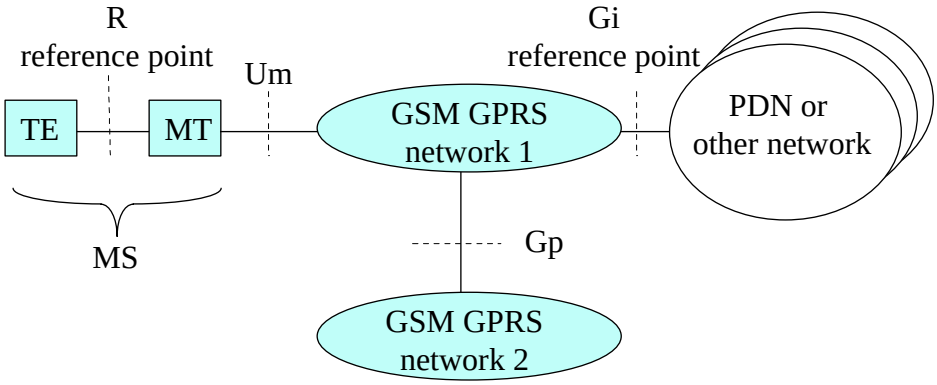
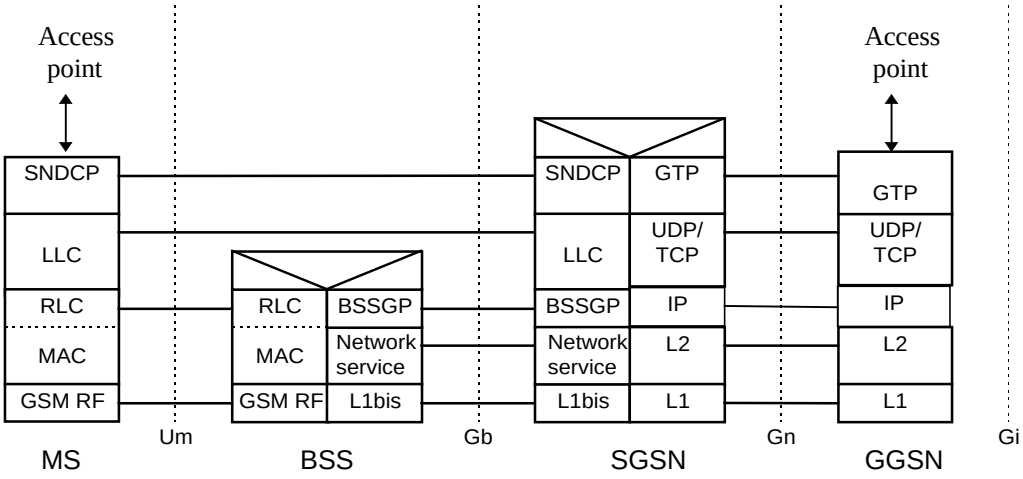


Figure 1: GPRS Access Interfaces and Reference Points

7 Interface to GPRS Bearer Services

The following Figure 2:, Transmission Plane , 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 3GPP -TS -03.60 [3], 3GPP TS 04.64, [8] and 3GPP TS 04.65 [9].



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

Figure 2: GPRS Transmission Plane

8 Subscription checking

Subscription is checked during the GPRS Attach procedure and also during the PDP Context Activation procedure as described in 3GPP TS 03.60 [3]. 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 Screening

Screening function's reside within the GPRS network and has have three levels as described in 3GPP TS 02.60 [2] and 3GPP TS 03.60 [3]. Screening may be applicable for only certain protocols. Screening is outside the scope of GPRS standardisation, however, the following types of screening shall be supported.

9.1 Network controlled screening

The PLMN administration and/or the GPRS service provider shall set basic screening functionality, if applicable, (e.g. firewall) to reduce the risk of fraud and misuse. This is to ensure the integrity of the network and to protect subscribers.

9.2 Subscription controlled screening

This will not be in GPRS phase 1.

9.3 User controlled screening

This will not be in GPRS phase 1.

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

10.1 General

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

GPRS shall support both ~~CCITT/~~ITU-T Recommendation X.121 and ~~CCITT/~~ITU-T Recommendation E.164 addressing.

GPRS shall provide support for ~~CCITT/~~ITU-T Recommendation X.25 and ~~CCITT/~~ITU-T Recommendation X.75.

The GPRS TE's shall have addresses provided , and controlled, by their GPRS operator. The PSDN TE sends data to the GPRS TE by use of that TE's GPRS 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 GSM GPRS data 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 GPRS 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 GPRS network.

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

10.2.1 X75 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 GPRS network will look like any other PSDN in all respects and uses X.75 addressing. Figure 4 shows the interconnecting protocol stacks to the GPRS bearer. The GPRS bearer is described in 3GPP TS 07.60 [10], which uses the protocols described in 3GPP TS 03.60 [3].

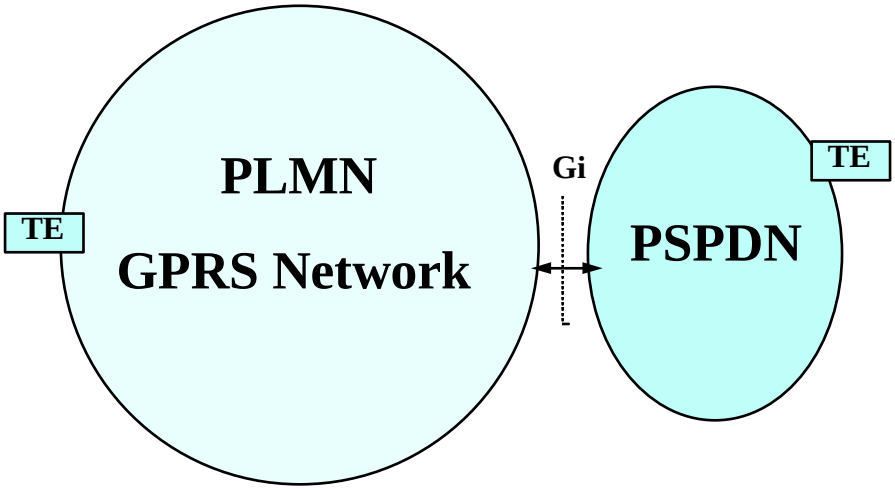


Figure 3: PSPDN Interworking with X.75 at Gi Reference Point

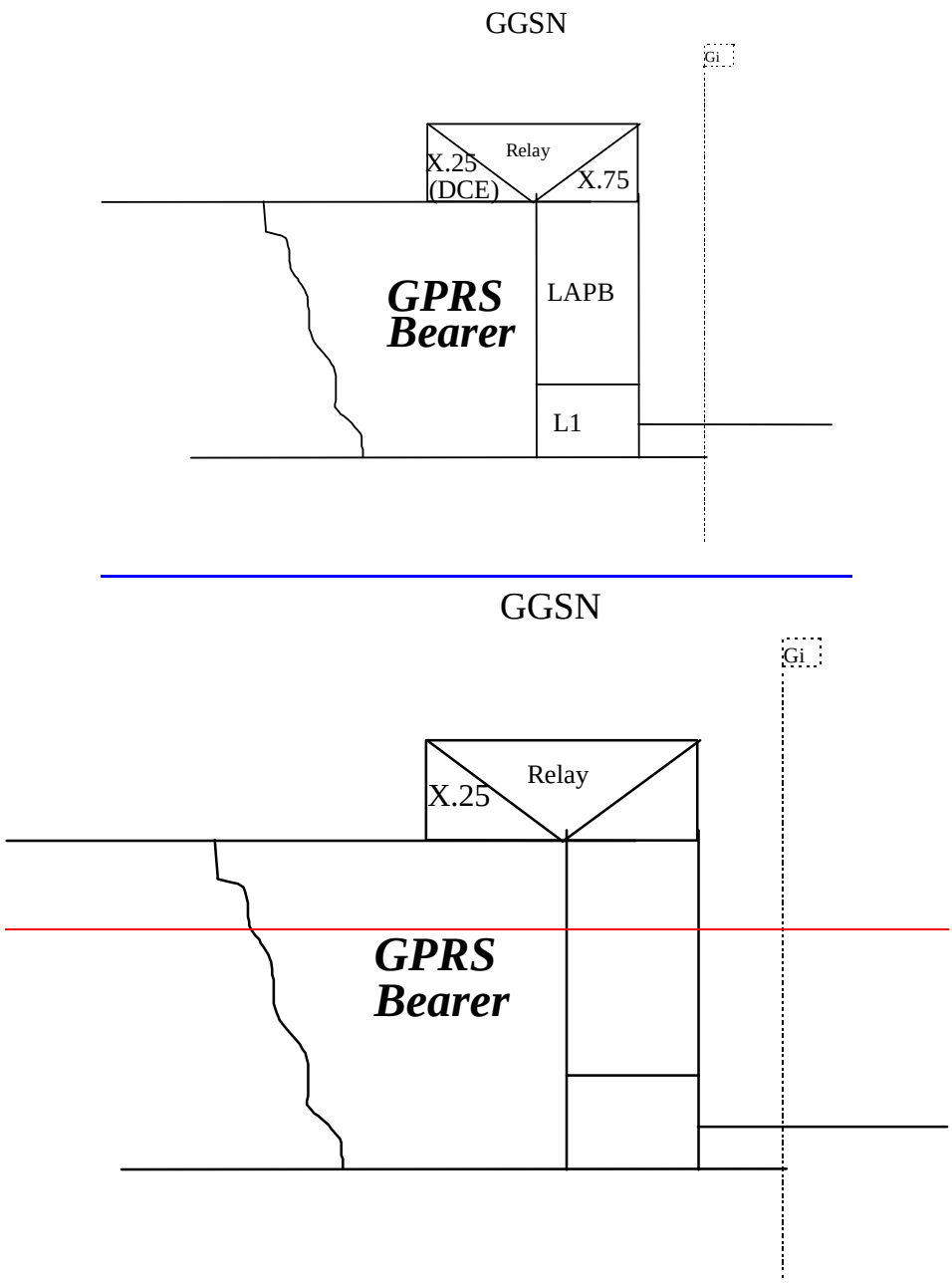


Figure 4: The Protocol Stack for the X.75 Gi Reference Point

10.2.1.1 Numbering and Addressing

A PLMN GPRS network 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.

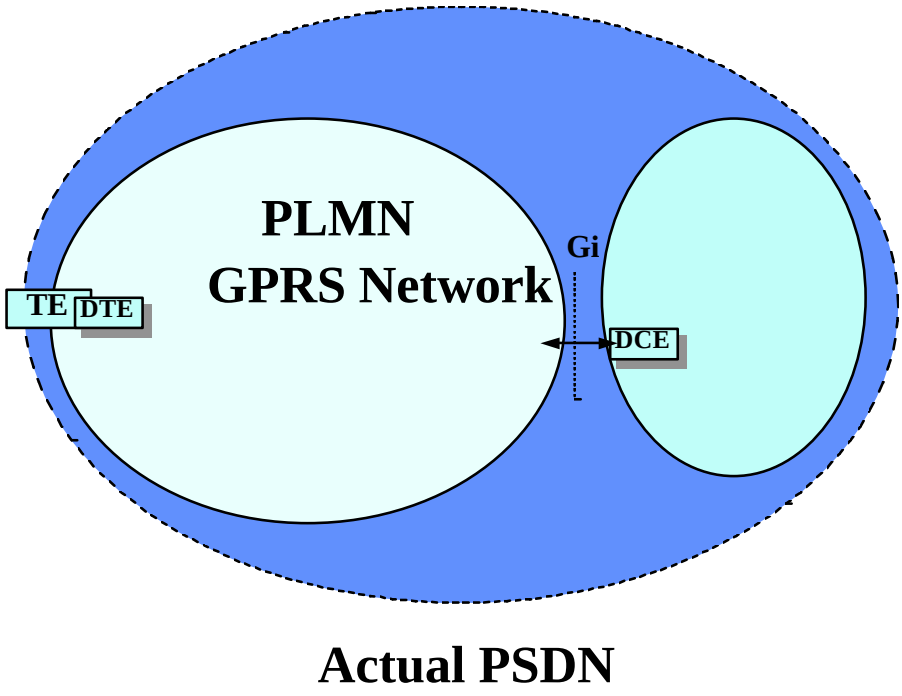
10.2.2 X25 Interworking at the Gi Reference Point

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 GPRS network. The DCE resides within the PSDN.

The GPRS 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~~ figure 6.



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

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

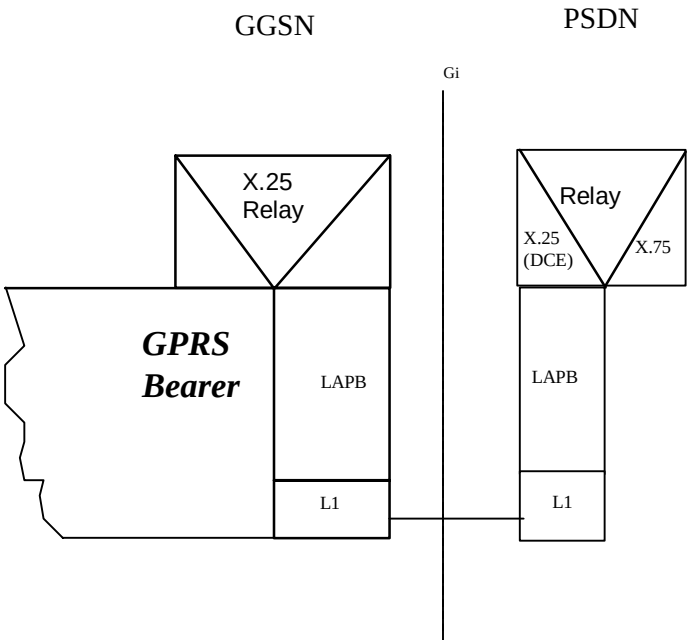


Figure 6: The Protocol Stack for the X.25 / Gi Reference point

Figure 6 shows the transmission plane only. In this case the GGSN shall resolve the association between the MS GPRS 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 GPRS 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 GPRS operator and the PSDN operator. The charging may also be collected in the GPRS network. If the VPLMN assigns the dynamic address, the charging of the GPRS 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 Recommendation 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 GPRS Interworking to PSDN Characteristics

~~The following t~~Table 0 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 GPRS 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 3GPP TS 03.60 [3].

Table ~~1~~0: PSPDN GPRS 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

GPRS 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, GPRS can operate IPv4 or ~~Ipv6~~IPv6. The interworking point with IP networks is at the Gi reference point as shown in ~~Figure~~ figure 7.

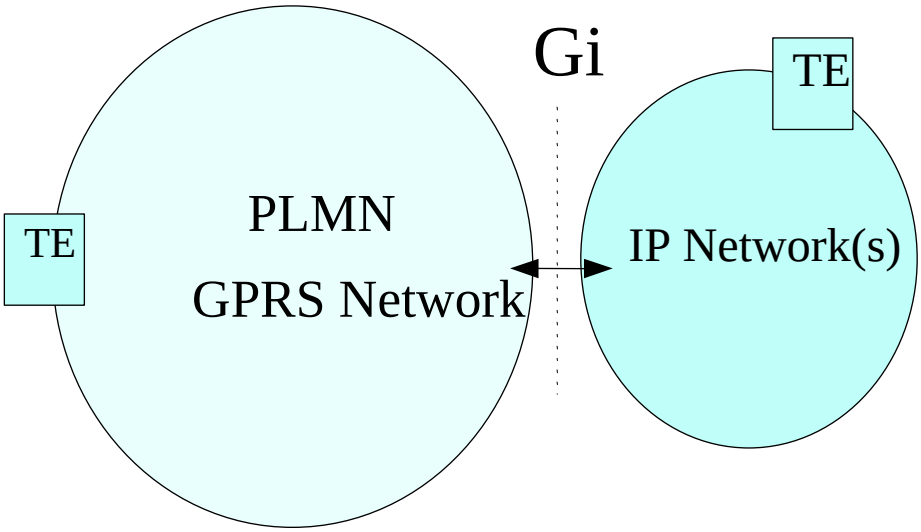


Figure 7: IP network interworking

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

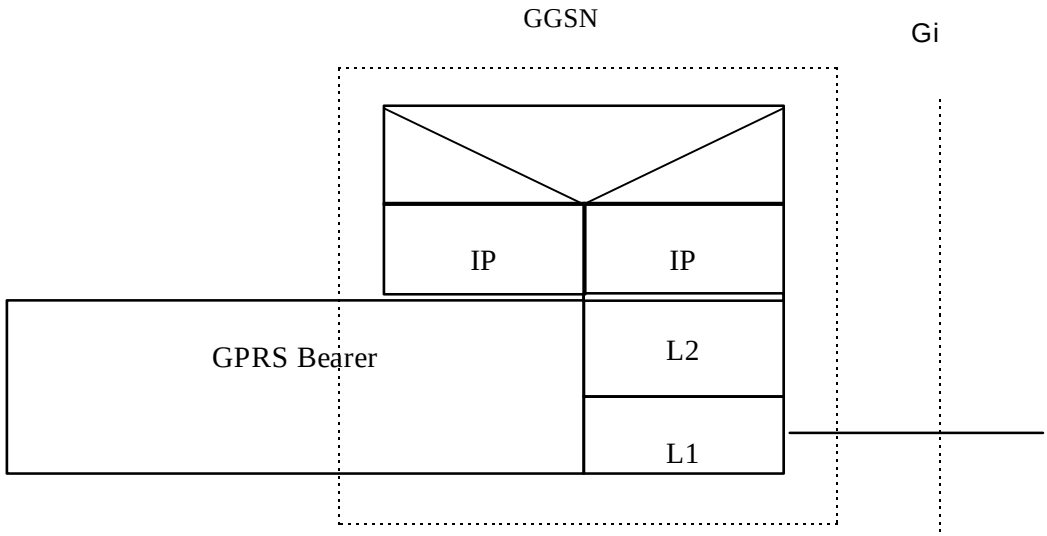


Figure 8: The protocol stacks for the GiIP reference point

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~~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.

The following working assumptions are valid in the generic case:

- A firewall is configured by the GPRS operator. In general, all applications that are using IP as the underlying protocol are supported, but the GPRS operator may restrict their usage.
- A Domain Name Server is managed by the GPRS operator. Alternatively, the Domain Name Server can be managed by the external IP network operator.

- From the GPRS network's point of view, the allocation of a dynamic IP address is done by the GGSN as described in 3GPP TS 03.60 [3]. The GGSN may allocate these addresses by itself or use an external device such as an DHCP server. This external device may be operated by an external organisation such as an ISP or Intranet operator.

11.2.1 Access to Internet, Intranet or ISP through GPRS

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 GPRS PLMN may offer:

- either direct transparent access to the Internet; or.
- or a non transparent access to the Intranet/ISP. In this case the GPRS PLMN, i.e. the GGSN, takes part in the functions listed above.

11.2.1.1 Transparent access to the Internet

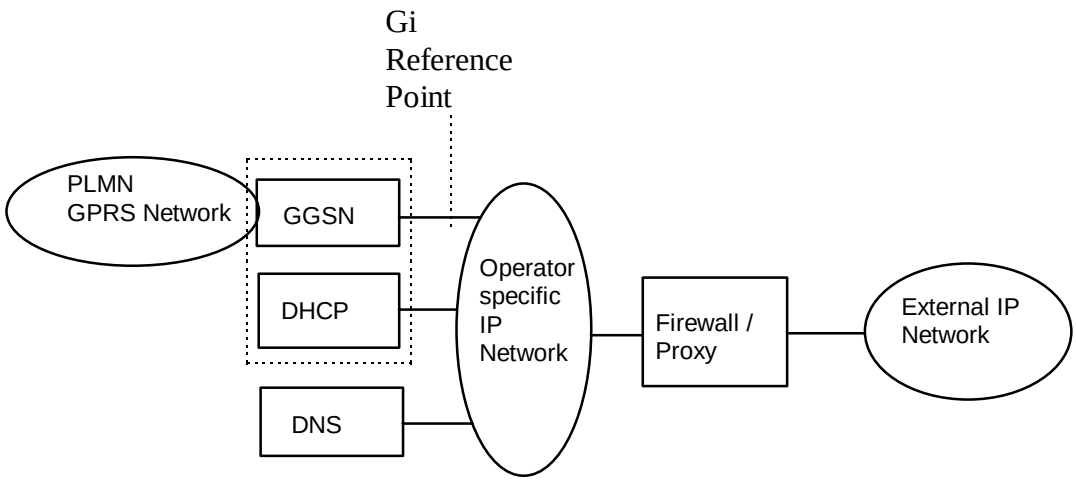


Figure 9: Example of the PDN Interworking Model, transparent case

In this case (see Ffigure 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 sectionsubclause deals with this specific case.

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

The used protocol stack is depicted in Ffigure 10.

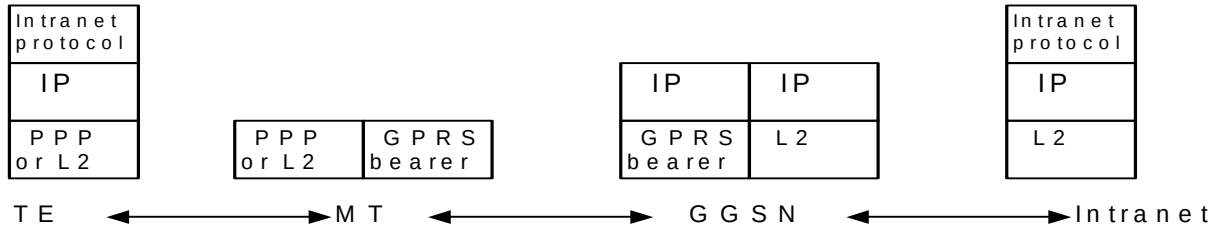


Figure 10: Transparent access to an Intranet

The communication between the GPRS 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 Pprotocol»".

User authentication and encryption of user data are done within the «"Intranet protocol»" if either of them is needed. This «"Intranet Pprotocol»" 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 [29]). 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 [30] and RFC 1827 [31]). 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 GPRS PLMN 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 GPRS PLMN operator and Intranet/ISP administrator.

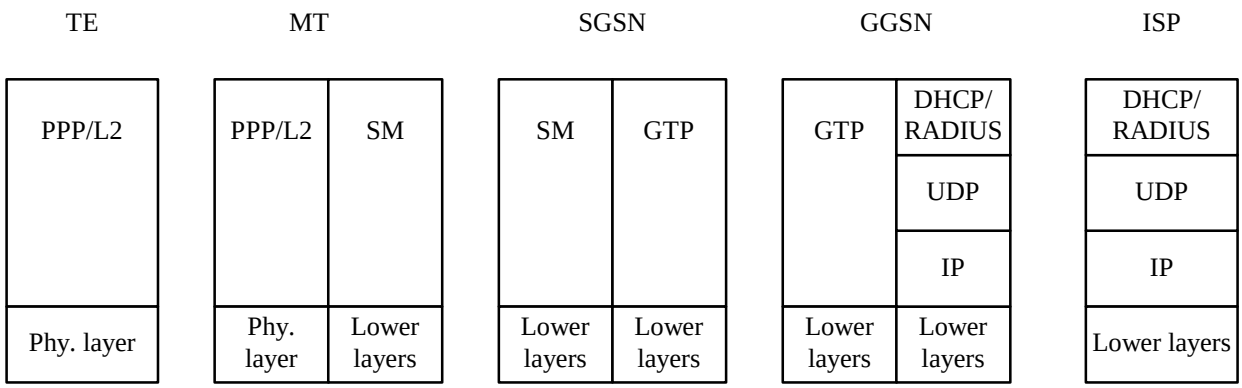


Figure 11: Signalling plane of non transparent case

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 1661 [21a]~~[20]~~ the GGSN shall respond with the following messages:

   - ~~Z~~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: ~~xample:~~ In the following example PPP is used as layer 2 protocol over the R reference point (figure 12).

The MT acts as a PPP server and translates Protocol Configuration Options into SM message IEs. GTP 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 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.

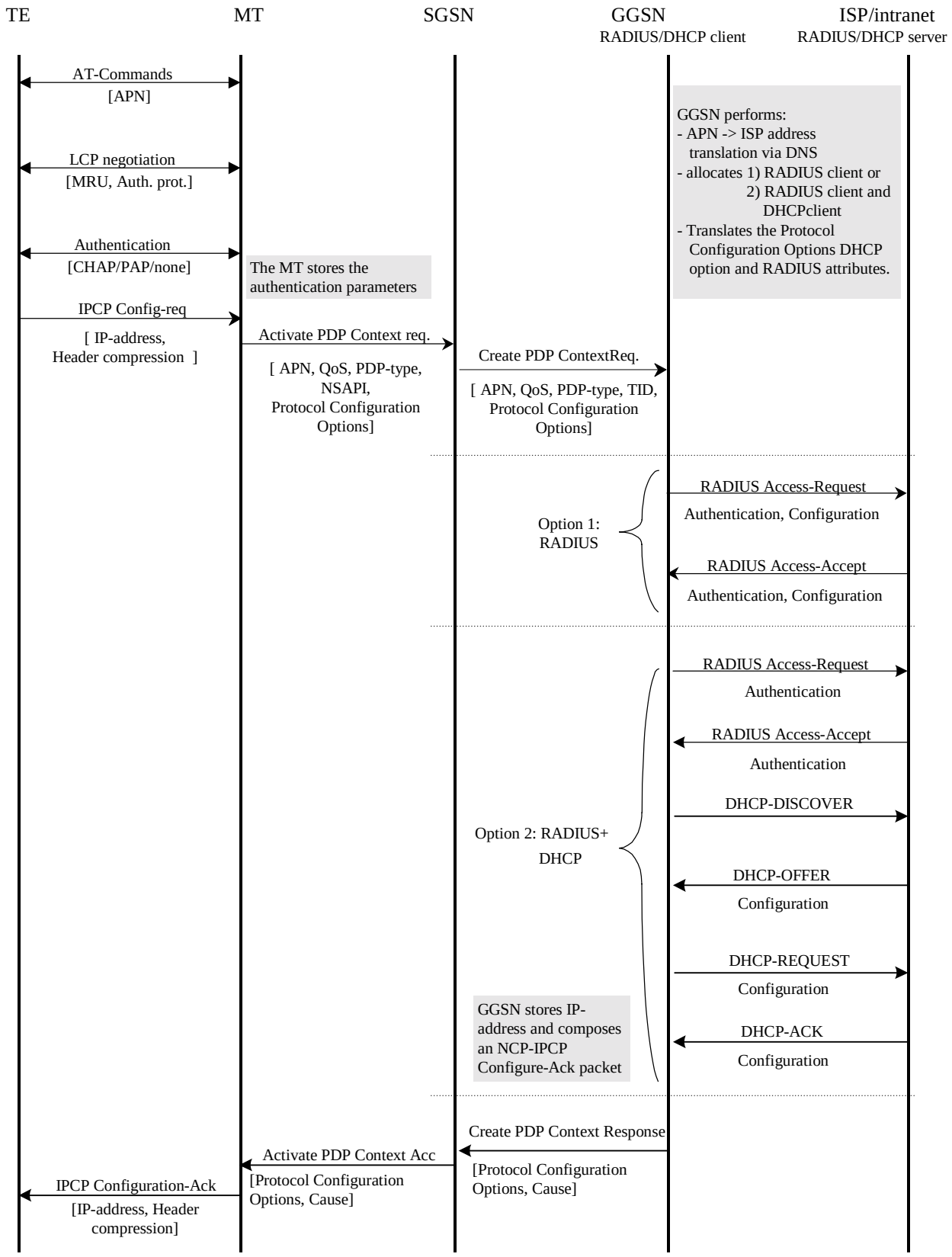


Figure 12: Example where PPP is used as layer 2 protocol over the R reference point

11.3 Numbering and Addressing

In the case of interworking with the 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 the private IP networks, the GPRS operator manages internally the subnetwork addresses.

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.
- The GPRS operator allocates (either on its own or in conjunction with an ISP) a dynamic IP address when the MS performs the PDP Context Activation procedure with dynamic address allocation as described in 3GPP -TS 03.60 [3].

11.4 Charging

The GPRS 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 Server (DNS)

Provision of Domain Name services shall be provided by the GPRS operators in the transparent case and the ISP in the non transparent case. Domain name registration is handled by RIPE (Réseaux IP Européens) in Europe (DNS documentation is provided in RFC 1034 [19] and RFC 1035[27]).

11.6 Screening

The way the GPRS operator is performing the operator controlled screening and the subscription controlled screening is out of the scope of ~~this specification~~the present document. 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' GPRS 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 RFC 1661[21a]. 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 GSM GPRS data network (see ~~F~~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.

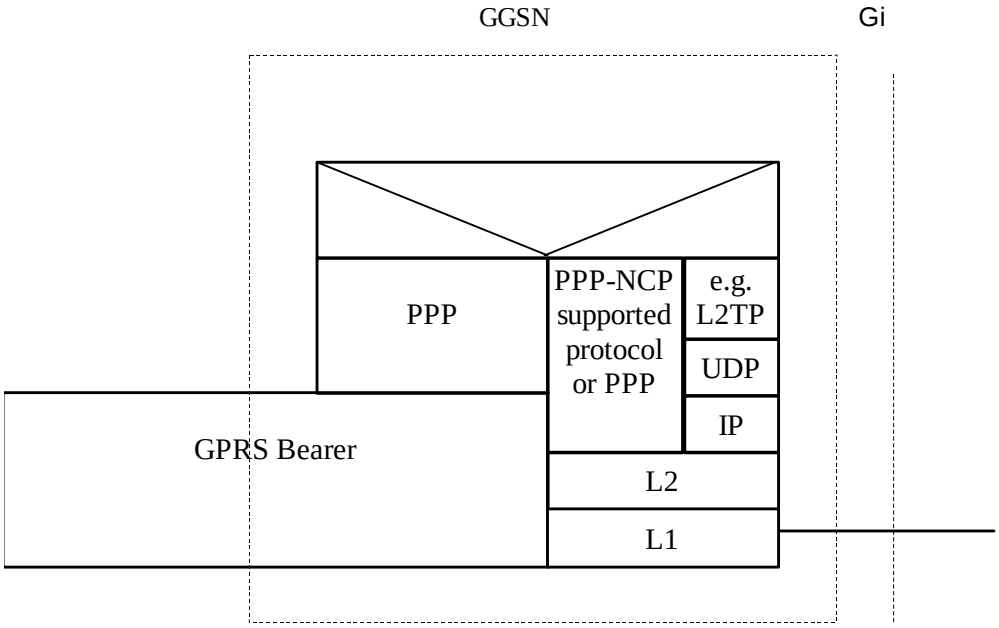


Figure 13: The protocol stacks for the Gi PPP reference point

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

In case the GGSN tunnells 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 GPRS

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 GPRS 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 GPRS PLMN may also offer access to networks based on any protocol supported by PPP through one of its Network Control Protocols (NCPs).

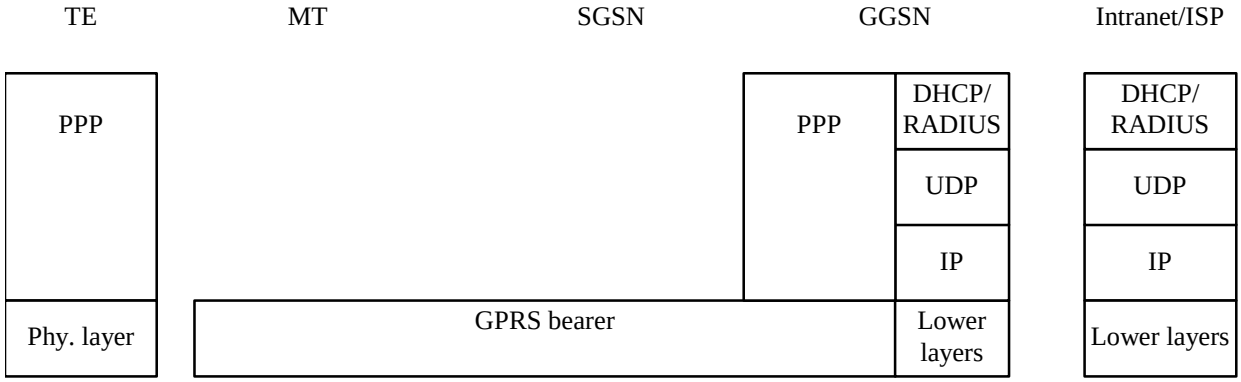


Figure 14: Protocol stack for direct access to IP-based Intranets/ISPs

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

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

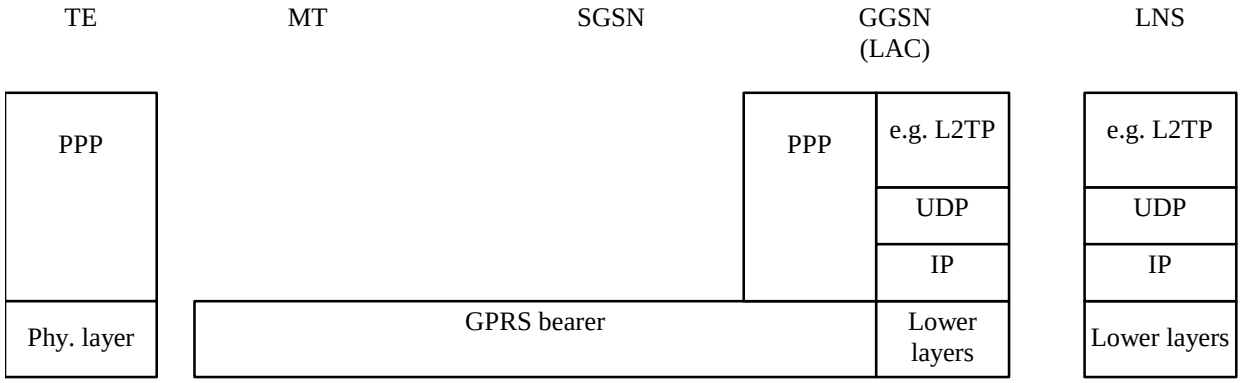


Figure 15: Protocol stack for virtual dial-up access with PPP frame tunnelling

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 GPRS PLMN 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 GPRS 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 end-to-end, or between the TE and the GGSN.

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

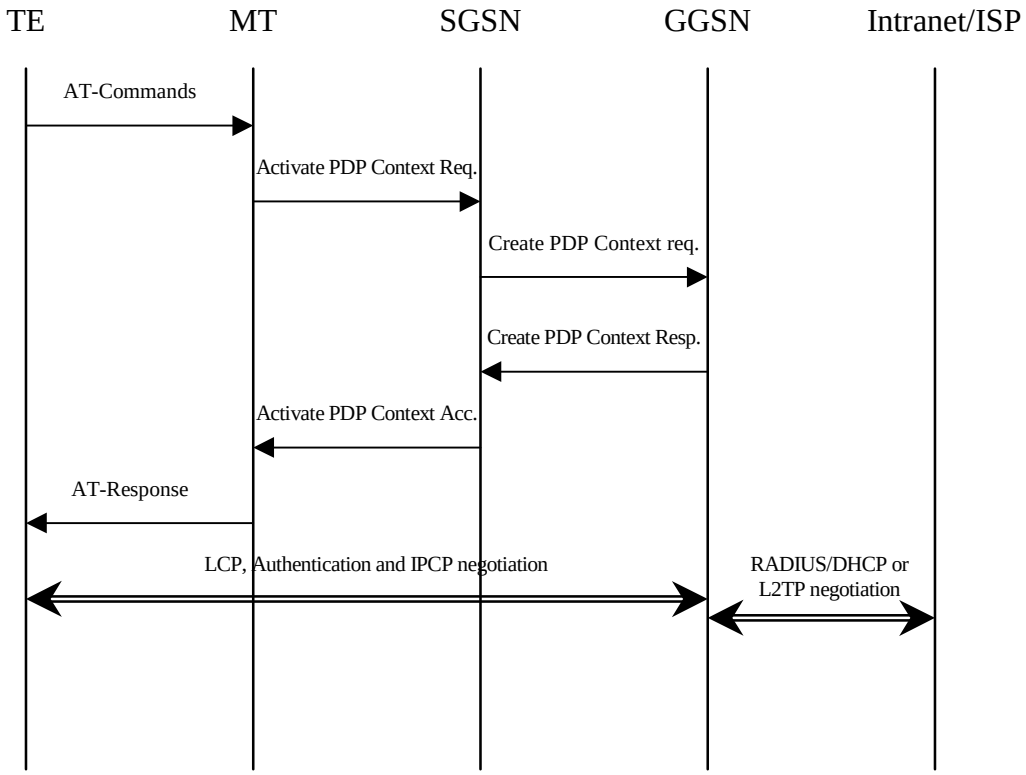


Figure 16

13 Internet Hosted Octet Stream Service (IHOSS)

~~**Void.**~~**Figure 17: Void**

Figure 18: Void

Figure 19: Void

Figure 20: Void

14 Interworking between GPRS networks

The primary reason for the interworking between the GPRS networks is to support roaming GPRS subscribers as described in 3GPP TS 03.60 [3]. The general model for GPRS network interworking is shown in ~~Figure~~ figure 21.

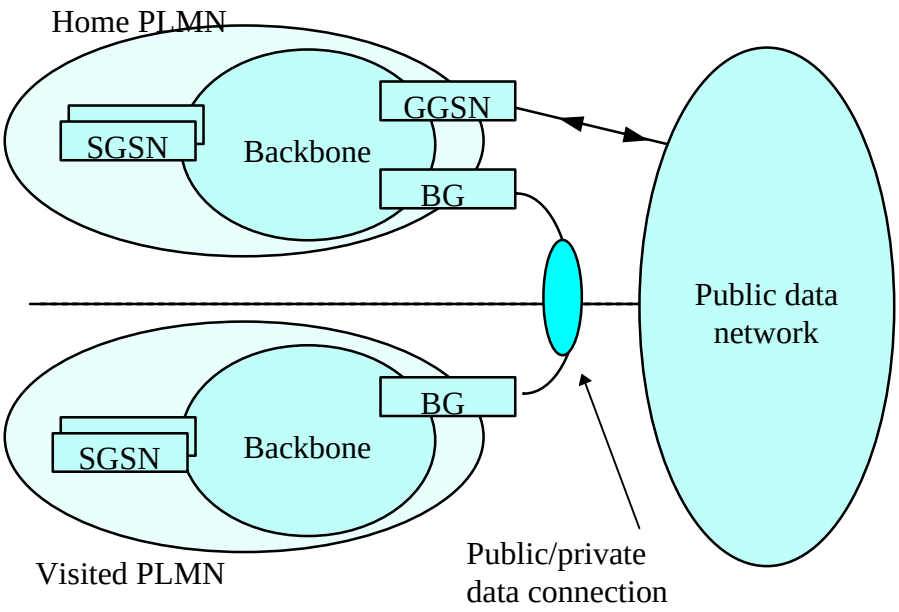


Figure 21: General interworking between GPRS networks to support roaming subscribers

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 03.60 [3].

The procedures to set the link between the SGSN in the VPLMN and the GGSN in the HPLMN is described in 3GPP TS 03.60 [3].

The inter-PLMN link may be any packet data network or dedicated link as described in 3GPP TS 03.60 [3]. The GPRS operators may have a dedicated inter-PLMN link to fulfil the QoS requirements of a certain protocol.

14.1 Security Agreements

Each GPRS operator may support IPsec (RFC 1825 [29]) and accompanying specifications for authentication (RFC 1826 [30]) and encryption (RFC 1827 [31]) as a basic set of security functionality in its border gateways. The GPRS operators may decide to use other security protocols based on bilateral agreements.

14.2 Routing protocol agreements

Each GPRS operator may support BGP (RFC 1771 [28]) as a basic set of routing functionality in its border gateways. The GPRS operators may decide to use other routing protocols based on bilateral agreements.

14.3 Charging agreements

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

There may be a requirement to collect charging information in the Border Gateway (see ~~F~~figure 12) and this is down to the normal interconnect agreement between PLMN and PDN operators.

15 Void

16 Usage of RADIUS on Gi interface

A GGSN may, on a per APN basis, use RADIUS authentication to authenticate a user and RADIUS accounting to provide information to an AAA (Authentication, Authorization and Accounting) server.

16.1 RADIUS Authentication

RADIUS Authentication shall be used according to RFC 2865 [23].

The RADIUS client function may reside in a GGSN. When the GGSN receives a Create PDP Context request message the RADIUS client function may send the authentication information to an authentication server, which is identified during the APN provisioning.

The authentication server checks that the user can be accepted. The response (when positive) may contain network information, such as an IP address for the user.

The information delivered during the Radius authentication can be used to automatically correlate the users identity (the MSISDN or IMSI) to the IP-address, assigned/confirmed by the GGSN or the authentication server respectively. The same procedure applies, in case of sending the authentication to a 'proxy' authentication server.

RADIUS Authentication is only applicable to the primary PDP context. When the GGSN receives an Access-Accept message from the authentication server it shall complete the PDP context activation procedure. If Access-Reject or no response is received, the GGSN shall reject the PDP Context Activation attempt with a suitable cause code, e.g. User Authentication failed.

16.2 RADIUS Accounting

RADIUS Accounting shall be used according to RFC 2866 [24].

The RADIUS accounting client function may reside in a GGSN. The RADIUS accounting client may send information to an accounting server, which is identified during the APN provisioning. The accounting server may store this information and use it to automatically identify the user. This information can be trusted because the GPRS network has authenticated the subscriber (i.e. SIM card and possibly other authentication methods).

RADIUS Accounting-Request Start and Stop messages may be used during both primary and secondary PDP context activation and deactivation procedures respectively.

The use of Accounting-Request STOP and in addition the Accounting ON and Accounting OFF messages may be used to ensure that information stored in the accounting server is synchronised with the GGSN information.

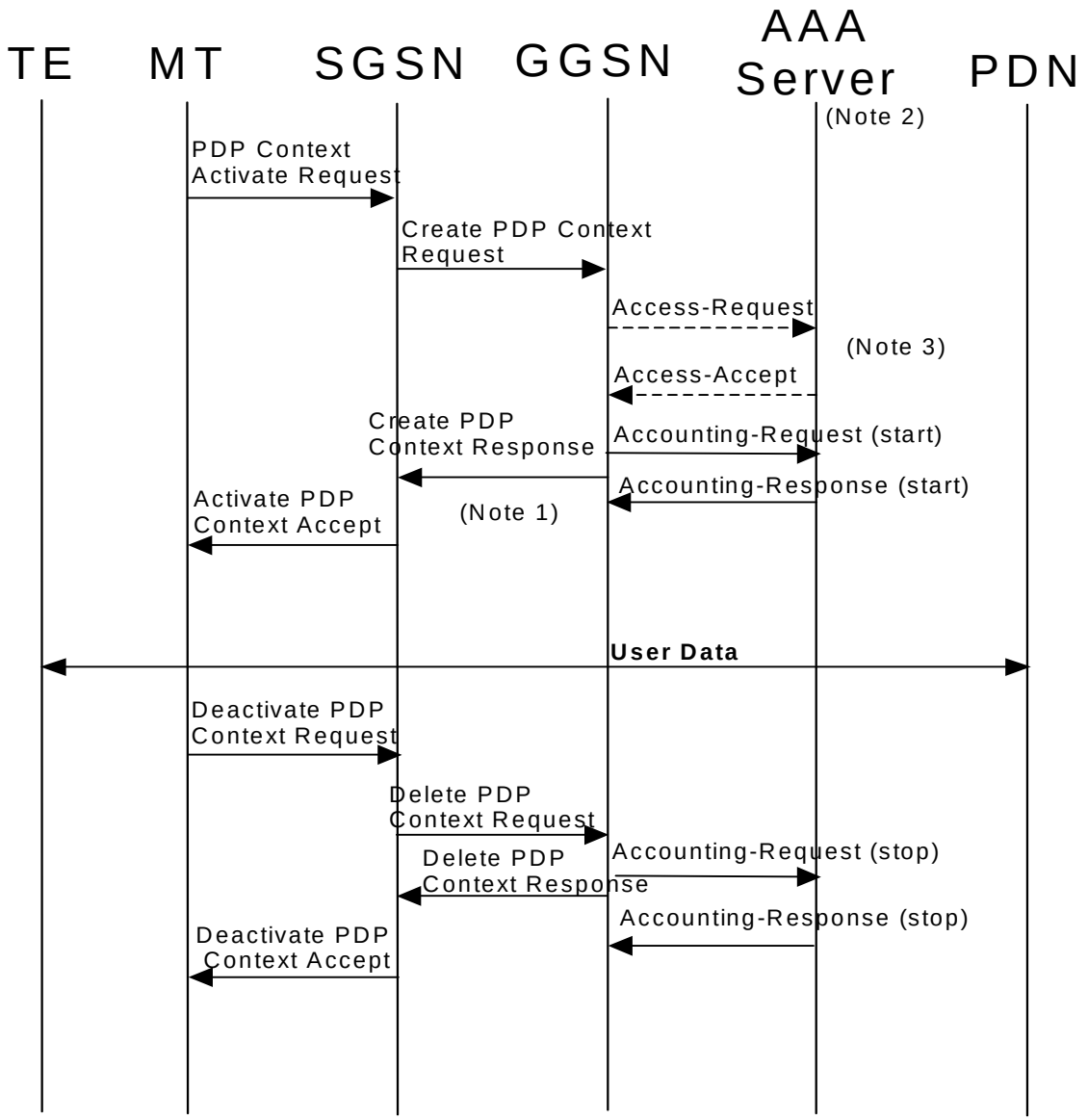
If the AAA server is used for IP address assignment, then, upon reception of a RADIUS Accounting-Request STOP message for all PDP contexts associated to a session defined by APN and IMSI or MSISDN, the AAA server may make the associated IP address available for assignment.

In order to avoid race conditions, the GGSN shall include a 3GPP Vendor-Specific sub-attribute "Session Stop indicator" when it sends the Accounting-Request STOP for the last PDP context of a PDP session and the PDP session is terminated- (i.e. the IP address and all GTP tunnels can be released). The AAA server shall not assume the PDP session terminated until an Accounting-Request STOP with the Session Stop indicator is received.

16.3 Authentication and accounting message flows

16.3.1 IP PDP type

The figure 22 represents the RADIUS message flows between a GGSN and an Authentication, Authorization and Accounting (AAA) server.



NOTE 1: If some external applications require RADIUS Accounting request (Start) information before they can process user packets, then the selected APN (GGSN) may be configured in such a way that the GGSN drops user data until the Accounting Response (START) is received from the AAA server. The GGSN may wait for the Accounting Response (START) before sending the CreatePDPContextResponse. The GGSN may reject the PDP context if the Accounting Response (START) is not received.
NOTE 2: Separate accounting and authentication servers may be used.
NOTE 3: The Access-Request message shall be used for primary PDP context only.

Figure 22: RADIUS message flow for PDP type IP (successful user authentication case)

When a GGSN receives a Create PDP Context Request message for a given APN, the GGSN may (depending on the configuration for this APN) send a RADIUS Access-Request to an AAA server. The AAA server authenticates and authorizes the user. If RADIUS is also responsible for IP address allocation the AAA server shall return the allocated IP address in the Access-Accept message.

Even if the GGSN was not involved in user authentication (e.g. transparent network access mode), it may send a RADIUS Accounting-Request START message to an AAA server. This message contains parameters, e.g. the tuple which includes the user-id and IP address, to be used by application servers (e.g. WAP gateway) in order to identify the user. This message also indicates to the AAA server that the user session has started.

If some external applications require RADIUS Accounting request (Start) information before they can process user packets, then the selected APN (GGSN) may be configured in such a way that the GGSN drops user data until the Accounting Response (START) is received from the AAA server. The GGSN may wait for the Accounting Response (START) before sending the CreatePDPContextResponse. The GGSN may reject the PDP context if the Accounting Response (START) is not received. The authentication and accounting servers may be separately configured for each APN.

When the GGSN receives a Delete PDP Context Request message and providing a RADIUS Accounting-Request START message was sent previously, the GGSN shall send a RADIUS Accounting-Request STOP message to the AAA server, which indicates the termination of this particular user session. The GGSN shall immediately send a Delete PDP context response, without waiting for an Accounting-Response STOP message from the AAA server.

The AAA server shall deallocate the IP address (if any) initially allocated to the subscriber, if there is no session for the subscriber.

Accounting-Request ON and Accounting-Request OFF messages may be sent from the GGSN to the AAA server to ensure the correct synchronization of the session information in the GGSN and the AAA server.

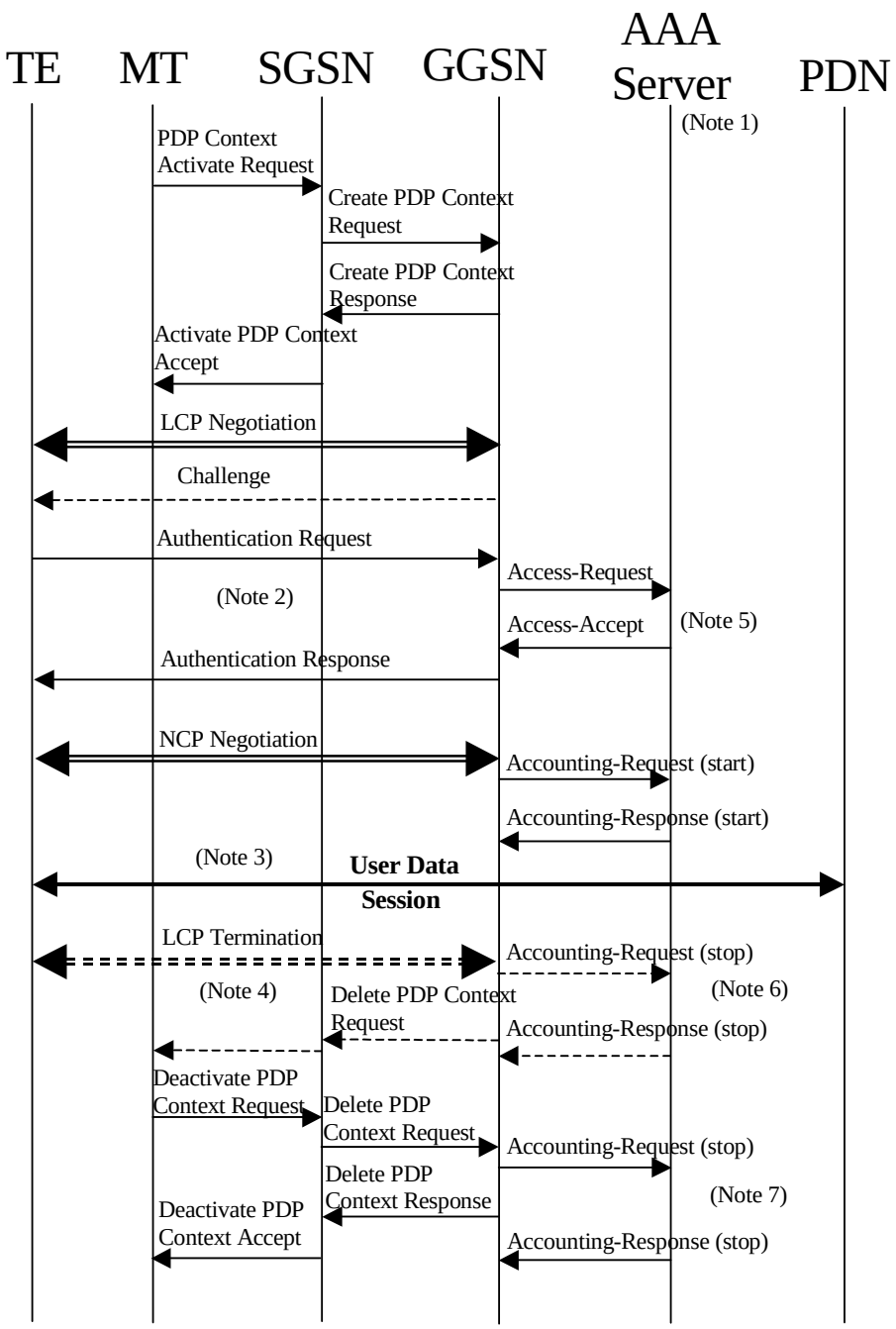
The GGSN may send an Accounting-Request ON message to the AAA server to indicate that a restart has occurred. The AAA server may then release the associated resources.

Prior to a scheduled restart, the GGSN may send Accounting-Request OFF message to the AAA server. The AAA server may then release the associated resources.

If an Access-Challenge is sent to the GGSN when an Access-Request message is pending and when IP PDP type is used, the GGSN shall silently discard the Access-Challenge message and it shall treat an Access-Challenge as though it had received an Access-Reject instead RFC 2865[23].

16.3.2 PPP PDP type

The figure 23 describes the RADIUS message flows between a GGSN and an Authentication, Authorization and Accounting (AAA) server for the case where PPP is terminated at the GGSN. ~~-~~The case where PPP is relayed to an LNS is beyond the scope of ~~this specification~~the present document.



NOTE 1: Separate accounting and Authentication servers may be used.
NOTE 2: Actual messages depend on the used authentication protocol (e.g. PAP, CHAP).
NOTE 3: If some external applications require RADIUS Accounting request (Start) information before they can process user packets, then the selected APN (GGSN) may be configured in such a way that the GGSN drops user data until the Accounting Response (START) is received from the AAA server. The GGSN may delete the PDP context if the Accounting Response (START) is not received.
NOTE 4: An LCP termination procedure may be performed. Either the MS or the GGSN may initiate the context deactivation.
NOTE 5: The Access-Request message shall be used for primary PDP context only.
NOTE 6: Network Initiated deactivation.
NOTE 7: User Initiated deactivation.

Figure 23: RADIUS message flow for PDP type PPP (successful user authentication case)

When a GGSN receives a Create PDP Context Request message for a given APN, the GGSN shall immediately send a Create PDP context response back to the SGSN. After PPP link setup, the authentication phase may take place. During Authentication phase, the GGSN sends a RADIUS Access-Request to an AAA server. The AAA server authenticates and authorizes the user. If RADIUS is also responsible for IP address allocation the AAA server shall return the allocated IP address in the Access-Accept message (if the user was authenticated).

If the user is not authenticated, the GGSN shall send a Delete PDP context request to the SGSN.

Even if the GGSN was not involved in user authentication (e.g. for PPP no authentication may be selected), it may send a RADIUS Accounting-Request START message to an AAA server. This message contains parameters, e.g. a tuple which includes the user-id and IP address, to be used by application servers (e.g. WAP gateway) in order to identify the user. This message also indicates to the AAA server that the user session has started, and the QoS parameters associated to the session.

If some external applications require RADIUS Accounting request (Start) information before they can process user packets, then the selected APN (GGSN) may be configured in such a way that the GGSN drops user data until the Accounting Response (START) is received from the AAA server. The GGSN may delete the PDP context if the Accounting Response (START) is not received. The Authentication and Accounting servers may be separately configured for each APN.

When the GGSN receives a Delete PDP Context Request message and providing a RADIUS Accounting-Request START message was sent previously, the GGSN shall send a RADIUS Accounting-Request STOP message to the AAA server, which indicates the termination of this particular user session. The GGSN shall immediately send a Delete PDP context response, without waiting for an Accounting-Response STOP message from the AAA server.

The AAA server shall deallocate the IP address (if any) initially allocated to the subscriber.

Accounting-Request ON and Accounting-Request OFF messages may be sent from the GGSN to the AAA server to ensure the correct synchronization of the session information in the GGSN and the AAA server.

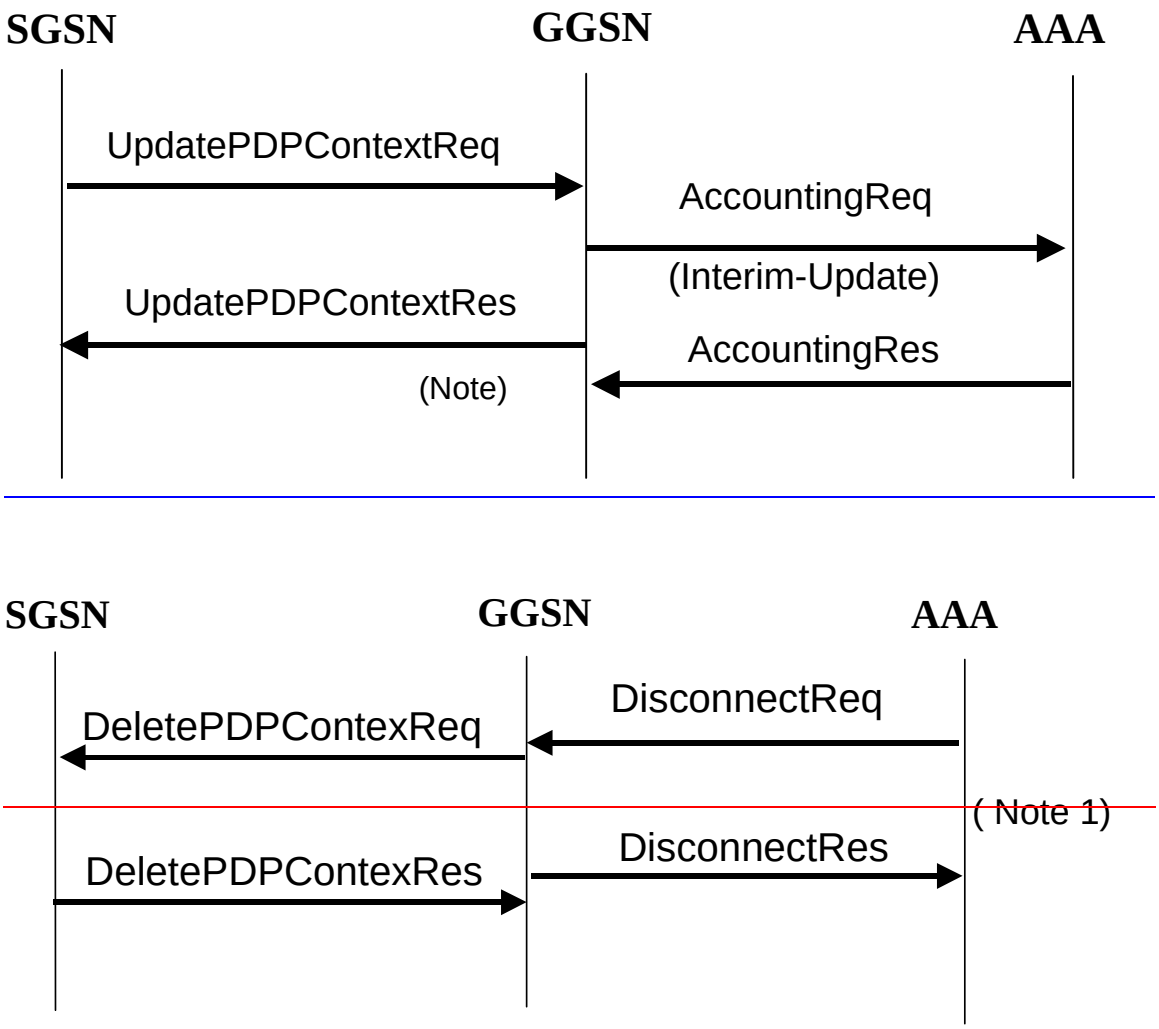
The GGSN may send an Accounting-Request ON message to the AAA server to indicate that a restart has occurred. The AAA server may then release the associated resources.

Prior to a scheduled restart, the GGSN may send Accounting-Request OFF message to the AAA server, the AAA server may then release the associated resources.

If an Access-Challenge is sent to the GGSN when using PPP PDP type, the GGSN shall handle it by PPP CHAP providing PPP CHAP was the selected Authentication protocol. If CHAP authentication was not selected, authentication shall fail RFC 2865[23].

16.3.3 Accounting Update

During the life of a PDP context some information related to this PDP context may change (i.e. SGSN address if a Inter-SGSN RA update occurs). Upon reception of an UpdatePDPContextRequest from the SGSN, the GGSN may send an Accounting Request Interim-Update to the AAA server to update the necessary information related to this PDP context (See figure 24). In such a case, the GGSN need not wait for the RADIUS AccountingResponse from the AAA server.

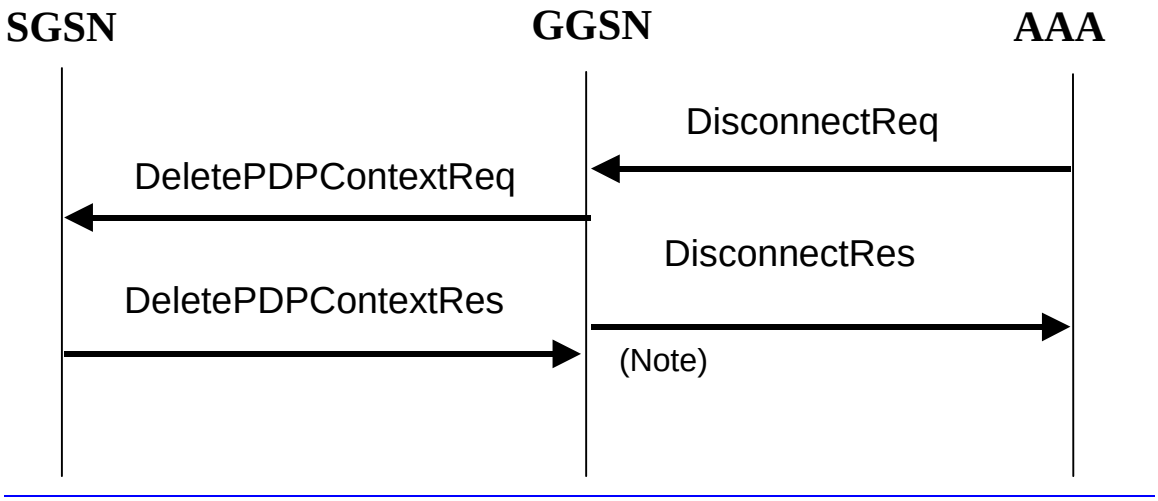


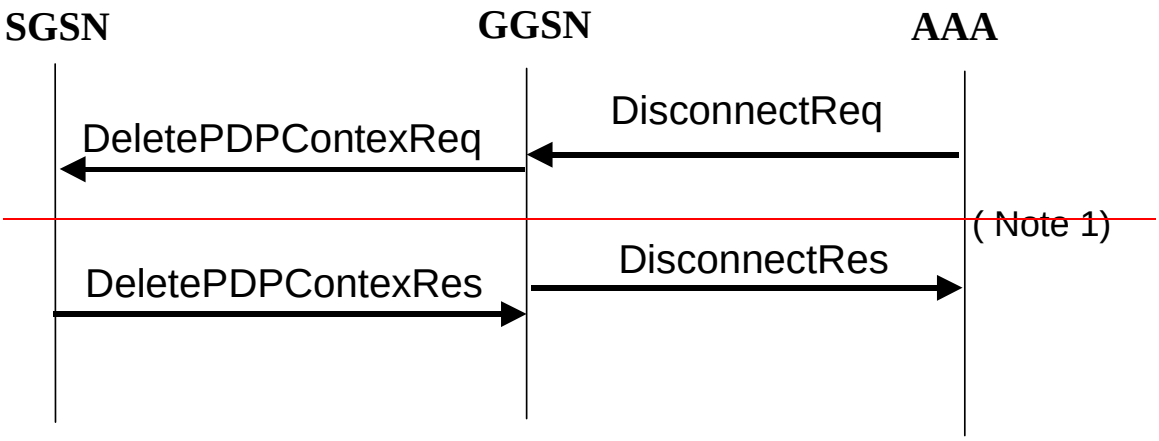
NOTE: As shown the GGSN need not wait for the RADIUS AccountingResponse from the AAA server message to send the UpdatePDPContextResponse to the SGSN. The GGSN may delete the PDP context if the AccountingResponse is not received from the AAA.

Figure 24: RADIUS for PDP context Update

16.3.4 AAA-Initiated PDP context termination

RADIUS is used as the protocol between the GGSN and a AAA server or proxy for applications (e.g. MMS) to deliver information related to GPRS user session. However some IP applications could need to interwork with the GGSN to terminate a particular PDP context. For this purpose, the AAA server or proxy may send a RADIUS Disconnect Request to the GGSN. As depicted in ~~Figure~~ figure 25, the GGSN may react by deleting the corresponding PDP context or silently discard the ~~Diconnect~~Disconnect Request message. For more information on RADIUS Disconnect, see RFC 2882[26]. If the GGSN deletes the corresponding PDP context, it need not wait for the DeletePDPContextResponse from the SGSN before sending the RADIUS DisconnectResponse to the AAA server.





N~~ote 1~~OTE:- As ~~showned~~showed on ~~F~~figure 25, the GGSN need not wait for the DeletePDPContextResponse from the SGSN to send the RADIUS DisconnectResponse to the AAA server.

Figure 25: PDP Context deletion with RADIUS

16.4 List of RADIUS attributes

The following tables describe the actual content of the RADIUS messages exchanged between the GGSN and the AAA server. Other RADIUS attributes may be used as defined in RADIUS RFC(s). Unless otherwise stated, when the encoding scheme of an attribute is specified as UTF-8 encoding, this shall be interpreted as UTF-8 hexadecimal encoding.

16.4.1 Access-Request message (sent from the GGSN to AAA server)

T~~he t~~able 1 describes the attributes of the Access-Request message.

Table 1: The attributes of the Access-Request message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username is provided by the user (extracted from the Protocol Configuration Options (PCO) field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used). If no username is available a generic username, configurable on a per APN basis, shall be present.	String	Mandatory
2	User-Password	User password provided by the user if PAP is used (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used). If no password is available a generic password, configurable on a per APN basis, shall be present.	String	Conditional Note 1
3	CHAP-Password	User password provided by the user if CHAP is used (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used).	String	Conditional Note 2
4	NAS-IP-Address	IP address of the GGSN for communication with the AAA server.	IPv4	Conditional Note 3
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 3
6	Service-Type	Indicates the type of service for this user	Framed	Optional
7	Framed-Protocol	Indicates the type of protocol for this user	7 (GPRS PDP Context)	Optional
8	Framed-IP-Address	IP address allocated for this user	IPv4	Conditional
9	Framed-IP-Netmask	Netmask for the user IP address	IPv4	Conditional
30	Called-Station-Id	Identifier for the target network	APN (UTF-8 encoded)	Mandatory
31	Calling-Station-Id	This attribute is the identifier for the MS, and it shall be configurable on a per APN basis.	MSISDN in international format according to 3GPP TS ~~23.003~~03.03 [25], UTF-8 encoded decimal. Note that there are no leading characters in front of the country code.	Optional
60	CHAP-Challenge	Challenge if CHAP is used (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used).	String	Conditional Note 2
61	NAS-Port-Type	Port type for the GGSN	As per RFC 2865 [23]	Optional
26/10415	3GPP Vendor-Specific	Sub-attributes according sub-clause 16.4.7	See sub-clause 16.4.7	Optional except sub-attribute 3 which is conditional
NOTE 1: Shall be present if PAP is used. NOTE 2: Shall be present if CHAP is used. NOTE 3: Either NAS-IP-Address or NAS-Identifier shall be present.				

16.4.2 Access-Accept (sent from AAA server to GGSN)

T~~he t~~able 2 describes the attributes of the Access-Accept message.

Table 2: The attributes of the Access-Accept message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username received in the Access-Request message or a substitute username provided by the AAA server. If the User-Name has been received in the Access-Accept message, this user-name shall be used in preference to the above	String	Optional
6	Service-Type	Indicates the type of service for this user	Framed	Optional
7	Framed-Protocol	Indicates the type of protocol for this user	7 (GPRS PDP Context)	Optional
8	Framed-IP-Address	IP address allocated for this user, if the AAA server is used to allocate IP address.	IPv4	Conditional
9	Framed-IP-Netmask	Netmask for the user IP address, if the AAA server is used to allocate IP netmask.	IPv4	Conditional
12	Framed-IP-MTU	MTU for the user towards this particular APN, MTU shall be less or equal to 1500	String	Optional
25	Class	Identifier to be used in all subsequent accounting messages.	String	Optional (~~NOTE~~ Note~~4~~)
27	Session-Timeout	Indicates the timeout value (in seconds) for the user session	32 bit unsigned Integer	Optional
28	Idle-Timeout	Indicates the timeout value (in seconds) for idle user session	32 bit unsigned Integer	Optional
26/311	MS- primary-DNS-server	Contains the primary DNS server address for this APN	Ipv4	Optional
26/311	MS-Secondary-DNS-Server	Contains the secondary DNS server address for this APN	IPv4	Optional
26/311	MS-Primary-NBNS-Server	Contains the primary NetBios name server address for this APN	IPv4	Optional
26/311	MS-Secondary-NBNS-Server	Contains the secondary NetBios server address for this APN	IPv4	Optional
NOTE ~~4~~: The presence of this attribute is conditional upon this attribute being received in the Access-Accept message.				

16.4.3 Accounting-Request START (sent from GGSN to AAA server)

T~~he t~~able 3 describes the attributes of the Accounting-Request START message.

Table 3: The attributes of the Accounting-Request START message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username provided by the user (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used). If no username is available a generic username, configurable on a per APN basis, shall be present. If the User-Name has been received in the Access-Accept message, this user-name shall be used in preference to the above	String	Optional
4	NAS-IP-Address	GGSN IP address for communication with the AAA server.	IPv4	Conditional Note 1~~3~~
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 1~~3~~
6	Service-Type	Indicates the type of service for this user	Framed	Optional
7	Framed Protocol	Indicates the type of protocol for this user	7 (GPRS PDP Context)	Optional
8	Framed-IP-Address	User IP address	IPv4	Mandatory
25	Class	Received in the access accept	String	Conditional (Note 2~~OTE 4~~)
30	Called-Station-Id	Identifier for the target network	APN (UTF-8 encoded)	Mandatory
31	Calling-Station-Id	This attribute is the identifier for the MS, and it shall be configurable on a per APN basis.	MSISDN in international format according to 3GPP TS ~~23.003~~03.03 [25], UTF-8 encoded decimal. Note that there are no leading characters in front of the country code.	Optional
40	Acct-Status-Type	Type of accounting message	START	Mandatory
41	Acct-Delay-Time	Indicates how many seconds the GGSN has been trying to send this record for, and can be subtracted from the time of arrival on the AAA server to find the approximate time (in seconds) of the event generating this Accounting-Request.	32 unsigned integer	Optional
44	Acct-Session-Id	User session identifier.	GGSN IP address and Charging-ID concatenated in a UTF-8 encoded hexadecimal. NOTE: The GGSN IP address is the same as that used in the GCDRs.	Mandatory
45	Acct-Authentic	Authentication method	RADIUS or LOCAL	Optional
61	NAS-Port-Type	Port type for the GGSN	As per RFC 2865 [23]	Optional
26/10415	3GPP Vendor-Specific	Sub-attributes according ~~sub-clause~~subclause 16.4.7.	See ~~sub-clause~~subclause 16.4.7	Optional except sub-attribute 3 which is

				conditional
NOTE 13: Either NAS-IP-Address or NAS-Identifier shall be present. NOTE 24: The presence of this attribute is conditional upon this attribute being received in the Access-Accept message.				

16.4.4 Accounting Request STOP (sent from GGSN to AAA server)

T~~he t~~able 4~~1~~ describes the attributes of the Accounting-Request STOP message.

Table 4: The attributes of the Accounting-Request STOP message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username provided by the user (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used). If no username is available a generic username, configurable on a per APN basis, shall be present. If the User-Name has been received in the Access-Accept message, this user-name shall be used in preference to the above	String	Optional
4	NAS-IP-Address	IP address of the GGSN for communication with the AAA server.	IPv4	Conditional Note 1~~3~~
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 1~~3~~
6	Service-Type	Indicates the type of service for this user	Framed	Optional
7	Framed Protocol	Indicates the type of protocol for this user	7 (GPRS PDP Context)	Optional
8	Framed-IP-Address	User IP address	IPv4	Mandatory
25	Class	Received in the access accept	String	Optional ~~-~~(Note 2~~OTE 4~~)
30	Called-Station-Id	Identifier for the target network	APN (UTF-8 encoded)	Mandatory
31	Calling-Station-Id	This attribute is the identifier for the MS, and it shall be configurable on a per APN basis.	MSISDN in international format according to 3GPP TS ~~23.003~~03.03 [25], UTF-8 encoded. Note that there are no leading characters in front of the country code.	Optional
40	Acct-Status-Type	Indicates the type of accounting request	STOP	Mandatory
41	Acct-Delay-Time	Indicates how many seconds the GGSN has been trying to send this record for, and can be subtracted from the time of arrival on the AAA server to find the approximate time of the event generating this Accounting-Request	Second	Optional
42	Acct-Input-Octets	GGSN counted number of octets sent by the user for the PDP context	32 bit unsigned integer	Optional
43	Acct-Output-Octets	GGSN counted number of octets received by the user for the PDP context	32 bit unsigned integer	Optional
44	Acct-Session-Id	User session identifier.	GGSN IP address and Charging-ID concatenated in a UTF-8 encoded hexadecimal. NOTE: The GGSN IP address is the same as that used in the GCDRs.	Mandatory
45	Acct-Authentic	Authentication method	RADIUS or LOCAL	Optional
46	Acct-Session-Time	Duration of the session	Second	Optional
47	Acct-Input-Packets	GGSN counted number of packets sent by the user	Packet	Optional
48	Acct-Output-Packets	GGSN counted number of packets received by the user	Packet	Optional
49	Acct-Terminate-Cause	Indicate how the session was terminated	See RFC 2866 [24]	Optional

Attr #	Attribute Name	Description	Content	Presence Requirement
61	NAS-Port-Type	Port type for the GGSN	As per RFC 2865 [23]	Optional
26/104 15	3GPP Vendor-Specific	Sub-attributes according to ~~sub-clause~~subclause 16.4.7.	See ~~sub-clause~~subclause 16.4.7	Optional except sub-attribute 3 which is conditional
NOTE 1~~3~~: Either NAS-IP-Address or NAS-Identifier shall be present. NOTE 2~~4~~: The presence of this attribute is conditional upon this attribute being received in the Access-Accept message.				

16.4.5 Accounting Request ON (optionally sent from GGSN to AAA server)

The table 5 describes the attributes of the Accounting-Request ON message.

Table 5: The attributes of the Accounting-Request ON message

Attr #	Attribute Name	Description	Content	Presence Requirement
4	NAS-IP-Address	IP address of the GGSN for communication with the AAA server.	IPv4	Conditional Note 3
30	Called-Station-ID	Identifier for the target network.	APN (UTF-8 encoded)	Optional
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 3
NOTE 3: Either NAS-IP-Address or NAS-Identifier shall be present.				

16.4.6 Accounting Request OFF (optionally sent from GGSN to AAA server)

The table 6 describes the attributes of the Accounting-Request OFF message.

Table 6: The attributes of the Accounting-Request OFF message

Attr #	Attribute Name	Description	Content	Presence Requirement
4	NAS-IP-Address	IP address of the GGSN for communication with the AAA server.	IPv4	Conditional Note 3
30	Called-Station-ID	Identifier for the target network.	APN (UTF-8 encoded)	Optional
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 3
NOTE 3: Either NAS-IP-Address or NAS-Identifier shall be present.				

16.4.7 Sub-attributes of the 3GPP Vendor-Specific attribute

The table 7 describes the sub-attributes of the 3GPP Vendor-Specific attribute of the Access-Request, Accounting-Request START, Accounting-Request STOP and Accounting-Request Interim-Update messages.

Table 7: The sub-attributes of the 3GPP Vendor-Specific attribute of the Access-Request, Accounting-Request START, Accounting-Request STOP and Accounting-Request Interim-Update messages

Sub-attr #	Sub-attribute Name	Description	Presence Requirement	Associated attribute (Location of Sub-attr)
1	3GPP-IMSI	IMSI for this user	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
2	3GPP-Charging-Id	Charging ID for this PDP Context (this together with the GGSN-Address constitutes a unique identifier for the PDP context).	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
3	3GPP-PDP Type	Type of PDP context, e.g. IP or PPP	Conditional (mandatory if attribute 7 is present)	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
4	3GPP-CG-Address	Charging Gateway IP address	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
5	3GPP-GPRS-Negotiated-QoS-Profile	QoS profile applied by GGSN	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
6	3GPP-SGSN-Address	SGSN IP address that is used by the GTP control plane for the handling of control messages. It may be used to identify the PLMN to which the user is attached.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
7	3GPP-GGSN-Address	GGSN IP address that is used by the GTP control plane for the context establishment. It is the same as the GGSN IP address used in the GCDRs.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
8	3GPP-IMSI-MCC-MNC	MCC and MNC extracted from the user's IMSI (first 5 or 6 digits, as applicable from the presented IMSI).	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
9	3GPP-GGSN- MCC-MNC	MCC-MNC of the network the GGSN belongs to.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
10	3GPP-NSAPI	Identifies a particular PDP context for the associated PDN and MSISDN/IMSI from creation to deletion.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP Accounting-Request Interim-Update
11	3GPP- Session-Stop-Indicator	Indicates to the AAA server that the last PDP context of a session is released and that the PDP	Optional	Accounting Request STOP

Sub-attr #	Sub-attribute Name	Description	Presence Requirement	Associated attribute (Location of Sub-attr)
		session has been terminated.		
12	3GPP- Selection-Mode	Contains the Selection mode for this PDP Context received in the Create PDP Context Request Message	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
18	3GPP-SGSN-MCC-MNC	MCC and MNC extracted from the RAI within the Create PDP Context Request or Update PDP Context Request message.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update

The RADIUS vendor Attribute is encoded as follows (as per RFC 2865 [23]).

Bits

Octets	8	7	6	5	4	3	2	1
1	Type = 26							
2	Length = n							
3	Vendor id octet 1							
4	Vendor id octet 2							
5	Vendor id octet 3							
6	Vendor id octet 4							
7-n	String							

n ≥ ~~>=~~7

3GPP Vendor Id = 10 415

The string part is encoded as follows:

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type =							
2	3GPP Length = m							
3 –m	3GPP value							

m ≥ ~~>=~~2 and m ≤ ~~<=~~ 248

The 3GPP specific attributes encoding is clarified below.

1 **-** 3GPP-***IMSI***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 1							
2	3GPP Length= m							
3-m	IMSI digits 1-n (UTF-8 encoded)							

3GPP Type: 1

n ≤ ~~<=~~15

Length: m =17

IMSI value: Text:

This is the UTF-8 encoded IMSI; The definition of IMSI shall be in accordance with 3GPP TS 03.03 [25] and 3GPP TS 09.60 [33]~~[26]~~. There shall be no padding characters between the MCC and MNC, and between the MNC and MSIN. If the IMSI is less than 15 digits, the padding in the GTP information element shall be removed by the GGSN and not encoded in this sub-attribute.

2 - 3GPP-***Charging ID***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 2							
2	3GPP Length= 6							
3	Charging ID value Octet 1							
4	Charging ID value Octet 2							
5	Charging ID value Octet 3							
6	Charging ID value Octet 4							

3GPP Type: 2

Length: 6

Charging ID value: 32 bits unsigned integer

3- 3GPP-***PDP type***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 3							
2	3GPP Length= 6							
3	PDP type octet 1							
4	PDP type octet 2							
5	PDP type octet 3							
6	PDP type octet 4							

3GPP Type: 3

Length: 6

PDP type value: Unsigned 32 bits integer

PDP type octet possible values:

0 = IP

1 = PPP

4 - 3GPP-***Charging Gateway address***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 4							
2	3GPP Length= 6							
3	Charging GW addr Octet 1							
4	Charging GW addr Octet 2							
5	Charging GW addr Octet 3							
6	Charging GW addr Octet 4							

3GPP Type: 4

Length: 6

Charging GW address value:- Address

5 - 3GPP-***GPRS Negotiated QoS profile***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 5							
2	3GPP Length= L							
3 -L	UTF-8 encoded QoS profile							

3GPP Type: 5

Length: -27 (release 99) or 11 (release 98)

QoS profile value: -Text

UTF-8 encoded QoS profile syntax:

"<Release indicator> – <release specific QoS IE UTF-8 encoding>"

<Release indicator> = UTF-8 encoded number :

"98" = Release 98

"99"= Release 99

<release specific QoS profile UTF-8 encoding> = UTF-8 encoded QoS profile for the release indicated by the release indicator.

The UTF-8 encoding of a QoS IE is defined as follows: each octet is described by 2 UTF-8 encoded digits, defining its hexadecimal representation. The QoS profile definition is in 3GPP TS ~~24.008~~04.08 [32].

The release 98 QoS profile data is 3 octets long, which then results in a 6 octets UTF-8 encoded string,

The release 99 QoS profile data is 11 octets long, which results in a 22 octets UTF-8 encoded string.

6 - 3GPP-***SGSN address***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 6							
2	3GPP Length= 6							
3	SGSN addr Octet 1							
4	SGSN addr Octet 2							
5	SGSN addr Octet 3							
6	SGSN addr Octet 4							

3GPP Type: 6

Length: 6

SGSN address value: -Address

7 -- 3GPP-***GGSN address***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 7							
2	3GPP Length= 6							
3	GGSN addr Octet 1							
4	GGSN addr Octet 2							
5	GGSN addr Octet 3							
6	GGSN addr Octet 4							

3GPP Type: 7

Length: 6

GGSN address value: -Address

8 - 3GPP-***IMSI MCC-MNC***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 8							
2	3GPP Length= n							
3	MCC digit1 (UTF-8 encoded)							
4	MCC digit2 (UTF-8 encoded)							
5	MCC digit3 (UTF-8 encoded)							
6	MNC digit1 (UTF-8 encoded)							
7	MNC digit2 (UTF-8 encoded)							
8	MNC digit3 if present (UTF-8 encoded)							

3GPP Type: 8

Length: n shall be 7 or 8 octets depending on the presence of MNC digit 3

MS address value: -text

This is the UTF-8 encoding of the MS MCC-MNC values. In accordance with 3GPP TS 03.03 [25] and 3GPP TS 09.60 [33][26] the MCC shall be 3 digits and the MNC shall be either 2 or 3 digits. There shall be no padding characters between the MCC and MNC.

9 - 3GPP-***GGSN MCC-MNC***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 9							
2	3GPP Length= n							
3	MCC digit1 (UTF-8 encoded)							
4	MCC digit2 (UTF-8 encoded)							
5	MCC digit3 (UTF-8 encoded)							
6	MNC digit1 (UTF-8 encoded)							
7	MNC digit2 (UTF-8 encoded)							
8	MNC digit3 if present (UTF-8 encoded)							

3GPP Type: 9

Length: n shall be 7 or 8 octets depending on the presence of MNC digit 3

GGSN address value:- text

This is the UTF-8 encoding of the GGSN MCC-MNC values. In accordance with 3GPP TS 03.03 [25] and 3GPP TS 09.60 [33]~~[26]~~ the MCC shall be 3 digits and the MNC shall be either 2 or 3 digits. There shall be no padding characters between the MCC and MNC.

10 - 3GPP-***NSAPI***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 10							
2	3GPP Length= 3							
3	NSAPI							

3GPP Type: 10

Length: 3

NSAPI value: text

It is the value of the NSAPI of the PDP context the RADIUS message is related to. It is encoded as its hexadecimal representation, using 1UTF-8 encoded digit.

11 - 3GPP-***Session Stop Indicator***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 11							
2	3GPP Length= 3							
3	1 1 1 1 1 1 1 1							

3GPP Type: 11

Length: -3

Value is set to all 1.

12 - 3GPP-***Selection-Mode***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 12							
2	3GPP Length= 1							
3	UTF-8 encoded Selection mode string							

3GPP Type: 12

Length: ~~-~~3

Selection mode value: Text

The format of this attribute shall be a character string consisting of a single digit, mapping from the binary value of the selection mode in the Create PDP Context message (3GPP TS 09.60 [33~~24~~]). Where 3GPP TS ~~29.060~~09.60 provides for interpretation of the value, e.g. map ~~"~~'3~~"~~' to ~~"~~'2~~"~~', this shall be done by the GGSN.

18 - 3GPP-SGSN ***MCC-MNC***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 18							
2	3GPP Length= n							
3	MCC digit1 (UTF-8 encoded)							
4	MCC digit2 (UTF-8 encoded)							
5	MCC digit3 (UTF-8 encoded)							
6	MNC digit1 (UTF-8 encoded)							
7	MNC digit2 (UTF-8 encoded)							
8	MNC digit3 if present (UTF-8 encoded)							

3GPP Type: 18

Length: n shall be 7 or 8 octets depending on the presence of MNC digit 3

SGSN address value: ~~-~~text

This is the UTF-8 encoding of the RAI MCC-MNC values. In accordance with 3GPP TS 03.03 [25] and 3GPP TS 09.60 [33]~~[24] and [41]~~ the MCC shall be 3 digits and the MNC shall be either 2 or 3 digits. There shall be no padding characters between the MCC and MNC.

16.4.8 Accounting Request Interim-Update (sent from GGSN to AAA server)

T~~he t~~able 8 describes the attributes of the Accounting-Request Interim-Update message.

Table 8: The attributes of the Accounting-Request Interim-Update message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username provided by the user (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used). If no username is available a generic username, configurable on a per APN basis, shall be present. If the User-Name has been received in the Access-Accept message, this user-name shall be used in preference to the above	String	Optional
4	NAS-IP-Address	IP address of the GGSN for communication with the AAA server.	IPv4	Conditional Note 13
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 13
6	Service-Type	Indicates the type of service for this user	Framed	Optional
7	Framed Protocol	Indicates the type of protocol for this user	7 (GPRS PDP Context)	Optional
8	Framed-IP-Address	User IP address	IPv4	Mandatory
25	Class	Received in the access accept	String	Optional (Note 2)
30	Called-Station-Id	Identifier for the target network	APN (UTF-8 encoded)	Mandatory
31	Calling-Station-Id	This attribute is the identifier for the MS, and it shall be configurable on a per APN basis.	MSISDN in international format according to 3GPP TS 23.00303.03 [25], UTF-8 encoded. Note that there are no leading characters in front of the country code.	Optional
40	Acct-Status-Type	Indicates the type of accounting request	Interim-Update	Mandatory
41	Acct-Delay-Time	Indicates how many seconds the GGSN has been trying to send this record for, and can be subtracted from the time of arrival on the AAA server to find the approximate time of the event generating this Accounting-Request	Second	Optional
42	Acct-Input-Octets	GGSN counted number of octets sent by the user for the PDP context	32 bit unsigned integer	Optional
43	Acct-Output-Octets	GGSN counted number of octets received by the user for the PDP context	32 bit unsigned integer	Optional
44	Acct-Session-Id	User session identifier.	GGSN IP address and Charging-ID concatenated in a UTF-8 encoded hexadecimal. NOTE: The GGSN IP address is the same as that used in the GCDRs.(Note 3)	Mandatory
45	Acct-Authentic	Authentication method	RADIUS or LOCAL	Optional

Attr #	Attribute Name	Description	Content	Presence Requirement
46	Acct-Session-Time	Duration of the session	Second	Optional
47	Acct-Input-Packets	GGSN counted number of packets sent by the user	Packet	Optional
48	Acct-Output-Packets	GGSN counted number of packets received by the user	Packet	Optional
61	NAS-Port-Type	Port type for the GGSN	As per RFC 2865 [23]	Optional
26/10415	3GPP Vendor-Specific	Sub-attributes according to ~~sub-clause~~subclause 16.4.7.	See ~~sub-clause~~subclause 16.4.7	Optional except sub-attribute 3 which is conditional
NOTE 1~~3~~: Either NAS-IP-Address or NAS-Identifier shall be present. NOTE 2~~4~~: The presence of this attribute is conditional upon this attribute being received in the Access-Accept message. NOTE 3: The GGSN IP address is the same as that used in the GCDRs.				

16.4.9 Disconnect Request (optionally sent from AAA server to GGSN)

T~~he t~~able 9 describes the attributes of the Disconnect-Request message.

Table 9: The attributes of the Disconnect-Request message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username provided by the user (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used). If no username is available a generic username, configurable on a per APN basis, shall be present. If the User-Name has been sent in the Access-Accept message, this user-name shall be used in preference to the above	String	Optional
8	Framed-IP-Address	User IP address	IPv4	Mandatory
44	Acct-Session-Id	User session identifier.	GGSN IP address and Charging-ID concatenated in a UTF-8 encoded hexadecimal. (Note) ~~NOTE: The GGSN IP address is the same as that used in the GCDRs.~~	Mandatory
NOTE: The GGSN IP address is the same as that used in the GCDRs.				

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~~ subclause 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~~the present document.

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

A.3.1 General

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

GPRS shall support both ITU-T Recommendation X.121 and ITU-T Recommendation E.164 addressing.

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

The GPRS TE's shall have addresses provided, and controlled, by their GPRS operator. The PSDN TE sends data to the GPRS TE by use of that TE's GPRS 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 GSM GPRS 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~~ A.2 shows the interconnecting protocol stacks to the GPRS bearer. The GPRS bearer is described in 3GPP TS 07.60 [10], which uses the protocols described in 3GPP TS 03.60 [3].

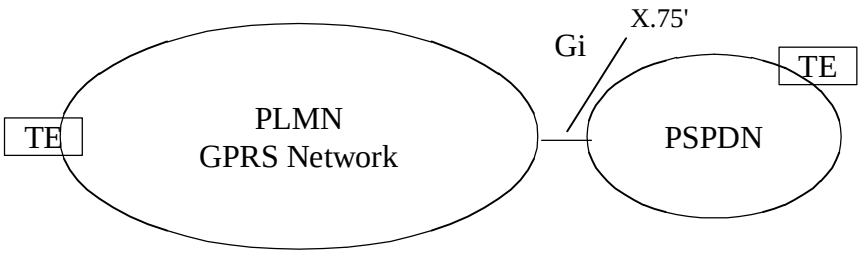


Figure A.1: PSPDN Interworking with X.75' at Gi Reference Point

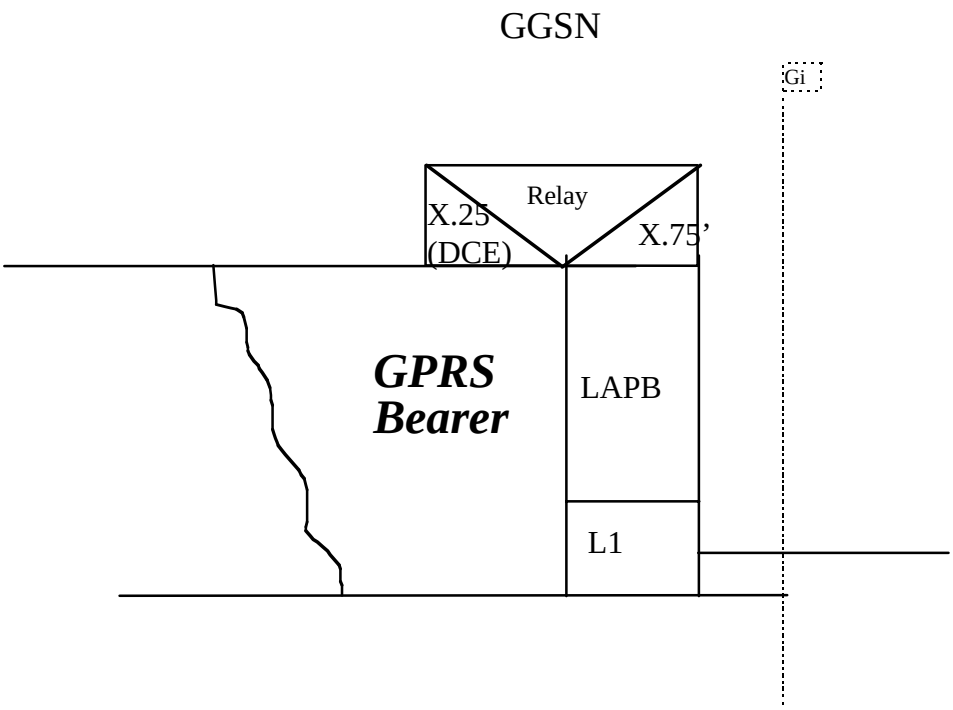


Figure A.2: The Protocol Stack for the X.75' Gi Reference Point

A.3.3 Numbering and Addressing

A PLMN GPRS network 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~~ subclause 10.3 in the main part of th~~is specification~~e present document.

A.3.6 The GPRS Interworking to PSDN Characteristics

These are the same as in subclause~~ection~~ 10.4 in the main part of the present document~~is specification~~.

Annex B (informative): Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
	s25	98-0101	A001		Access to an Intranet or ISP through GPRS	5.0.0	6.0.0
	s26	98-0292	A002		Authentication protocol when accessing an intranet or ISP through GPRS	6.0.0	6.1.0
	s26	98-0292	A003		Clarifications to Intranet/ISP Interworking section	6.0.0	6.1.0
	s26	98-0292	A004		Architecture Diagrams	6.0.0	6.1.0
	s26	98-0292	A005		Editorial review of 09.61	6.0.0	6.1.0
	s26				Correction of Word 95/97 problem (incomplete incorporation of CR A003 into V6.1.0)	6.1.0	6.2.0
	s27	98-0735	A006		Protocol Configuration Options at PDP context activation failure	6.2.0	6.3.0
	s27	98-0735	A008		Clarifications on IP interworking	6.2.0	6.3.0
	s28	99-0062	A011		X.75' interface specifications at GGSN-PSPDN (Gi) interface	6.3.0	7.0.0
	s29	99-0058	A012		Access to PDNs and ISPs with the PDP-type PPP	7.0.0	7.1.0
	s29	99-0058	A013		GPRS Internet Hosted Octet Stream Service (IHOSS)	7.0.0	7.1.0
	TSG#6	NP-99431	A015		ICPC ~~negotiations~~negotiations for interworking at the Mtfor NT IP	7.1.0	7.2.0
03-2001	TSG#11	NP-010044	A016		Removal of IHOSS and OSP	7.2.0	7.3.0
09-2001	TSG#13	NP-010530	A018	2	Standard method for information delivery (MSISDN; IP address…) between GPRS and external PDN using RADIUS	7.3.0	7.4.0
12-2001	TSG#14	NP-010572	A022	1	Correction to the Calling-Station-Id attribute	7.4.0	7.5.0
12-2001	TSG#14	NP-010572	A024	1	Correction to 3GPP Vendor specify attribute 3GPP-IMSI	7.4.0	7.5.0
12-2001	TSG#14	NP-010572	A026		Correction to 3GPP vendor specific attributes containing MCC-MNC	7.4.0	7.5.0
12-2001	TSG#14	NP-010672	A028		Standard method for information update between GPRS and external PDN using RADIUS	7.4.0	7.5.0
12-2001	TSG#14	NP-010672	A029		Standard method for interworking between GPRS and external PDN using RADIUS	7.4.0	7.5.0
03-2002	TSG#15	NP-020080	A032		Change of associated attribute for 3GPP-NSAPI	7.5.0	7.6.0
06-2002	TSG#16	NP-020295	A036		Corrections to the 3GPP RADIUS attributes	7.6.0	7.7.0
06-2002	TSG#16	NP-020295	A038	1	Clarification on the Radius Flows	7.6.0	7.7.0
12-2002	TSG#18	NP-020613	A040	1	RADIUS enhancement for identification of VPLMN	7.7.0	7.8.0

3GPP TSG-CN WG3 Meeting #27
Dublin, Ireland, 10th - 14th February 2003.

Tdoc ⌘N3-030122

CR-Form-v7

CHANGE REQUEST

⌘ **29.061** **CR** **081** ⌘**rev** **1** ⌘ Current version: **3.11.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	Correction of References and specification Corrections
Source:	⌘	TSG_CN WG3 *[Siemens AG, MCC]*
Work item code:	⌘	TEI
Date:	⌘	11/02/2003
Category:	⌘	**A**
Release:	⌘	R99

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Inconsistencies in the specification, Missing and incorrect references
Summary of change:	⌘	Correction of incorrect and missing reference and general specification clean-up
Consequences if not approved:	⌘	Inconsistencies and errors in the referencing. Possible misunderstanding when reading specification.

Clauses affected:	⌘	Most of the specification			
Other specs affected:	⌘	**Y**	**N**		
			X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

3GPP TS 29.061 V3.11.0 (2002-12)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Core Network; ~~Packet Domain;~~ Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and ~~-~~Packet Data Networks (PDN) (Release 1999)

Keywords

UMTS, GSM, packet mode, interworking, PLMN, PDN

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

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. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

~~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: "Abbreviations and acronyms".

[2] 3GPP TS 22.060: "General Packet Radio Service (GPRS)~~:~~ Service Description; Stage 1~~ Service Description~~".

[3] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service Description; Stage 2".

[4] 3GPP TS 03.61: "General Packet Radio Service (GPRS); ~~Point~~ Point-to-Multipoint Multicast Service Description; Stage 2".

[5] 3GPP TS 03.62: "General Packet Radio Service (GPRS); Point-to-Multipoint Group Call Service Description; Stage 2".

[6] 3GPP TS 03.64: "General Packet Radio Service (GPRS); Overall description of the GPRS radio interface; Stage 2~~Overall description of the Radio interface; Stage 2~~".

[7] 3GPP TS 04.60: "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: "General Packet Radio Service (GPRS); Mobile Station - Serving GPRS Support Node (MS-SGSN) Logical Link Control (LLC) layer specification~~Logical Link Control (LLC)~~".

[9] 3GPP TS 24.065: "General Packet Radio Service (GPRS); Mobile Station (MS) - Serving GPRS Support Node (SGSN); Subnetwork Dependent Convergence Protocol (SNDCP)".

[10] 3GPP TS 27.060: "Packet Domain; Mobile Station (MS) supporting Packet Switched Services".

[11] ITU-T Recommendation E.164: "The international public telecommunication numbering plan~~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~~ names - ~~Concepts~~ concepts and ~~Facilities~~facilities" (STD 7).

[20] Void.

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

[21b] IETF RFC 1662 (1994): "PPP in HDLC-like Framing" (STD 51).

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

[23] 3GPP TS 24.008: "Mobile radio interface layer 3 specification; Core Network ~~Protocols~~protocols; ~~–~~ Stage 3".

[24] 3GPP TS 29.060: "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp ~~Interface~~interface".

[25] IETF RFC 2794 (2000)~~, Pat R. Calhoun and Charles E. Perkins~~: "Mobile IP Network ~~Address~~ Access Identifier Extension for IPv4", P. Calhoun, C. Perkins~~March 2000~~.

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

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

[28] IETF RFC 2373 (1998): "IP V~~v~~ersion 6 Addressing Architecture".

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

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

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

[32] IETF RFC 1112 (1989)~~, S.E. Deering~~: "Host extensions for IP multicasting", S.E. Deering.

[33] IETF RFC 2236 (1997)~~, W. Fenner~~: "Internet Group Management Protocol, Version 2", W. Fenner.

[34] IETF RFC 2362 (1998)~~, D. Estrin and al~~: "Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification", D. Estrin, D. Farinacci, A. Helmy, D. Thaler, S. Deering, M. Handley, V. Jacobson, C. Liu, P. Sharma, L. Wei.

[35] IETF RFC 1075 (1988)~~, D. Waitzman and al~~: "Distance Vector Multicast Routing Protocol", D. Waitzman, C. Partridge, S.E. Deering.

[36] IETF RFC 1585 (1994)~~, J. Moy~~: "MOSPF: Analysis and Experience", J. Moy~~.~~.

[37] IETF RFC 2290 (1998)~~, J. Solomon, S. Glass~~: "Mobile-IPv4 Configuration Option for PPP IPCP ", J. Solomon, S. Glass.

[38] IETF RFC 2865 (2000)~~, C. Rigney, S. Willens, A. Rubens, W. Simpson~~: "Remote Authentication Dial In User Service (RADIUS)", C. Rigney, S. Willens, A. Rubens, W. Simpson.

[39] IETF RFC 2866 (2000)~~:, C. Rigney, Livingston:~~ "~~-~~RADIUS Accounting~~-~~", C. Rigney, Livingston.

[40] 3GPP TS 23.003: "~~Network; -~~Numbering, addressing and identification".

[41] IETF RFC 2882 (2000)~~, D. Mitton~~: "Network Access Servers Requirements: Extended RADIUS Practices", D. Mitton.

[42] 3GPP TR 21.905: "~~-~~Vocabulary for 3GPP Specifications".

[43] IETF RFC 2472 (1998)~~, D. Haskins, E. Allen~~: ~~"~~"IP Version 6 over PPP~~"~~", D. Haskins, E. Allen.

[44] IETF RFC 2461 (1998)~~, T. Narten, E. Nordmark, W. Simpson~~: ~~"~~"Neighbor Discovery for IP Version 6 (IPv6)~~"~~", T. Narten, E. Nordmark, W. Simpson~~-~~.

[45] IETF RFC 3118 (2001)~~, R. Droms, W. Arbaugh~~: ~~"~~"Authentication for DHCP Messages~~"~~", R. Droms, W. Arbaugh.

[46] IETF Internet-Draft: ~~"~~"Dynamic Host Configuration Protocol for IPv6 (DHCPv6)~~"~~", draft-ietf-dhc-dhcpv6-~~24~~28.txt, work in progress.

[47] 3GPP TS 24.229: ~~"~~"IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3~~"~~".

[48] IETF RFC 2710 (1999)~~, S. Deering, W. Fenner, B. Haberman~~: ~~"~~"Multicast Listener Discovery (MLD) for IPv6~~"~~", S. Deering, W. Fenner, B. Haberman.

[49] IETF RFC 2460 (1998)~~, S.Deering,, R.Hinden~~: ~~"~~"Internet Protocol, Version 6 (IPv6) Specification~~"~~", S.Deering,, R.Hinden.

[50] IETF RFC 3162 (2001)~~, B. Adoba, G. Zorn, D. Mitton~~: ~~"~~"RADIUS and IPv6~~"~~", B. Adoba, G. Zorn, D. Mitton.

[51] IETF RFC 2548 (1999)~~, G.Zorn~~: ~~"~~"Microsoft Vendor-specific RADIUS Attributes~~"~~", G.Zorn.

[52] IETF RFC 1035 (1987): "Domain names - implementation and specification".

[53] IETF RFC 1771 (1995): "A Border Gateway Protocol 4 (BGP-4)".

[54] IETF RFC 1825 (1995): "Security Architecture for the Internet Protocol".

[55] IETF RFC 1826 (1995): "IP Authentication Header".

[56] IETF RFC 1827 (1995): "IP Encapsulating Security Payload (ESP)".

3 Definitions, abbreviations and symbols

3.1 Definitions

For the purposes of the present document, the ~~following~~ terms and definitions given in 3GPP TS 22.060 [2] and 3GPP TS ~~-~~23.060 [3], 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
DHCPv6	Dynamic Host Configuration Protocol version 6
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
IPCP	IP Control Protocol (PPP NCP for IPv4)
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPV6CP	IPv6 Control Protocol (PPP NCP for IPv6)
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
LAC	L2TP Access Concentrator
LAN	Local Area Network
LNS	L2TP Network Server
MIP	Mobile IP
MLD	Multicast Listener Discovery
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 Independent 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 [2] and 3GPP TS 23.060 [3].

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 [40] 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.

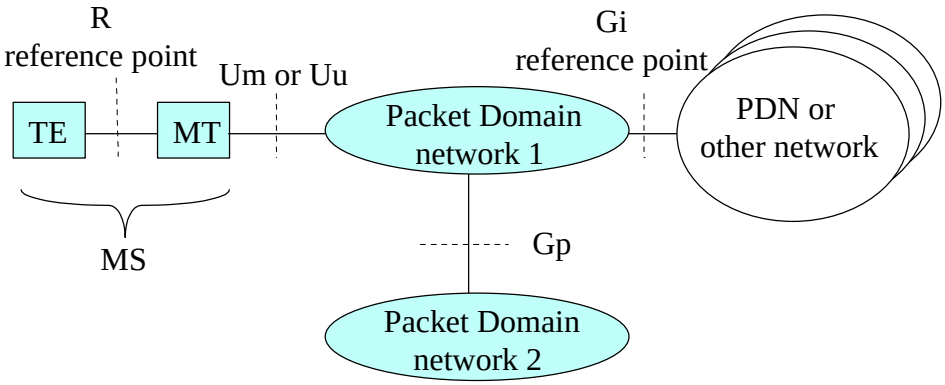


Figure 1: Packet Domain Access Interfaces and Reference Points

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 [3].

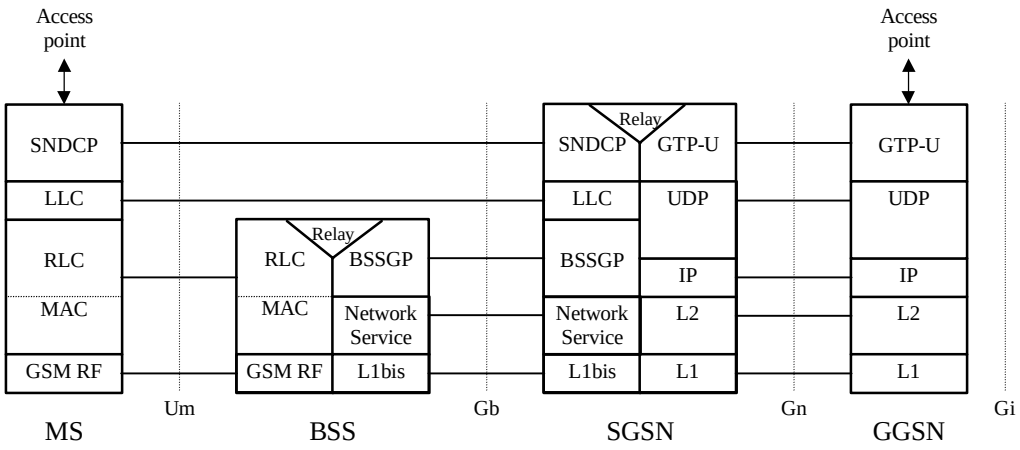


Figure 2a: User Plane for Packet Domain services in GSM

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 [3].

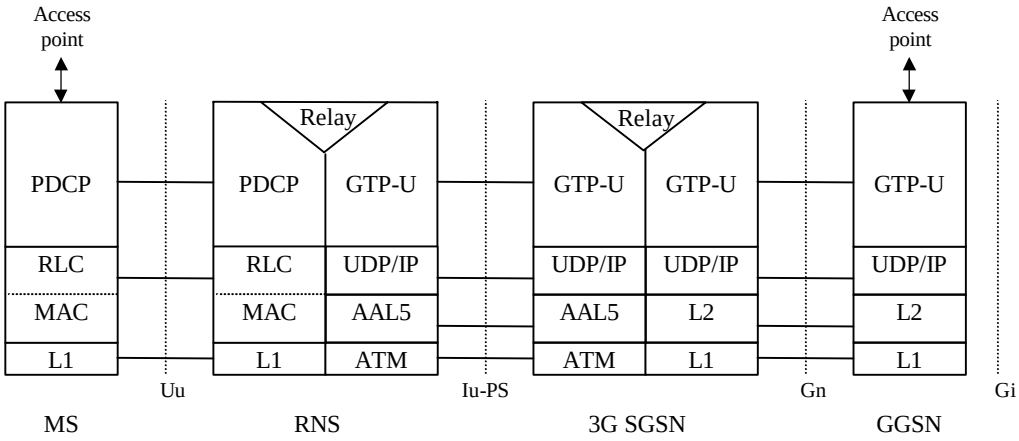


Figure 2b: User Plane for Packet Domain services in UMTS

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 [3]. 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 [2] and 3GPP TS 23.060 [3]. 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>~~**Figure 3: Void**

Figure 4: Void

Figure 5: Void

Figure 6: 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~~IPv6. The interworking point with IP networks is at the Gi reference point as shown in figure 7.

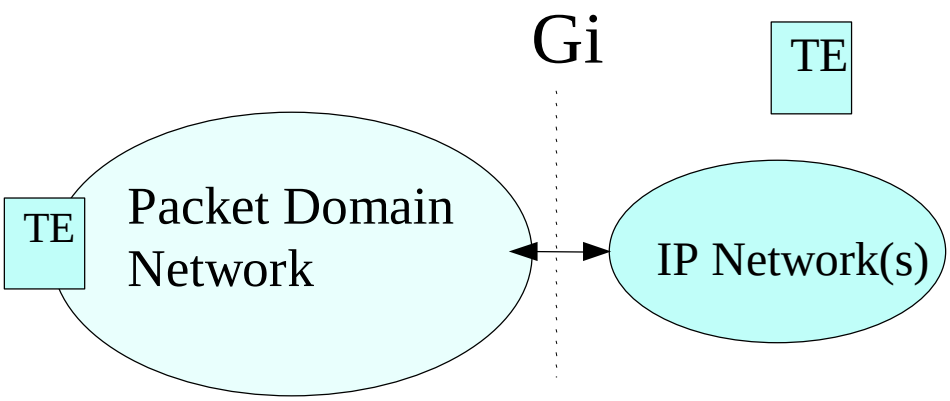


Figure 7: IP network interworking

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.

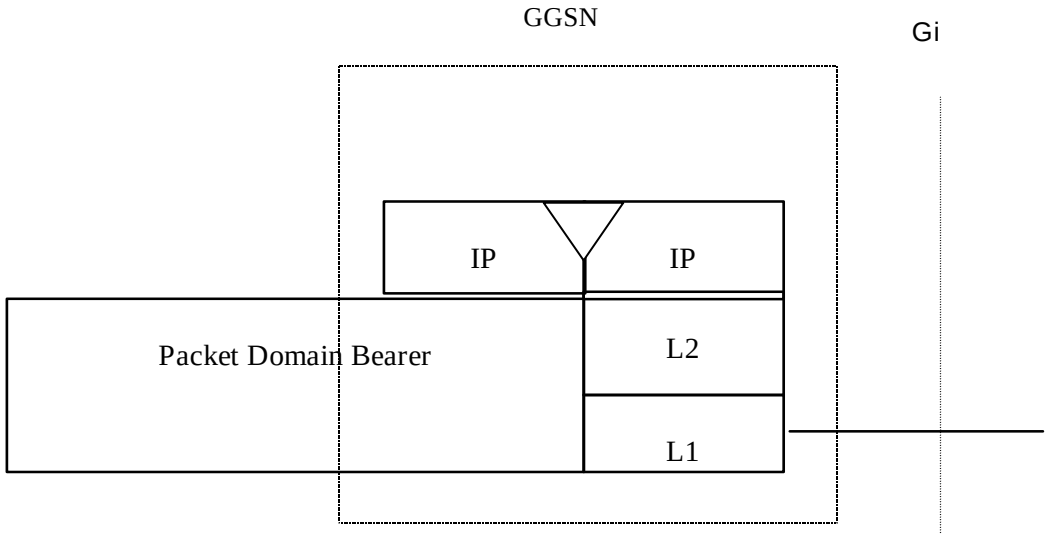


Figure 8: The protocol stacks for the IP / Gi reference point

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, IPv6 address autoconfiguration, 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.

The mechanisms for host configuration and user authentication described in this ~~section~~subclause and its sub-~~section~~clauses are only applicable to the activation of the first context activated for a specific PDP address (using the ~~"~~'PDP Context Activation Procedure~~"~~'). The activation of any subsequent PDP contexts for that PDP address, using the ~~"~~'Secondary PDP Context Activation Procedure~~"~~', as well as the use of TFTs, is described in 3GPP TS 23.060 [3].

11.2.1.1 Transparent access to the Internet

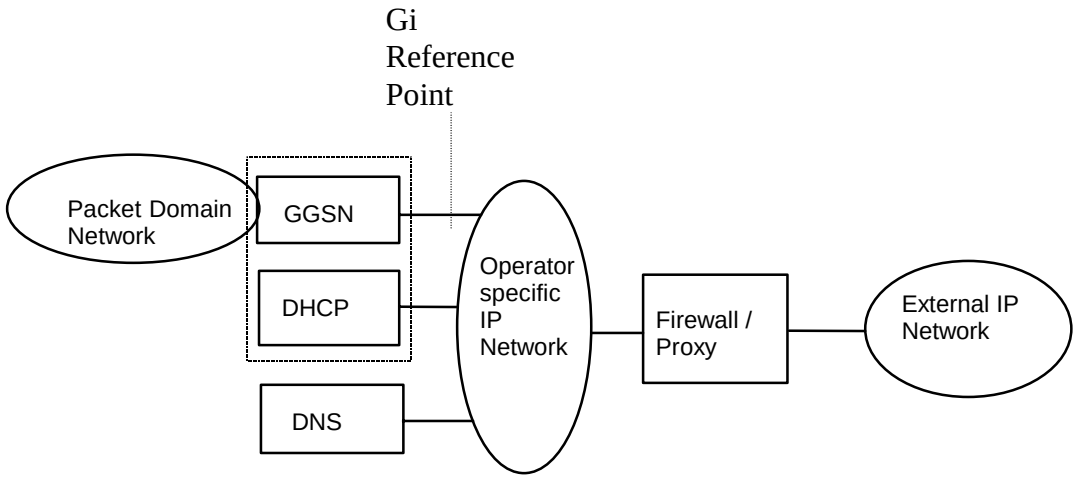


Figure 9: Example of the PDN Interworking Model, transparent case

In this case (see figure 9):

- the MS is given an address or IPv6 Prefix belonging to the operator addressing space. The address or IPv6 Prefix 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 or IPv6 Prefix is used for packet forwarding between the Internet and the GGSN and within the packet domain. With IPv6, either Stateless or Stateful Address Autoconfiguration shall be used to assign an IPv6 address to the MS. These procedures are as described in the IPv6 non-transparent access case except that the addresses belong to the operator addressing space. The use of stateful or stateless is configured per APN.

- 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.

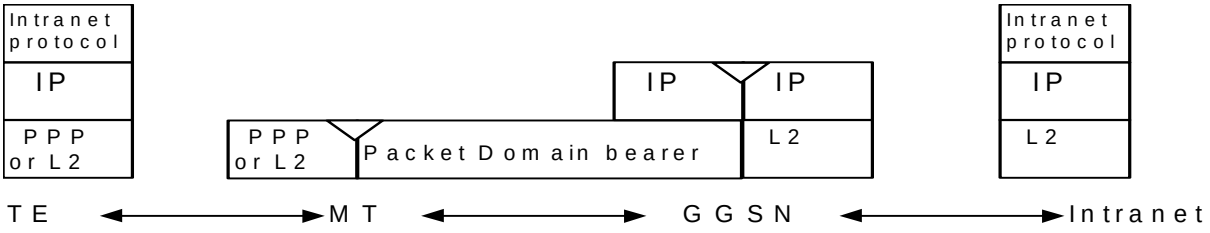


Figure 10: Transparent access to an Intranet

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 Pprotocol»".

User authentication and encryption of user data are done within the «"Intranet protocol»" if either of them is needed. This «"Intranet Pprotocol»" 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 [54]). 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 [55] and RFC 1827 [56]). In this case private IP tunnelling within public IP takes place.

11.2.1.2 IPv4 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 AAA, 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 AAA, DHCP, …, belonging to the Intranet/ISP;

- the protocol configuration options are retrieved (if requested by the MS at PDP context activation) from some server (AAA 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.

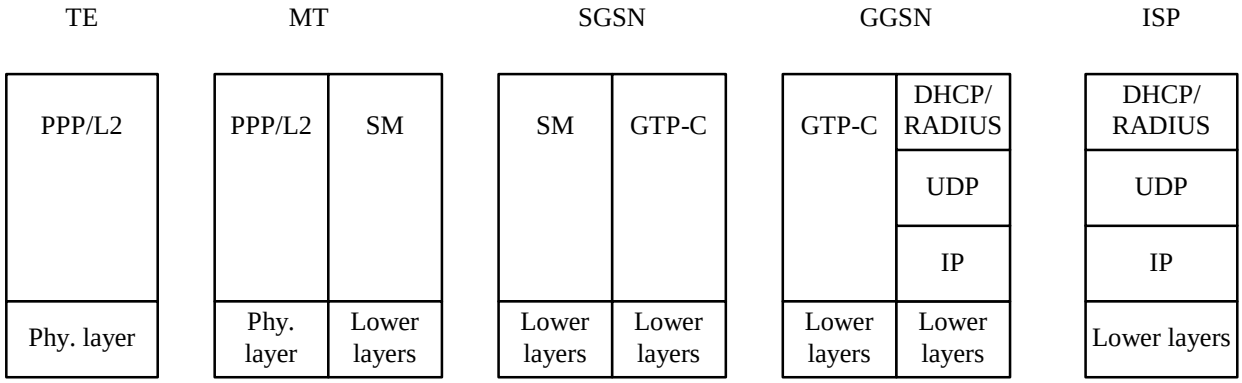


Figure 11a: Signalling plane of non transparent case

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 AAA 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 AAA 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 1661 [21a] and RFC 1662 [21b] 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.

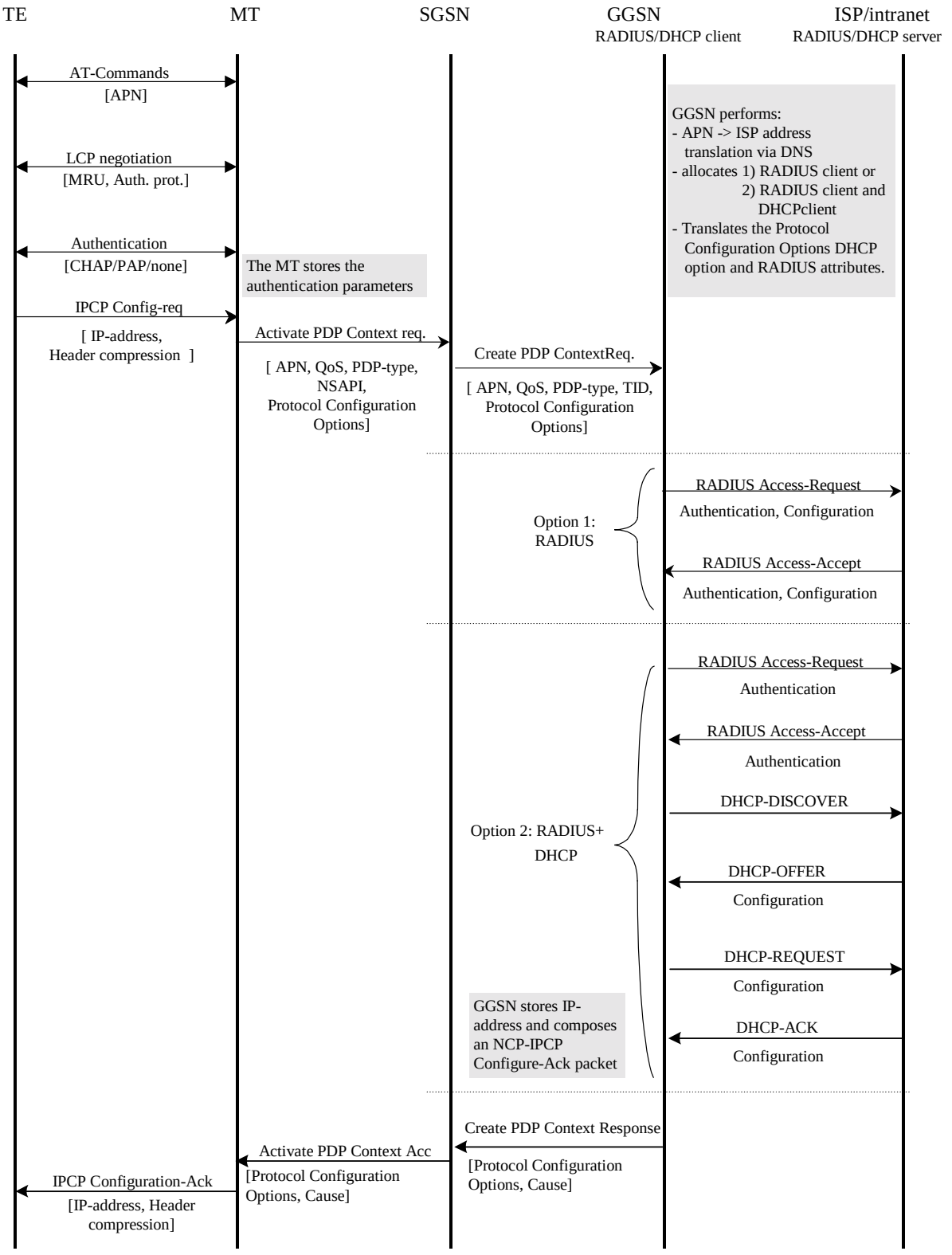


Figure 11b: PDP Context Activation for the IPv4 Non-transparent case

11.2.1.3 IPv6 Non Transparent access to an Intranet or ISP

When using IPv6 Address Autoconfiguration (either Stateless or Stateful), the process of setting up the access to an Intranet or ISP involves two signalling phases. The first signalling phase is done in the control plane and consists of the PDP context activation, followed by a second signalling phase done in the user plane.

The user plane signalling phase shall be either stateless or stateful. ~~-~~The stateless procedure, which involves only the MS and the GGSN, is described in subclause ~~"~~"IPv6 Stateless Address Autoconfiguration~~"~~". The stateful procedure, which involves the MS, GGSN (as DHCP relay agent) and one or several DHCP servers on the Intranet or ISP, is described in subclause ~~"~~"IPv6 Stateful Address Autoconfiguration~~"~~".

Whether to use stateless or stateful address autoconfiguration procedure is configured per APN in the GGSN. For APNs configured as stateless, the GGSN shall only use the Prefix part of the IPv6 address for forwarding of mobile terminated IP packets. The size of the prefix shall be according to the maximum prefix length for a global IPv6 address as specified in the IPv6 Addressing Architecture, see RFC 2373 [28].

Stateful and Stateless Autoconfiguration may also co-exist. In that case, the MS shall use Stateless to configure the address and Stateful to configure additional parameters only. The MS shall not use Stateless and Stateful Address Autoconfiguration simultaneously since GPRS only supports one prefix per PDP Context (see 3GPP TS 23.060 [3]).

The selection between Stateful and Stateless Autoconfiguration is dictated by the Router Advertisements sent by the GGSN as described in the corresponding subclauses below and according to the principles defined in RFC 2461 [44] and RFC 2462 [29].

For MS, IPv6 Stateless Address Autoconfiguration is mandatory, and IPv6 Stateful Address Autoconfiguration is optional.

11.2.1.3.1 IPv6 PDP Context Activation

In this case:

- ~~The~~ the GGSN provides the MS with an IPv6 Prefix belonging to the Intranet/ISP addressing space. A dynamic IPv6 address shall be given using either stateless or stateful address autoconfiguration. This IPv6 address is used for packet forwarding within the packet domain and for packet forwarding on the Intranet/ISP;
- the MS may send an authentication request at PDP context activation and the GGSN may request user authentication from a server, e.g. AAA, …, belonging to the Intranet/ISP;
- the protocol configuration options are retrieved (if requested by the MS at PDP context activation) from some server, e.g. AAA, …, belonging to the Intranet/ISP;
- in order to avoid any conflict between the link-local address of the MS and that of the GGSN, the Interface-Identifier used by the MS to build its link-local address shall be assigned by the GGSN. The GGSN ensures the uniqueness of this interface-identifier. The MT shall then enforce the use of this Interface-Identifier by the TE. This is valid for both stateless and stateful address autoconfiguration.
- 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 over the insecure connection. This security protocol is defined by mutual agreement between PLMN operator and Intranet/ISP administrator.

In the following signalling flow example, PPP is used as layer 2 protocol over the R reference point. The MT behaves 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 RADIUS authentication. The result of the host authentication is carried via GTP-C back to the SGSN, which then relays the result to the MT. The MT finalises the IPV6CP negotiation by sending an IPV6CP Configure-Ack message to the TE with the appropriate options included, e.g~~.~~. Interface-Identifier. The Interface-Identifier shall be used in the TE to create a link-local address to be able to perform the IPv6 address autoconfiguration (see subclauses 11.2.1.3.2 and 11.2.1.3.3).

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 IPv6 Interface-Identifier negotiation by sending the IPV6CP Configure-Request message to the MT.

5) The MT sends the Activate PDP Context Request message to the SGSN, including the Protocol Configuration Options. The Protocol Configuration Options may contain negotiated LCP options such as negotiated Authentication Protocol as well as any authentication data previously stored in the MT. The MS shall for dynamic address allocation leave PDP Address empty and set PDP Type to IPv6. The SGSN sends the Create PDP context request message to the chosen GGSN including the unmodified Protocol Configuration Options.

6) The GGSN deduces from local configuration data associated with the APN:

   - IPv6 address allocation type (stateless or stateful);
   - the source of IPv6 Prefixes in the stateless case (GGSN internal prefix pool, or external address allocation server);
   - any server(s) to be used for address allocation, authentication and/or protocol configuration options retrieval (e.g. IMS related configuration, see 3GPP TS 24.229 [47]);
   - the protocol e.g. RADIUS, to be used with the server(s);
   - the communication and security feature needed to communicate with the server(s);

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

   - GGSN internal Prefix pool for IPv6 prefix allocation and no authentication;
   - GGSN internal Prefix pool for IPv6 prefix allocation and RADIUS for authentication. The AAA server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the GGSN;
   - RADIUS for authentication and IPv6 prefix allocation. The AAA server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the GGSN;

NOTE: DHCPv6 may be used for IPv6 prefix allocation when an appropriate RFC becomes available.

IPv6 Prefixes in a GGSN internal Prefix pool shall be configurable and structured per APN.

The GGSN shall in the PDP Address IE in the Create PDP Context Response return an IPv6 address composed of a Prefix and an Interface-Identifier. The Interface-Identifier may have any value and it does not need to be unique within or across APNs. It shall however not conflict with the Interface-Identifier the GGSN has selected for its own side of the MS-GGSN link. The Prefix assigned by the GGSN or the external AAA server shall be globally or site-local unique, if stateless address autoconfiguration is configured on this APN. If, on the other hand, stateful address autoconfiguration is configured on the APN, the Prefix part of the IPv6 address returned in the PDP Address IE shall be set to the link-local prefix (FE80::/64).

The GGSN shall analyse the requested values of all the protocol options contained in the received Protocol Configurations Options IE. The GGSN response shall be in accordance with the relevant PPP or IPCPv6 standards RFC 1661 [21a], RFC 1662 [21b] and RFC 2472 [43].

7) The GGSN sends back to the SGSN a Create PDP Context Response message, containing the PDP Address IE and the Protocol Configuration Options IE. The cause value shall be set according to the outcome of the host authentication and configuration.

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

9) The MT extracts the Interface-Identifier from the address received in the PDP Address IE and ignores the Prefix part. If this Interface-Identifier is identical to the tentative Interface-Identifier indicated in the IPV6CP Configure-Request message sent from the TE , the MT sends an IPV6CP Configure Ack packet, indicating this Interface-Identifier, to the TE.

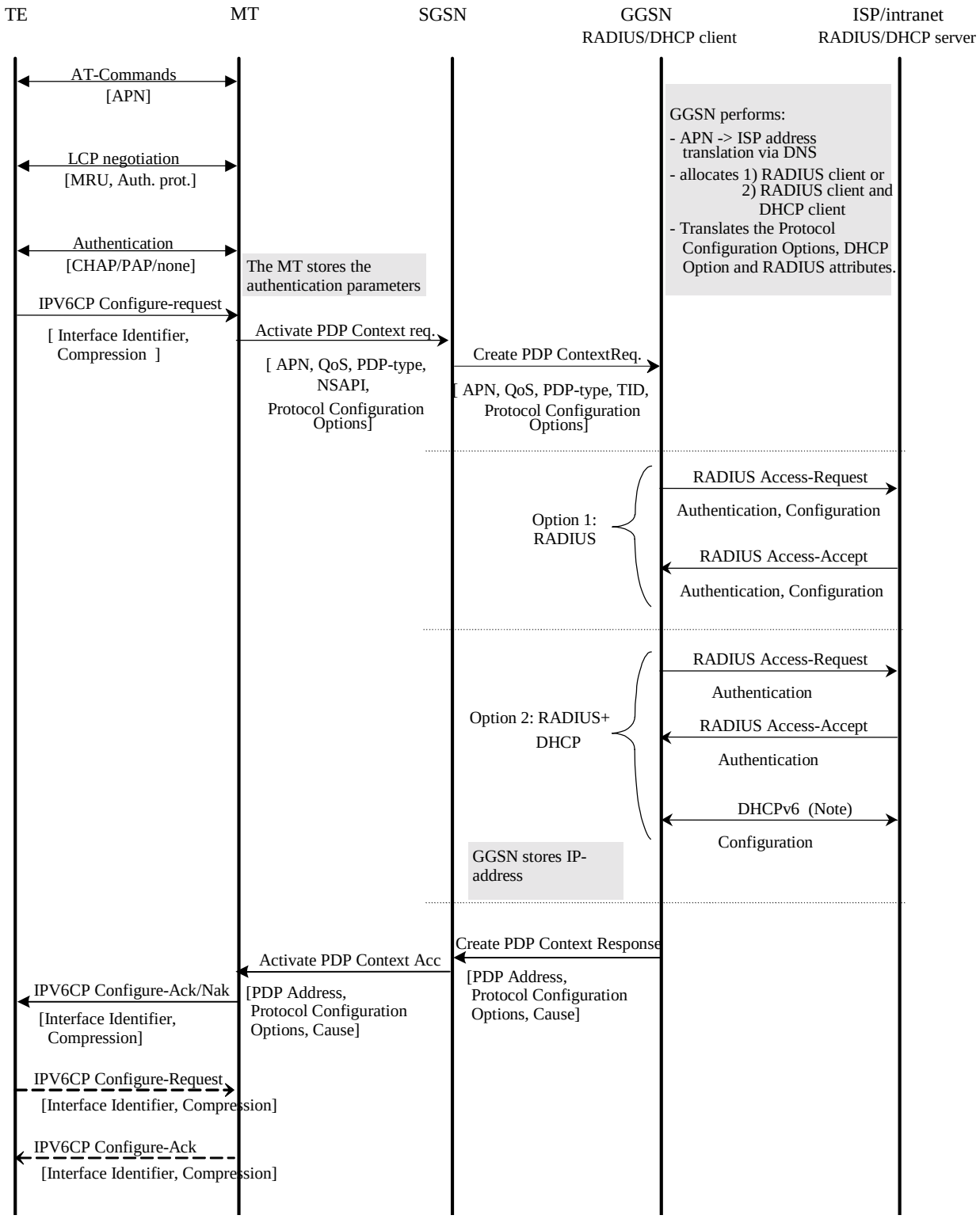
If the Interface-Identifier extracted from the address contained in the PDP Address IE is not identical to the tentative Interface-Identifier indicated in the IPV6CP Configure-Request message sent from the TE, the MT sends an IPV6CP Configure-Nak packet, indicating the Interface-Identifier extracted from the address contained in the PDP Address IE, to the TE. The TE then sends a new IPV6CP Configure-Request message to the MT, indicating the same Interface-Identifier as was indicated in the received IPV6CP Configure Nak (as indicated by the dotted IPV6CP Configure-Request and Configure-Ack in ~~the f~~figure ~~below~~11ba). Finally the MT responds with a IPV6CP Configure Ack packet.

In case a PDP Context Reject was sent to the MS the MT sends an LCP Terminate-Request to the TE.

10) When the TE has accepted the Interface-Identifier given by the MT, the user plane link from the TE to the GGSN and the external ISP/Intranet is established and the IPv6 address autoconfiguration may proceed.

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.

An LCP Terminate-request causes a PDP context deactivation.



NOTE~~ote 1~~: DHCPv6 may be used for IPv6 prefix allocation when an appropriate RFC becomes available.

Figure 11ba: PDP Context Activation for the IPv6 Non-transparent case

Figure 11ba ~~above~~ is valid for both Stateless and Stateful Address Autoconfiguration case. In the Stateful case though, ~~option~~ option 2 does not apply and option 1 may only be used for authentication. The use of DHCPv6 above is different and used in a different context than when used for Stateful Address Autoconfiguration as in subclause 11.2.1.3.3.

11.2.1.3.2 IPv6 Stateless Address Autoconfiguration

As described in 3GPP TS 23.060 [3], a PDP Context of PDP type IPv6 activated by means of the IPv6 Stateless Address Autoconfiguration Procedure is uniquely identified by the prefix part of the IPv6 address only. The MS may select any value for the Interface-Identifier part of the address. The only exception is the Interface-Identifier for the link-local address used by the MS (see RFC 2373 [28]). This Interface-Identifier shall be assigned by the GGSN to avoid any conflict between the link-local address of the MS and that of the GGSN itself. This is described in subclause "IPv6 PDP Context Activation" above.

For IPv6 the PDP Context Activation phase is followed by an address autoconfiguration phase. The procedure describing APNs configured to use Stateless Address Autoconfiguration, may be as follows:

1) After the first phase of setting up IPv6 access to an Intranet or ISP, the MS shall use the IPv6 Interface-Identifier, as provided by the GGSN, to create its IPv6 Link-Local Unicast Address according to RFC 2373 [28].

   Before the MS can communicate with other hosts or MSes on the Intranet/ISP, the MS must obtain an IPv6 Global or Site-Local Unicast Address. The simplest way is the IPv6 Stateless Address Autoconfiguration procedure described below and in 3GPP TS 23.060 [3]. The procedure is consistent with RFC 2462 [29].

   The procedure below takes place through signalling in the user plane. It is done on the link between the MS and the GGSN. From the MS perspective the GGSN is now the first router on the link.

2) After the GGSN has sent a Create PDP Context Response message to the SGSN, it shall start sending Router Advertisements periodically on the new MS-GGSN link established by the PDP Context. The MS may issue a Router Solicitation directly after the user plane establishment. This shall trigger the GGSN to send a Router Advertisement immediately.

   To indicate to the MS that stateless address autoconfiguration shall be performed, the GGSN shall leave the M-flag cleared in the Router Advertisement messages. An MS shall not perform stateless and stateful address autoconfiguration simultaneously, since multiple prefixes are not allowed in GPRS. The O-flag may be set though, since it does not result in additional addresses being acquired (see below).

   The Prefix sent in the Router Advertisements shall be identical to the Prefix returned in the Create PDP Context Response. The Prefix is contained in the Prefix Information Option of the Router Advertisements and shall have the A-flag set ("Autonomous address configuration flag") and the L-flag cleared (i.e. the prefix should not be used for on-link determination). The lifetime of the prefix shall be set to infinity. In practice, the lifetime of a Prefix will be the lifetime of its PDP Context. There shall be exactly one Prefix included in the Router Advertisements.

   The handling of Router Advertisements shall be consistent with what is specified in RFC 2461 [44]. For the MS--GGSN link however, some specific handling shall apply. The randomisation part to determine when Router Advertisements shall be sent may be omitted since the GGSN is the only router on the link. Furthermore, some 3GPP specific protocol constants and default values shall apply (see subclause "IPv6 Router Configuration Variables in the GGSN"). These relate to the periodicity of the Router Advertisements initially and during continued operation. The motivation for this is to have a faster user-plane set-up even in bad radio conditions and to minimize MS power consumption during long continued operation.

3) When creating a Global or Site-Local Unicast Address, the MS may use the Interface-Identifier received during the PDP Context Activation phase or it may generate a new Interface-Identifier. There is no restriction on the value of the Interface-Identifier of the Global or Site-Local Unicast Address, since the Prefix is unique. Interface-Identifiers shall in any case be 64-bit long.

   Since the GGSN guarantees that the Prefix is unique, the MS does not need to perform any Duplicate Address Detection on addresses it creates. That is, the 'DupAddrDetectTransmits' variable in the MS should have a value of zero. If the MS finds more than one Prefix in the Router Advertisement message, it shall only consider the first one and silently discard the others. The GGSN shall not generate any globally unique IPv6 addresses for itself using the Prefix assigned to the MS in the Router Advertisement.

If the O-flag ("Other stateful configuration flag") was set in the Router Advertisement, the MS may start a DHCP session to retrieve additional configuration parameters. See subclause 13.2.2 "Other configuration by the Intranet or ISP". If the MS is not DHCP capable, the O-flag may be ignored.

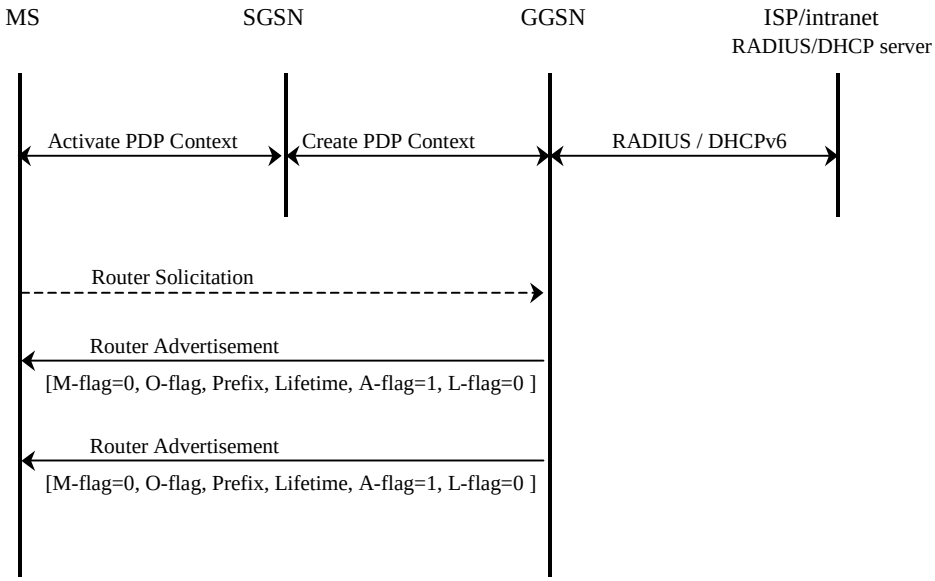


Figure 11bb: IPv6 Stateless Address Autoconfiguration

11.2.1.3.3 IPv6 Stateful Address Autoconfiguration

For IPv6 the PDP Context Activation phase is followed by an address autoconfiguration phase. For APNs configured to use Stateful Address Autoconfiguration, the procedure may for example look like below. A more detailed description of Stateful Address Autoconfiguration is described in clause "Interworking with PDN (DHCP)". Support of DHCP is not mandatory in the MS.

1) After the first phase of setting up IPv6 access to an Intranet or ISP, the MS shall use the IPv6 Interface-Identifier, as provided by the GGSN, to create its IPv6 Link-Local Unicast Address according to RFC 2373 [28].

2) After the GGSN has sent a Create PDP Context Response message to the SGSN, it shall start sending Router Advertisements periodically on the new MS-GGSN link established by the PDP Context. The MS may issue a Router Solicitation directly after the user plane establishment. This shall trigger the GGSN to send a Router Advertisement immediately. This shall be consistent with what is specified in RFC 2461 [44]. For the MS-GGSN link however, some 3GPP specific protocol constants and default values shall apply (see subclause "IPv6 Router Configuration Variables in the GGSN").

To indicate to the MS that Stateful Address Autoconfiguration shall be performed, the Router Advertisements shall not contain any Prefix-Information option and the M-flag ("Managed Address Configuration Flag") shall be set.

3) When the MS has received a Router Advertisement with the M-flag set, it shall start a DHCPv6 configuration as described in subclause "Address allocation using DHCPv6" including a request for an IPv6 address.

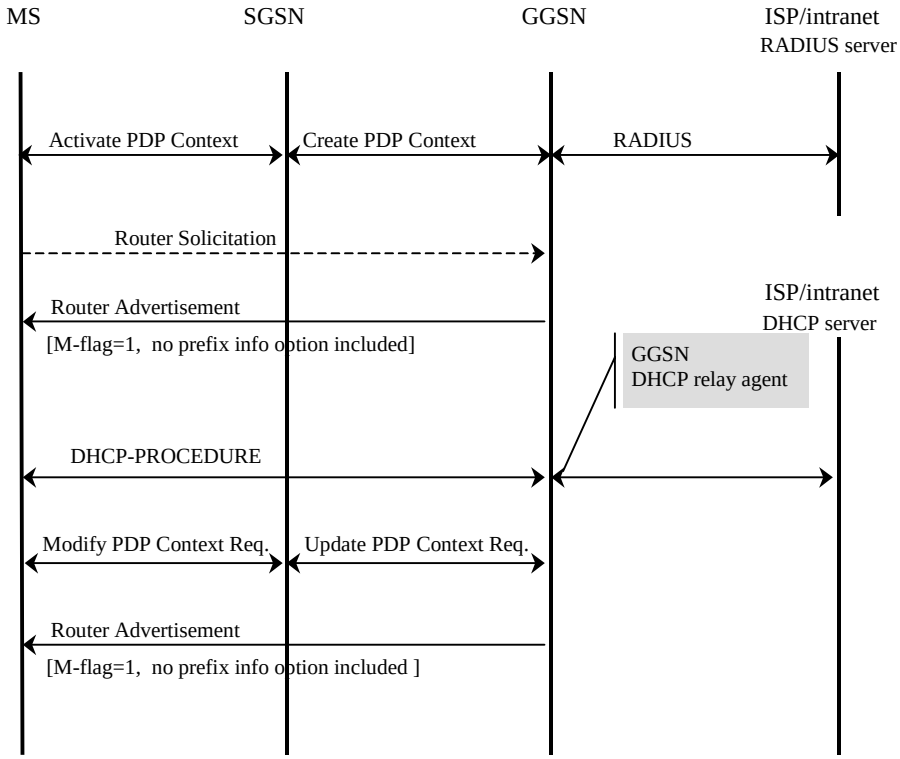


Figure 11bc: IPv6 Stateful Address Autoconfiguration

11.2.1.3.4 IPv6 Router Configuration Variables in the GGSN

For IPv6 Stateless and Stateful Address Autoconfiguration to work properly the GGSN shall behave as an IPv6 router towards the MS. In this respect the GGSN shall be consistent with the RFCs specifying this process (for example RFC 2462 [29] and RFC 2461 [44]), unless stated otherwise in this or other 3GPP specifications.

RFC 2461 [44] specifies a set of conceptual router configuration variables. Some of these variables require particular attention in GPRS in order to preserve radio resources and MS power consumption while still allowing for appropriate robustness and fast user-plane set-up time even in bad radio conditions, or simply because they have a particular meaning in GPRS. These particular variables are listed below with appropriate (default) values and shall be configurable per APN. The values specified hereafter are specific to GPRS and supersede those specified in RFC 2461 [44].

MaxRtrAdvInterval:

Shall have a default value of 21 600 seconds (6 h).

MinRtrAdvInterval

Shall have a default value of 0.75 ×~~*~~ MaxRtrAdvInterval i.e.16 200 s~~econds~~ (4~~.~~,5 h).

AdvValidLifetime

Shall have a value giving Prefixes infinite lifetime, i.e. 0xFFFFFFFF. The assigned prefix remains Preferred until PDP Context Deactivation.

AdvPreferredLifetime

Shall have a value giving Prefixes infinite lifetime, i.e. 0xFFFFFFFF. The assigned prefix remains Preferred until PDP Context Deactivation.

RFC 2461 [44] also specifies a number of protocol constants. The following shall have specific values for GPRS:

MAX_INITIAL_RTR_ADVERT_INTERVAL

This constant may be a variable within GPRS. It may have a value that gradually increases (exponentially or by some other means) with the number of initial Router Advertisements sent. This will enable a fast set-up of the MS-GGSN link in most cases, while still allowing the MS to receive a Router Advertisement within the initial phase, even in case of bad radio conditions or slow response time, without having to send a large number of initial Router Advertisements.

MAX_INITIAL_RTR_ADVERTISEMENTS

This is the number of Router Advertisements sent during the initial phase after the MS-GGSN link has been established. The value of this constant shall be chosen carefully, and in conjunction with MAX_INITIAL_RTR_ADVERT_INTERVAL, so as to not overload the radio interface while still allowing the MS to complete its configuration in a reasonable delay. For instance, the default value could be chosen so that initial Router Advertisements are sent for at least 30 s~~econds~~.

After the initial phase, the periodicity is controlled by the MaxRtrAdvInterval and the MinRtrAdvInterval constants.

11.2.1.4 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 RFC 2002 [30]. Mobile IP (MIP) is a mobility management protocol developed by IETF. The Mobile IP Foreign Agent (FA) RFC 2002 [30] is located in the Core Network in the GGSN. MIP also uses a Home Agent (HA) RFC 2002 [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~~tunnelled 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 RFC 2002 [30] are sent with UDP.

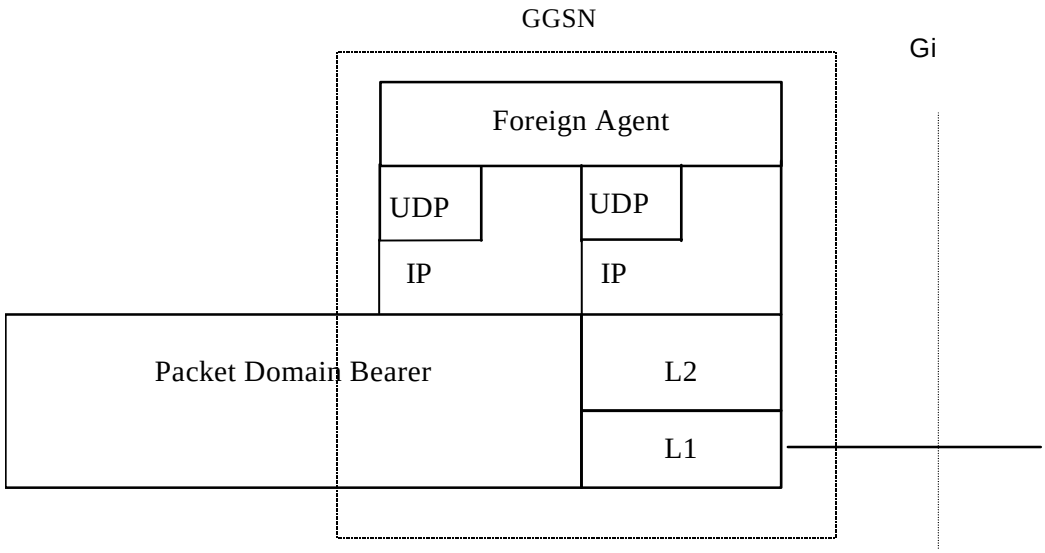


Figure 11c: The protocol stacks for the Gi IP reference point in the MIP signalling plane

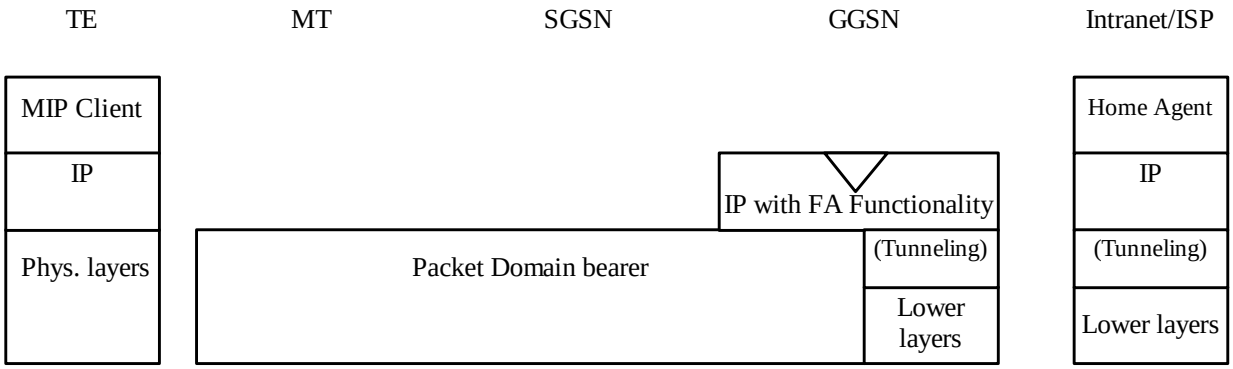


Figure 11d: Protocol stacks for user access with MIP

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 (RFC 2794 [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. In this example the MS is separated into a TE and MT, with AT commands and PPP used in-between (see 3GPP TS 27.060 [10]). The PS attach procedures have been omitted for clarity.

IPv4 - Registration UMTS/GPRS + MIP , FA care-of address

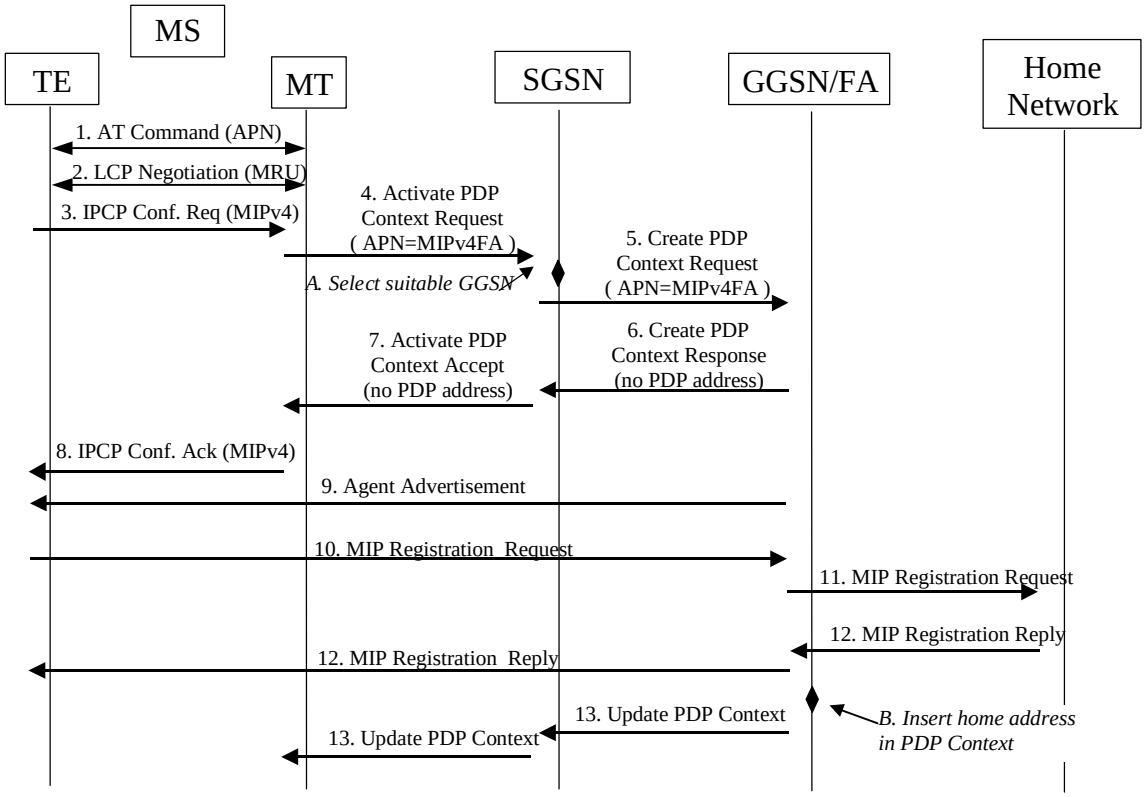


Figure 11e: Example of PDP Context activation with Mobile IP registration (the PS attach procedure not included)

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 RFC 2290 [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 RFC 2794 [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 RFC 2002 [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 RFC 2002 [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 RFC 2794 [25], RFC 2486 [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 case of IPv6, a global IPv6 prefix can be obtained from the same sources.

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

1. the GPRS operator manages internally the subnetwork addresses or IPv6 prefixes. Each private network is assigned a unique subnetwork address or range of IPv6 prefixes. 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 or IPv6 prefix, is unique.

~~Note~~NOTE:~~-~~ In IPv6 ~~“~~"site-local addresses~~”~~" replace ~~“~~"private addresses~~”~~" in IPv4, see RFC 2373 [28]. Site-local addresses may be used when a site (e.g. a corporate network) requires local administration of its address space.

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

- The PLMN operator allocates a static IP address (IPv4 or IPv6) 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 (IPv4 or IPv6) address or IPv6 prefix as described in 3GPP TS 23.060 [3].

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 [19] and RFC 1035 [52].)

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 (IPv4) and/or MLD (IPv6) and one or more Inter-Router Multicast protocols, such as DVMRP, MOSPF, or PIM-SM.

IGMP/MLD is an integral part of IP. All hosts wishing to receive IP multicasts are required to implement IGMP (or equivalent) and class-D IPv4 addresses or MLD and IPv6 multicast according to RFC 2710 [48]. IGMP/MLD 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/MLD 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 or MLD Report 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.

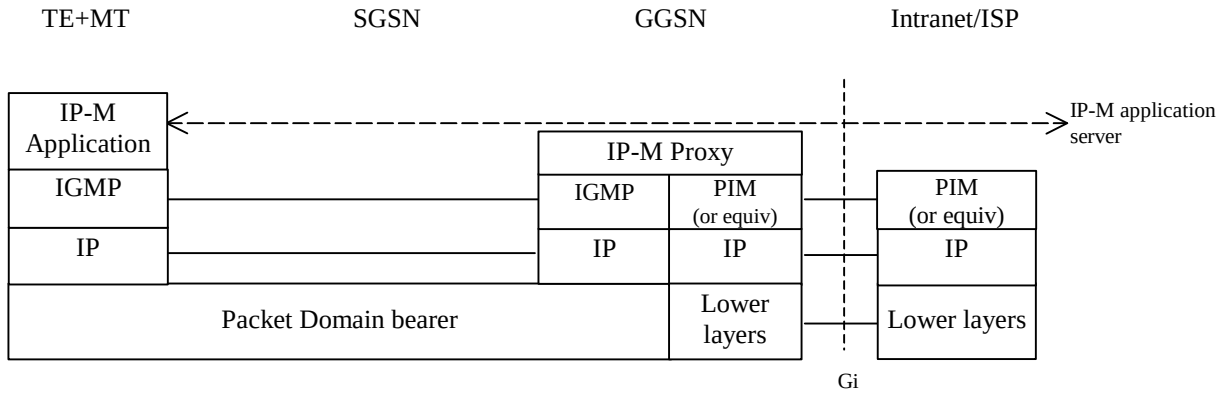


Figure 12: Protocol configuration for IP-Multicast handling (control plane)

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 RFC 1661 [21a] and RFC 1662 [21b]. 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.

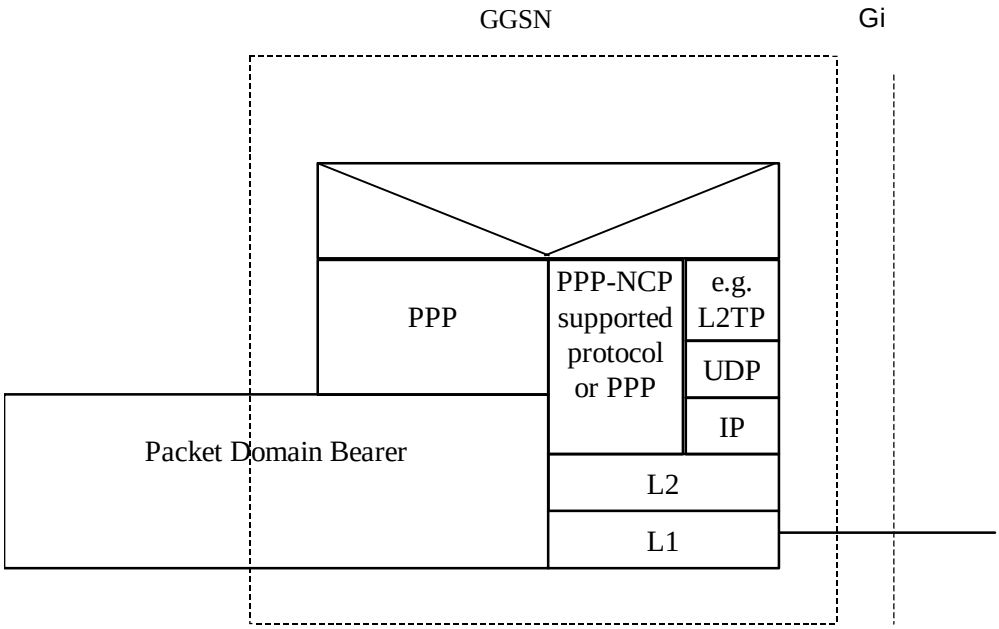


Figure 13: The protocol stacks for the Gi PPP reference point

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);

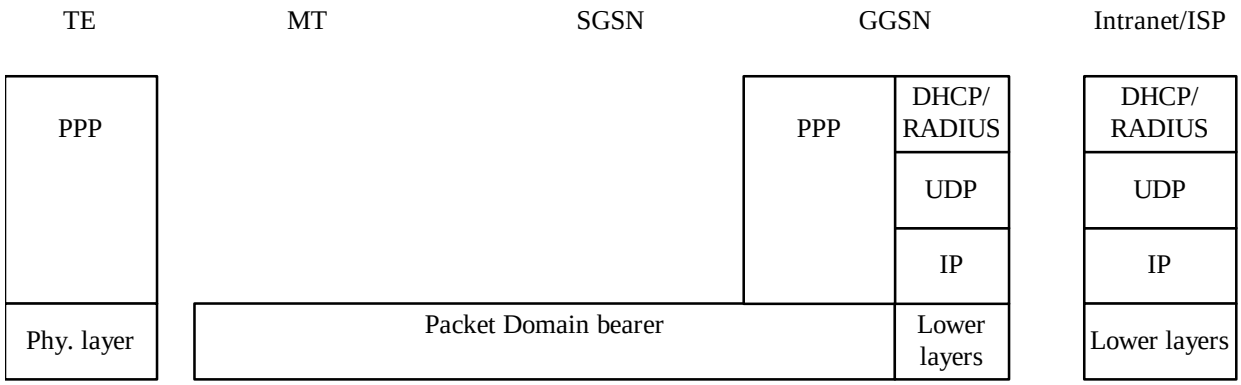


Figure 14: Protocol stack for direct access to IP-based Intranets/ISPs

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

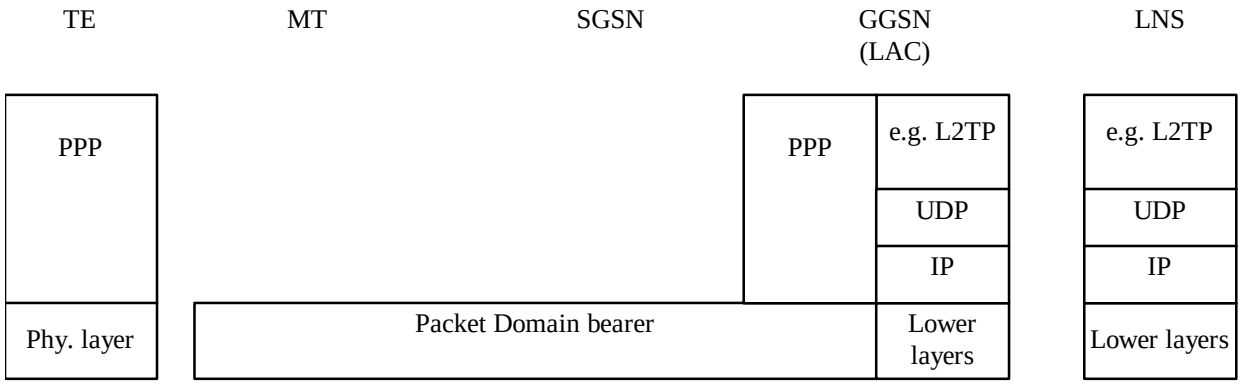


Figure 15: Protocol stack for virtual dial-up access with PPP frame tunnelling

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 AAA, 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 AAA 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 AAA 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 NCP 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.

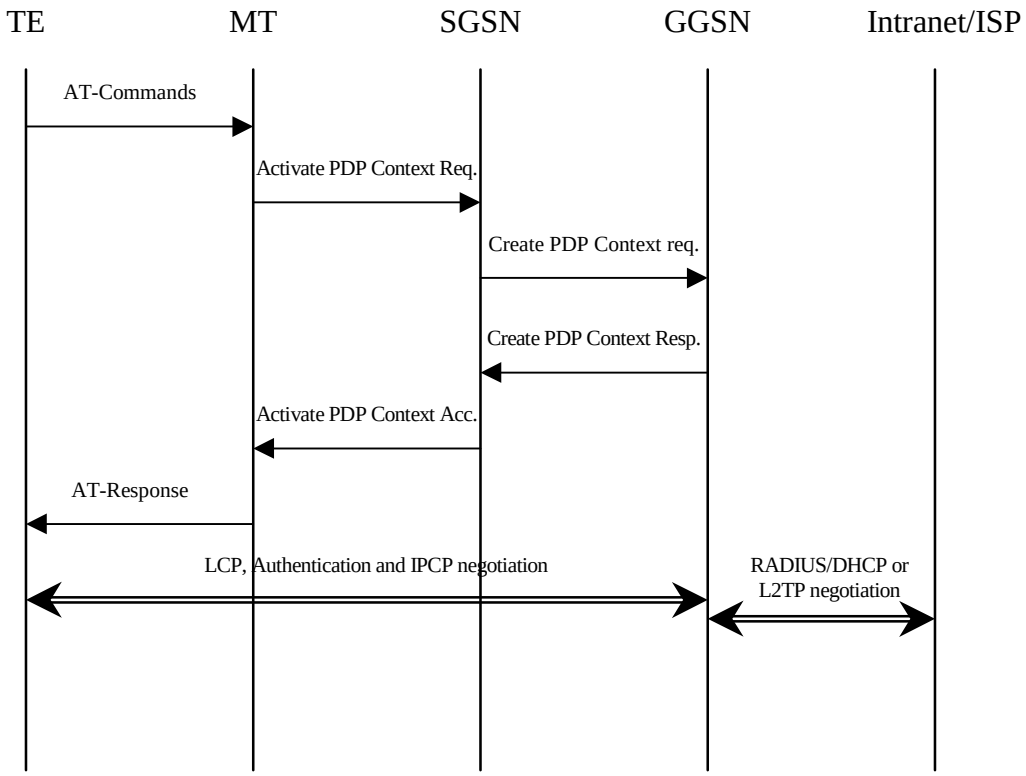


Figure 16a

13 Interworking with PDN (DHCP)

13.1 General

In current LAN environments the most commonly used configuration protocol is DHCP (Dynamic Host Configuration Protocol, RFC 2131 [26]) and DHCPv6 when the DHCPv6 IETF internet-draft [46]~~it~~ becomes an RFC standard~~ [46]~~. 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 th~~is specification~~e present document.

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 RFC 1661 [21a] and RFC 1662 [21b] 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.

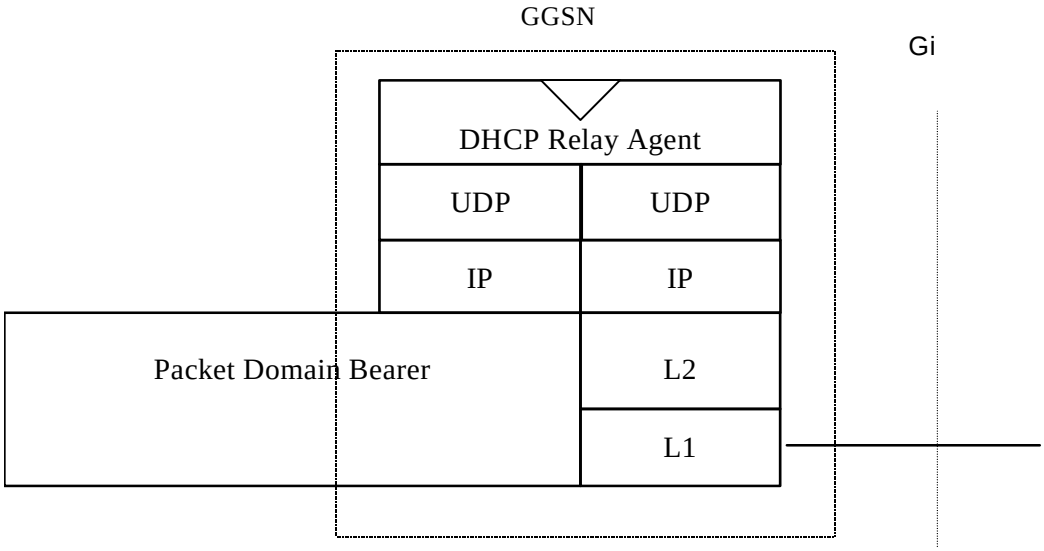


Figure 16b: The protocol stacks for the Gi IP reference point for DHCP

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 (see RFC 3118 [45]).

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

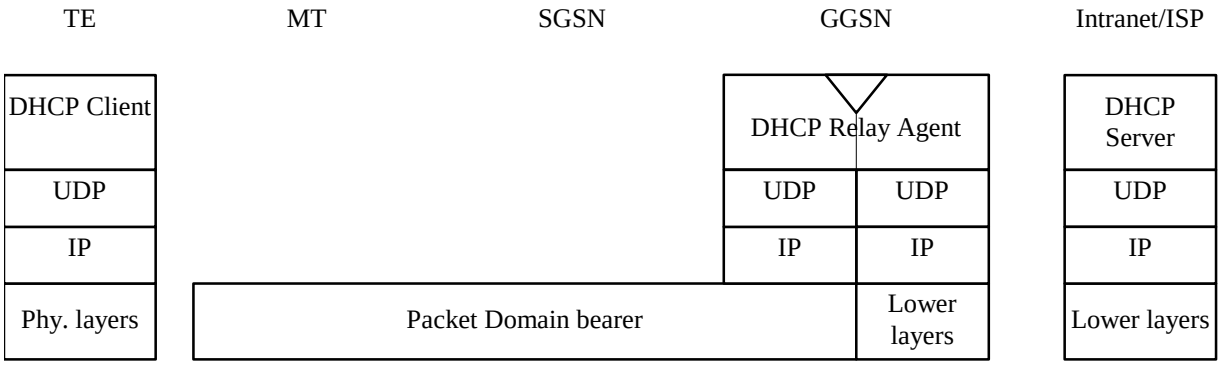


Figure 16c: Protocol stack for access with DHCP end-to-end

13.2.1.1 Address allocation using DHCPv4

The following description bullet items describe the DHCPv4 signal flow. For a detailed description of the DHCP messages refer to RFC 2131 [26] and RFC 1542~~[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.

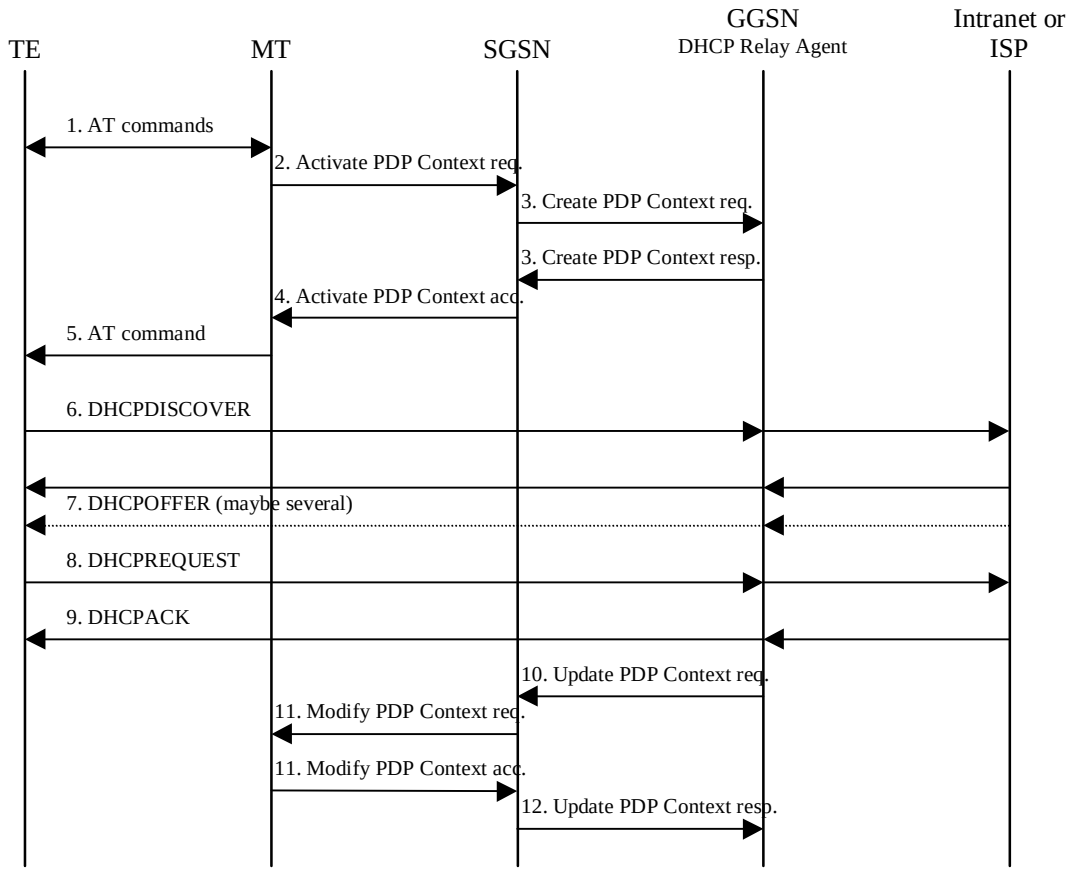


Figure 16d: DHCPv4 signal flow

13.2.1.2 Address allocation using DHCPv6

The following description bullet items describe the signal flow. For a detailed description of the DHCPv6 messages refer to the DHCPv6 IETF Internet-draft [46]. In the context of IPv6, address allocation through DHCP is also referred to as Stateful Address Autoconfiguration. The end-to-end protocol configuration is depicted in figure 16e.

The PDP Context activation part and the initial Router Advertisement that triggers the MS to do the Stateful Address Autoconfiguration is described in subclause "IPv6 Non Transparent access to an Intranet or ISP".

1)1) The TE sends a SOLICIT message with the IP destination address set to the All_DHCP_Relay_Agents_and_Servers multicast address defined in the DHCPv6 IETF Internet-draft [46]. The source address is the link local address created by the MS. The SOLICIT message shall contain one IA option.

2)2) The GGSN creates a RELAY-FORWARD message. The "Client-Message" option shall include the entire SOLICIT message. The GGSN sends the message to the DHCP server(s) configured for the APN using unicast addresses or All_DHCP_Servers multicast address. More details on the parameters for the RELAY-

FORWARD are found in the DHCPv6 IETF Internet-draft [46]. The GGSN may store a PDP Context ID in the Interface-Id option if this aids it in handling the Relay-Reply (the DHCP server will echo the Interface-Id option).

3)3) DHCP servers receiving the RELAY-FORWARD message including the SOLICIT request reply by sending a RELAY-REPLY message. The "Server-Message" option includes the ADVERTISE message with an offered IP address.

4)4) GGSN extracts the ADVERTISE messages and forwards the messages to the proper MS.

5)5) The TE chooses one of the possibly several ADVERTISE messages and sends a REQUEST confirming its choice and requesting additional configuration information.

6)6) GGSN embeds the REQUEST in the "Client-Message" option of the RELAY-FORWARD and sends it as explained in step 2.

7)7) The selected DHCP server receives the RELAY-FORWARD and replies with a RELAY-REPLY. The "Server-Message" option includes the REPLY message containing the configuration information requested by the TE.

8)8) The GGSN extracts the REPLY message and forwards it to the proper MS. GGSN also extracts IA option information such as the allocated MS IPv6 address and its lifetime and stores it in the corresponding PDP context. The GGSN shall silently discard any Neighbour Solicitation message sent by the MS to perform Duplicate Address Detection (see 3GPP TS 23.060 [3]).

9)9) The GGSN 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 IPv6 address.

10)10) The SGSN sends a Modify PDP Context Request to the MT with the allocated IPv6 address in the PDP Address information element.

11)11) The MT acknowledges by sending a Modify PDP Context Accept to the SGSN.

12)12) The SGSN sends an Update PDP Context Response to the GGSN. The PDP context has been successfully updated with the allocated IPv6 address.

13)In the Stateful Address Autoconfiguration, Router Advertisements sent by GGSN on the MS-GGSN link shall not contain any Prefix Information option, even when GGSN has knowledge of the Prefix of the MS through the DHCP relay agent. The Prefix need not be advertised since the MS is the only host on the link and Stateless Address Autoconfiguration shall not be performed concurrently to Stateful Address Autoconfiguration.

EXAMPLE: In the following example a successful PDP context activation with use of DHCPv6 from end to end is shown.

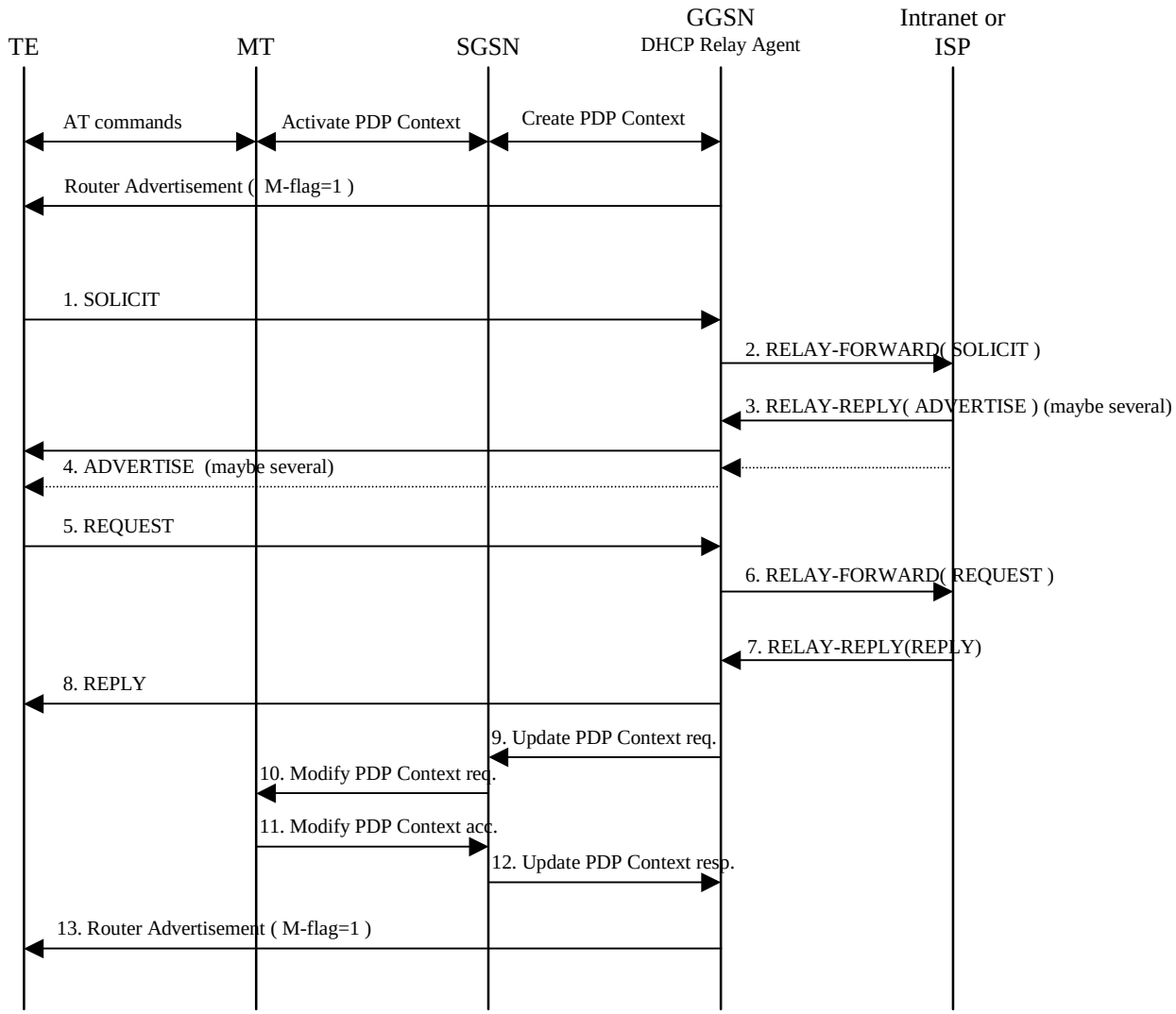


Figure 16e: DHCPv6 signal flow

13.2.2 Other configuration by the Intranet or ISP (IPv6 only)

When using IPv6, in some situations the MS may need additional configuration information from the Intranet or ISP besides the IP address. It may for example be IMS related configuration options (see 3GPP TS 24.229 [47]). If the MS is DHCP capable and the IPv6 address has been allocated using Stateless Address Autoconfiguration, the MS may use a procedure as in the example below to configure additional external network protocol parameters, or other parameters that apply to the Intranet or ISP. The GGSN shall in this case indicate to the MS that there is additional configuration information to retrieve by setting the O-flag in the Router Advertisements. This shall be configured per APN in the GGSN.

The following description bullet items describe an example of a signal flow, where the MS directs an Information-Request to the All_DHCP_Relay_Agents_and_Servers multicast address. The MS may also direct the message to a specific server instead of all servers. For a detailed description of the DHCPv6 messages refer to the DHCPv6 IETF Internet-draft [46]. The sequence is depicted in figure 16f.

1) A Router Advertisement with the O-flag set, is sent from GGSN to TE to indicate to it to retrieve other configuration information.

2) The TE sends an INFORMATION-REQUEST message with the IP destination address set to the All_DHCP_Relay_Agents_and_Servers multicast address defined in the DHCPv6 IETF Internet-draft [46].

The source address shall be the link-local address of the MS. The DHCP relay agent in the GGSN shall forward the message.

~~3)~~3) DHCP servers receiving the forwarded INFORMATION-REQUEST message, reply by sending a RELAY-REPLY message, with the ~~"~~"server-message~~"~~" option including a REPLY message with the requested configuration parameters.

The TE chooses one of the possibly several REPLY messages and extracts the configuration information.

EXAMPLE: In the following example a request for information with use of DHCPv6 from end to end is shown.

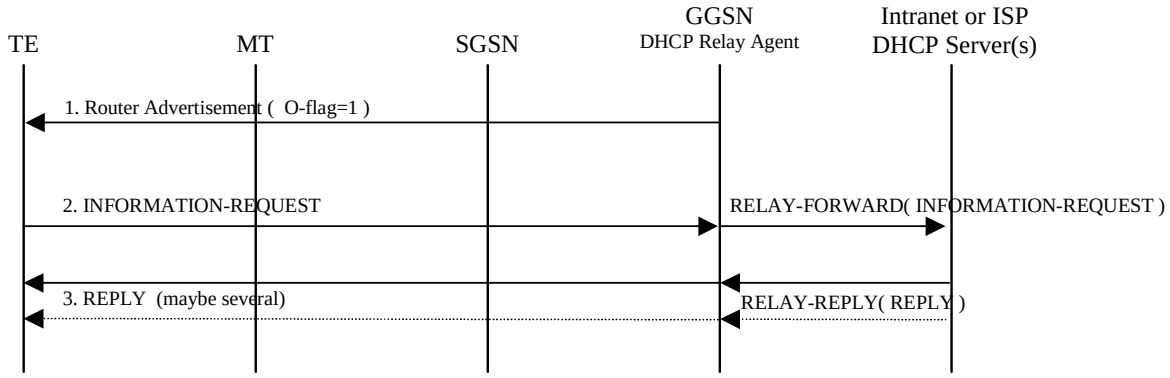


Figure 16f: DHCPv6 Other configuration signal flow

14 Internet Hosted Octet Stream Service (IHOSS)

~~Void.~~**Figure 17: Void**

Figure 18: Void

Figure 19: Void

Figure 20: Void

15 Interworking between Packet Domains

The primary reason for the interworking between Packet Domains is to support roaming subscribers as described in 3GPP TS 23.060 [3]. The general model for Packet Domain interworking is shown in figure 21.

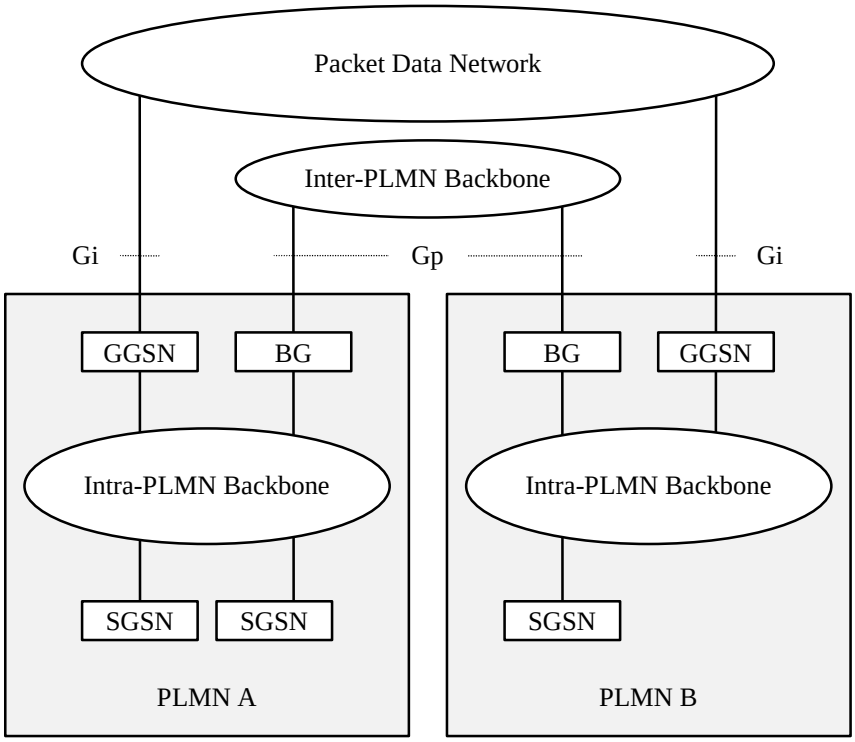


Figure 21: General interworking between Packet Domains to support roaming subscribers.

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 [3].

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 [3].

The inter-PLMN link may be any packet data network or dedicated link as described in 3GPP TS 23.060 [3]. 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 [54]) and accompanying specifications for authentication (RFC 1826 [55]) and encryption (RFC 1827 [56]) 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 [53]) 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.

16 Usage of RADIUS on Gi interface

A GGSN may, on a per APN basis, use RADIUS authentication to authenticate a user and RADIUS accounting to provide information to an AAA (Authentication, Authorization and Accounting) server.

16.1 RADIUS Authentication

RADIUS Authentication shall be used according to RFC 2865 [38] and RFC 3162 [50].

The RADIUS client function may reside in a GGSN. When the GGSN receives a Create PDP Context request message the RADIUS client function may send the authentication information to an authentication server, which is identified during the APN provisioning.

The authentication server checks that the user can be accepted. The response (when positive) may contain network information, such as an IP address or IPv6 prefix for the user.

The information delivered during the RADIUS authentication can be used to automatically correlate the users identity (the MSISDN or IMSI) to the IP-address or IPv6 prefix, assigned/confirmed by the GGSN or the authentication server respectively. The same procedure applies, in case of sending the authentication to a 'proxy' authentication server.

RADIUS Authentication is only applicable to the primary PDP context. When the GGSN receives an Access-Accept message from the authentication server it shall complete the PDP context activation procedure. If Access-Reject or no response is received, the GGSN shall reject the PDP Context Activation attempt with a suitable cause code, e.g. User Authentication failed.

16.2 RADIUS Accounting

RADIUS Accounting shall be used according to RFC 2866 [39] and RFC 3162 [50].

The RADIUS accounting client function may reside in a GGSN. The RADIUS accounting client may send information to an accounting server, which is identified during the APN provisioning. The accounting server may store this information and use it to automatically identify the user. This information can be trusted because the GPRS network has authenticated the subscriber (i.e. SIM card and possibly other authentication methods).

RADIUS Accounting-Request Start and Stop messages may be used during both primary and secondary PDP context activation and deactivation procedures respectively.

The use of Accounting-Request STOP and in addition the Accounting ON and Accounting OFF messages may be used to ensure that information stored in the accounting server is synchronised with the GGSN information.

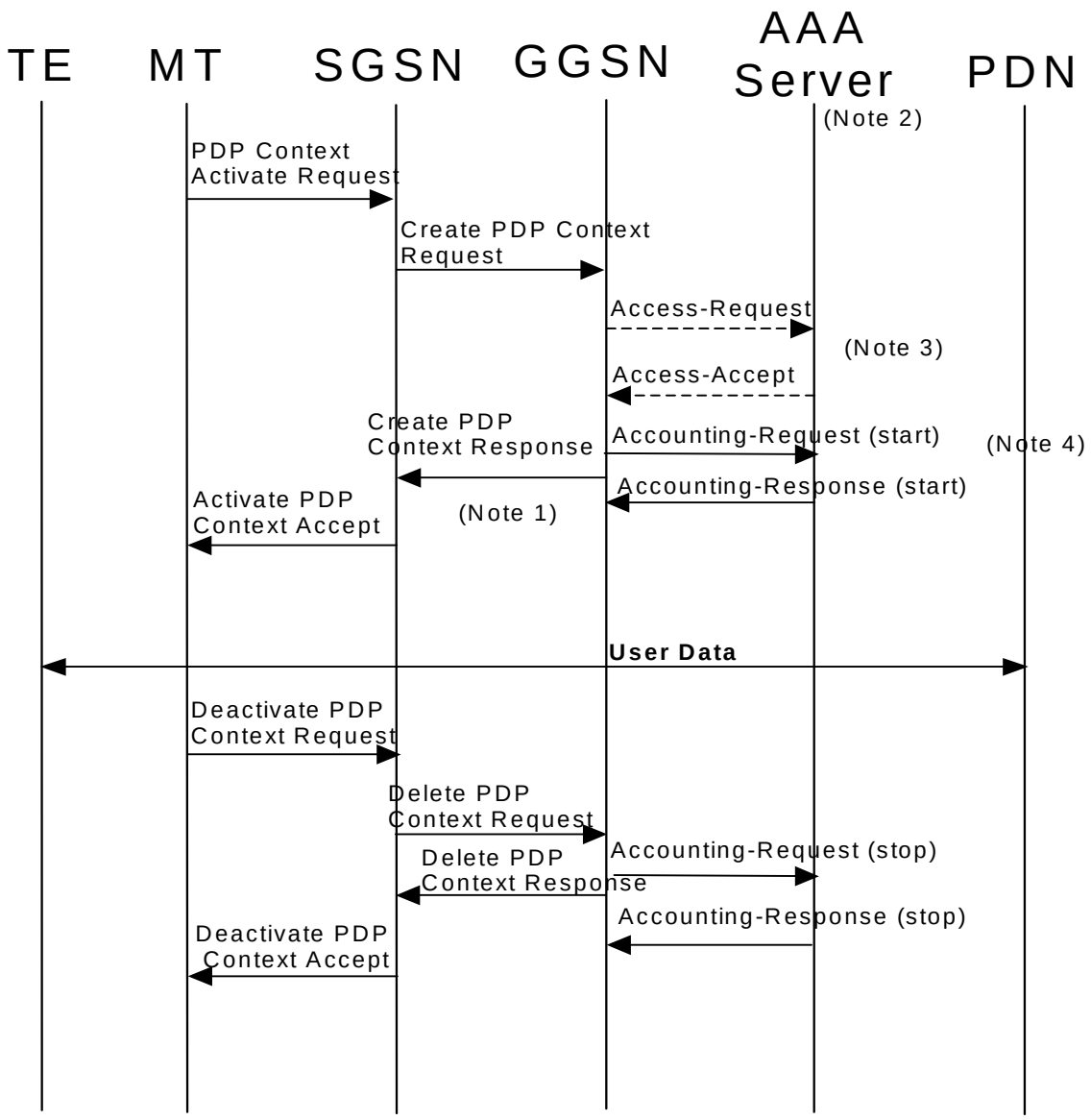
If the AAA server is used for IP address or IPv6 prefix assignment, then, upon reception of a RADIUS Accounting-Request STOP message for all PDP contexts associated to a session defined by APN and IMSI or MSISDN, the AAA server may make the associated IP address or IPv6 prefix available for assignment.

In order to avoid race conditions, the GGSN shall include a 3GPP Vendor-Specific sub-attribute "Session Stop indicator" when it sends the Accounting-Request STOP for the last PDP context of a PDP session and the PDP session is terminated (i.e. the IP address or IPv6 prefix and all GTP tunnels can be released). The AAA server shall not assume the PDP session terminated until an Accounting-Request STOP with the Session Stop indicator is received.

16.3 Authentication and accounting message flows

16.3.1 IP PDP type

The figure 22 represents the RADIUS message flows between a GGSN and an Authentication, Authorization and Accounting (AAA) server.



NOTE 1: If some external applications require RADIUS Accounting request (Start) information before they can process user packets, then the selected APN (GGSN) may be configured in such a way that the GGSN drops user data until the Accounting Response (START) is received from the AAA server. The GGSN may wait for the Accounting Response (START) before sending the CreatePDPContextResponse. The GGSN may reject the PDP context if the Accounting Response (START) is not received.
NOTE 2: Separate accounting and authentication servers may be used.
NOTE 3: The Access-Request message shall be used for primary PDP context only.
NOTE 4: The Accounting-Request (Start) message may be sent at a later stage, e.g. after IPv6 address has been assigned and PDP Context updated, in case of a stateful address autoconfiguration.

Figure 22: RADIUS message flow for PDP type IP (successful user authentication case)

When a GGSN receives a Create PDP Context Request message for a given APN, the GGSN may (depending on the configuration for this APN) send a RADIUS Access-Request to an AAA server. The AAA server authenticates and authorizes the user. If RADIUS is also responsible for IP address or IPv6 prefix allocation the AAA server shall return the allocated IP address or IPv6 prefix in the Access-Accept message.

Even if the GGSN was not involved in user authentication (e.g. transparent network access mode), it may send a RADIUS Accounting-Request START message to an AAA server. This message contains parameters, e.g. the tuple which includes the user-id and IP address or IPv6 prefix, to be used by application servers (e.g. WAP gateway) in order to identify the user. This message also indicates to the AAA server that the user session has started.

If some external applications require RADIUS Accounting request (Start) information before they can process user packets, then the selected APN (GGSN) may be configured in such a way that the GGSN drops user data until the Accounting Response (START) is received from the AAA server. The GGSN may wait for the Accounting Response (START) before sending the CreatePDPContextResponse. The GGSN may reject the PDP context if the Accounting Response (START) is not received. The authentication and accounting servers may be separately configured for each APN.

At a stateful address autoconfiguration, no IP address or IPv6 prefix is available at PDP context activation. In that case the GGSN may wait to send the Accounting-Request START message until the TE receives its IP address in a DHCP-REPLY.

When the GGSN receives a Delete PDP Context Request message and providing a RADIUS Accounting-Request START message was sent previously, the GGSN shall send a RADIUS Accounting-Request STOP message to the AAA server, which indicates the termination of this particular user session. The GGSN shall immediately send a Delete PDP context response, without waiting for an Accounting-Response STOP message from the AAA server.

The AAA server shall deallocate the IP address or IPv6 prefix (if any) initially allocated to the subscriber, if there is no session for the subscriber.

Accounting-Request ON and Accounting-Request OFF messages may be sent from the GGSN to the AAA server to ensure the correct synchronization of the session information in the GGSN and the AAA server.

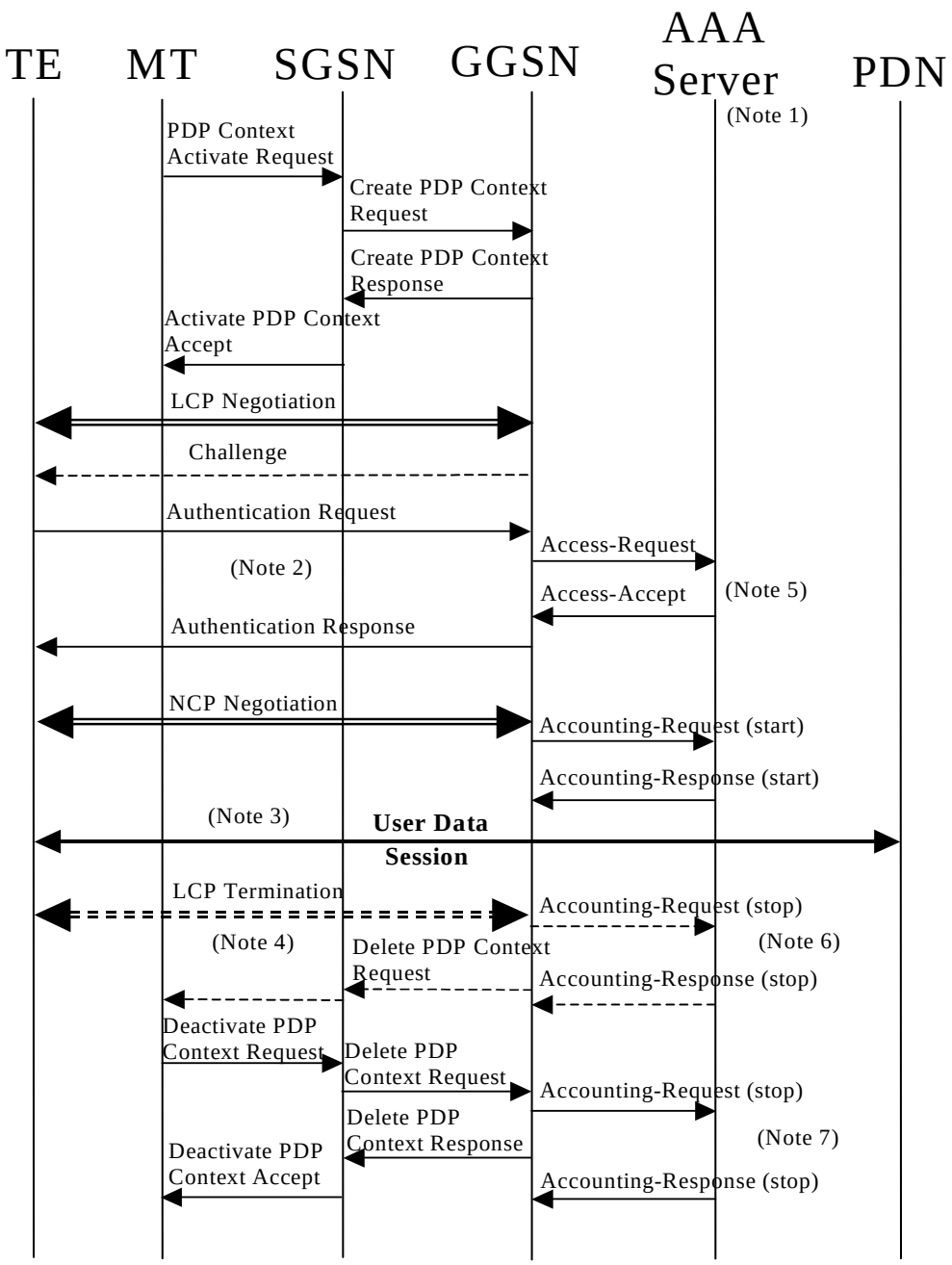
The GGSN may send an Accounting-Request ON message to the AAA server to indicate that a restart has occurred. The AAA server may then release the associated resources.

Prior to a scheduled restart, the GGSN may send Accounting-Request OFF message to the AAA server. The AAA server may then release the associated resources.

If an Access-Challenge is sent to the GGSN when an Access-Request message is pending and when IP PDP type is used, the GGSN shall silently discard the Access-Challenge message and it shall treat an Access-Challenge as though it had received an Access-Reject instead RFC 2865 [38].

16.3.2 PPP PDP type

~~The f~~Figure 23 describes the RADIUS message flows between a GGSN and an Authentication, Authorization and Accounting (AAA) server for the case where PPP is terminated at the GGSN. The case where PPP is relayed to an LNS is beyond the scope of ~~this specification~~the present document.



NOTE 1: Separate accounting and Authentication servers may be used.
NOTE 2: Actual messages depend on the used authentication protocol (e.g. PAP, CHAP).
NOTE 3: If some external applications require RADIUS Accounting request (Start) information before they can process user packets, then the selected APN (GGSN) may be configured in such a way that the GGSN drops user data until the Accounting Response (START) is received from the AAA server. The GGSN may delete the PDP context if the Accounting Response (START) is not received.
NOTE 4: An LCP termination procedure may be performed. Either the MS or the GGSN may initiate the context deactivation.
NOTE 5: The Access-Request message shall be used for primary PDP context only.
NOTE 6: Network Initiated deactivation.
NOTE 7: User Initiated deactivation.

Figure 23: RADIUS message flow for PDP type PPP (successful user authentication case)

When a GGSN receives a Create PDP Context Request message for a given APN, the GGSN shall immediately send a Create PDP context response back to the SGSN. After PPP link setup, the authentication phase may take place. During Authentication phase, the GGSN sends a RADIUS Access-Request to an AAA server. The AAA server authenticates and authorizes the user. If RADIUS is also responsible for IP address allocation the AAA server shall return the allocated IP address or IPv6 prefix in the Access-Accept message (if the user was authenticated).

If the user is not authenticated, the GGSN shall send a Delete PDP context request to the SGSN.

Even if the GGSN was not involved in user authentication (e.g. for PPP no authentication may be selected), it may send a RADIUS Accounting-Request START message to an AAA server. This message contains parameters, e.g. a tuple which includes the user-id and IP address or IPv6 prefix, to be used by application servers (e.g. WAP gateway) in order to identify the user. This message also indicates to the AAA server that the user session has started, and the QoS parameters associated to the session.

If some external applications require RADIUS Accounting request (Start) information before they can process user packets, then the selected APN (GGSN) may be configured in such a way that the GGSN drops user data until the Accounting Response (START) is received from the AAA server. The GGSN may delete the PDP context if the Accounting Response (START) is not received. The Authentication and Accounting servers may be separately configured for each APN.

When the GGSN receives a Delete PDP Context Request message and providing a RADIUS Accounting-Request START message was sent previously, the GGSN shall send a RADIUS Accounting-Request STOP message to the AAA server, which indicates the termination of this particular user session. The GGSN shall immediately send a Delete PDP context response, without waiting for an Accounting-Response STOP message from the AAA server.

The AAA server shall deallocate the IP address or IPv6 prefix (if any) initially allocated to the subscriber.

Accounting-Request ON and Accounting-Request OFF messages may be sent from the GGSN to the AAA server to ensure the correct synchronization of the session information in the GGSN and the AAA server.

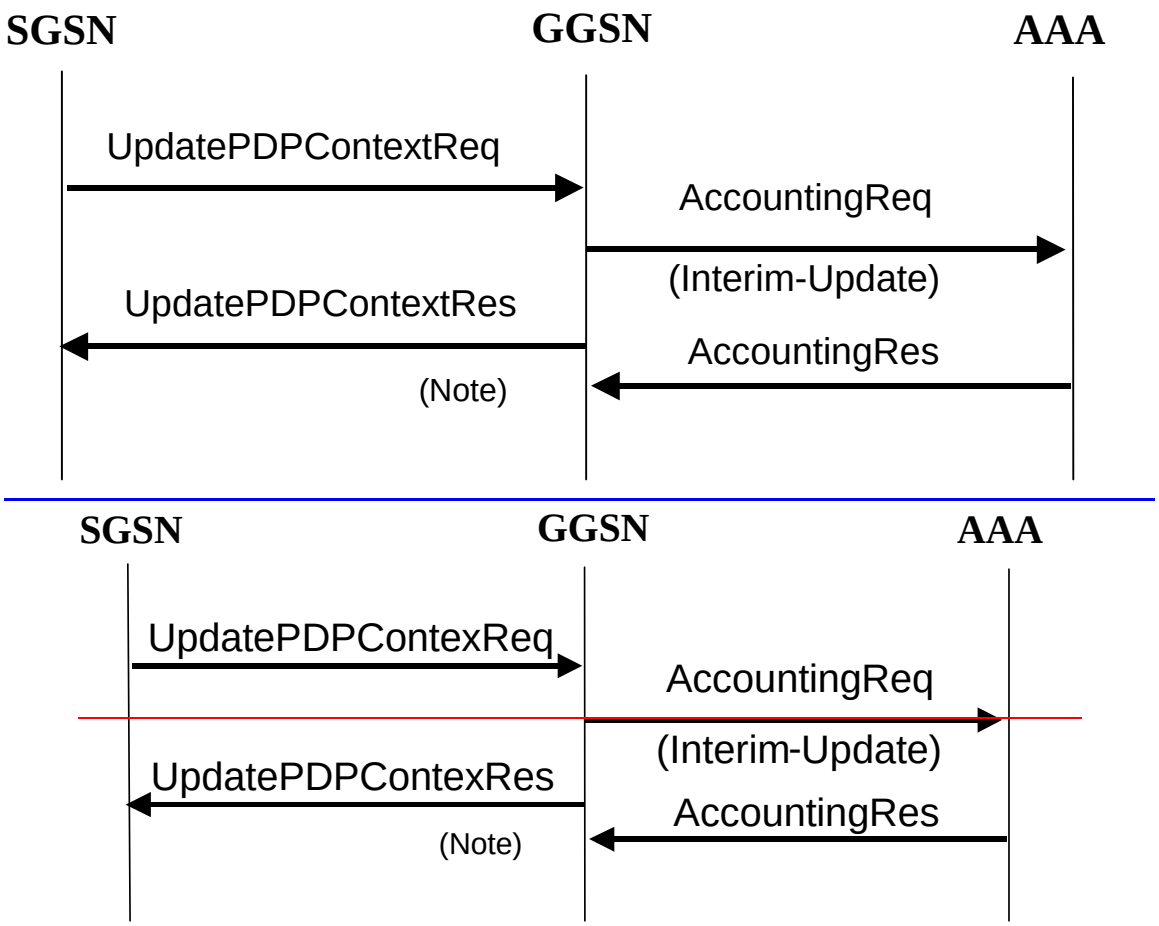
The GGSN may send an Accounting-Request ON message to the AAA server to indicate that a restart has occurred. The AAA server may then release the associated resources.

Prior to a scheduled restart, the GGSN may send Accounting-Request OFF message to the AAA server, the AAA server may then release the associated resources.

If an Access-Challenge is sent to the GGSN when using PPP PDP type, the GGSN shall handle it by PPP CHAP providing PPP CHAP was the selected Authentication protocol. If CHAP authentication was not selected, authentication shall fail RFC 2865 [38].

16.3.3 Accounting Update

During the life of a PDP context some information related to this PDP context may change (i.e. SGSN address if a Inter-SGSN RA update occurs). Upon reception of an UpdatePDPContextRequest from the SGSN, the GGSN may send an Accounting Request Interim-Update to the AAA server to update the necessary information related to this PDP context (See figure 24). In such a case, the GGSN need not wait for the RADIUS AccountingResponse from the AAA server message before sending the UpdatePDPContextResponse to the SGSN. The GGSN may delete the PDP context if the AccountingResponse is not received from the AAA.

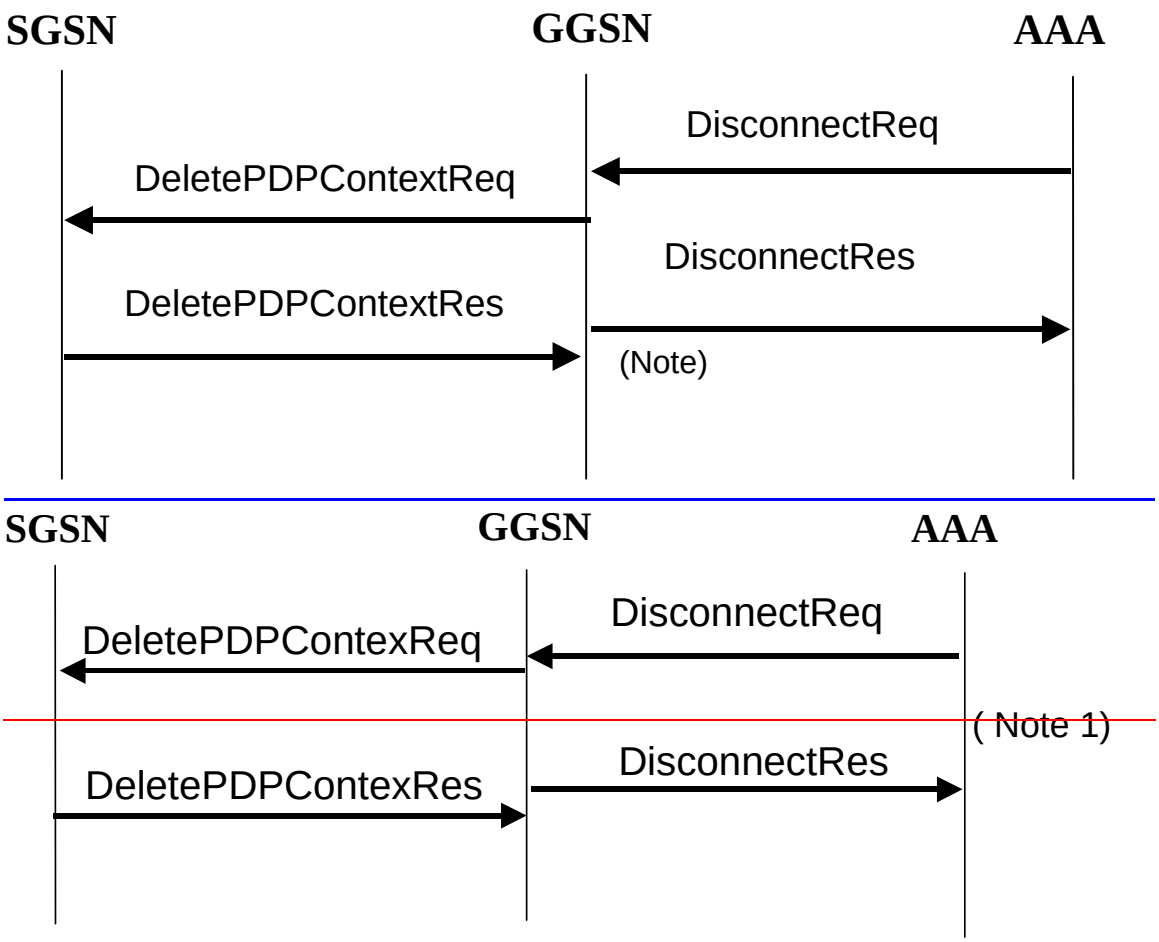


NOTE 1: As shown the GGSN need not wait for the RADIUS AccountingResponse from the AAA server message to send the UpdatePDPContextResponse to the SGSN. The GGSN may delete the PDP context if the AccountingResponse is not received from the AAA.

Figure 24: RADIUS for PDP context Update

16.3.4 AAA-Initiated PDP context termination

RADIUS is used as the protocol between the GGSN and a AAA server or proxy for applications (e.g. MMS) to deliver information related to GPRS user session. However some IP applications could need to interwork with the GGSN to terminate a particular PDP context. For this purpose, the AAA server or proxy may send a RADIUS Disconnect Request to the GGSN. As depicted in figure 25, the GGSN may react by deleting the corresponding PDP context or silently discard the Disconnect Request message. For more information on RADIUS Disconnect, see RFC 2882 [41]. If the GGSN deletes the corresponding PDP context, it need not wait for the DeletePDPContextResponse from the SGSN before sending the RADIUS DisconnectResponse to the AAA server.



Note 1OTE: As showed on Ffigure 25, the GGSN need not wait for the DeletePDPContextResponse from the SGSN to send the RADIUS DisconnectResponse to the AAA server.

Figure 25: PDP Context deletion with RADIUS

16.4 List of RADIUS attributes

The following tables describe the actual content of the RADIUS messages exchanged between the GGSN and the AAA server. Other RADIUS attributes may be used as defined in RADIUS RFC(s). Unless otherwise stated, when the encoding scheme of an attribute is specified as UTF-8 encoding, this shall be interpreted as UTF-8 hexadecimal encoding.

16.4.1 Access-Request message (sent from the GGSN to AAA server)

The table 1 describes the attributes of the Access-Request message.

Table 1: The attributes of the Access-Request message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username is provided by the user (extracted from the Protocol Configuration Options (PCO) field of	String	Mandatory

Attr #	Attribute Name	Description	Content	Presence Requirement
		the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used). If no username is available a generic username, configurable on a per APN basis, shall be present.		
2	User-Password	User password provided by the user if PAP is used (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used). If no password is available a generic password, configurable on a per APN basis, shall be present.	String	Conditional Note 1
3	CHAP-Password	User password provided by the user if CHAP is used (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used).	String	Conditional Note 2
4	NAS-IP-Address	IP address of the GGSN for communication with the AAA server.	IPv4	Conditional Notes 3 and~~,~~ ~~5~~4
95	NAS-IPv6-Address	IP address of the GGSN for communication with the AAA server.	IPv6	Conditional Notes 3 and~~,~~ ~~5~~4
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 3
6	Service-Type	Indicates the type of service for this user	Framed	Optional
7	Framed-Protocol	Indicates the type of protocol for this user	7 (GPRS PDP Context)	Optional
8	Framed-IP-Address	IP address allocated for this user	IPv4	Conditional Note ~~5~~4
9	Framed-IP-Netmask	Netmask for the user IP address	IPv4	Conditional Note ~~5~~4
97	Framed-IPv6-Prefix	IPv6 address prefix allocated for this user	IPv6	Conditional Note ~~5~~4
96	Framed-Interface-Id	User IPv6 Interface Identifier	IPv6	Conditional Notes ~~5~~4 and~~,~~ ~~6~~5
30	Called-Station-Id	Identifier for the target network	APN (UTF-8 encoded)	Mandatory
31	Calling-Station-Id	This attribute is the identifier for the MS, and it shall be configurable on a per APN basis.	MSISDN in international format according to 3GPP TS 23.003 [40], UTF-8 encoded decimal. ~~Note that there are no leading characters in front of the country code.~~ (Note 6)	Optional
60	CHAP-Challenge	Challenge if CHAP is used (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used).	String	Conditional Note 2
61	NAS-Port-Type	Port type for the GGSN	As per RFC 2865 [38]	Optional
26/10415	3GPP Vendor-Specific	Sub-attributes according ~~sub-clause~~subclause 16.4.7	See ~~sub-clause~~subclause 16.4.7	Optional except sub-attribute 3 which is conditional

Attr #	Attribute Name	Description	Content	Presence Requirement
NOTE 1: Shall be present if PAP is used. NOTE 2: Shall be present if CHAP is used. NOTE 3: Either NAS-IP-Address or NAS-Identifier shall be present. NOTE 45: Either IPv4 or IPv6 address/prefix attribute shall be present. The IP protocol version for end-user and network may be different. NOTE 56: Included if the prefix alone is not unique for the user. This may be the case, for example, if address is assigned using stateful address autoconfiguration or if a static IPv6 address. NOTE 6: There are no leading characters in front of the country code				

16.4.2 Access-Accept (sent from AAA server to GGSN)

The table 2 describes the attributes of the Access-Accept message. See RFC 2548 [51] for definition of MS specific attributes.

Table 2: The attributes of the Access-Accept message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username received in the Access-Request message or a substitute username provided by the AAA server. If the User-Name has been received in the Access-Accept message, this user-name shall be used in preference to the above	String	Optional
6	Service-Type	Indicates the type of service for this user	Framed	Optional
7	Framed-Protocol	Indicates the type of protocol for this user	7 (GPRS PDP Context)	Optional
8	Framed-IP-Address	IP address allocated for this user, if the AAA server is used to allocate IP address.	IPv4	Conditional Note 25
9	Framed-IP-Netmask	Netmask for the user IP address, if the AAA server is used to allocate IP netmask.	IPv4	Conditional Note 25
97	Framed-IPv6-Prefix	IPv6 address prefix allocated for this user, if the AAA server is used to allocate IP address prefixes.	IPv6	Conditional Note 25
100	Framed-IPv6-Pool	Name of the prefix pool for the specific APN	IPv6	Optional Note 25
12	Framed-IP-MTU	MTU for the user towards this particular APN, MTU shall be less or equal to 1500	String	Optional
25	Class	Identifier to be used in all subsequent accounting messages.	String	Optional (NOTE Note 14)
27	Session-Timeout	Indicates the timeout value (in seconds) for the user session	32 bit unsigned Integer	Optional
28	Idle-Timeout	Indicates the timeout value (in seconds) for idle user session	32 bit unsigned Integer	Optional
26/311	MS- Primary-DNS-server	Contains the primary DNS server address for this APN	IPv4	Optional Note 37
26/311	MS-Secondary-DNS-Server	Contains the secondary DNS server address for this APN	IPv4	Optional Note 37
26/311	MS-Primary-NBNS-Server	Contains the primary NetBios name server address for this APN	IPv4	Optional Note 37
26/311	MS-Secondary-NBNS-Server	Contains the secondary NetBios server address for this APN	IPv4	Optional Note 37
26/10415 /17	3GPP-IPv6-DNS-Servers	List of IPv6 addresses of DNS servers for this APN	IPv6	Optional Note 37
NOTE 14: The presence of this attribute is conditional upon this attribute being received in the Access-Accept message. NOTE 25: Either IPv4 or IPv6 address/prefix attribute shall be present. The IP protocol version for end-user and network may be different. NOTE 37: Either IPv4 or IPv6 address attribute shall be present.				

16.4.3 Accounting-Request START (sent from GGSN to AAA server)

The table 3 describes the attributes of the Accounting-Request START message.

Table 3: The attributes of the Accounting-Request START message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username provided by the user (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used). If no username is available a generic username, configurable on a per APN basis, shall be present. If the User-Name has been received in the Access-Accept message, this user-name shall be used in preference to the above	String	Optional
4	NAS-IP-Address	GGSN IP address for communication with the AAA server.	IPv4	Conditional Notes 31 and 35
95	NAS-IPv6-Address	GGSN IPv6 address for communication with the AAA server.	IPv6	Conditional Notes 31 and 35
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 31
6	Service-Type	Indicates the type of service for this user	Framed	Optional
7	Framed Protocol	Indicates the type of protocol for this user	7 (GPRS PDP Context)	Optional
8	Framed-IP-Address	User IP address	IPv4	Conditional Note 35
97	Framed-IPv6-Prefix	User IPv6 Prefix	IPv6	Conditional Note 35
96	Framed-Interface-Id	User IPv6 Interface Identifier	IPv6	Conditional Notes 35 and 46
25	Class	Received in the access accept	String	Conditional (NoteOTE 24)
30	Called-Station-Id	Identifier for the target network	APN (UTF-8 encoded)	Mandatory
31	Calling-Station-Id	This attribute is the identifier for the MS, and it shall be configurable on a per APN basis.	MSISDN in international format according to 3GPP TS 23.003 [40], UTF-8 encoded decimal. Note that there are no leading characters in front of the country code. (Note 6)	Optional
40	Acct-Status-Type	Type of accounting message	START	Mandatory
41	Acct-Delay-Time	Indicates how many seconds the GGSN has been trying to send this record for, and can be subtracted from the time of arrival on the AAA server to find the approximate time (in seconds) of the event generating this Accounting-Request.	32 unsigned integer	Optional

Attr #	Attribute Name	Description	Content	Presence Requirement
44	Acct-Session-Id	User session identifier.	GGSN IP address (IPv4 or IPv6) and Charging-ID concatenated in a UTF-8 encoded hexadecimal. ~~NOTE: The GGSN IP address is the same as that used in the GCDRs.~~(Note 5)	Mandatory
45	Acct-Authentic	Authentication method	RADIUS or LOCAL	Optional
61	NAS-Port-Type	Port type for the GGSN	As per RFC 2865 [38]	Optional
26/10415	3GPP Vendor-Specific	Sub-attributes according ~~sub-clause~~subclause 16.4.7.	See ~~sub-clause~~subclause 16.4.7	Optional except sub-attribute 3 which is conditional
NOTE 1~~3~~: Either NAS-IP-Address or NAS-Identifier shall be present. NOTE 4~~2~~: The presence of this attribute is conditional upon this attribute being received in the Access-Accept message. NOTE 3~~5~~: ~~-~~Either IPv4 or IPv6 address/prefix attribute shall be present. The IP protocol version for end-user and network may be different. NOTE 4~~6~~: ~~-~~Included if the prefix alone is not unique for the user. This may be the case, for example, if address is assigned using stateful address autoconfiguration or if a static IPv6 address. NOTE 5: The GGSN IP address is the same as that used in the GCDRs. NOTE 6: There are no leading characters in front of the country code.				

16.4.4 Accounting Request STOP (sent from GGSN to AAA server)

T~~he t~~able 4 describes the attributes of the Accounting-Request STOP message.

Table 4: The attributes of the Accounting-Request STOP message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username provided by the user (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used). If no username is available a generic username, configurable on a per APN basis, shall be present. If the User-Name has been received in the Access-Accept message, this user-name shall be used in preference to the above	String	Optional
4	NAS-IP-Address	IP address of the GGSN for communication with the AAA server.	IPv4	Conditional Notes ~~3~~1 and 3~~, 5~~
95	NAS-IPv6-Address	IP address of the GGSN for communication with the AAA server.	IPv6	Conditional Notes ~~3~~1 and 3~~, 5~~
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note ~~3~~1
6	Service-Type	Indicates the type of service for this user	Framed	Optional
7	Framed Protocol	Indicates the type of protocol for this user	7 (GPRS PDP Context)	Optional
8	Framed-IP-Address	User IP address	IPv4	Conditional

Attr #	Attribute Name	Description	Content	Presence Requirement
				Note ~~5~~3
97	Framed-IPv6-Prefix	User IPv6 Prefix	IPv6	Conditional Note ~~5~~3
96	Framed-Interface-Id	User IPv6 Interface Identifier	IPv6	Conditional Notes ~~5~~3 and 4~~, 6~~
25	Class	Received in the access accept	String	Optional (N~~OTE 4~~ote 2)
30	Called-Station-Id	Identifier for the target network	APN (UTF-8 encoded)	Mandatory
31	Calling-Station-Id	This attribute is the identifier for the MS, and it shall be configurable on a per APN basis.	MSISDN in international format according to 3GPP TS 23.003 [40], UTF-8 encoded. ~~Note that there are no leading characters in front of the country code.~~ (Note 6)	Optional
40	Acct-Status-Type	Indicates the type of accounting request	STOP	Mandatory
41	Acct-Delay-Time	Indicates how many seconds the GGSN has been trying to send this record for, and can be subtracted from the time of arrival on the AAA server to find the approximate time of the event generating this Accounting-Request	Second	Optional
42	Acct-Input-Octets	GGSN counted number of octets sent by the user for the PDP context	32 bit unsigned integer	Optional
43	Acct-Output-Octets	GGSN counted number of octets received by the user for the PDP context	32 bit unsigned integer	Optional
44	Acct-Session-Id	User session identifier.	GGSN IP address (IPv4 or IPv6) and Charging-ID concatenated in a UTF-8 encoded hexadecimal. ~~NOTE: The GGSN IP address is the same as that used in the GCDRs.~~(Note 5)	Mandatory
45	Acct-Authentic	Authentication method	RADIUS or LOCAL	Optional
46	Acct-Session-Time	Duration of the session	Second	Optional
47	Acct-Input-Packets	GGSN counted number of packets sent by the user	Packet	Optional
48	Acct-Output-Packets	GGSN counted number of packets received by the user	Packet	Optional
49	Acct-Terminate-Cause	Indicate how the session was terminated	See RFC 2866 [39]	Optional
61	NAS-Port-Type	Port type for the GGSN	As per RFC 2865 [38]	Optional
26/10415	3GPP Vendor-Specific	Sub-attributes according to ~~sub-clause~~subclause 16.4.7.	See ~~sub-clause~~subclause 16.4.7	Optional except sub-attribute 3 which is conditional

Attr #	Attribute Name	Description	Content	Presence Requirement
NOTE 1~~3~~: Either NAS-IP-Address or NAS-Identifier shall be present. NOTE 2~~4~~: The presence of this attribute is conditional upon this attribute being received in the Access-Accept message. NOTE 3~~5~~:-Either IPv4 or IPv6 address/prefix attribute shall be present. The IP protocol version for end-user and network may be different. NOTE 4~~6~~:-Included if the prefix alone is not unique for the user. This may be the case, for example, if address is assigned using stateful address autoconfiguration or if a static IPv6 address. NOTE 5: The GGSN IP address is the same as that used in the GCDRs. NOTE 6: There are no leading characters in front of the country code				

16.4.5 Accounting Request ON (optionally sent from GGSN to AAA server)

T~~he t~~able 5 describes the attributes of the Accounting-Request ON message.

Table 5: The attributes of the Accounting-Request ON message

Attr #	Attribute Name	Description	Content	Presence Requirement
4	NAS-IP-Address	IP address of the GGSN for communication with the AAA server.	IPv4	Conditional Notes 1 and 2~~3, 7~~
95	NAS-IPv6-Address	IP address of the GGSN for communication with the AAA server.	IPv6	Conditional Notes 1 and 2~~3, 7~~
30	Called-Station-ID	Identifier for the target network.	APN (UTF-8 encoded)	Optional
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 1~~3~~
NOTE ~~3~~1: Either NAS-IP-Address or NAS-Identifier shall be present. NOTE 2~~:7.~~ Either IPv4 or IPv6 address attribute shall be present.				

16.4.6 Accounting Request OFF (optionally sent from GGSN to AAA server)

T~~he t~~able 6 describes the attributes of the Accounting-Request OFF message.

Table 6: The attributes of the Accounting-Request OFF message

Attr #	Attribute Name	Description	Content	Presence Requirement
4	NAS-IP-Address	IP address of the GGSN for communication with the AAA server.	IPv4	Conditional Notes ~~3, 7~~1 and 2
95	NAS-IPv6-Address	IP address of the GGSN for communication with the AAA server.	IPv6	Conditional Notes ~~3, 7~~1 and 2
30	Called-Station-ID	Identifier for the target network.	APN (UTF-8 encoded)	Optional
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note ~~3~~1
NOTE 1~~3~~: Either NAS-IP-Address or NAS-Identifier shall be present. NOTE 2~~7~~: Either IPv4 or IPv6 address attribute shall be present.				

16.4.7 Sub-attributes of the 3GPP Vendor-Specific attribute

~~The table below~~Table 7 describes the sub-attributes of the 3GPP Vendor-Specific attribute of the Access-Request, Accounting-Request START, Accounting-Request STOP and Accounting-Request Interim-Update messages.

Table 7: The sub-attributes of the 3GPP Vendor-Specific attribute of the Access-Request, ~~-~~Accounting-Request START, Accounting-Request STOP ~~-~~and Accounting-Request Interim-Update messages

Sub-attr #	Sub-attribute Name	Description	Presence Requirement	Associated attribute (Location of Sub-attr)

Sub-attr #	Sub-attribute Name	Description	Presence Requirement	Associated attribute (Location of Sub-attr)
1	3GPP-IMSI	IMSI for this user	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
2	3GPP-Charging-Id	Charging ID for this PDP Context (this together with the GGSN-Address constitutes a unique identifier for the PDP context).	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
3	3GPP-PDP Type	Type of PDP context, e.g. IP or PPP	Conditional (mandatory if attribute 7 is present)	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
4	3GPP-CG-Address	Charging Gateway IP address	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
5	3GPP-GPRS-QoS-Negotiated-Profile	QoS profile applied by GGSN	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
6	3GPP-SGSN-Address	SGSN IP address that is used by the GTP control plane for the handling of control messages. It may be used to identify the PLMN to which the user is attached.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
7	3GPP-GGSN-Address	GGSN IP address that is used by the GTP control plane for the context establishment. It is the same as the GGSN IP address used in the GCDRs.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
8	3GPP-IMSI-MCC-MNC	MCC and MNC extracted from the user's IMSI (first 5 or 6 digits, as applicable from the presented IMSI).	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
9	3GPP-GGSN- MCC-MNC	MCC-MNC of the network the GGSN belongs to.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
10	3GPP-NSAPI	Identifies a particular PDP	Optional	Access-Request, Accounting-Request

Sub-attr #	Sub-attribute Name	Description	Presence Requirement	Associated attribute (Location of Sub-attr)
		context for the associated PDN and MSISDN/IMSI from creation to deletion.		START, Accounting-Request STOP Accounting-Request Interim-Update
11	3GPP- Session-Stop-Indicator	Indicates to the AAA server that the last PDP context of a session is released and that the PDP session has been terminated.	Optional	Accounting Request STOP
12	3GPP- Selection-Mode	Contains the Selection mode for this PDP Context received in the Create PDP Context Request Message	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
13	3GPP-Charging-Characteristics	Contains the charging characteristics for this PDP Context received in the Create PDP Context Request Message (only available in R99 and later releases)	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
14	3GPP-CG-IPv6-Address	Charging Gateway IPv6 address	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
15	3GPP-SGSN-IPv6-Address	SGSN IPv6 address that is used by the GTP control plane for the handling of control messages. It may be used to identify the PLMN to which the user is attached.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
16	3GPP-GGSN-IPv6-Address	GGSN IPv6 address that is used by the GTP control plane for the context establishment.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
17	3GPP- IPv6-DNS-Servers	List of IPv6 addresses of DNS servers for an APN	Optional	Access-Accept
18	3GPP-SGSN-MCC-MNC	MCC and MNC extracted from the RAI within the Create PDP Context Request or Update PDP Context Request message.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update

The RADIUS vendor Attribute is encoded as follows (as per RFC 2865 [38])

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1	Type = 26							
2	Length = n							
3	Vendor id octet 1							
4	Vendor id octet 2							
5	Vendor id octet 3							
6	Vendor id octet 4							
7-n	String							

n ≥ ~~>=~~7

3GPP Vendor Id = 10415

The string part is encoded as follows:

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1	3GPP type =							
2	3GPP Length = m							
3 –m	3GPP value							

m ≥ ~~>=~~2 and m ≤ ~~<=~~ 248

The 3GPP specific attributes encoding is clarified below.

1 **-** ~~-~~3GPP-***IMSI***

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1	3GPP type = 1							
2	3GPP Length= m							
3-m	IMSI digits 1-n (UTF-8 encoded)							

3GPP Type: 1

n ≤ ~~<=~~15

Length: m =17

IMSI value: Text:

This is the UTF-8 encoded IMSI; The definition of IMSI shall be in accordance with 3GPP TS 23.003 [40] and 3GPP TS 29.060 [24]~~[41]~~. There shall be no padding characters between the MCC and MNC, and between the MNC and MSIN. If the IMSI is less than 15 digits, the padding in the GTP information element shall be removed by the GGSN and not encoded in this sub-attribute.

2 - 3GPP-***Charging ID***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 2							
2	3GPP Length= 6							
3	Charging ID value Octet 1							
4	Charging ID value Octet 2							
5	Charging ID value Octet 3							
6	Charging ID value Octet 4							

3GPP Type: 2

Length: 6

Charging ID value: 32 bits unsigned integer

3 - 3GPP-***PDP type***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 3							
2	3GPP Length= 6							
3	PDP type octet 1							
4	PDP type octet 2							
5	PDP type octet 3							
6	PDP type octet 4							

3GPP Type: 3

Length: 6

PDP type value: Unsigned 32 bits integer

PDP type octet possible values:

0 = IPv4

1 = PPP

2 = IPv6

4 - 3GPP-***Charging Gateway address***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 4							
2	3GPP Length= 6							
3	Charging GW addr Octet 1							
4	Charging GW addr Octet 2							
5	Charging GW addr Octet 3							
6	Charging GW addr Octet 4							

3GPP Type: 4

Length: 6

Charging GW address value: -Address

5 **-** 3GPP-***GPRS Negotiated QoS profile***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 5							
2	3GPP Length= L							
3 -L	UTF-8 encoded QoS profile							

3GPP Type: 5

Length: -27 (release 99) or 11 (release 98)

QoS profile value: Text

UTF-8 encoded QoS profile syntax:

“"<Release indicator> – <release specific QoS IE UTF-8 encoding>”"

<Release indicator> = UTF-8 encoded number :

“"98”" = Release 98

“"99”"= Release 99

<release specific QoS profile UTF-8 encoding> = UTF-8 encoded QoS profile for the release indicated by the release indicator.

The UTF-8 encoding of a QoS IE is defined as follows: each octet is described by 2 UTF-8 encoded digits, defining its hexadecimal representation. The QoS profile definition is in 3GPP TS 24.008 [23].

The release 98 QoS profile data is 3 octets long, which then results in a 6 octets UTF-8 encoded string,

The release 99 QoS profile data is 11 octets long, which results in a 22 octets UTF-8 encoded string.

6 **-** 3GPP-***SGSN address***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 6							
2	3GPP Length= 6							
3	SGSN addr Octet 1							
4	SGSN addr Octet 2							
5	SGSN addr Octet 3							
6	SGSN addr Octet 4							

3GPP Type: 6

Length: 6

SGSN address value: -Address

7 - 3GPP-***GGSN address***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 7							
2	3GPP Length= 6							
3	GGSN addr Octet 1							
4	GGSN addr Octet 2							
5	GGSN addr Octet 3							
6	GGSN addr Octet 4							

3GPP Type: 7

Length: 6

GGSN address value: -Address

8 - 3GPP-***IMSI MCC-MNC***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 8							
2	3GPP Length= n							
3	MCC digit1 (UTF-8 encoded)							
4	MCC digit2 (UTF-8 encoded)							
5	MCC digit3 (UTF-8 encoded)							
6	MNC digit1 (UTF-8 encoded)							
7	MNC digit2 (UTF-8 encoded)							
8	MNC digit3 if present (UTF-8 encoded)							

3GPP Type: 8

Length: n shall be 7 or 8 octets depending on the presence of MNC digit 3

MS address value: -text

This is the UTF-8 encoding of the MS MCC-MNC values. In accordance with 3GPP TS 23.003 [40] and 3GPP TS 29.060 [24] ~~[41]~~ the MCC shall be 3 digits and the MNC shall be either 2 or 3 digits. There shall be no padding characters between the MCC and MNC.

9 - 3GPP-***GGSN MCC-MNC***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 9							
2	3GPP Length= n							
3	MCC digit1 (UTF-8 encoded)							
4	MCC digit2 (UTF-8 encoded)							
5	MCC digit3 (UTF-8 encoded)							
6	MNC digit1 (UTF-8 encoded)							
7	MNC digit2 (UTF-8 encoded)							
8	MNC digit3 if present (UTF-8 encoded)							

3GPP Type: 9

Length: n shall be 7 or 8 octets depending on the presence of MNC digit 3

GGSN address value: ~~-~~text

This is the UTF-8 encoding of the GGSN MCC-MNC values. In accordance with 3GPP TS 23.003 [40] and 3GPP TS 29.060 [24] ~~[41]~~ the MCC shall be 3 digits and the MNC shall be either 2 or 3 digits. There shall be no padding characters between the MCC and MNC.

10 - 3GPP-***NSAPI***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 10							
2	3GPP Length= 3							
3	NSAPI							

3GPP Type: 10

Length: 3

NSAPI value: text

It is the value of the NSAPI of the PDP context the RADIUS message is related to. It is encoded as its hexadecimal representation, using 1UTF-8 encoded digit.

11 - 3GPP-***Session Stop Indicator***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 11							
2	3GPP Length= 3							
3	1 1 1 1 1 1 1 1							

3GPP Type: 11

Length: -3

-Value is set to all 1.

12 - 3GPP-***Selection-Mode***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 12							
2	3GPP Length= 1							
3	UTF-8 encoded Selection mode string							

3GPP Type: 12

Length: -3

Selection mode value: Text

The format of this attribute shall be a character string consisting of a single digit, mapping from the binary value of the selection mode in the Create PDP Context message (3GPP TS 29.060 [24]). Where 3GPP TS 29.060 [24] provides for interpretation of the value, e.g. map -'3-' to -'2-', this shall be done by the GGSN.

13 - 3GPP-***Charging-Characteristics***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 13							
2	3GPP Length= 6							
3-6	UTF-8 encoded Charging Characteristics value							

3GPP Type: 13

Length: -6

Charging characteristics value: -Text

The charging characteristics is value is the value of the 2 octets value field taken from the GTP IE described in 3GPP TS 29.060 [24], subclause~~section~~ 7.7.23.

Each octet of this IE field value is represented via 2 UTF-8 encoded digits, defining its hexadecimal representation.

14 - 3GPP-***Charging Gateway IPv6 address***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 14							
2	3GPP Length= 18							
3	Charging GW IPv6 addr Octet 1							
4	Charging GW IPv6 addr Octet 2							
5-18	Charging GW IPv6 addr Octet 3-16							

3GPP Type: 14

Length: 18

Charging GW IPv6 address value: IPv6 Address

15 - 3GPP-***SGSN IPv6 address***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 15							
2	3GPP Length= 18							
3	SGSN IPv6 addr Octet 1							
4	SGSN IPv6 addr Octet 2							
5-18	SGSN IPv6 addr Octet 3-16							

3GPP Type: 15

Length: 18

SGSN IPv6 address value: IPv6 Address

16 -- 3GPP-***GGSN IPv6 address***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 16							
2	3GPP Length= 18							
3	GGSN IPv6 addr Octet 1							
4	GGSN IPv6 addr Octet 2							
5-18	GGSN IPv6 addr Octet 3-16							

3GPP Type: 16

Length: 18

GGSN IPv6 address value: IPv6 Address

17 -- 3GPP-***IPv6-DNS-Servers***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 17							
2	3GPP Length= m							
3-18	(1st) DNS IPv6 addr Octet 1-16							
19-34	(2nd) DNS IPv6 addr Octet 1-16							
k-m	(n-th) DNS IPv6 addr Octet 1-16							

3GPP Type: 17

Length: m = n × *16 + 2; –n ≥ >=1 and n ≤ <=15;— k = m-15

IPv6 DNS Server value: -IPv6 Address The 3GPP- IPv6-DNS-Servers Attribute provides a list of one or more (-'n-') IPv6 addresses of Domain Name Server (DNS) servers for an APN. The DNS servers are listed in the order of preference for use by a client resolver, i.e. the first is -'Primary DNS Server-', the second is -'Secondary DNS Server-' etc. The attribute may be included in Access-Accept packets.

18 - 3GPP-***SGSN MCC-MNC***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 18							
2	3GPP Length= n							
3	MCC digit1 (UTF-8 encoded)							
4	MCC digit2 (UTF-8 encoded)							
5	MCC digit3 (UTF-8 encoded)							
6	MNC digit1 (UTF-8 encoded)							
7	MNC digit2 (UTF-8 encoded)							
8	MNC digit3 if present (UTF-8 encoded)							

3GPP Type: 18

Length: n shall be 7 or 8 octets depending on the presence of MNC digit 3

SGSN address value: -text

This is the UTF-8 encoding of the RAI MCC-MNC values. In accordance with 3GPP TS 23.003 [40] and 3GPP TS 29.060 [24] ~~and [41]~~ the MCC shall be 3 digits and the MNC shall be either 2 or 3 digits. There shall be no padding characters between the MCC and MNC.

16.4.8 Accounting Request Interim-Update (sent from GGSN to AAA server)

T~~he t~~able 8 describes the attributes of the Accounting-Request Interim-Update message.

Table 8: The attributes of the Accounting-Request Interim-Update message

Attr #	Attribute Name	Description	Content	Presence Requirement

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username provided by the user (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used). If no username is available a generic username, configurable on a per APN basis, shall be present. If the User-Name has been received in the Access-Accept message, this user-name shall be used in preference to the above	String	Optional
4	NAS-IP-Address	IP address of the GGSN for communication with the AAA server.	IPv4	Conditional Notes ~~3, 5~~1 and 3
95	NAS-IPv6-Address	IP address of the GGSN for communication with the AAA server.	IPv6	Conditional Notes 1 and ~~3~~3, ~~5~~
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 1~~3~~
6	Service-Type	Indicates the type of service for this user	Framed	Optional
7	Framed Protocol	Indicates the type of protocol for this user	7 (GPRS PDP Context)	Optional
8	Framed-IP-Address	User IP address	IPv4	Conditional Note 3~~5~~
97	Framed-IPv6-Prefix	User IPv6 address	IPv6	Conditional Note 3~~5~~
96	Framed-Interface-Id	User IPv6 Interface Identifier	IPv6	Conditional Notes 3 and 4~~5, 6~~
25	Class	Received in the access accept	String	Optional (Note 2~~OTE 4~~)
30	Called-Station-Id	Identifier for the target network	APN (UTF-8 encoded)	Mandatory
31	Calling-Station-Id	This attribute is the identifier for the MS, and it shall be configurable on a per APN basis.	MSISDN in international format according to 3GPP TS 23.003 [40], UTF-8 encoded. ~~Note that there are no leading characters in front of the country code.~~ (Note 6).	Optional
40	Acct-Status-Type	Indicates the type of accounting request	Interim-Update	Mandatory
41	Acct-Delay-Time	Indicates how many seconds the GGSN has been trying to send this record for, and can be subtracted from the time of arrival on the AAA server to find the approximate time of the event generating this Accounting-Request	Second	Optional
42	Acct-Input-Octets	GGSN counted number of octets sent by the user for the PDP context	32 bit unsigned integer	Optional
43	Acct-Output-Octets	GGSN counted number of octets received by the user for the PDP context	32 bit unsigned integer	Optional
44	Acct-Session-Id	User session identifier.	GGSN IP address (IPv4 or IPV6) and Charging-ID concatenated in a UTF-8 encoded hexadecimal. ~~NOTE: The GGSN IP address is the~~	Mandatory

Attr #	Attribute Name	Description	Content	Presence Requirement
			~~same as that used in the GCDRs.~~(Note 5)	
45	Acct-Authentic	Authentication method	RADIUS or LOCAL	Optional
46	Acct-Session-Time	Duration of the session	Second	Optional
47	Acct-Input-Packets	GGSN counted number of packets sent by the user	Packet	Optional
48	Acct-Output-Packets	GGSN counted number of packets received by the user	Packet	Optional
61	NAS-Port-Type	Port type for the GGSN	As per RFC 2865 [38]	Optional
26/10415	3GPP Vendor-Specific	Sub-attributes according to ~~sub-clause~~subclause 16.4.7.	See ~~sub-clause~~subclause 16.4.7	Optional except sub-attribute 3 which is conditional

NOTE ~~3~~1: Either NAS-IP-Address or NAS-Identifier shall be present.
NOTE 2~~4~~: The presence of this attribute is conditional upon this attribute being received in the Access-Accept message
NOTE 3~~5~~:~~-~~Either IPv4 or IPv6 address/prefix attribute shall be present. The IP protocol version for end-user and network may be different.
NOTE 4~~6~~:~~-~~Included if the prefix alone is not unique for the user. This may be the case, for example, if address is assigned using stateful address autoconfiguration or if a static IPv6 address.
NOTE 5: The GGSN IP address is the same as that used in the GCDRs.
NOTE 6: There are no leading characters in front of the country code.

16.4.9 Disconnect Request (optionally sent from AAA server to GGSN)

T~~he t~~able 9 describes the attributes of the Disconnect-Request message.

Table 9: The attributes of the Disconnect-Request message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username provided by the user (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used). If no username is available a generic username, configurable on a per APN basis, shall be present. If the User-Name has been sent in the Access-Accept message, this user-name shall be used in preference to the above	String	Optional
8	Framed-IP-Address	User IP address	IPv4	Conditional Note 2~~8~~
97	Framed-IPv6-Prefix	User IPv6 address	IPv6	Conditional Note 2~~8~~
96	Framed-Interface-Id	User IPv6 Interface Identifier	IPv6	Conditional Notes ~~6~~1 and 2~~, 8~~
44	Acct-Session-Id	User session identifier.	GGSN IP address (IPv4 or IPv6) and Charging-ID concatenated in a UTF-8 encoded hexadecimal. ~~NOTE: The GGSN IP address is the same as that used in the GCDRs.~~(Note 3)	Mandatory
NOTE 1~~6~~: ~~-~~Included if the prefix alone is not unique for the user. This may be the case, for example, if address is assigned using stateful address autoconfiguration or if a static IPv6 address. NOTE 2~~8~~: ~~-~~Either IPv4 or IPv6 address/prefix attribute shall be present. NOTE 3: The GGSN IP address is the same as that used in the GCDRs.				

Annex A (informative): Interworking PCS1900 with PSDNs

~~<VOID>~~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
06-2001	TSG#12	NP-010256	017		Clarifications on the non-transparent access mode	3.5.0	3.6.0
06-2001	TSG#12	NP-010256	019		Set the use of PPP between the MT and TE as an option when interworking with MIPv4	3.5.0	3.6.0
09-2001	TSG#13	NP-010530	022		Standard method for information delivery (MSISDN; IP address) between GPRS and external PDN using RADIUS	3.6.0	3.7.0
12-2001	TSG#14	NP-010572	027	1	Correction to the Calling-Station-Id attribute	3.7.0	3.8.0
12-2001	TSG#14	NP-010572	029	1	Correction to 3GPP Vendor specify attribute 3GPP-IMSI	3.7.0	3.8.0
12-2001	TSG#14	NP-010572	031		Correction to 3GPP vendor specific attributes containing MCC-MNC	3.7.0	3.8.0
12-2001	TSG#14	NP-010672	033		Standard method for interworking between GPRS and external PDN using RADIUS	3.7.0	3.8.0
12-2001	TSG#14	NP-010672	034		Standard method for information update between GPRS and external PDN using RADIUS	3.7.0	3.8.0
03-2002	TSG#15	NP-020080	037		Change of associated attribute for 3GPP-NSAPI	3.8.0	3.9.0
06-2002	TSG#16	NP-020295	047	2	Clarification on the Radius Flows	3.9.0	3.10.0
06-2002	TSG#16	NP-020295	053	1	Corrections to the 3GPP RADIUS attributes	3.9.0	3.10.0
06-2002	TSG#16	NP-020171	059		Address autoconfiguration of IPv6 terminals and IPv6 update	3.9.0	3.10.0
12-2002	TSG#18	NP-020613	064		Correction of figure for Radius Accounting Update	3.10.0	3.11.0
12-2002	TSG#18	NP-020614	068		Correction related to IPv6	3.10.0	3.11.0
12-2002	TSG#18	NP-020613	070		RADIUS enhancement for identification of VPLMN	3.10.0	3.11.0

3GPP TSG-CN WG3 Meeting #27
Dublin, Ireland, 10th - 14th February 2003.

Tdoc ⌘N3-030123

CR-Form-v7

CHANGE REQUEST

⌘ **29.061** **CR** **082** ⌘ **rev** **1** ⌘ Current version: **4.6.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Correction of References and specification Corrections
Source:	⌘	TSG_CN WG3 *[Siemens AG, MCC]*
Work item code:	⌘	TEI
Date:	⌘	11/02/2003
Category:	⌘	**A**
Release:	⌘	Rel-4

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Inconsistencies in the specification, Missing and incorrect references
Summary of change:	⌘	Correction of incorrect and missing reference and general specification clean-up
Consequences if not approved:	⌘	Inconsitencies and errors in the referencing. Possible mis understanfing when reading specification.

Clauses affected:	⌘	Most of the specification			
Other specs affected:	⌘	**Y**	**N**		
			X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

3GPP TS 29.061 V4.6.0 (2002-12)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Core Network;
~~Packet Domain;~~
Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and ~~Packet Data~~ Packet Data Networks (PDN)
(Release 4)

Keywords

UMTS, GSM, packet mode, interworking, PLMN, PDN

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

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. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

~~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] Void.

[2] 3GPP TS 22.060: "General Packet Radio Service (GPRS); Service Description~~:~~; Stage 1 ~~Service Description~~".

[3] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service Description; Stage 2".

[4] 3GPP TS 03.61: "~~Point-to-~~Multipoint Multicast Service Description; Stage 2".

[5] 3GPP TS 03.62: "~~Point-to-~~Multipoint Group Call Service Description; Stage 2".

[6] 3GPP TS 03.64: "General Packet Radio Service (GPRS); Overall description of the GPRS radio interface; Stage 2~~Overall description of the Radio interface; Stage 2~~".

[7] 3GPP TS 04.60: "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: "General Packet Radio Service (GPRS); Mobile Station - Serving GPRS Support Node (MS-SGSN) Logical Link Control (LLC) layer specification~~Logical Link Control (LLC)~~".

[9] 3GPP TS 24.065: "General Packet Radio Service (GPRS); Mobile Station (MS) - Serving GPRS Support Node(SGSN); Subnetwork Dependent Convergence Protocol (SNDCP)".

[10] 3GPP TS 27.060: "Packet Domain; Mobile Station (MS) supporting Packet Switched Services".

[11] ITU-T Recommendation E.164: "The international public telecommunication numbering plan~~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~~ names ~~-~~ ~~Concepts~~ concepts and ~~Facilities~~facilities" (STD 7).

[20] Void.

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

[21b] IETF RFC 1662 (1994): "PPP in HDLC-like Framing".

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

[23] 3GPP TS 24.008: "Mobile radio interface layer 3 specification; Core Network ~~Protocols~~protocols; ~~–~~ Stage 3".

[24] 3GPP TS 29.060: "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp ~~Interface~~interface".

[25] IETF RFC 2794 (2000)~~, Pat R. Calhoun and Charles E. Perkins~~: "Mobile IP Network Address Identifier Extension for IPv4", P. Calhoun, C. Perkins~~, 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 RFC 2373 (1998): "IP ~~version~~ Version 6 Addressing Architecture".

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

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

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

[32] IETF RFC 1112 (1989)~~, S.E. Deering~~: "Host extensions for IP multicasting", S.E. Deering.

[33] IETF RFC 2236 (1997)~~, W. Fenner~~: "Internet Group Management Protocol, Version 2", W. Fenner.

[34] IETF RFC 2362 (1998)~~, D. Estrin and al~~: "Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification", D. Estrin, D. Farinacci, A. Helmy, D. Thaler, S. Deering, M. Handley, V. Jacobson, C. Liu, P. Sharma, L. Wei.

[35] IETF RFC 1075 (1988)~~, D. Waitzman and al~~: "Distance Vector Multicast Routing Protocol", D. Waitzman, C. Partridge, S.E. Deering.

[36] IETF RFC 1585 (1994)~~, J. Moy~~: "MOSPF: Analysis and Experience", J. Moy~~-~~.

[37] IETF RFC 2290 (1998)~~, J. Solomon, S. Glass~~: "Mobile-IPv4 Configuration Option for PPP IPCP ", J. Solomon, S. Glass.

[38] IETF RFC 2865 (2000)~~, C. Rigney, S. Willens, A. Rubens, W. Simpson~~: "Remote Authentication Dial In User Service (RADIUS)", C. Rigney, S. Willens, A. Rubens, W. Simpson.

[39] IETF RFC2866 (2000)~~, C. Rigney, Livingston~~: "~~-~~RADIUS Accounting~~-~~", C. Rigney, Livingston.

[40] 3GPP TS 23.003: "~~3rd Generation Partnership Project; Technical Specification Group Core Network;~~ Numbering, addressing and identification".

[41] IETF RFC 2882 (2000)~~, D. Mitton~~: "Network Access Servers Requirements: Extended RADIUS Practices", D. Mitton.

[42] 3GPP TR 21.905: "-Vocabulary for 3GPP Specifications".

[43] IETF RFC 2472 (1998)~~, D. Haskins, E. Allen~~: ~~"~~"IP Version 6 over PPP~~"~~", D. Haskins, E. Allen.

[44] IETF RFC 2461 (1998)~~, T. Narten, E. Nordmark, W. Simpson~~: ~~"~~"Neighbor Discovery for IP Version 6 (IPv6)~~"~~", T. Narten, E. Nordmark, W. Simpson.

[45] IETF RFC 3118 (2001)~~, R. Droms, W. Arbaugh~~: ~~"~~"Authentication for DHCP Messages~~"~~", R. Droms, W. Arbaugh.

[46] IETF Internet-Draft: ~~"~~"Dynamic Host Configuration Protocol for IPv6 (DHCPv6)~~"~~", draft-ietf-dhc-dhcpv6-2~~4~~8.txt, work in progress.

[47] 3GPP TS 24.229: ~~"~~"IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3~~"~~".

[48] IETF RFC 2710 (1999)~~, S. Deering, W. Fenner, B. Haberman~~: ~~"~~"Multicast Listener Discovery (MLD) for IPv6~~"~~", S. Deering, W. Fenner, B. Haberman.

[49] IETF RFC 2460 (1998)~~, S.Deering,, R.Hinden~~: ~~"~~"Internet Protocol, Version 6 (IPv6) Specification~~"~~", S.Deering,, R.Hinden.

[50] IETF RFC 3162 (2001)~~, B. Adoba, G. Zorn, D. Mitton~~: ~~"~~"RADIUS and IPv6~~"~~", B. Adoba, G. Zorn, D. Mitton.

[51] IETF RFC 2548 (1999)~~, G.Zorn~~: ~~"~~"Microsoft Vendor-specific RADIUS Attributes~~"~~"-, G.Zorn.

[52] IETF RFC 1035 (1987): "Domain names - implementation and specification".

[53] IETF RFC 1771 (1995): "A Border Gateway Protocol 4 (BGP-4)".

[54] IETF RFC 1825 (1995): "Security Architecture for the Internet Protocol".

[55] IETF RFC 1826 (1995): "IP Authentication Header".

[56] IETF RFC 1827 (1995): "IP Encapsulating Security Payload (ESP)".

3 Definitions, abbreviations and symbols

3.1 Definitions

For the purposes of the present document, the ~~following~~ terms and definitions given in 3GPP TS 22.060 [2] and 3GPP TS -23.060 [3] 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

DHCPv6	Dynamic Host Configuration Protocol version 6
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
IPCP	IP Control Protocol (PPP NCP for IPv4)
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPV6CP	IPv6 Control Protocol (PPP NCP for IPv6)
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
LAC	L2TP Access Concentrator
LAN	Local Area Network
LNS	L2TP Network Server
MIP	Mobile IP
MLD	Multicast Listener Discovery
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 Independent 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 [2] and 3GPP TS 23.060 [3].

4.2 Key characteristics of PSDN

~~<VOID>~~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 [40] 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.

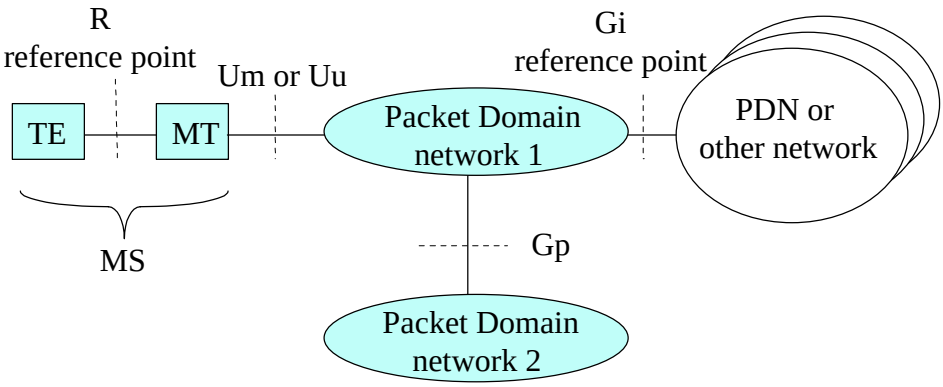


Figure 1: Packet Domain Access Interfaces and Reference Points

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 [3].

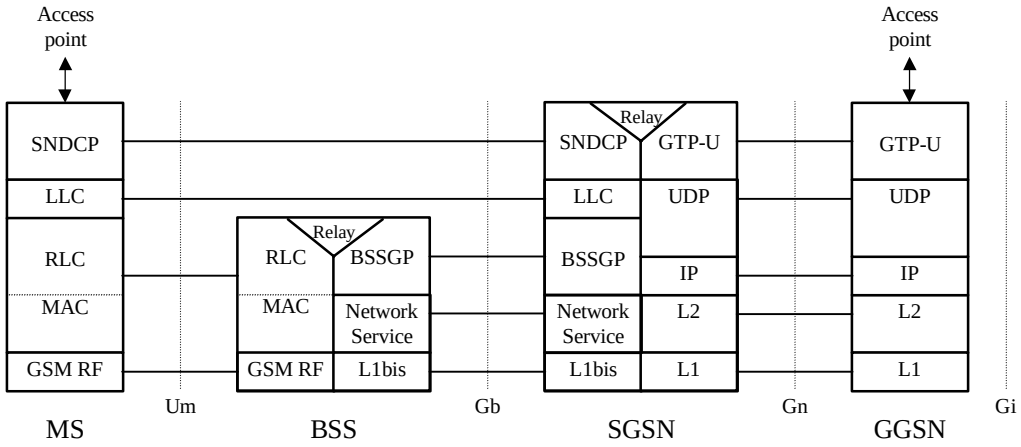


Figure 2a: User Plane for Packet Domain services in GSM

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 [3].

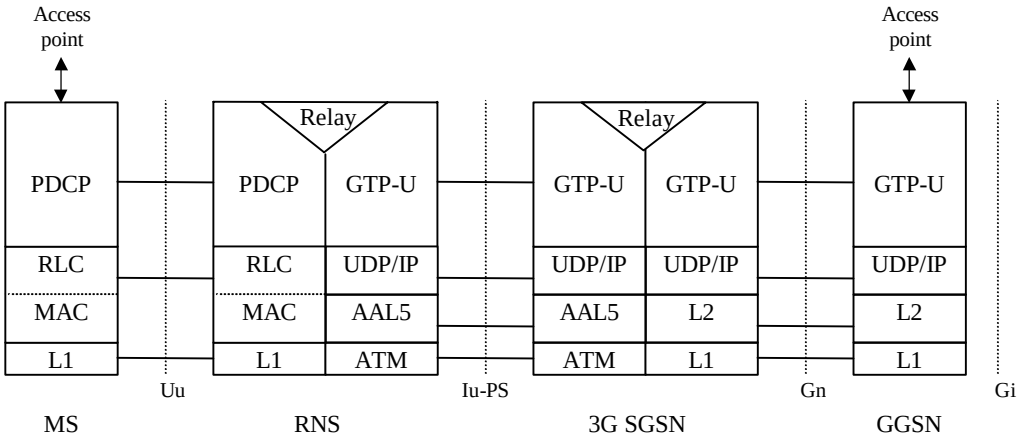


Figure 2b: User Plane for Packet Domain services in UMTS

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 [3]. 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 [2] and 3GPP TS 23.060 [3]. 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)

Figure 3: Void

Figure 4: Void

Figure 5: Void

Figure 6: Void~~<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~~IPv6. The interworking point with IP networks is at the Gi reference point as shown in figure 7.

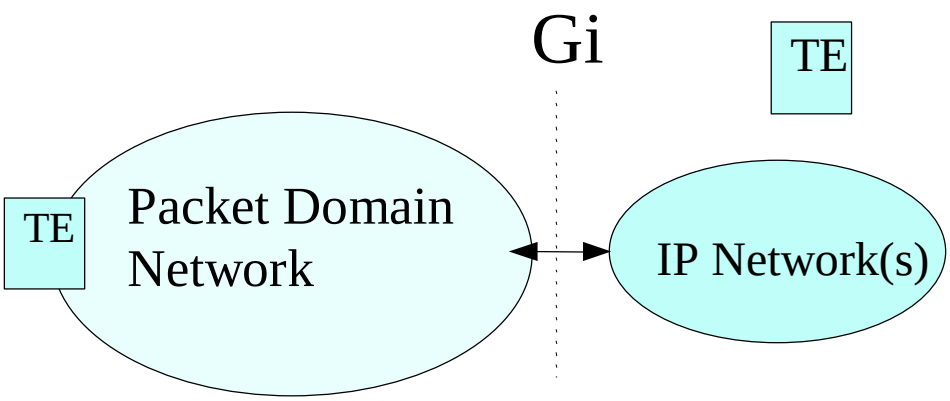


Figure 7: IP network interworking

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.

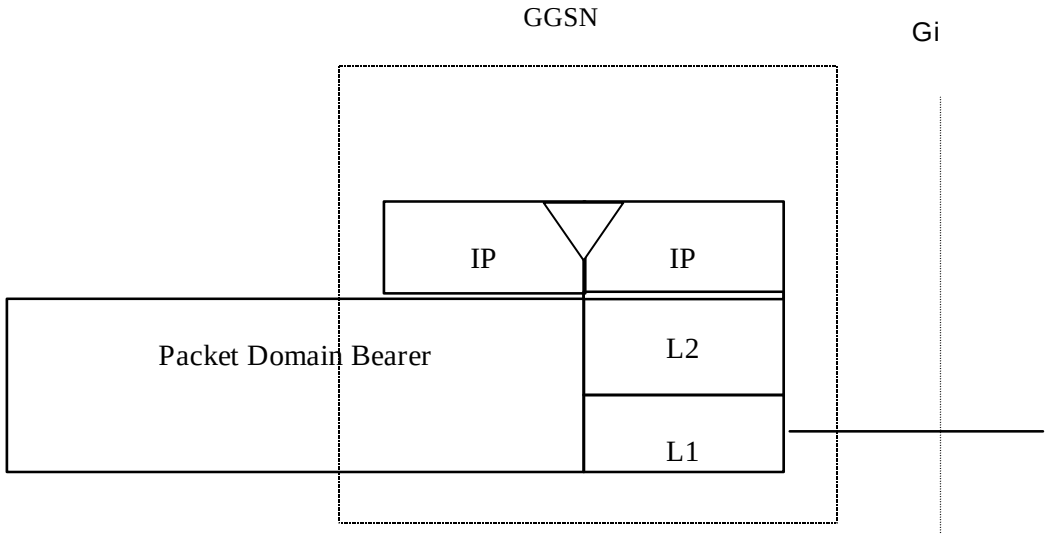


Figure 8: The protocol stacks for the IP / Gi reference point

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, IPv6 address autoconfiguration, 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.

The mechanisms for host configuration and user authentication described in this ~~section~~subclause and its sub-~~section~~clauses are only applicable to the activation of the first context activated for a specific PDP address (using the ~~"~~'PDP Context Activation Procedure~~"~~'). The activation of any subsequent PDP contexts for that PDP address, using the ~~"~~'Secondary PDP Context Activation Procedure~~"~~', as well as the use of TFTs, is described in 3GPP TS 23.060 [3].

11.2.1.1 Transparent access to the Internet

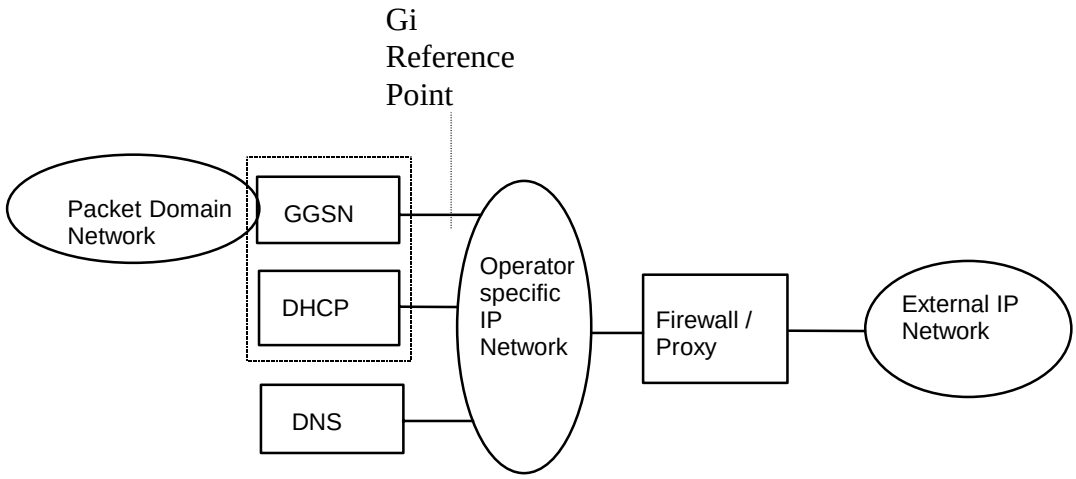


Figure 9: Example of the PDN Interworking Model, transparent case

In this case (see figure 9):

- the MS is given an address or IPv6 Prefix belonging to the operator addressing space. The address or IPv6 Prefix 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 or IPv6 Prefix is used for packet forwarding between the Internet and the GGSN and within the packet domain. With IPv6, either Stateless or Stateful Address Autoconfiguration shall be used to assign an IPv6 address to the MS. These procedures are as described in the IPv6 non-transparent access case except that the addresses belong to the operator addressing space. The use of stateful or stateless is configured per APN.

- 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.

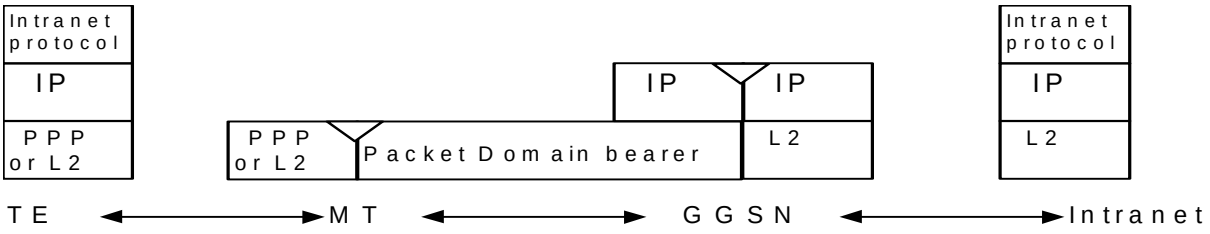


Figure 10: Transparent access to an Intranet

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 pProtocol»".

User authentication and encryption of user data are done within the «"Intranet pProtocol»" 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 [54]). 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 [55] and RFC 1827 [56]). In this case private IP tunnelling within public IP takes place.

11.2.1.2 IPv4 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 AAA, 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 AAA, DHCP, …, belonging to the Intranet/ISP;

- the protocol configuration options are retrieved (if requested by the MS at PDP context activation) from some server (AAA 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.

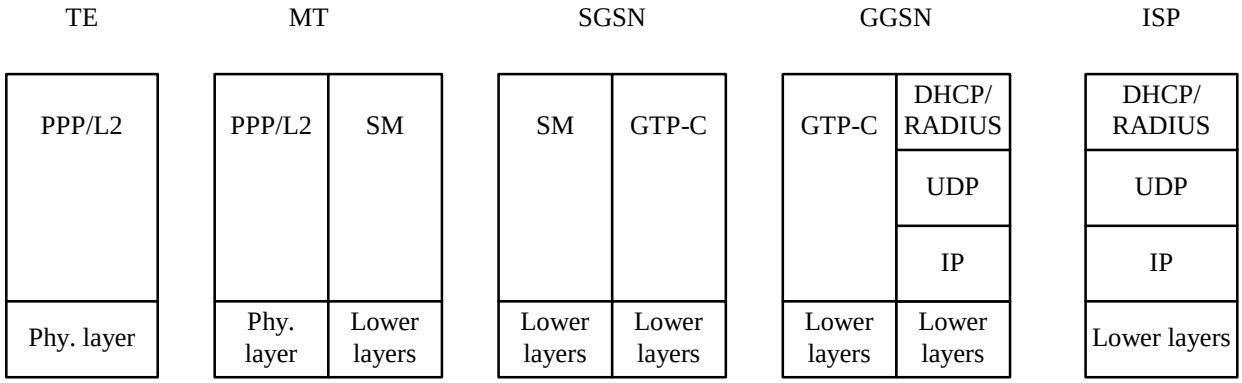


Figure 11a: Signalling plane of non transparent case

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 AAA 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 AAA 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 1661 [21a] and RFC 1662 [21b] 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.

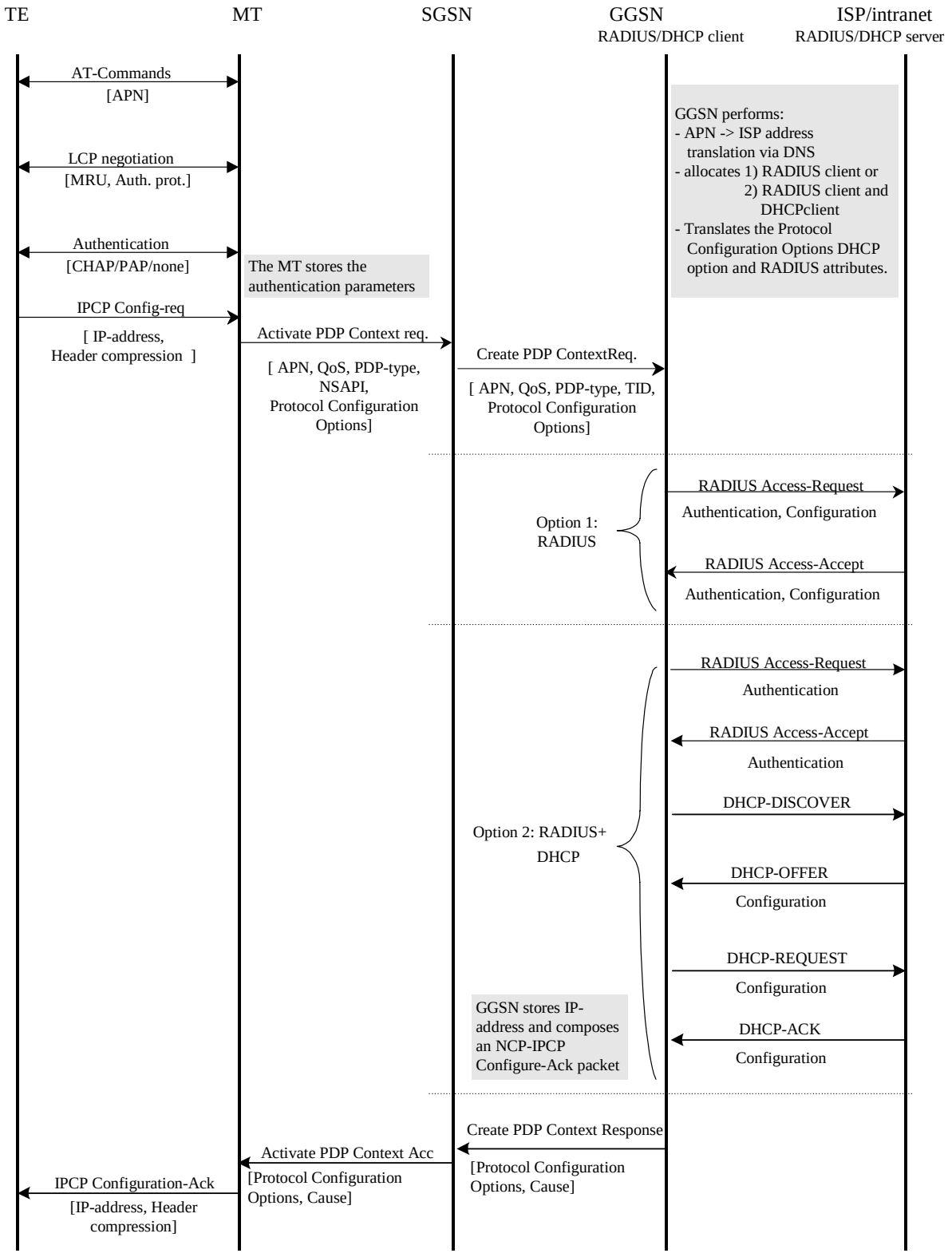


Figure 11b: PDP Context Activation for the IPv4 Non-transparent case

11.2.1.3 IPv6 Non Transparent access to an Intranet or ISP

When using IPv6 Address Autoconfiguration (either Stateless or Stateful), the process of setting up the access to an Intranet or ISP involves two signalling phases. The first signalling phase is done in the control plane and consists of the PDP context activation, followed by a second signalling phase done in the user plane.

The user plane signalling phase shall be either stateless or stateful. The stateless procedure, which involves only the MS and the GGSN, is described in subclause "IPv6 Stateless Address Autoconfiguration". The stateful procedure, which involves the MS, GGSN (as DHCP relay agent) and one or several DHCP servers on the Intranet or ISP, is described in subclause "IPv6 Stateful Address Autoconfiguration".

Whether to use stateless or stateful address autoconfiguration procedure is configured per APN in the GGSN. For APNs configured as stateless, the GGSN shall only use the Prefix part of the IPv6 address for forwarding of mobile terminated IP packets. The size of the prefix shall be according to the maximum prefix length for a global IPv6 address as specified in the IPv6 Addressing Architecture, see RFC 2373 [28].

Stateful and Stateless Autoconfiguration may also co-exist. In that case, the MS shall use Stateless to configure the address and Stateful to configure additional parameters only. The MS shall not use Stateless and Stateful Address Autoconfiguration simultaneously since GPRS only supports one prefix per PDP Context (see 3GPP TS 23.060 [3]).

The selection between Stateful and Stateless Autoconfiguration is dictated by the Router Advertisements sent by the GGSN as described in the corresponding subclauses below and according to the principles defined in RFC 2461 [44] and RFC 2462 [29].

For MS, IPv6 Stateless Address Autoconfiguration is mandatory, and IPv6 Stateful Address Autoconfiguration is optional.

11.2.1.3.1 IPv6 PDP Context Activation

In this case:

- The GGSN provides the MS with an IPv6 Prefix belonging to the Intranet/ISP addressing space. A dynamic IPv6 address shall be given using either stateless or stateful address autoconfiguration. This IPv6 address is used for packet forwarding within the packet domain and for packet forwarding on the Intranet/ISP;
- the MS may send an authentication request at PDP context activation and the GGSN may request user authentication from a server, e.g. AAA, …, belonging to the Intranet/ISP;
- the protocol configuration options are retrieved (if requested by the MS at PDP context activation) from some server, e.g. AAA, …, belonging to the Intranet/ISP;
- in order to avoid any conflict between the link-local address of the MS and that of the GGSN, the Interface-Identifier used by the MS to build its link-local address shall be assigned by the GGSN. The GGSN ensures the uniqueness of this interface-identifier. The MT shall then enforce the use of this Interface-Identifier by the TE. This is valid for both stateless and stateful address autoconfiguration.
- 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 over the insecure connection. This security protocol is defined by mutual agreement between PLMN operator and Intranet/ISP administrator.

In the following signalling flow example, PPP is used as layer 2 protocol over the R reference point. The MT behaves 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 RADIUS authentication. The result of the host authentication is carried via GTP-C back to the SGSN, which then relays the result to the MT. The MT finalises the IPV6CP negotiation by sending an IPV6CP Configure-Ack message to the TE with the appropriate options included, e.g. Interface-Identifier. The Interface-Identifier shall be used in the TE to create a link-local address to be able to perform the IPv6 address autoconfiguration (see subclauses 11.2.1.3.2 and 11.2.1.3.3).

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 IPv6 Interface-Identifier negotiation by sending the IPV6CP Configure-Request message to the MT.

5) The MT sends the Activate PDP Context Request message to the SGSN, including the Protocol Configuration Options. The Protocol Configuration Options may contain negotiated LCP options such as negotiated Authentication Protocol as well as any authentication data previously stored in the MT. The MS shall for dynamic address allocation leave PDP Address empty and set PDP Type to IPv6. The SGSN sends the Create PDP context request message to the chosen GGSN including the unmodified Protocol Configuration Options.

6) The GGSN deduces from local configuration data associated with the APN:

   - IPv6 address allocation type (stateless or stateful);
   - the source of IPv6 Prefixes in the stateless case (GGSN internal prefix pool, or external address allocation server);
   - any server(s) to be used for address allocation, authentication and/or protocol configuration options retrieval (e.g. IMS related configuration, see 3GPP TS 24.229 [47]);
   - the protocol e.g. RADIUS, to be used with the server(s);
   - the communication and security feature needed to communicate with the server(s);

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

   - GGSN internal Prefix pool for IPv6 prefix allocation and no authentication;
   - GGSN internal Prefix pool for IPv6 prefix allocation and RADIUS for authentication. The AAA server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the GGSN;
   - RADIUS for authentication and IPv6 prefix allocation. The AAA server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the GGSN;

NOTE: DHCPv6 may be used for IPv6 prefix allocation when an appropriate RFC becomes available.

   IPv6 Prefixes in a GGSN internal Prefix pool shall be configurable and structured per APN.

   The GGSN shall in the PDP Address IE in the Create PDP Context Response return an IPv6 address composed of a Prefix and an Interface-Identifier. The Interface-Identifier may have any value and it does not need to be unique within or across APNs. It shall however not conflict with the Interface-Identifier the GGSN has selected for its own side of the MS-GGSN link. The Prefix assigned by the GGSN or the external AAA server shall be globally or site-local unique, if stateless address autoconfiguration is configured on this APN. If, on the other hand, stateful address autoconfiguration is configured on the APN, the Prefix part of the IPv6 address returned in the PDP Address IE shall be set to the link-local prefix (FE80::/64).

   The GGSN shall analyse the requested values of all the protocol options contained in the received Protocol Configurations Options IE. The GGSN response shall be in accordance with the relevant PPP or IPCPv6 standards RFC 1661 [21a], RFC 1662 [21b] and RFC 2472 [43].

7) The GGSN sends back to the SGSN a Create PDP Context Response message, containing the PDP Address IE and the Protocol Configuration Options IE. The cause value shall be set according to the outcome of the host authentication and configuration.

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

9) The MT extracts the Interface-Identifier from the address received in the PDP Address IE and ignores the Prefix part. If this Interface-Identifier is identical to the tentative Interface-Identifier indicated in the IPV6CP Configure-Request message sent from the TE-, the MT sends an IPV6CP Configure Ack packet, indicating this Interface-Identifier, to the TE.

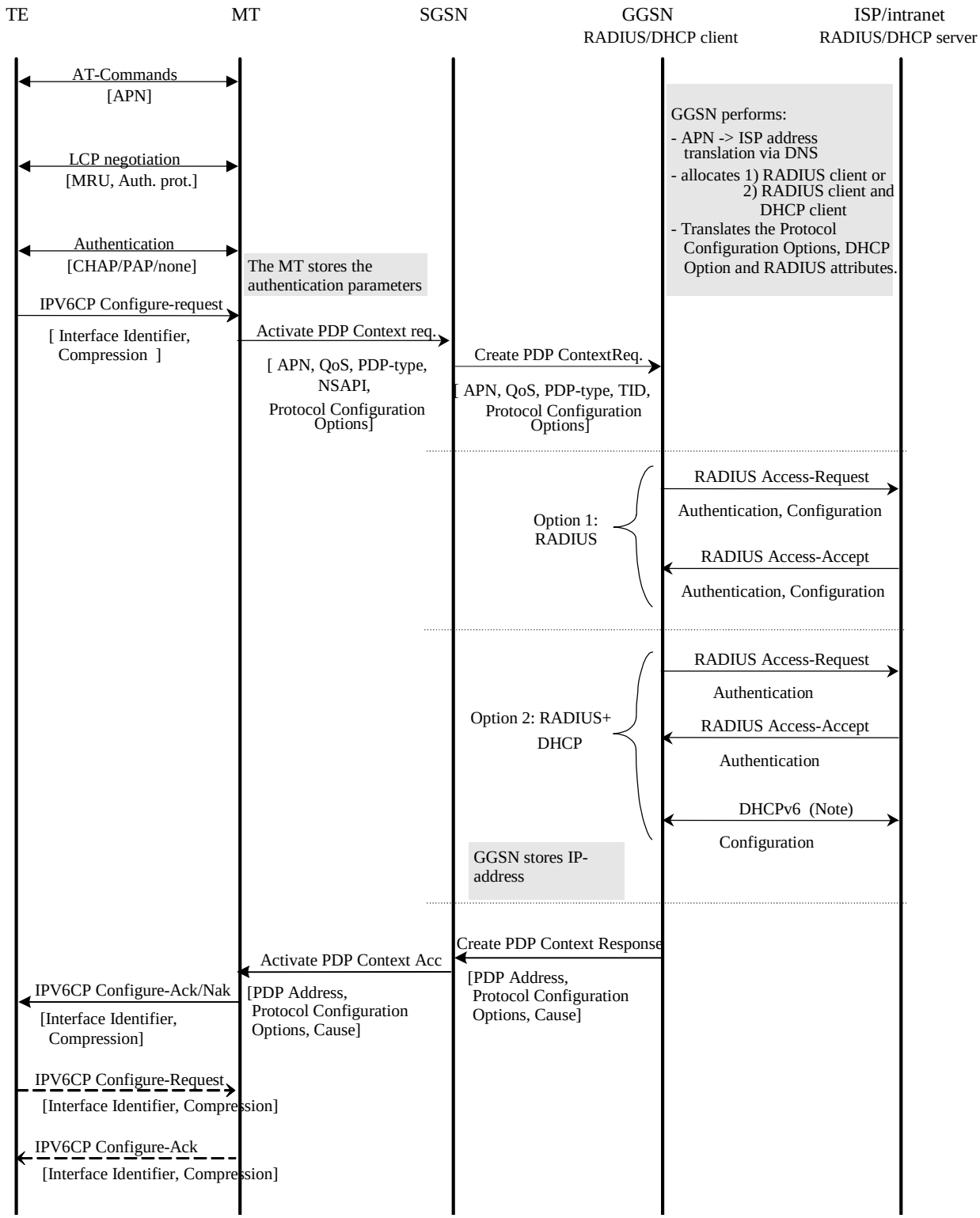
If the Interface-Identifier extracted from the address contained in the PDP Address IE is not identical to the tentative Interface-Identifier indicated in the IPV6CP Configure-Request message sent from the TE, the MT sends an IPV6CP Configure-Nak packet, indicating the Interface-Identifier extracted from the address contained in the PDP Address IE, to the TE. The TE then sends a new IPV6CP Configure-Request message to the MT, indicating the same Interface-Identifier as was indicated in the received IPV6CP Configure Nak (as indicated by the dotted IPV6CP Configure-Request and Configure-Ack in the figure below). Finally the MT responds with a IPV6CP Configure Ack packet.

In case a PDP Context Reject was sent to the MS the MT sends an LCP Terminate-Request to the TE.

10) When the TE has accepted the Interface-Identifier given by the MT, the user plane link from the TE to the GGSN and the external ISP/Intranet is established and the IPv6 address autoconfiguration may proceed.

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.

An LCP Terminate-request causes a PDP context deactivation.



NOTE~~ote 1~~: DHCPv6 may be used for IPv6 prefix allocation when an appropriate RFC becomes available.

Figure 11ba: PDP Context Activation for the IPv6 Non-transparent case

Figure 11ba ~~above~~ is valid for both Stateless and Stateful Address Autoconfiguration case. In the Stateful case though, option 2 does not apply and option 1 may only be used for authentication. The use of DHCPv6 above is different and used in a different context than when used for Stateful Address Autoconfiguration as in subclause 11.2.1.3.3.

11.2.1.3.2 IPv6 Stateless Address Autoconfiguration

As described in 3GPP TS 23.060 [3], a PDP Context of PDP type IPv6 activated by means of the IPv6 Stateless Address Autoconfiguration Procedure is uniquely identified by the prefix part of the IPv6 address only. The MS may select any value for the Interface-Identifier part of the address. The only exception is the Interface-Identifier for the link-local address used by the MS (see RFC 2373 [28]). This Interface-Identifier shall be assigned by the GGSN to avoid any conflict between the link-local address of the MS and that of the GGSN itself. This is described in subclause "IPv6 PDP Context Activation" above.

For IPv6 the PDP Context Activation phase is followed by an address autoconfiguration phase. The procedure describing APNs configured to use Stateless Address Autoconfiguration, may be as follows:

1) After the first phase of setting up IPv6 access to an Intranet or ISP, the MS shall use the IPv6 Interface-Identifier, as provided by the GGSN, to create its IPv6 Link-Local Unicast Address according to RFC 2373 [28].

   Before the MS can communicate with other hosts or MSes on the Intranet/ISP, the MS must obtain an IPv6 Global or Site-Local Unicast Address. The simplest way is the IPv6 Stateless Address Autoconfiguration procedure described below and in 3GPP TS 23.060 [3]. The procedure is consistent with RFC 2462 [29].

   The procedure below takes place through signalling in the user plane. It is done on the link between the MS and the GGSN. From the MS perspective the GGSN is now the first router on the link.

2) After the GGSN has sent a Create PDP Context Response message to the SGSN, it shall start sending Router Advertisements periodically on the new MS-GGSN link established by the PDP Context. The MS may issue a Router Solicitation directly after the user plane establishment. This shall trigger the GGSN to send a Router Advertisement immediately.

   To indicate to the MS that stateless address autoconfiguration shall be performed, the GGSN shall leave the M-flag cleared in the Router Advertisement messages. An MS shall not perform stateless and stateful address autoconfiguration simultaneously, since multiple prefixes are not allowed in GPRS. The O-flag may be set though, since it does not result in additional addresses being acquired (see below).

   The Prefix sent in the Router Advertisements shall be identical to the Prefix returned in the Create PDP Context Response. The Prefix is contained in the Prefix Information Option of the Router Advertisements and shall have the A-flag set ("Autonomous address configuration flag") and the L-flag cleared (i.e. the prefix should not be used for on-link determination). The lifetime of the prefix shall be set to infinity. In practice, the lifetime of a Prefix will be the lifetime of its PDP Context. There shall be exactly one Prefix included in the Router Advertisements.

   The handling of Router Advertisements shall be consistent with what is specified in RFC 2461 [44]. For the MS-GGSN link however, some specific handling shall apply. The randomisation part to determine when Router Advertisements shall be sent may be omitted since the GGSN is the only router on the link. Furthermore, some 3GPP specific protocol constants and default values shall apply (see subclause "IPv6 Router Configuration Variables in the GGSN"). These relate to the periodicity of the Router Advertisements initially and during continued operation. The motivation for this is to have a faster user-plane set-up even in bad radio conditions and to minimize MS power consumption during long continued operation.

3) When creating a Global or Site-Local Unicast Address, the MS may use the Interface-Identifier received during the PDP Context Activation phase or it may generate a new Interface-Identifier. There is no restriction on the value of the Interface-Identifier of the Global or Site-Local Unicast Address, since the Prefix is unique. Interface-Identifiers shall in any case be 64-bit long.

   Since the GGSN guarantees that the Prefix is unique, the MS does not need to perform any Duplicate Address Detection on addresses it creates. That is, the 'DupAddrDetectTransmits' variable in the MS should have a value of zero. If the MS finds more than one Prefix in the Router Advertisement message, it shall only consider the first one and silently discard the others. The GGSN shall not generate any globally unique IPv6 addresses for itself using the Prefix assigned to the MS in the Router Advertisement.

If the O-flag ("Other stateful configuration flag") was set in the Router Advertisement, the MS may start a DHCP session to retrieve additional configuration parameters. See subclause 13.2.2 "Other configuration by the Intranet or ISP". If the MS is not DHCP capable, the O-flag may be ignored.

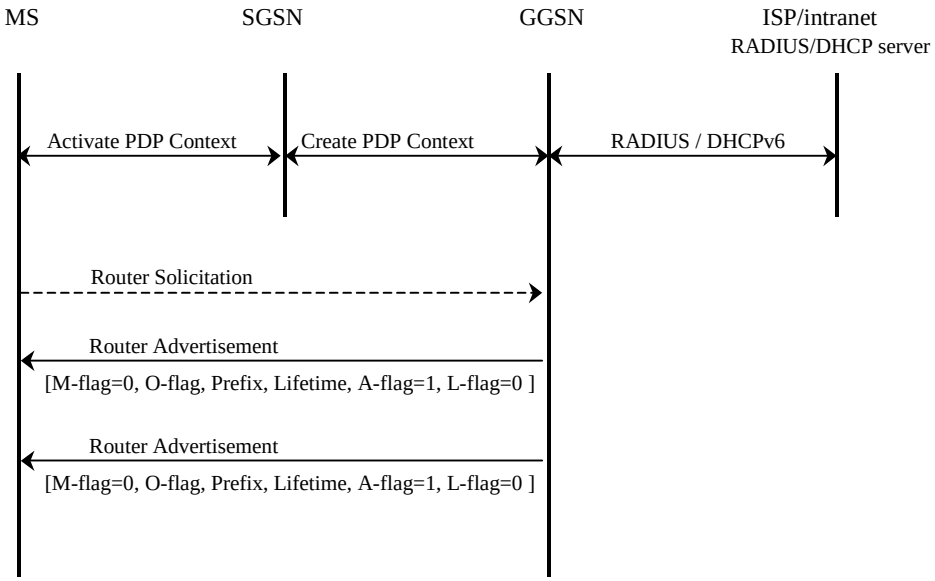


Figure 11bb: IPv6 Stateless Address Autoconfiguration

11.2.1.3.3 IPv6 Stateful Address Autoconfiguration

For IPv6 the PDP Context Activation phase is followed by an address autoconfiguration phase. For APNs configured to use Stateful Address Autoconfiguration, the procedure may for example look like below. A more detailed description of Stateful Address Autoconfiguration is described in clause "Interworking with PDN (DHCP)". Support of DHCP is not mandatory in the MS.

1) After the first phase of setting up IPv6 access to an Intranet or ISP, the MS shall use the IPv6 Interface Identifier, as provided by the GGSN, to create its IPv6 Link-Local Unicast Address according to RFC 2373 [28].

2) After the GGSN has sent a Create PDP Context Response message to the SGSN, it shall start sending Router Advertisements periodically on the new MS-GGSN link established by the PDP Context. The MS may issue a Router Solicitation directly after the user plane establishment. This shall trigger the GGSN to send a Router Advertisement immediately. This shall be consistent with what is specified in RFC 2461 [44]. For the MS-GGSN link however, some 3GPP specific protocol constants and default values shall apply (see subclause "IPv6 Router Configuration Variables in the GGSN").

To indicate to the MS that Stateful Address Autoconfiguration shall be performed, the Router Advertisements shall not contain any Prefix-Information option and the M-flag ("Managed Address Configuration Flag") shall be set.

3) When the MS has received a Router Advertisement with the M-flag set, it shall start a DHCPv6 configuration as described in subclause "Address allocation using DHCPv6" including a request for an IPv6 address.

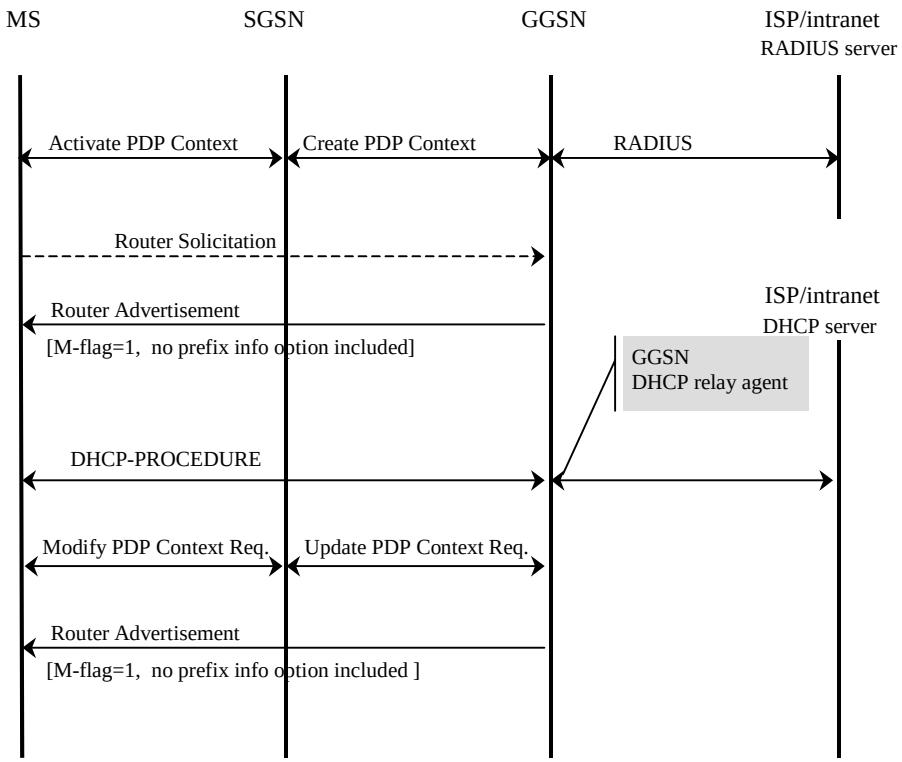


Figure 11bc: IPv6 Stateful Address Autoconfiguration

11.2.1.3.4 IPv6 Router Configuration Variables in the GGSN

For IPv6 Stateless and Stateful Address Autoconfiguration to work properly the GGSN shall behave as an IPv6 router towards the MS. In this respect the GGSN shall be consistent with the RFCs specifying this process (for example RFC 2462 [29] and RFC 2461 [44]), unless stated otherwise in this or other 3GPP specifications.

RFC 2461 [44] specifies a set of conceptual router configuration variables. Some of these variables require particular attention in GPRS in order to preserve radio resources and MS power consumption while still allowing for appropriate robustness and fast user-plane set-up time even in bad radio conditions, or simply because they have a particular meaning in GPRS. These particular variables are listed below with appropriate (default) values and shall be configurable per APN. The values specified hereafter are specific to GPRS and supersede those specified in RFC 2461 [44].

MaxRtrAdvInterval

Shall have a default value of 21 600 ~~seconds~~ (6 h).

MinRtrAdvInterval

Shall have a default value of 0.75 ~~*~~ MaxRtrAdvInterval i.e.16 200 ~~seconds~~ (4.5 h).

AdvValidLifetime

Shall have a value giving Prefixes infinite lifetime, i.e. 0xFFFFFFFF. The assigned prefix remains Preferred until PDP Context Deactivation.

AdvPreferredLifetime

Shall have a value giving Prefixes infinite lifetime, i.e. 0xFFFFFFFF. The assigned prefix remains Preferred until PDP Context Deactivation.

RFC 2461 [44] also specifies a number of protocol constants. The following shall have specific values for GPRS:

MAX_INITIAL_RTR_ADVERT_INTERVAL

This constant may be a variable within GPRS. It may have a value that gradually increases (exponentially or by some other means) with the number of initial Router Advertisements sent. This will enable a fast set-up of the MS-GGSN link in most cases, while still allowing the MS to receive a Router Advertisement within the initial phase, even in case of bad radio conditions or slow response time, without having to send a large number of initial Router Advertisements.

MAX_INITIAL_RTR_ADVERTISEMENTS

This is the number of Router Advertisements sent during the initial phase after the MS-GGSN link has been established. The value of this constant shall be chosen carefully, and in conjunction with MAX_INITIAL_RTR_ADVERT_INTERVAL, so as to not overload the radio interface while still allowing the MS to complete its configuration in a reasonable delay. For instance, the default value could be chosen so that initial Router Advertisements are sent for at least 30 s~~econds~~.

After the initial phase, the periodicity is controlled by the MaxRtrAdvInterval and the MinRtrAdvInterval constants.

11.2.1.4 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 RFC 2002 [30]. Mobile IP (MIP) is a mobility management protocol developed by IETF. The Mobile IP Foreign Agent (FA) RFC 2002 [30] is located in the Core Network in the GGSN. MIP also uses a Home Agent (HA) RFC 2002 [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 RFC 2002 [30] are sent with UDP.

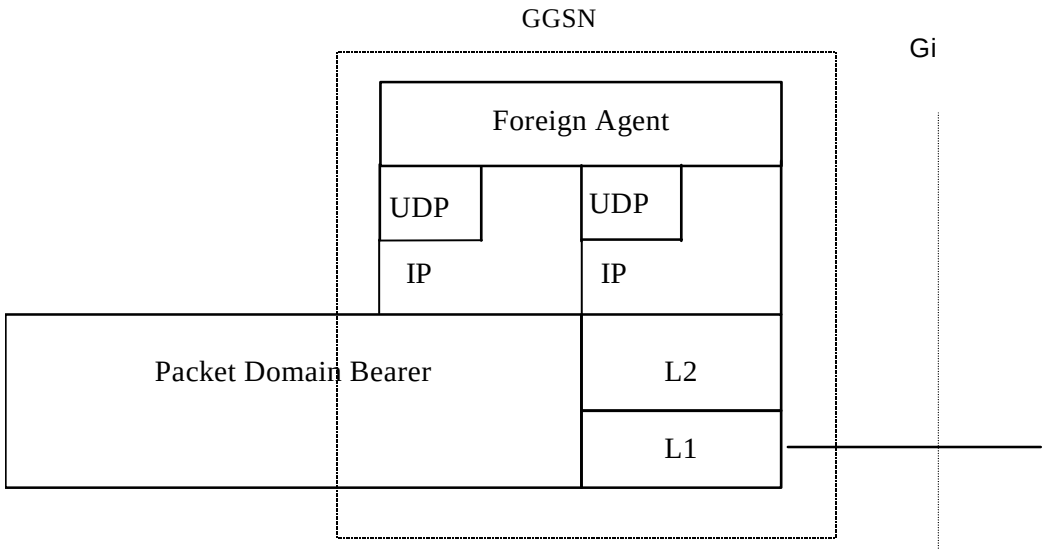


Figure 11c: The protocol stacks for the Gi IP reference point in the MIP signalling plane

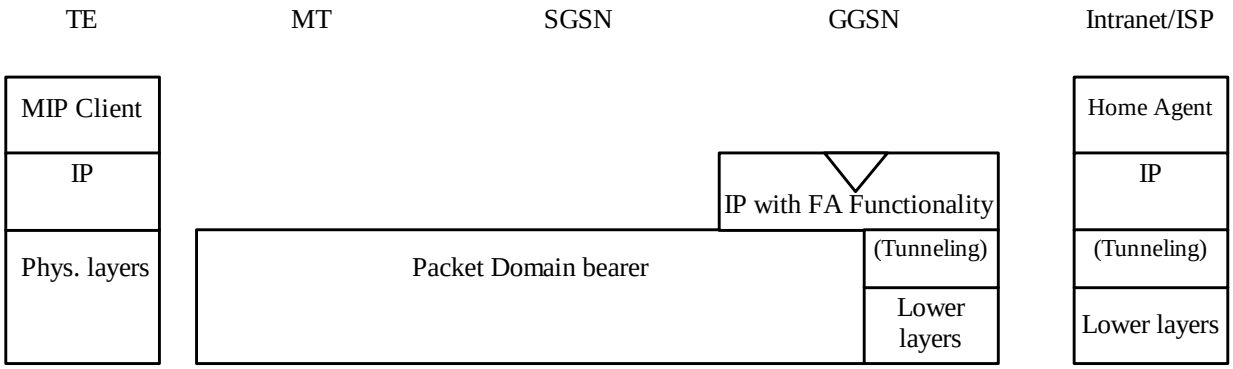


Figure 11d: Protocol stacks for user access with MIP

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 RFC 2794 [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. In this example the MS is separated into a TE and MT, with AT commands and PPP used in-between (see 3GPP TS 27.060 [10]). The PS attach procedures have been omitted for clarity.

IPv4 - Registration UMTS/GPRS + MIP , FA care-of address

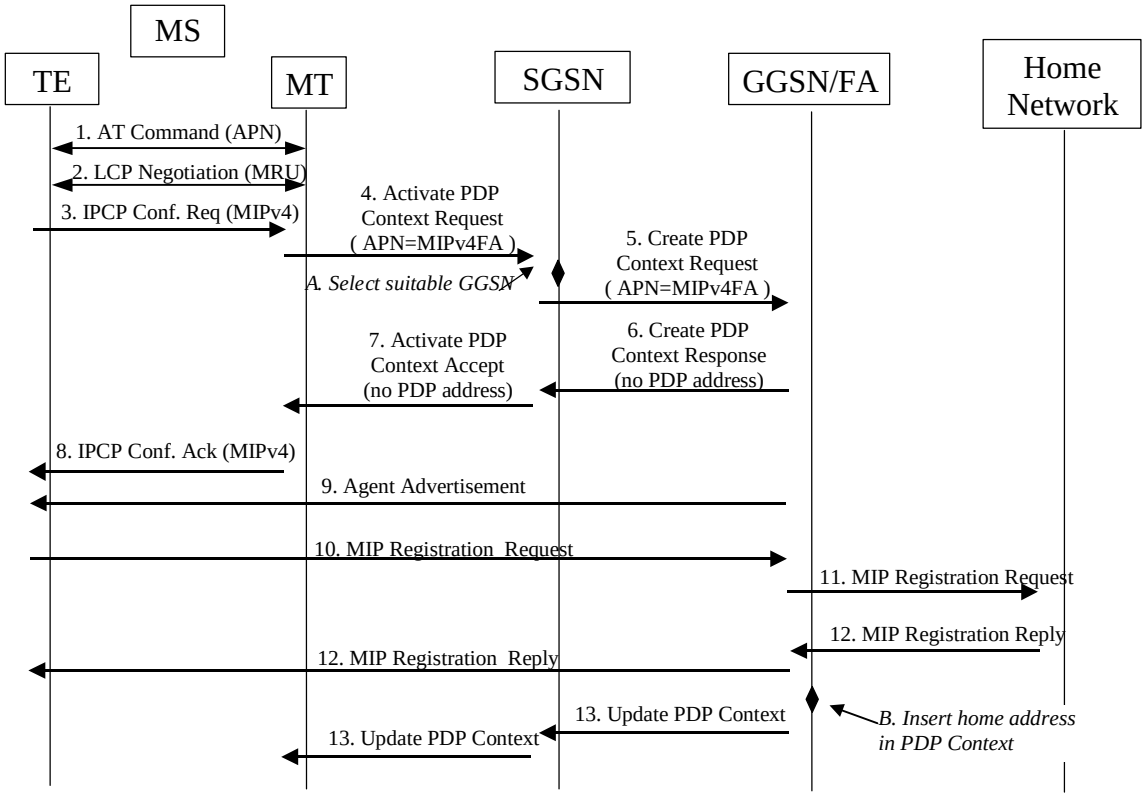


Figure 11e: Example of PDP Context activation with Mobile IP registration -(the PS attach procedure not included)

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 RFC 2290 [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 RFC 2794 [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 RFC 2002 [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 RFC 2002 [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 RFC 2794 [25], RFC 2486 [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 case of IPv6, a global IPv6 prefix can be obtained from the same sources.

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

1. the GPRS operator manages internally the subnetwork addresses or IPv6 prefixes. Each private network is assigned a unique subnetwork address or range of IPv6 prefixes. 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 or IPv6 prefix, is unique.

~~Note~~NOTE:~~-~~ In IPv6 ~~"~~"site-local addresses~~"~~" replace ~~"~~"private addresses~~"~~" in IPv4, see RFC 2373 [28]. Site-local addresses may be used when a site (e.g. a corporate network) requires local administration of its address space.

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

- The PLMN operator allocates a static IP address (IPv4 or IPv6) 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 (IPv4 or IPv6) address or IPv6 prefix as described in 3GPP TS 23.060 [3].

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 [19] and RFC 1035 [52]).

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 (IPv4) and/or MLD (IPv6) and one or more Inter-Router Multicast protocols, such as DVMRP, MOSPF, or PIM-SM.

IGMP/MLD is an integral part of IP. All hosts wishing to receive IP multicasts are required to implement IGMP (or equivalent) and class-D IPv4 addresses of MLD and IPv6 multicast according to RFC 2710 [48]. IGMP/MLD 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/MLD 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 or MLD Report 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.

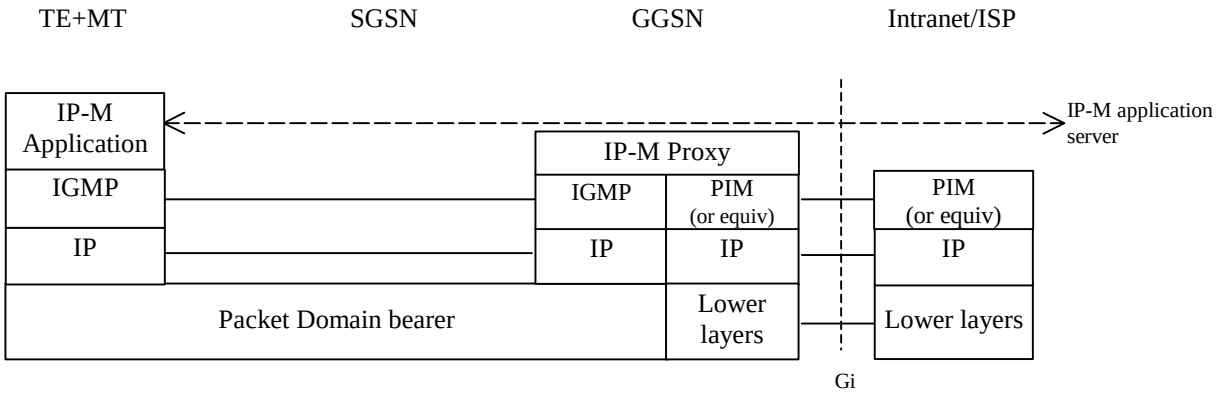


Figure 12: Protocol configuration for IP-Multicast handling (control plane)

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 RFC 1661 [21a] and RFC 1662 [21b]. 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.

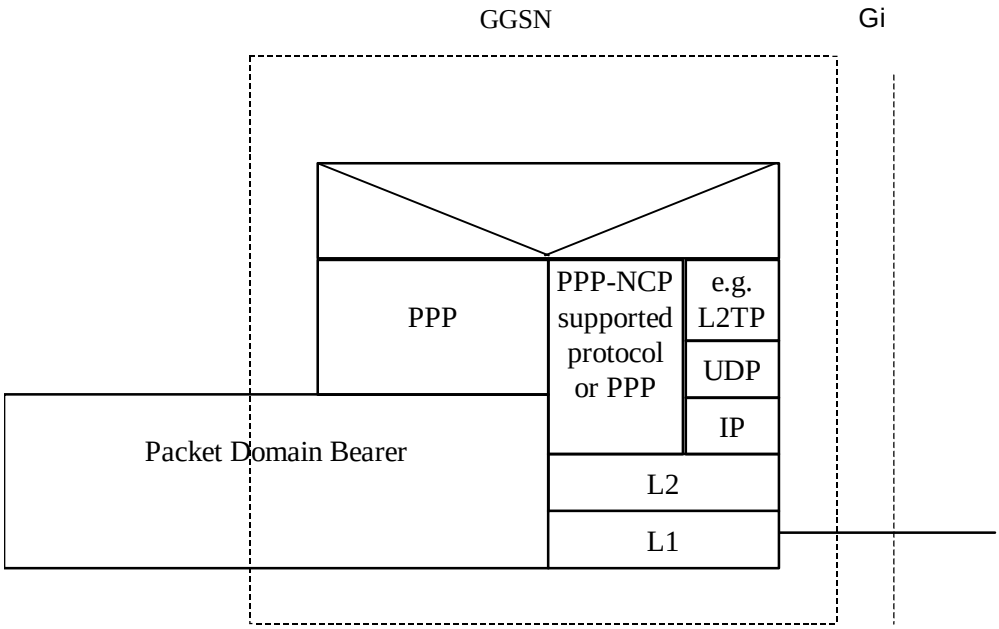


Figure 13: The protocol stacks for the Gi PPP reference point

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);

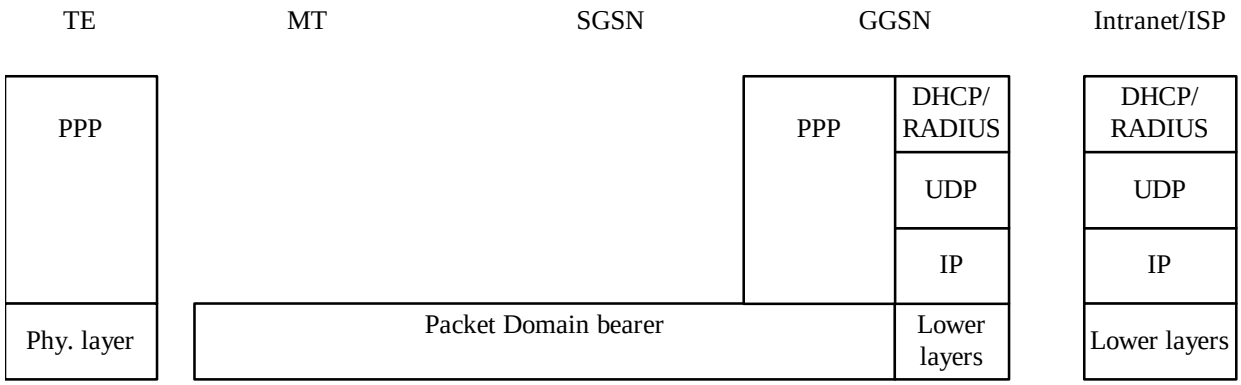


Figure 14: Protocol stack for direct access to IP-based Intranets/ISPs

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

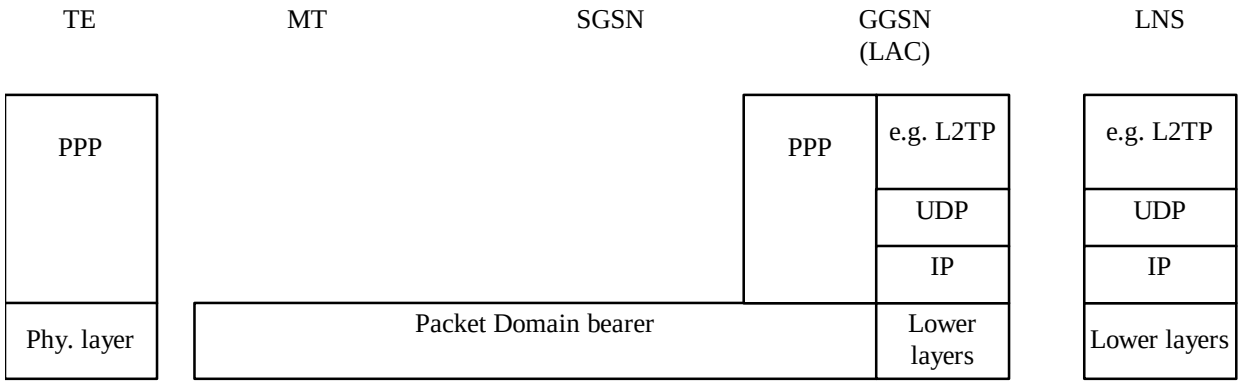


Figure 15: Protocol stack for virtual dial-up access with PPP frame tunnelling

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 AAA, 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 AAA 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 AAA 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 NCP 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.

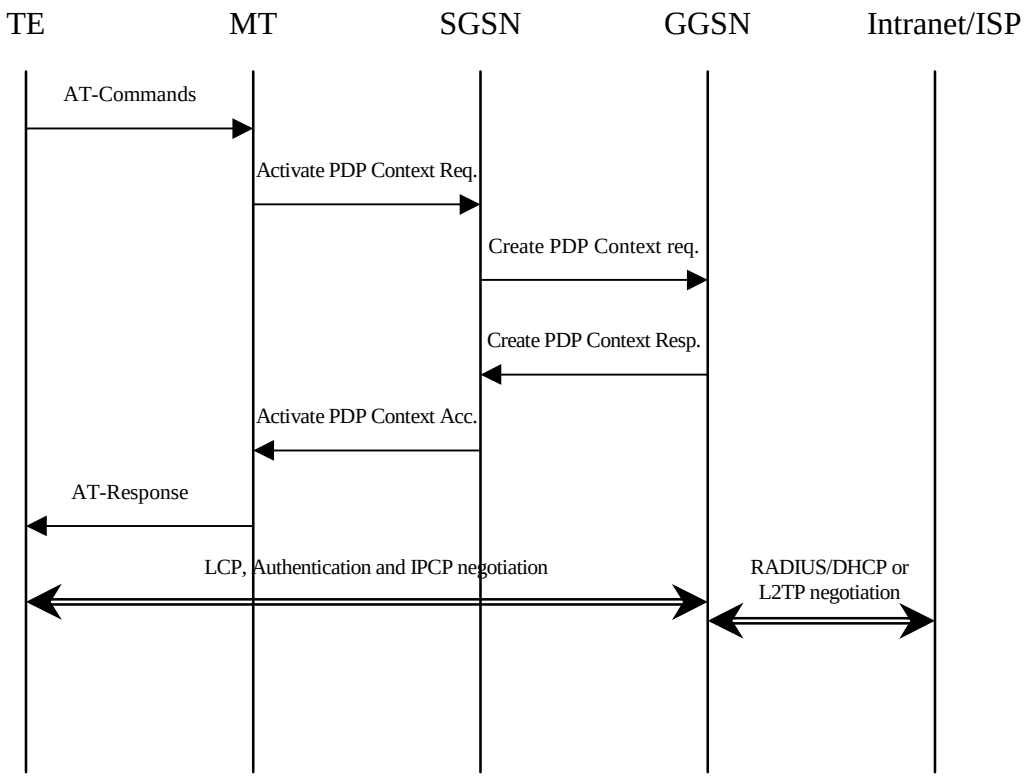


Figure 16a

13 Interworking with PDN (DHCP)

13.1 General

In current LAN environments the most commonly used configuration protocol is DHCP (Dynamic Host Configuration Protocol, RFC 2131 [26]) and DHCPv6 when the DHCPv6 IETF Internet-Draft [46]~~it~~ becomes an RFC standard~~ [46]~~.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 present document.

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 RFC 1661 [21a] and RFC 1662 [21b] 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.

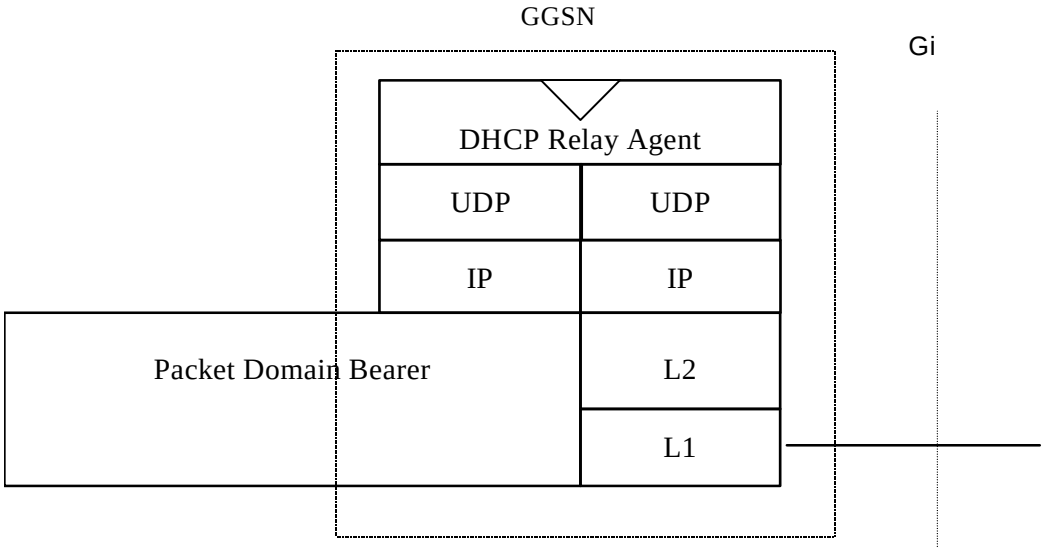


Figure 16b: The protocol stacks for the Gi IP reference point for DHCP

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 (see RFC 3118 [45]).

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

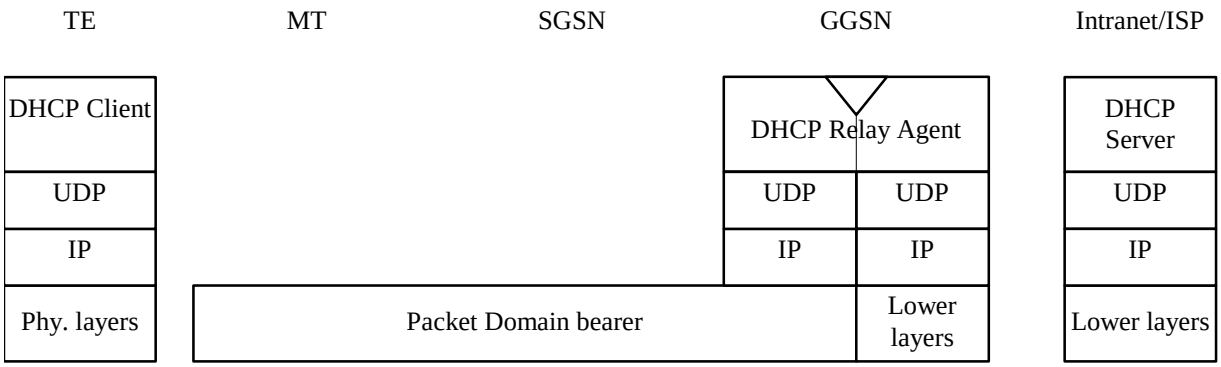


Figure 16c: Protocol stack for access with DHCP end-to-end

13.2.1.1 Address allocation using DHCPv4

The following description bullet items describe the DHCPv4 signal flow. For a detailed description of the DHCP messages refer to RFC 2131 [26] and RFC 1542, [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.

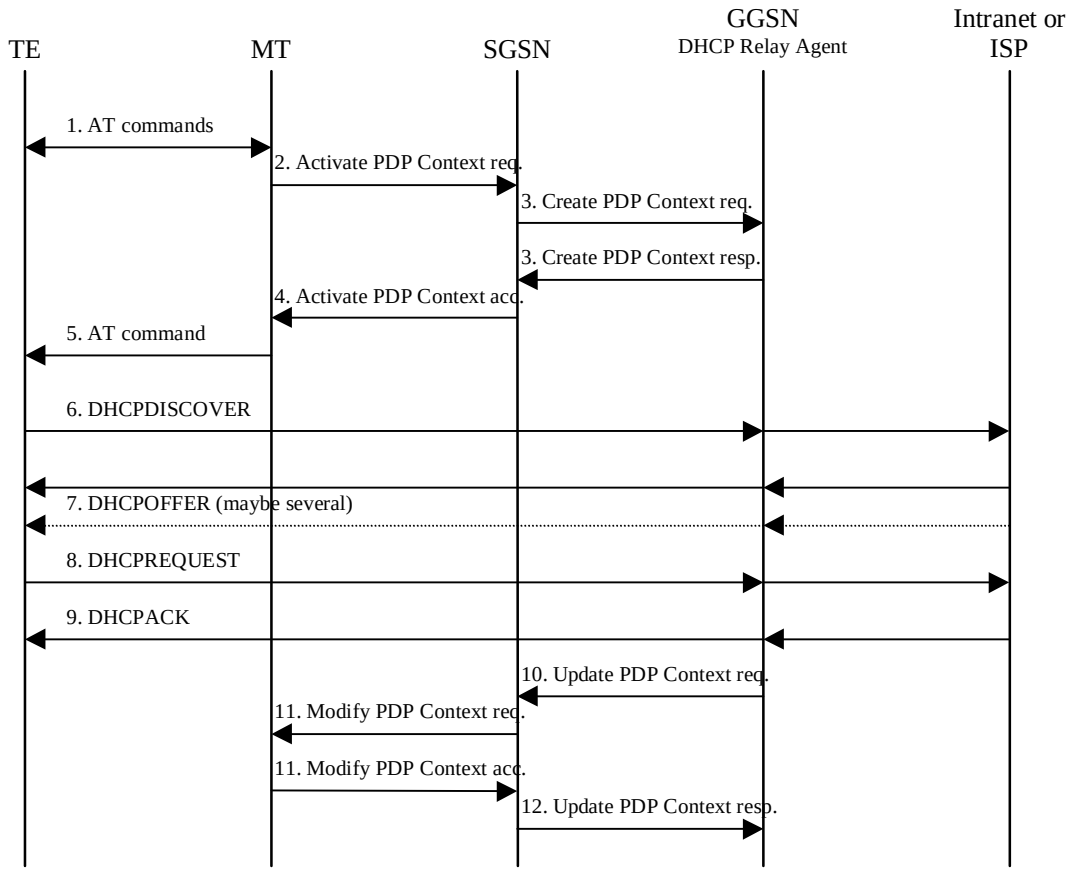


Figure 16d: DHCPv4 signal flow

13.2.1.2 Address allocation using DHCPv6

The following description bullet items describe the signal flow. For a detailed description of the DHCPv6 messages refer to the DHCPv6 IETF Internet-draft [46]. In the context of IPv6, address allocation through DHCP is also referred to as Stateful Address Autoconfiguration. The end-to-end protocol configuration is depicted in figure 16e.

The PDP Context activation part and the initial Router Advertisement that triggers the MS to do the Stateful Address Autoconfiguration is described in subclause "IPv6 Non Transparent access to an Intranet or ISP".

~~1)~~1) The TE sends a SOLICIT message with the IP destination address set to the All_DHCP_Relay_Agents_and_Servers multicast address defined in the DHCPv6 IETF Internet-draft [46]. The source address is the link local address created by the MS. The SOLICIT message shall contain one IA option.

2)2) The GGSN creates a RELAY-FORWARD message. The “"Client-Message”" option shall include the entire SOLICIT message. The GGSN sends the message to the DHCP server(s) configured for the APN using unicast addresses or All_DHCP_Servers multicast address. More details on the parameters for the RELAY-FORWARD are found in the DHCPv6 IETF Internet-draft [46]. The GGSN may store a PDP Context ID in the Interface-Id option if this aids it in handling the Relay-Reply (the DHCP server will echo the Interface-Id option).

3)3) DHCP servers receiving the RELAY-FORWARD message including the SOLICIT request reply by sending a RELAY-REPLY message. The “"Server-Message”" option includes the ADVERTISE message with an offered IP address.

4)4) GGSN extracts the ADVERTISE messages and forwards the messages to the proper MS.

5)5) The TE chooses one of the possibly several ADVERTISE messages and sends a REQUEST confirming its choice and requesting additional configuration information.

6)6) GGSN embeds the REQUEST in the “"Client-Message”" option of the RELAY-FORWARD and sends it as explained in step 2.

7)7) The selected DHCP server receives the RELAY-FORWARD and replies with a RELAY-REPLY. The “"Server-Message”" option includes the REPLY message containing the configuration information requested by the TE.

8)8) The GGSN extracts the REPLY message and forwards it to the proper MS. GGSN also extracts IA option information such as the allocated MS IPv6 address and its lifetime and stores it in the corresponding PDP context. The GGSN shall silently discard any Neighbour Solicitation message sent by the MS to perform Duplicate Address Detection (see 3GPP TS 23.060 [3]).

9)9) The GGSN 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 IPv6 address.

10)10) The SGSN sends a Modify PDP Context Request to the MT with the allocated IPv6 address in the PDP Address information element.

11)11) The MT acknowledges by sending a Modify PDP Context Accept to the SGSN.

12)12) The SGSN sends an Update PDP Context Response to the GGSN. The PDP context has been successfully updated with the allocated IPv6 address.

13)13) In the Stateful Address Autoconfiguration, Router Advertisements sent by GGSN on the MS-GGSN link shall not contain any Prefix Information option, even when GGSN has knowledge of the Prefix of the MS through the DHCP relay agent. The Prefix need not be advertised since the MS is the only host on the link and Stateless Address Autoconfiguration shall not be performed concurrently to Stateful Address Autoconfiguration.

EXAMPLE: In the following example a successful PDP context activation with use of DHCPv6 from end to end is shown.

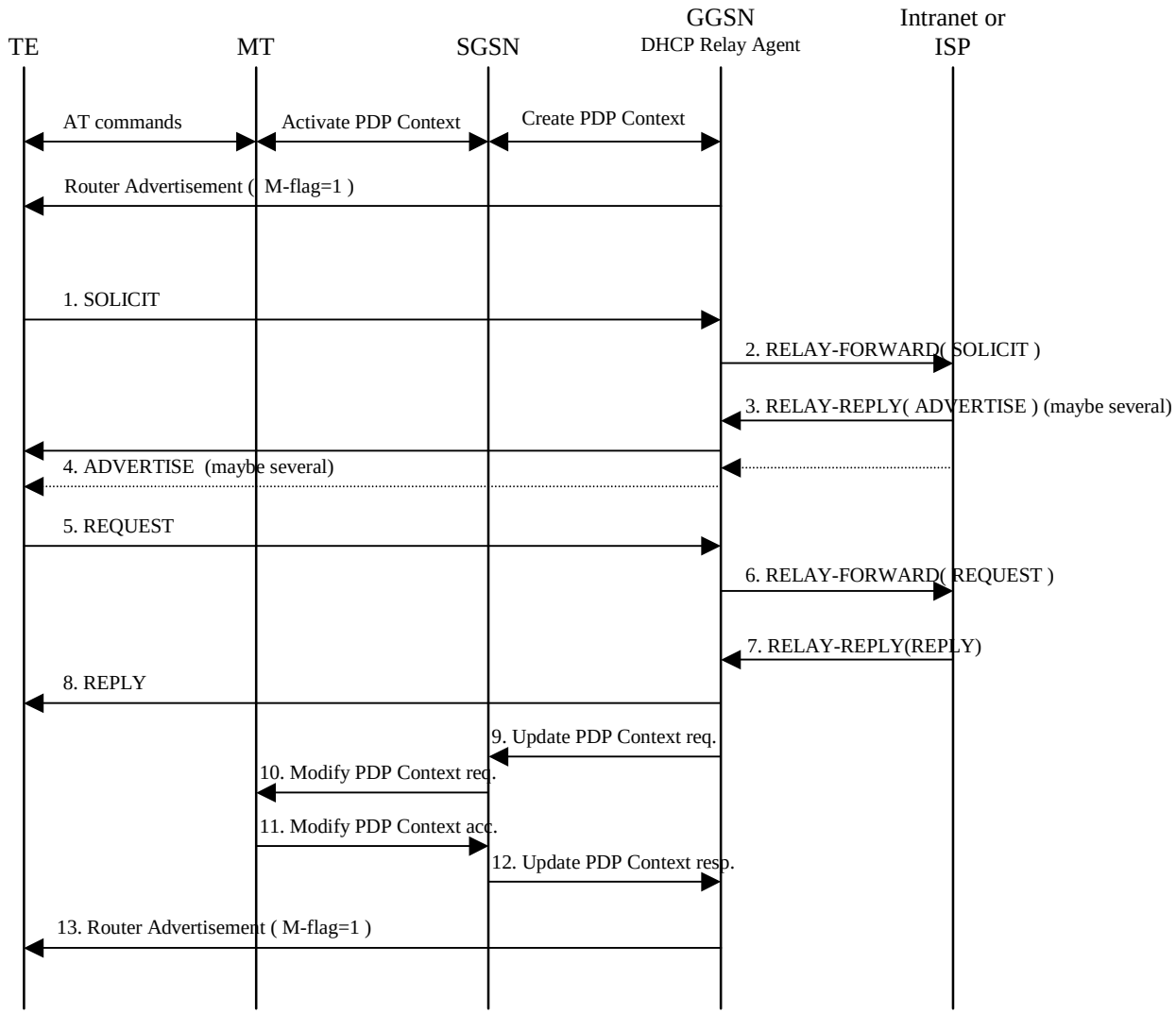


Figure 16e: DHCPv6 signal flow

13.2.2 Other configuration by the Intranet or ISP (IPv6 only)

When using IPv6, in some situations the MS may need additional configuration information from the Intranet or ISP besides the IP address. It may for example be IMS related configuration options (see 3GPP TS 24.229 [47]). If the MS is DHCP capable and the IPv6 address has been allocated using Stateless Address Autoconfiguration, the MS may use a procedure as in the example below to configure additional external network protocol parameters, or other parameters that apply to the Intranet or ISP. The GGSN shall in this case indicate to the MS that there is additional configuration information to retrieve by setting the O-flag in the Router Advertisements. This shall be configured per APN in the GGSN.

The following description bullet items describe an example of a signal flow, where the MS directs an Information-Request to the All_DHCP_Relay_Agents_and_Servers multicast address. The MS may also direct the message to a specific server instead of all servers. For a detailed description of the DHCPv6 messages refer to the DHCPv6 IETF Internet-draft [46]. The sequence is depicted in figure 16f.

1) A Router Advertisement with the O-flag set, is sent from GGSN to TE to indicate to it to retrieve other configuration information.

2) The TE sends an INFORMATION-REQUEST message with the IP destination address set to the All_DHCP_Relay_Agents_and_Servers multicast address defined in the DHCPv6 IETF Internet-draft [46]. The source address shall be the link-local address of the MS. The DHCP relay agent in the GGSN shall forward the message.

3) DHCP servers receiving the forwarded INFORMATION-REQUEST message, reply by sending a RELAY-REPLY message, with the "server-message" option including a REPLY message with the requested configuration parameters.

The TE chooses one of the possibly several REPLY messages and extracts the configuration information.

EXAMPLE: In the following example a request for information with use of DHCPv6 from end to end is shown.

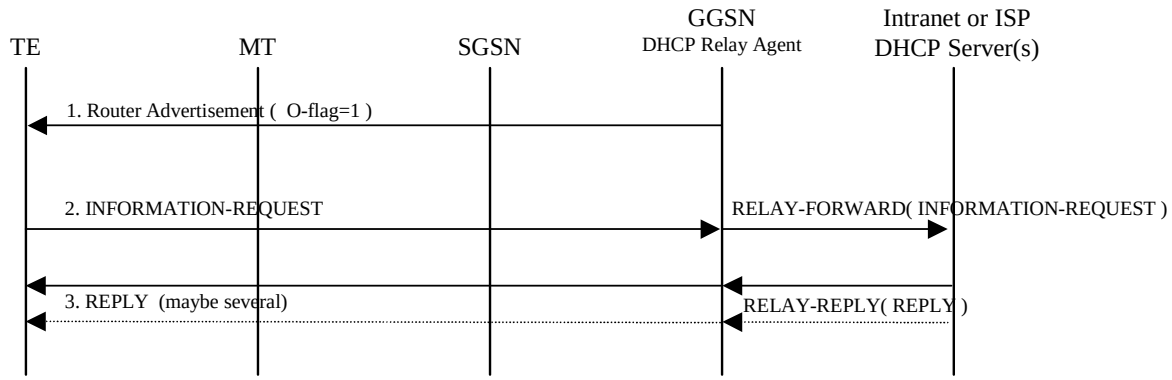


Figure 16f: DHCPv6 Other configuration signal flow

14 Internet Hosted Octet Stream Service (IHOSS)

~~Void.~~ **Figure 17: Void**

Figure 18: Void

Figure 19: Void

Figure 20: Void

15 Interworking between Packet Domains

The primary reason for the interworking between Packet Domains is to support roaming subscribers as described in 3GPP TS 23.060 [3]. The general model for Packet Domain interworking is shown in figure 21.

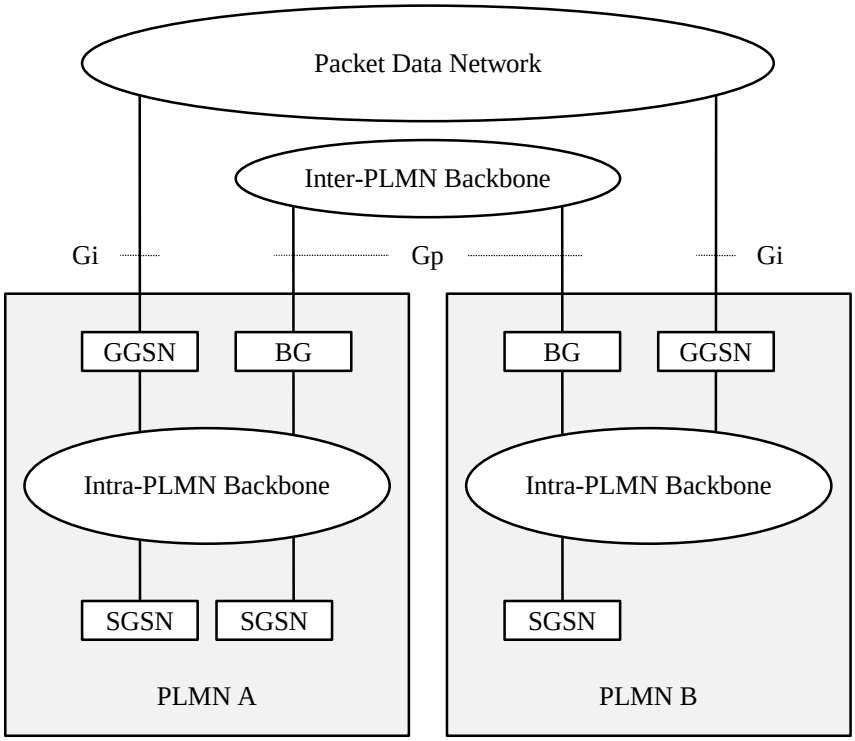


Figure 21: General interworking between Packet Domains to support roaming subscribers.

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 [3].

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 [3].

The inter-PLMN link may be any packet data network or dedicated link as described in 3GPP TS 23.060 [3]. 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 [54]) and accompanying specifications for authentication (RFC 1826 [55]) and encryption (RFC 1827 [56]) 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 [53]) 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.

16 Usage of RADIUS on Gi interface

A GGSN may, on a per APN basis, use RADIUS authentication to authenticate a user and RADIUS accounting to provide information to an AAA (Authentication, Authorization and Accounting) server.

16.1 RADIUS Authentication

RADIUS Authentication shall be used according to RFC 2865 [38] and RFC 3162 [50].

The RADIUS client function may reside in a GGSN. When the GGSN receives a Create PDP Context request message the RADIUS client function may send the authentication information to an authentication server, which is identified during the APN provisioning.

The authentication server checks that the user can be accepted. The response (when positive) may contain network information, such as an IP address or IPv6 prefix for the user.

The information delivered during the RADIUS authentication can be used to automatically correlate the users identity (the MSISDN or IMSI) to the IP-address or IPv6 prefix, assigned/confirmed by the GGSN or the authentication server respectively. The same procedure applies, in case of sending the authentication to a 'proxy' authentication server.

RADIUS Authentication is only applicable to the primary PDP context. When the GGSN receives an Access-Accept message from the authentication server it shall complete the PDP context activation procedure. If Access-Reject or no response is received, the GGSN shall reject the PDP Context Activation attempt with a suitable cause code, e.g. User Authentication failed.

16.2 RADIUS Accounting

RADIUS Accounting shall be used according to RFC 2866 [39] and RFC 3162 [50].

The RADIUS accounting client function may reside in a GGSN. The RADIUS accounting client may send information to an accounting server, which is identified during the APN provisioning. The accounting server may store this information and use it to automatically identify the user. This information can be trusted because the GPRS network has authenticated the subscriber (i.e. SIM card and possibly other authentication methods).

RADIUS Accounting-Request Start and Stop messages may be used during both primary and secondary PDP context activation and deactivation procedures respectively.

The use of Accounting-Request STOP and in addition the Accounting ON and Accounting OFF messages may be used to ensure that information stored in the accounting server is synchronised with the GGSN information.

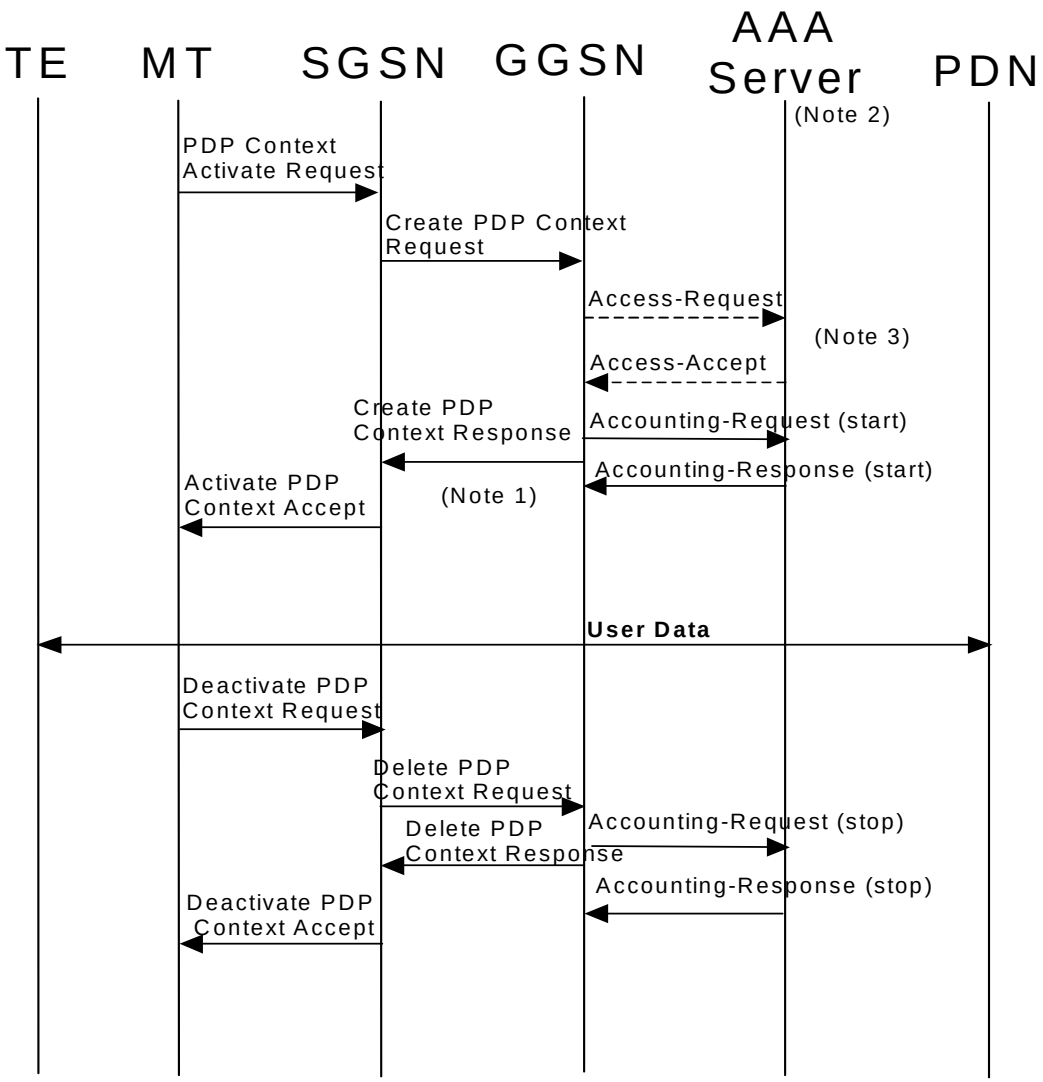
If the AAA server is used for IP address or IPv6 prefix assignment, then, upon reception of a RADIUS Accounting-Request STOP message for all PDP contexts associated to a session defined by APN and IMSI or MSISDN, the AAA server may make the associated IP address or IPv6 prefix available for assignment.

In order to avoid race conditions, the GGSN shall include a 3GPP Vendor-Specific sub-attribute "Session Stop indicator" when it sends the Accounting-Request STOP for the last PDP context of a PDP session and the PDP session is terminated (i.e. the IP address or IPv6 prefix and all GTP tunnels can be released). The AAA server shall not assume the PDP session terminated until an Accounting-Request STOP with the Session Stop indicator is received.

16.3 Authentication and accounting message flows

16.3.1 IP PDP type

~~The f~~Figure 22 represents the RADIUS message flows between a GGSN and an Authentication, Authorization and Accounting (AAA) server.



NOTE 1: If some external applications require RADIUS Accounting request (Start) information before they can process user packets, then the selected APN (GGSN) may be configured in such a way that the GGSN drops user data until the Accounting Response (START) is received from the AAA server. The GGSN may wait for the Accounting Response (START) before sending the CreatePDPContextResponse. The GGSN may reject the PDP context if the Accounting Response (START) is not received.
NOTE 2: Separate accounting and authentication servers may be used.
NOTE 3: The Access-Request message shall be used for primary PDP context only.
NOTE 4: The Accounting-Request (Start) message may be sent at a later stage, e.g. after IPv6 address has been assigned and PDP Context updated, in case of a stateful address autoconfiguration.

Figure 22: RADIUS message flow for PDP type IP (successful user authentication case)

When a GGSN receives a Create PDP Context Request message for a given APN, the GGSN may (depending on the configuration for this APN) send a RADIUS Access-Request to an AAA server. The AAA server authenticates and authorizes the user. If RADIUS is also responsible for IP address or IPv6 prefix allocation the AAA server shall return the allocated IP address or IPv6 prefix in the Access-Accept message.

Even if the GGSN was not involved in user authentication (e.g. transparent network access mode), it may send a RADIUS Accounting-Request START message to an AAA server. This message contains parameters, e.g. the tuple which includes the user-id and IP address or IPv6 prefix, to be used by application servers (e.g. WAP gateway) in order to identify the user. This message also indicates to the AAA server that the user session has started.

At a stateful address autoconfiguration, no IP address or IPv6 prefix is available at PDP context activation. In that case the GGSN may wait to send the Accounting-Request START message until the TE receives its IP address in a DHCP-REPLY.

If some external applications require RADIUS Accounting request (Start) information before they can process user packets, then the selected APN (GGSN) may be configured in such a way that the GGSN drops user data until the Accounting Response (START) is received from the AAA server. The GGSN may wait for the Accounting Response (START) before sending the CreatePDPContextResponse. The GGSN may reject the PDP context if the Accounting Response (START) is not received. The authentication and accounting servers may be separately configured for each APN.

When the GGSN receives a Delete PDP Context Request message and providing a RADIUS Accounting-Request START message was sent previously, the GGSN shall send a RADIUS Accounting-Request STOP message to the AAA server, which indicates the termination of this particular user session. The GGSN shall immediately send a Delete PDP context response, without waiting for an Accounting-Response STOP message from the AAA server.

The AAA server shall deallocate the IP address or IPv6 prefix (if any) initially allocated to the subscriber, if there is no session for the subscriber.

Accounting-Request ON and Accounting-Request OFF messages may be sent from the GGSN to the AAA server to ensure the correct synchronization of the session information in the GGSN and the AAA server.

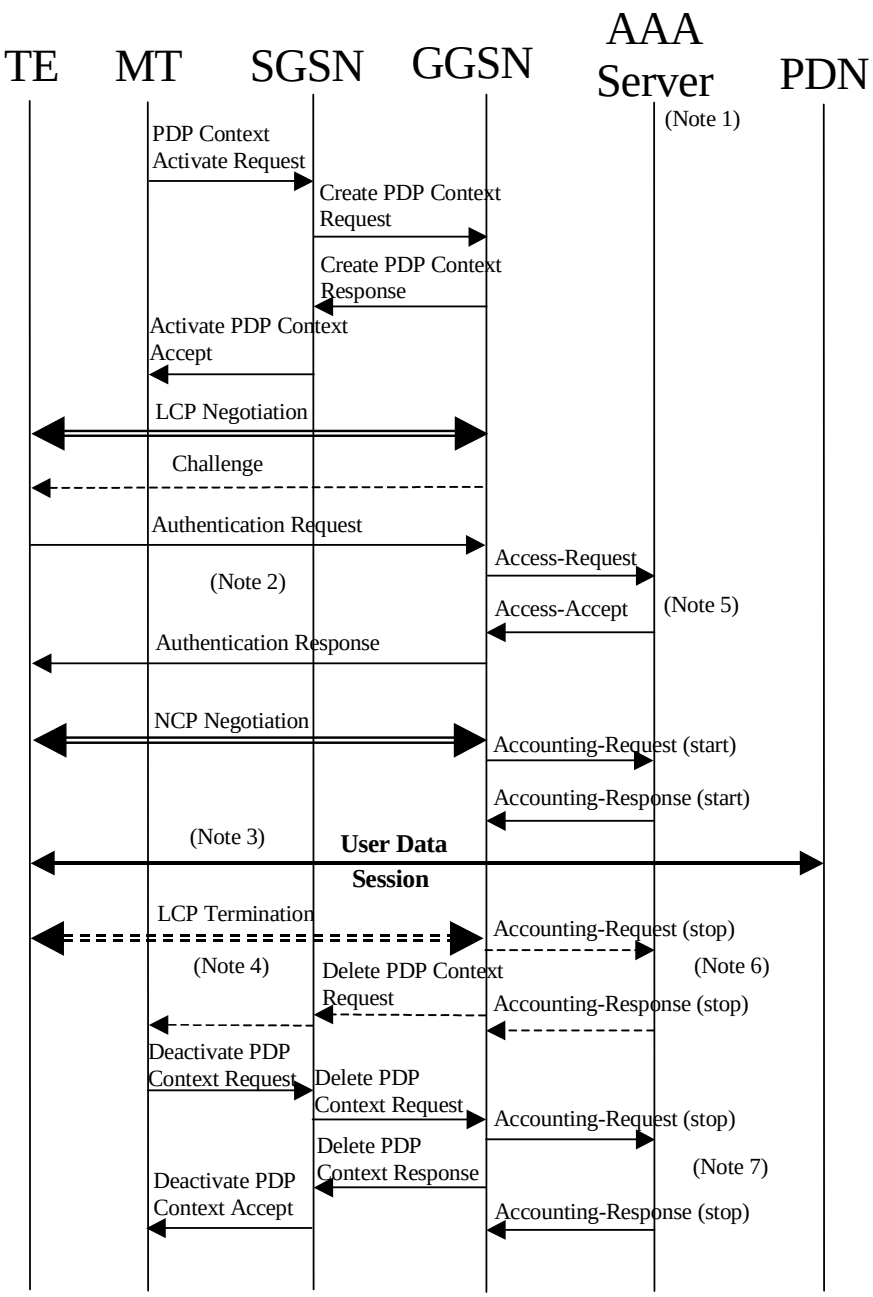
The GGSN may send an Accounting-Request ON message to the AAA server to indicate that a restart has occurred. The AAA server may then release the associated resources.

Prior to a scheduled restart, the GGSN may send Accounting-Request OFF message to the AAA server. The AAA server may then release the associated resources.

If an Access-Challenge is sent to the GGSN when an Access-Request message is pending and when IP PDP type is used, the GGSN shall silently discard the Access-Challenge message and it shall treat an Access-Challenge as though it had received an Access-Reject instead RFC 2865 [38].

16.3.2 PPP PDP type

~~The f~~Figure 23 describes the RADIUS message flows between a GGSN and an Authentication, Authorization and Accounting (AAA) server for the case where PPP is terminated at the GGSN. ~~-~~The case where PPP is relayed to an LNS is beyond the scope of ~~this specification~~the present document.



NOTE 1: Separate accounting and Authentication servers may be used.
NOTE 2: Actual messages depend on the used authentication protocol (e.g. PAP, CHAP).
NOTE 3: If some external applications require RADIUS Accounting request (Start) information before they can process user packets, then the selected APN (GGSN) may be configured in such a way that the GGSN drops user data until the Accounting Response (START) is received from the AAA server. The GGSN may delete the PDP context if the Accounting Response (START) is not received.
NOTE 4: An LCP termination procedure may be performed. Either the MS or the GGSN may initiate the context deactivation.
NOTE 5: The Access-Request message shall be used for primary PDP context only.
NOTE 6: Network Initiated deactivation.
NOTE 7: User Initiated deactivation.

Figure 23: RADIUS message flow for PDP type PPP (successful user authentication case)

When a GGSN receives a Create PDP Context Request message for a given APN, the GGSN shall immediately send a Create PDP context response back to the SGSN. After PPP link setup, the authentication phase may take place. During Authentication phase, the GGSN sends a RADIUS Access-Request to an AAA server. The AAA server authenticates and authorizes the user. If RADIUS is also responsible for IP address allocation the AAA server shall return the allocated IP address or IPv6 prefix in the Access-Accept message (if the user was authenticated).

If the user is not authenticated, the GGSN shall send a Delete PDP context request to the SGSN.

Even if the GGSN was not involved in user authentication (e.g. for PPP no authentication may be selected), it may send a RADIUS Accounting-Request START message to an AAA server. This message contains parameters, e.g. a tuple which includes the user-id and IP address or IPv6 prefix, to be used by application servers (e.g. WAP gateway) in order to identify the user. This message also indicates to the AAA server that the user session has started, and the QoS parameters associated to the session.

If some external applications require RADIUS Accounting request (Start) information before they can process user packets, then the selected APN (GGSN) may be configured in such a way that the GGSN drops user data until the Accounting Response (START) is received from the AAA server. The GGSN may delete the PDP context if the Accounting Response (START) is not received. The Authentication and Accounting servers may be separately configured for each APN.

When the GGSN receives a Delete PDP Context Request message and providing a RADIUS Accounting-Request START message was sent previously, the GGSN shall send a RADIUS Accounting-Request STOP message to the AAA server, which indicates the termination of this particular user session. The GGSN shall immediately send a Delete PDP context response, without waiting for an Accounting-Response STOP message from the AAA server.

The AAA server shall deallocate the IP address or IPv6 prefix (if any) initially allocated to the subscriber.

Accounting-Request ON and Accounting-Request OFF messages may be sent from the GGSN to the AAA server to ensure the correct synchronization of the session information in the GGSN and the AAA server.

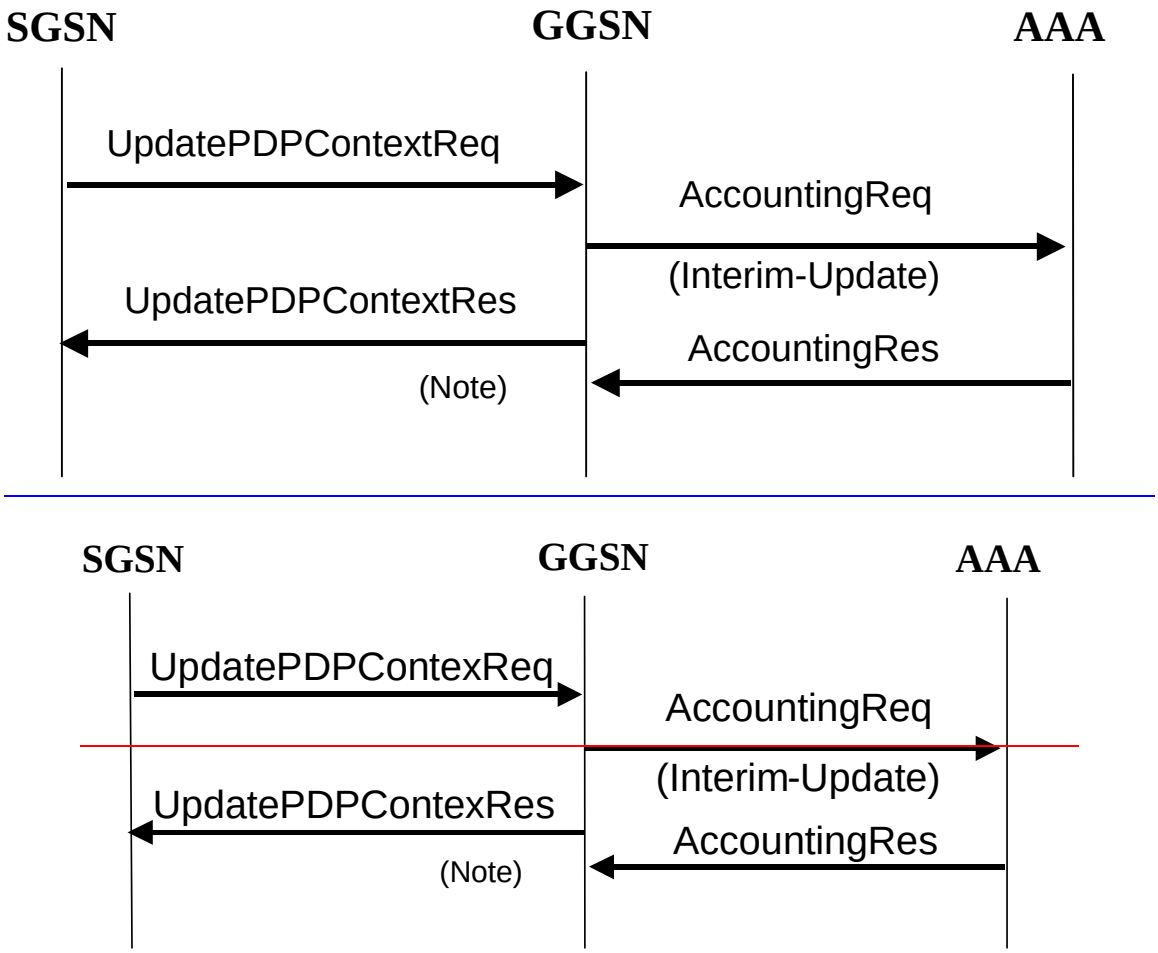
The GGSN may send an Accounting-Request ON message to the AAA server to indicate that a restart has occurred. The AAA server may then release the associated resources.

Prior to a scheduled restart, the GGSN may send Accounting-Request OFF message to the AAA server, the AAA server may then release the associated resources.

If an Access-Challenge is sent to the GGSN when using PPP PDP type, the GGSN shall handle it by PPP CHAP providing PPP CHAP was the selected Authentication protocol. If CHAP authentication was not selected, authentication shall fail RFC 2865 [38].

16.3.3 Accounting Update

During the life of a PDP context some information related to this PDP context may change (i.e. SGSN address if a Inter--SGSN RA update occurs). Upon reception of an UpdatePDPContextRequest from the SGSN, the GGSN may send an Accounting Request Interim-Update to the AAA server to update the necessary information related to this PDP context (sSee Ffigure 24). In such a case, the GGSN need not wait for the RADIUS AccountingResponse from the AAA server message before sending the UpdatePDPContextResponse to the SGSN. The GGSN may delete the PDP context if the AccountingResponse is not received from the AAA.

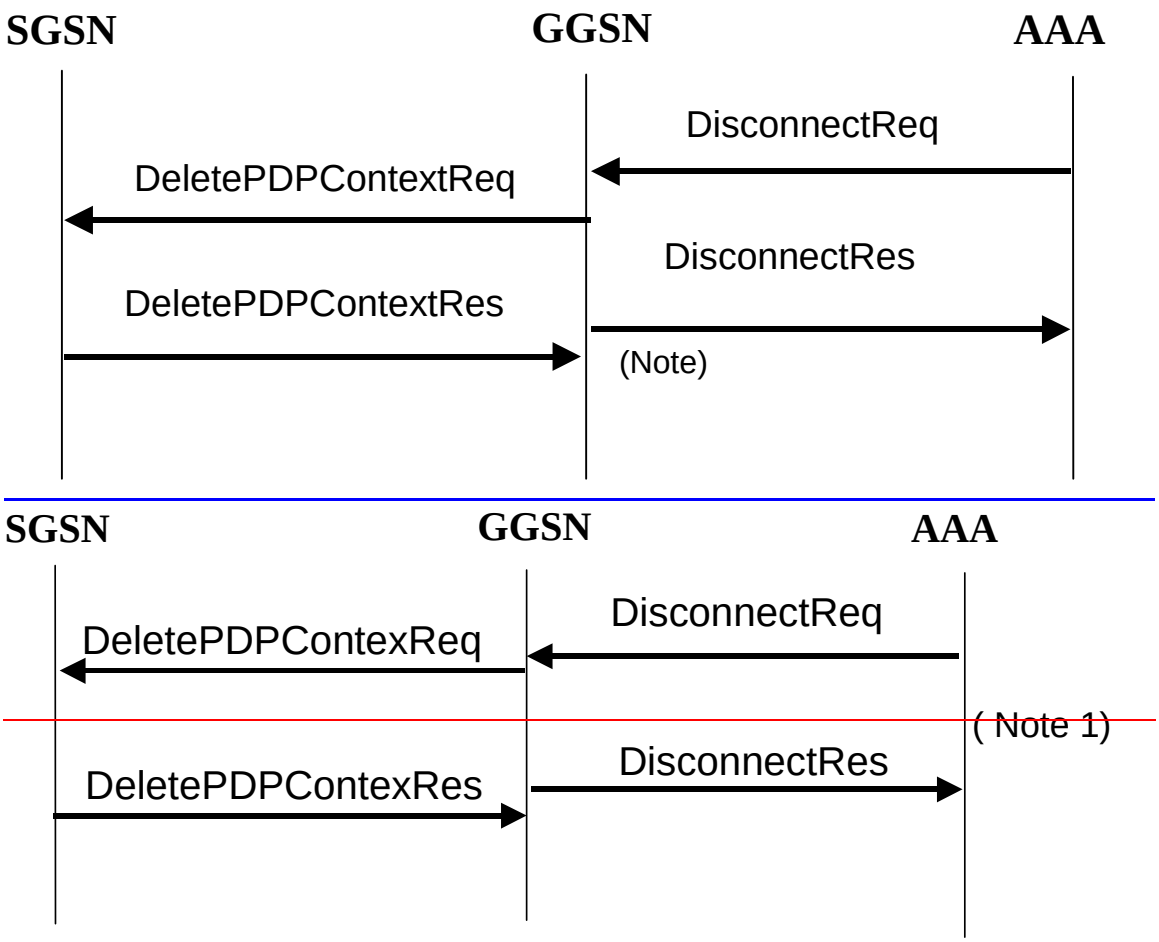


NOTEote 1:- As shown the GGSN need not wait for the RADIUS AccountingResponse from the AAA server message to send the UpdatePDPContextResponse to the SGSN. The GGSN may delete the PDP context if the AccountingResponse is not received from the AAA.

Figure 24: RADIUS for PDP context Update

16.3.4 AAA-Initiated PDP context termination

RADIUS is used as the protocol between the GGSN and a AAA server or proxy for applications (e.g. MMS) to deliver information related to GPRS user session. However some IP applications could need to interwork with the GGSN to terminate a particular PDP context. For this purpose, the AAA server or proxy may send a RADIUS Disconnect Request to the GGSN. As depicted in Figure figure 25, the GGSN may react by deleting the corresponding PDP context or silently discard the Disconnect Request message. For more information on RADIUS Disconnect, see RFC 2882 [41]. If the GGSN deletes the corresponding PDP context, it need not wait for the DeletePDPContextResponse from the SGSN before sending the RADIUS DisconnectResponse to the AAA server.



NOTEote 1:- As showed on Figure 25, the GGSN need not wait for the DeletePDPContextResponse from the SGSN to send the RADIUS DisconnectResponse to the AAA server.

Figure 25: PDP Context deletion with RADIUS

16.4 List of RADIUS attributes

The following tables describe the actual content of the RADIUS messages exchanged between the GGSN and the AAA server. Other RADIUS attributes may be used as defined in RADIUS RFC(s). Unless otherwise stated, when the encoding scheme of an attribute is specified as UTF-8 encoding, this shall be interpreted as UTF-8 hexadecimal encoding.

16.4.1 Access-Request message (sent from the GGSN to AAA server)

The table 1 describes the attributes of the Access-Request message.

Table 1: The attributes of the Access-Request message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username is provided by the user (extracted from the Protocol Configuration Options (PCO) field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used). If no username is available a generic username, configurable on a per APN basis, shall	String	Mandatory

Attr #	Attribute Name	Description	Content	Presence Requirement
		be present.		
2	User-Password	User password provided by the user if PAP is used (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used). If no password is available a generic password, configurable on a per APN basis, shall be present.	String	Conditional Note 1
3	CHAP-Password	User password provided by the user if CHAP is used (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used).	String	Conditional Note 2
4	NAS-IP-Address	IP address of the GGSN for communication with the AAA server.	IPv4	Conditional Notes 3 and 4, 5
95	NAS-IPv6-Address	IP address of the GGSN for communication with the AAA server.	IPv6	Conditional Notes 3, 53 and 4
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 23
6	Service-Type	Indicates the type of service for this user	Framed	Optional
7	Framed-Protocol	Indicates the type of protocol for this user	7 (GPRS PDP Context)	Optional
8	Framed-IP-Address	IP address allocated for this user	IPv4	Conditional Note 45
9	Framed-IP-Netmask	Netmask for the user IP address	IPv4	Conditional Note 45
97	Framed-IPv6-Prefix	IPv6 address prefix allocated for this user	IPv6	Conditional Note 54
96	Framed-Interface-Id	User IPv6 Interface Identifier	IPv6	Conditional Notes 5, 64 and 5
30	Called-Station-Id	Identifier for the target network	APN (UTF-8 encoded)	Mandatory
31	Calling-Station-Id	This attribute is the identifier for the MS, and it shall be configurable on a per APN basis.	MSISDN in international format according to 3GPP TS 23.003 [40], UTF-8 encoded decimal. Note that there are no leading characters in front of the country code. (Note 6).	Optional
60	CHAP-Challenge	Challenge if CHAP is used (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used).	String	Conditional Note 2
61	NAS-Port-Type	Port type for the GGSN	As per RFC 2865 [38]	Optional
26/10415	3GPP Vendor-Specific	Sub-attributes according sub-clausesubclause 16.4.7	See sub-clausesubclause 16.4.7	Optional except sub-attribute 3 which is conditional

NOTE 1: Shall be present if PAP is used.
NOTE 2: Shall be present if CHAP is used.
NOTE 3: Either NAS-IP-Address or NAS-Identifier shall be present.
NOTE 54: Either IPv4 or IPv6 address/prefix attribute shall be present. The IP protocol version for end-user and network may be different.
NOTE 56: Included if the prefix alone is not unique for the user. This may be the case, for example, if address is assigned using stateful address autoconfiguration or if a static IPv6 address.
NOTE 6: There are no leading characters in front of the country code.

16.4.2 Access-Accept (sent from AAA server to GGSN)

T~~he t~~able 2 describes the attributes of the Access-Accept message. See RFC 2548 [51] for definition of MS specific attributes.

Table 2: The attributes of the Access-Accept message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username received in the Access-Request message or a substitute username provided by the AAA server. If the User-Name has been received in the Access-Accept message, this user-name shall be used in preference to the above	String	Optional
6	Service-Type	Indicates the type of service for this user	Framed	Optional
7	Framed-Protocol	Indicates the type of protocol for this user	7 (GPRS PDP Context)	Optional
8	Framed-IP-Address	IP address allocated for this user, if the AAA server is used to allocate IP address.	IPv4	Conditional Note 3~~5~~
9	Framed-IP-Netmask	Netmask for the user IP address, if the AAA server is used to allocate IP netmask.	IPv4	Conditional Note 2~~5~~
97	Framed-IPv6-Prefix	IPv6 address prefix allocated for this user, if the AAA server is used to allocate IP address prefixes.	IPv6	Conditional Note 2~~5~~
100	Framed-IPv6-Pool	Name of the prefix pool for the specific APN	IPv6	Optional Note 2~~5~~
12	Framed-IP-MTU	MTU for the user towards this particular APN, MTU shall be less or equal to 1500	String	Optional
25	Class	Identifier to be used in all subsequent accounting messages.	String	Optional (N~~OTE 4~~ote 1)
27	Session-Timeout	Indicates the timeout value (in seconds) for the user session	32 bit unsigned Integer	Optional
28	Idle-Timeout	Indicates the timeout value (in seconds) for idle user session	32 bit unsigned Integer	Optional
26/311	MS- Primary-DNS-server	Contains the primary DNS server address for this APN	IPv4	Optional Note 3~~7~~
26/311	MS-Secondary-DNS-Server	Contains the secondary DNS server address for this APN	IPv4	Optional Note 3~~7~~
26/311	MS-Primary-NBNS-Server	Contains the primary NetBios name server address for this APN	IPv4	Optional Note 3~~7~~
26/311	MS-Secondary-NBNS-Server	Contains the secondary NetBios server address for this APN	IPv4	Optional Note 3~~7~~
26/10415 /17	3GPP-IPv6-DNS-Servers	List of IPv6 addresses of DNS servers for this APN	IPv6	Optional Note 3~~7~~
NOTE 1~~4~~: The presence of this attribute is conditional upon this attribute being received in the Access-Accept message NOTE 2~~5~~: Either IPv4 or IPv6 address/prefix attribute shall be present. The IP protocol version for end-user and network may be different. NOTE 3~~7~~: Either IPv4 or IPv6 address attribute shall be present.				

16.4.3 Accounting-Request START (sent from GGSN to AAA server)

T~~he t~~able 3 describes the attributes of the Accounting-Request START message.

Table 3: The attributes of the Accounting-Request START message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username provided by the user (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used). If no username is available a generic username, configurable on a per APN basis, shall be present. If the User-Name has been received in the Access-Accept message, this user-name shall be used in preference to the above	String	Optional
4	NAS-IP-Address	GGSN IP address for communication with the AAA server.	IPv4	Conditional Notes 1 and 3~~3, 5~~
95	NAS-IPv6-Address	GGSN IPv6 address for communication with the AAA server.	IPv6	Conditional Notes 1 and 3~~3, 5~~
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 1~~3~~
6	Service-Type	Indicates the type of service for this user	Framed	Optional
7	Framed Protocol	Indicates the type of protocol for this user	7 (GPRS PDP Context)	Optional
8	Framed-IP-Address	User IP address	IPv4	Conditional Note 3~~5~~
97	Framed-IPv6-Prefix	User IPv6 Prefix	IPv6	Conditional Note ~~5~~3
96	Framed-Interface-Id	User IPv6 Interface Identifier	IPv6	Conditional Notes ~~5~~3 and 4~~, 6~~
25	Class	Received in the access accept	String	Conditional (Note ~~OTE~~ 2~~4~~)
30	Called-Station-Id	Identifier for the target network	APN (UTF-8 encoded)	Mandatory
31	Calling-Station-Id	This attribute is the identifier for the MS, and it shall be configurable on a per APN basis.	MSISDN in international format according to 3GPP TS 23.003 [40], UTF-8 encoded decimal. (Note 6)~~ Note that there are no leading characters in front of the country code.~~	Optional
40	Acct-Status-Type	Type of accounting message	START	Mandatory
41	Acct-Delay-Time	Indicates how many seconds the GGSN has been trying to send this record for, and can be subtracted from the time of arrival on the AAA server to find the approximate time (in seconds) of the event generating this Accounting-Request.	32 unsigned integer	Optional

Attr #	Attribute Name	Description	Content	Presence Requirement
44	Acct-Session-Id	User session identifier.	GGSN IP address (IPv4 or IPv6) and Charging-ID concatenated in a UTF-8 encoded hexadecimal. ~~NOTE: The GGSN IP address is the same as that used in the GCDRs.~~(Note 5)	Mandatory
45	Acct-Authentic	Authentication method	RADIUS or LOCAL	Optional
61	NAS-Port-Type	Port type for the GGSN	As per RFC 2865 [38]	Optional
26/10415	3GPP Vendor-Specific	Sub-attributes according ~~sub-clause~~subclause 16.4.7.	See ~~sub-clause~~subclause 16.4.7	Optional except sub-attribute 3 which is conditional
NOTE 1~~3~~: Either NAS-IP-Address or NAS-Identifier shall be present. NOTE 2~~4~~: The presence of this attribute is conditional upon this attribute being received in the Access-Accept message NOTE 3~~5~~: ~~-~~Either IPv4 or IPv6 address/prefix attribute shall be present. The IP protocol version for end-user and network may be different. NOTE 4~~6~~: ~~-~~Included if the prefix alone is not unique for the user. This may be the case, for example, if address is assigned using stateful address autoconfiguration or if a static IPv6 address. NOTE 5: The GGSN IP address is the same as that used in the GCDRs. NOTE 6: There are no leading characters in front of the country code.				

16.4.4 Accounting Request STOP (sent from GGSN to AAA server)

T~~he t~~able 4 describes the attributes of the Accounting-Request STOP message.

Table 4: The attributes of the Accounting-Request STOP message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username provided by the user (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used). If no username is available a generic username, configurable on a per APN basis, shall be present. If the User-Name has been received in the Access-Accept message, this user-name shall be used in preference to the above	String	Optional
4	NAS-IP-Address	IP address of the GGSN for communication with the AAA server.	IPv4	Conditional Notes 1 and 3~~, 5~~
95	NAS-IPv6-Address	IP address of the GGSN for communication with the AAA server.	IPv6	Conditional Notes 1 and 3~~, 5~~
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 1~~3~~
6	Service-Type	Indicates the type of service for this user	Framed	Optional
7	Framed Protocol	Indicates the type of protocol for this user	7 (GPRS PDP Context)	Optional
8	Framed-IP-Address	User IP address	IPv4	Conditional

Attr #	Attribute Name	Description	Content	Presence Requirement
				Note 35
97	Framed-IPv6-Prefix	User IPv6 Prefix	IPv6	Conditional Note 53
96	Framed-Interface-Id	User IPv6 Interface Identifier	IPv6	Conditional Notes 5, 63 and 4
25	Class	Received in the access accept	String	Optional (Note NOTE 24)
30	Called-Station-Id	Identifier for the target network	APN (UTF-8 encoded)	Mandatory
31	Calling-Station-Id	This attribute is the identifier for the MS, and it shall be configurable on a per APN basis.	MSISDN in international format according to 3GPP TS 23.003 [40], UTF-8 encoded. (Note 6). Note that there are no leading characters in front of the country code.	Optional
40	Acct-Status-Type	Indicates the type of accounting request	STOP	Mandatory
41	Acct-Delay-Time	Indicates how many seconds the GGSN has been trying to send this record for, and can be subtracted from the time of arrival on the AAA server to find the approximate time of the event generating this Accounting-Request	Second	Optional
42	Acct-Input-Octets	GGSN counted number of octets sent by the user for the PDP context	32 bit unsigned integer	Optional
43	Acct-Output-Octets	GGSN counted number of octets received by the user for the PDP context	32 bit unsigned integer	Optional
44	Acct-Session-Id	User session identifier.	GGSN IP address (IPv4 or IPv6) and Charging-ID concatenated in a UTF-8 encoded hexadecimal. NOTE: The GGSN IP address is the same as that used in the GCDRs.(Note 5)	Mandatory
45	Acct-Authentic	Authentication method	RADIUS or LOCAL	Optional
46	Acct-Session-Time	Duration of the session	Second	Optional
47	Acct-Input-Packets	GGSN counted number of packets sent by the user	Packet	Optional
48	Acct-Output-Packets	GGSN counted number of packets received by the user	Packet	Optional
49	Acct-Terminate-Cause	Indicate how the session was terminated	See RFC 2866 [39]	Optional
61	NAS-Port-Type	Port type for the GGSN	As per RFC 2865 [38]	Optional
26/10415	3GPP Vendor-Specific	Sub-attributes according to sub-clausesubclause 16.4.7.	See sub-clausesubclause 16.4.7	Optional except sub-attribute 3 which is conditional

Attr #	Attribute Name	Description	Content	Presence Requirement
NOTE 1~~3~~: Either NAS-IP-Address or NAS-Identifier shall be present. NOTE 2~~4~~: The presence of this attribute is conditional upon this attribute being received in the Access-Accept message NOTE 3~~5~~: Either IPv4 or IPv6 address/prefix attribute shall be present. The IP protocol version for end-user and network may be different. NOTE ~~6~~4: Included if the prefix alone is not unique for the user. This may be the case, for example, if address is assigned using stateful address autoconfiguration or if a static IPv6 address. NOTE 5: The GGSN IP address is the same as that used in the GCDRs. NOTE 6: There are no leading characters in front of the country code.				

16.4.5 Accounting Request ON (optionally sent from GGSN to AAA server)

T~~he t~~able 5 describes the attributes of the Accounting-Request ON message.

Table 5: The attributes of the Accounting-Request ON message

Attr #	Attribute Name	Description	Content	Presence Requirement
4	NAS-IP-Address	IP address of the GGSN for communication with the AAA server.	IPv4	Conditional Notes 1 and 2 ~~3, 7~~
95	NAS-IPv6-Address	IP address of the GGSN for communication with the AAA server.	IPv6	Conditional Notes 1 and 2 ~~3, 7~~
30	Called-Station-ID	Identifier for the target network.	APN (UTF-8 encoded)	Optional
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 1~~3~~
NOTE 1~~3~~: Either NAS-IP-Address or NAS-Identifier shall be present. NOTE 2~~7~~: Either IPv4 or IPv6 address attribute shall be present.				

16.4.6 Accounting Request OFF (optionally sent from GGSN to AAA server)

T~~he t~~able 6 describes the attributes of the Accounting-Request OFF message.

Table 6: The attributes of the Accounting-Request OFF message

Attr #	Attribute Name	Description	Content	Presence Requirement
4	NAS-IP-Address	IP address of the GGSN for communication with the AAA server.	IPv4	Conditional Notes 1 and 2 ~~3, 7~~
95	NAS-IPv6-Address	IP address of the GGSN for communication with the AAA server.	IPv6	Conditional Notes 1 and 2 ~~3, 7~~
30	Called-Station-ID	Identifier for the target network.	APN (UTF-8 encoded)	Optional
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 1~~3~~
NOTE 1~~3~~: Either NAS-IP-Address or NAS-Identifier shall be present. NOTE ~~7~~2: ~~-~~Either IPv4 or IPv6 address attribute shall be present.				

16.4.7 Sub-attributes of the 3GPP Vendor-Specific attribute

The table 7 describes the sub-attributes of the 3GPP Vendor-Specific attribute of the Access-Request, Accounting-Request START, Accounting-Request STOP and Accounting-Request Interim-Update messages.

Table 7: The sub-attributes of the 3GPP Vendor-Specific attribute of the Access-Request, Accounting-Request START, Accounting-Request STOP and Accounting-Request Interim-Update messages

Sub-attr #	Sub-attribute Name	Description	Presence Requirement	Associated attribute (Location of Sub-attr)
1	3GPP-IMSI	IMSI for this user	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
2	3GPP-Charging-Id	Charging ID for this PDP Context (this together with the GGSN-Address constitutes a unique identifier for the PDP context).	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
3	3GPP-PDP Type	Type of PDP context, e.g. IP or PPP	Conditional (mandatory if attribute 7 is present)	Access-Request Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
4	3GPP-CG-Address	Charging Gateway IP address	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
5	3GPP-GPRS-Negotiated-QoS-Profile	QoS profile applied by GGSN	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
6	3GPP-SGSN-Address	SGSN IP address that is used by the GTP control plane for the handling of control messages. It may be used to identify the PLMN to which the user is attached.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
7	3GPP-GGSN-Address	GGSN IP address that is used by the GTP control plane for the context establishment. It is the same as the GGSN IP address used in the GCDRs.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
8	3GPP-IMSI-MCC-MNC	MCC and MNC extracted from the user's IMSI (first 5	Optional	Access-Request, Accounting-Request START, Accounting-

Sub-attr #	Sub-attribute Name	Description	Presence Requirement	Associated attribute (Location of Sub-attr)
		or 6 digits, as applicable from the presented IMSI).		Request STOP, Accounting-Request Interim-Update
9	3GPP-GGSN- MCC-MNC	MCC-MNC of the network the GGSN belongs to.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
10	3GPP-NSAPI	Identifies a particular PDP context for the associated PDN and MSISDN/IMSI from creation to deletion.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP Accounting-Request Interim-Update
11	3GPP- Session-Stop-Indicator	Indicates to the AAA server that the last PDP context of a session is released and that the PDP session has been terminated.	Optional	Accounting Request STOP
12	3GPP- Selection-Mode	Contains the Selection mode for this PDP Context received in the Create PDP Context Request Message	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
13	3GPP-Charging-Characteristics	Contains the charging characteristics for this PDP Context received in the Create PDP Context Request Message (only available in R99 and later releases)	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
14	3GPP-CG-IPv6-Address	Charging Gateway IPv6 address	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
15	3GPP-SGSN-IPv6-Address	SGSN IPv6 address that is used by the GTP control plane for the handling of control messages. It may be used to identify the PLMN to which the user is attached.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
16	3GPP-GGSN-IPv6-Address	GGSN IPv6 address that is used by the GTP control plane for the context establishment.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update

Sub-attr #	Sub-attribute Name	Description	Presence Requirement	Associated attribute (Location of Sub-attr)
17	3GPP- IPv6-DNS-Servers	List of IPv6 addresses of DNS servers for an APN	Optional	Access-Accept
18	3GPP-SGSN-MCC-MNC	MCC and MNC extracted from the RAI within the Create PDP Context Request or Update PDP Context Request message.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update

The RADIUS vendor Attribute is encoded as follows (as per RFC 2865 [38])

Bits

Octets	8	7	6	5	4	3	2	1
1	-Type = 26							
2	Length = n							
3	Vendor id octet 1							
4	Vendor id octet 2							
5	Vendor id octet 3							
6	Vendor id octet 4							
7-n	String							

n ≥ ~~>=~~7

3GPP Vendor Id = 10415

The string part is encoded as follows:

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type =							
2	3GPP Length = m							
3 –m	3GPP value							

m ≥ ~~>=~~2 and m ≤ ~~<=~~ 248

The 3GPP specific attributes encoding is clarified below.

1 - 3GPP-***IMSI***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 1							
2	3GPP Length= m							
3-m	IMSI digits 1-n (UTF-8 encoded)							

3GPP Type: 1

n ≤ ~~<=~~15

Length: m = 17

IMSI value: Text:

This is the UTF-8 encoded IMSI; The definition of IMSI shall be in accordance with 3GPP TS 23.003 [40] and 3GPP TS 29.060 [24] ~~and [41]~~. There shall be no padding characters between the MCC and MNC, and between the MNC and MSIN. If the IMSI is less than 15 digits, the padding in the GTP information element shall be removed by the GGSN and not encoded in this sub-attribute.

2 - 3GPP-***Charging ID***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 2							
2	3GPP Length= 6							
3	Charging ID value Octet 1							
4	Charging ID value Octet 2							
5	Charging ID value Octet 3							
6	Charging ID value Octet 4							

3GPP Type: 2

Length: 6

Charging ID value: 32 bits unsigned integer

3 - 3GPP-***PDP type***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 3							
2	3GPP Length= 6							
3	PDP type octet 1							
4	PDP type octet 2							
5	PDP type octet 3							
6	PDP type octet 4							

3GPP Type: 3

Length: 6

PDP type value: Unsigned 32 bits integer

PDP type octet possible values:

0 = IPv4

1 = PPP

2 = IPv6

4 - 3GPP-***Charging Gateway address***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 4							
2	3GPP Length= 6							
3	Charging GW addr Octet 1							
4	Charging GW addr Octet 2							
5	Charging GW addr Octet 3							
6	Charging GW addr Octet 4							

3GPP Type: 4

Length: 6

Charging GW address value: Address

5 - 3GPP-***GPRS Negotiated QoS profile***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 5							
2	3GPP Length= L							
3 -L	UTF-8 encoded QoS profile							

3GPP Type: 5

Length: 27 (release 99) or 11 (release 98)

QoS profile value: -Text

UTF-8 encoded QoS profile syntax:

"<Release indicator> – <release specific QoS IE UTF-8 encoding>"

<Release indicator> = UTF-8 encoded number :

"98" = Release 98

"99"= Release 99

<release specific QoS profile UTF-8 encoding> = UTF-8 encoded QoS profile for the release indicated by the release indicator.

The UTF-8 encoding of a QoS IE is defined as follows: each octet is described by 2 UTF-8 encoded digits, defining its hexadecimal representation. The QoS profile definition is in 3GPP TS 24.008 [23].

The release 98 QoS profile data is 3 octets long, which then results in a 6 octets UTF-8 encoded string,

The release 99 QoS profile data is 11 octets long, which results in a 22 octets UTF-8 encoded string.

6 - 3GPP-***SGSN address***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 6							
2	3GPP Length= 6							
3	SGSN addr Octet 1							
4	SGSN addr Octet 2							
5	SGSN addr Octet 3							
6	SGSN addr Octet 4							

3GPP Type: 6

Length: 6

SGSN address value: -Address

7 - 3GPP-***GGSN address***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 7							
2	3GPP Length= 6							
3	GGSN addr Octet 1							
4	GGSN addr Octet 2							
5	GGSN addr Octet 3							
6	GGSN addr Octet 4							

3GPP Type: 7

Length: 6

GGSN address value:- Address

8 - 3GPP-***IMSI MCC-MNC***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 8							
2	3GPP Length= n							
3	MCC digit1 (UTF-8 encoded)							
4	MCC digit2 (UTF-8 encoded)							
5	MCC digit3 (UTF-8 encoded)							
6	MNC digit1 (UTF-8 encoded)							
7	MNC digit2 (UTF-8 encoded)							
8	MNC digit3 if present (UTF-8 encoded)							

3GPP Type: 8

Length: n shall be 7 or 8 octets depending on the presence of MNC digit 3

MS address value: -text

This is the UTF-8 encoding of the MS MCC-MNC values. -In accordance with 3GPP TS 23.003 [40] and 3GPP TS 29.060 [24] ~~and [41]~~ the MCC shall be 3 digits and the MNC shall be either 2 or 3 digits. There shall be no padding characters between the MCC and MNC.

9 - 3GPP-***GGSN MCC-MNC***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 9							
2	3GPP Length= n							
3	MCC digit1 (UTF-8 encoded)							
4	MCC digit2 (UTF-8 encoded)							
5	MCC digit3 (UTF-8 encoded)							
6	MNC digit1 (UTF-8 encoded)							
7	MNC digit2 (UTF-8 encoded)							
8	MNC digit3 if present (UTF-8 encoded)							

3GPP Type: 9

Length: n shall be 7 or 8 octets depending on the presence of MNC digit 3

GGSN address value: -text

This is the UTF-8 encoding of the GGSN MCC-MNC values. In accordance with 3GPP TS 23.003 [40] and 3GPP TS 29.060 [24] ~~and [41]~~ the MCC shall be 3 digits and the MNC shall be either 2 or 3 digits. There shall be no padding characters between the MCC and MNC.

10 - 3GPP-***NSAPI***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 10							
2	3GPP Length= 3							
3	NSAPI							

3GPP Type: 10

Length: 3

NSAPI value: text

It is the value of the NSAPI of the PDP context the RADIUS message is related to. It is encoded as its hexadecimal representation, using 1UTF-8 encoded digit.

11 - 3GPP-***Session Stop Indicator***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 11							
2	3GPP Length= 3							
3	1 1 1 1 1 1 1 1							

3GPP Type: 11

Length: -3

-Value is set to all 1.

12 - 3GPP-***Selection-Mode***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 12							
2	3GPP Length= 1							
3	UTF-8 encoded Selection mode string							

3GPP Type: 12

Length: -3

Selection mode value: Text

The format of this attribute shall be a character string consisting of a single digit, mapping from the binary value of the selection mode in the Create PDP Context message (3GPP TS 29.060 [24]). Where 3GPP TS 29.060 [24] provides for interpretation of the value, e.g. map -'3-' to -'2-', this shall be done by the GGSN.

13 - 3GPP-***Charging-Characteristics***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 13							
2	3GPP Length= 6							
3-6	UTF-8 encoded Charging Characteristics value							

3GPP Type: 13

Length: -6

Charging characteristics value: -Text

___The charging characteristics is value is the value of the 2 octets value field taken from the GTP IE described in 3GPP TS 29.060 [24], subclause~~section~~ 7.7.23.

___Each octet of this IE field value is represented via 2 UTF-8 encoded digits, defining its hexadecimal representation.

14 - 3GPP-***Charging Gateway IPv6 address***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 14							
2	3GPP Length= 18							
3	Charging GW IPv6 addr Octet 1							
4	Charging GW IPv6 addr Octet 2							
5-18	Charging GW IPv6 addr Octet 3-16							

3GPP Type: 14

Length: 18

Charging GW IPv6 address value: IPv6 Address

15 - 3GPP-***SGSN IPv6 address***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 15							
2	3GPP Length= 18							
3	SGSN IPv6 addr Octet 1							
4	SGSN IPv6 addr Octet 2							
5-18	SGSN IPv6 addr Octet 3-16							

3GPP Type: 15

Length: 18

SGSN IPv6 address value:- IPv6 Address

16 - 3GPP-***GGSN IPv6 address***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 16							
2	3GPP Length= 18							
3	GGSN IPv6 addr Octet 1							
4	GGSN IPv6 addr Octet 2							
5-18	GGSN IPv6 addr Octet 3-16							

3GPP Type: 16

Length: 18

GGSN IPv6 address value: IPv6 Address

17 - 3GPP-***IPv6-DNS-Servers***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 17							
2	3GPP Length= m							
3-18	(1st) DNS IPv6 addr Octet 1-16							
19-34	(2nd) DNS IPv6 addr Octet 1-16							
k-m	(n-th) DNS IPv6 addr Octet 1-16							

3GPP Type: 17

Length: m = n × *16 + 2;– n ≥ >=1 and n ≤ <=15; —k = m-15

IPv6 DNS Server value: -IPv6 Address The 3GPP- IPv6-DNS-Servers Attribute provides a list of one or more (-'n-') IPv6 addresses of Domain Name Server (DNS) servers for an APN. The DNS servers are listed in the order of preference for use by a client resolver, i.e. the first is -'Primary DNS Server-', the second is -'Secondary DNS Server-' etc. The attribute may be included in Access-Accept packets.

18 - 3GPP-***SGSN MCC-MNC***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 18							
2	3GPP Length= n							
3	MCC digit1 (UTF-8 encoded)							
4	MCC digit2 (UTF-8 encoded)							
5	MCC digit3 (UTF-8 encoded)							
6	MNC digit1 (UTF-8 encoded)							
7	MNC digit2 (UTF-8 encoded)							
8	MNC digit3 if present (UTF-8 encoded)							

3GPP Type: 18

Length: n shall be 7 or 8 octets depending on the presence of MNC digit 3

SGSN address value: -text

This is the UTF-8 encoding of the RAI MCC-MNC values. In accordance with 3GPP TS 23.003 [40] and 3GPP TS 29.060 [24] and [41] the MCC shall be 3 digits and the MNC shall be either 2 or 3 digits. There shall be no padding characters between the MCC and MNC.

16.4.8 Accounting Request Interim-Update (sent from GGSN to AAA server)

The table 8 describes the attributes of the Accounting-Request Interim-Update message.

Table 8: The attributes of the Accounting-Request Interim-Update message

Attr #	Attribute Name	Description	Content	Presence Requirement

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username provided by the user (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used). If no username is available a generic username, configurable on a per APN basis, shall be present. If the User-Name has been received in the Access-Accept message, this user-name shall be used in preference to the above	String	Optional
4	NAS-IP-Address	IP address of the GGSN for communication with the AAA server.	IPv4	Conditional Notes 1and 3~~,~~ ~~5~~
95	NAS-IPv6-Address	IP address of the GGSN for communication with the AAA server.	IPv6	Conditional Notes 1 and 3~~,~~ ~~5~~
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 1~~3~~
6	Service-Type	Indicates the type of service for this user	Framed	Optional
7	Framed Protocol	Indicates the type of protocol for this user	7 (GPRS PDP Context)	Optional
8	Framed-IP-Address	User IP address	IPv4	Conditional Note 3~~5~~
97	Framed-IPv6-Prefix	User IPv6 address	IPv6	Conditional Note 3~~5~~
96	Framed-Interface-Id	User IPv6 Interface Identifier	IPv6	Conditional Notes 3and 4 ~~5, 6~~
25	Class	Received in the access accept	String	Optional (N~~OTE 4~~ote 2)
30	Called-Station-Id	Identifier for the target network	APN (UTF-8 encoded)	Mandatory
31	Calling-Station-Id	This attribute is the identifier for the MS, and it shall be configurable on a per APN basis.	MSISDN in international format according to 3GPP TS 23.003 [40], UTF-8 encoded. ~~(~~Note 6)~~ Note that there are no leading characters in front of the country code.~~	Optional
40	Acct-Status-Type	Indicates the type of accounting request	Interim-Update	Mandatory
41	Acct-Delay-Time	Indicates how many seconds the GGSN has been trying to send this record for, and can be subtracted from the time of arrival on the AAA server to find the approximate time of the event generating this Accounting-Request	Second	Optional
42	Acct-Input-Octets	GGSN counted number of octets sent by the user for the PDP context	32 bit unsigned integer	Optional
43	Acct-Output-Octets	GGSN counted number of octets received by the user for the PDP context	32 bit unsigned integer	Optional
44	Acct-Session-Id	User session identifier.	GGSN IP address (IPv4 or IPV6) and Charging-ID concatenated in a UTF-8 encoded hexadecimal. ~~NOTE: The GGSN IP address is the~~	Mandatory

Attr #	Attribute Name	Description	Content	Presence Requirement
			~~same as that used in the GCDRs.~~(Note 5)	
45	Acct-Authentic	Authentication method	RADIUS or LOCAL	Optional
46	Acct-Session-Time	Duration of the session	Second	Optional
47	Acct-Input-Packets	GGSN counted number of packets sent by the user	Packet	Optional
48	Acct-Output-Packets	GGSN counted number of packets received by the user	Packet	Optional
61	NAS-Port-Type	Port type for the GGSN	As per RFC 2865 [38]	Optional
26/10415	3GPP Vendor-Specific	Sub-attributes according to ~~sub-clause~~subclause 16.4.7.	See ~~sub-clause~~subclause 16.4.7	Optional except sub-attribute 3 which is conditional

NOTE 1~~3~~: Either NAS-IP-Address or NAS-Identifier shall be present.
NOTE 2~~4~~: The presence of this attribute is conditional upon this attribute being received in the Access-Accept message
NOTE 3~~5~~: Either IPv4 or IPv6 address/prefix attribute shall be present. The IP protocol version for end-user and network may be different.
NOTE 4~~6~~: Included if the prefix alone is not unique for the user. This may be the case, for example, if address is assigned using stateful address autoconfiguration or if a static IPv6 address.
NOTE 5: GGSN IP address is the same as that used in the GCDRs.
NOTE 6: There are no leading characters in front of the country code.

16.4.9 Disconnect Request (optionally sent from AAA server to GGSN)

T~~he t~~able 9 describes the attributes of the Disconnect-Request message.

Table 9: The attributes of the Disconnect-Request message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username provided by the user (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used). If no username is available a generic username, configurable on a per APN basis, shall be present. If the User-Name has been sent in the Access-Accept message, this user-name shall be used in preference to the above	String	Optional
8	Framed-IP-Address	User IP address	IPv4	Conditional Note 2~~8~~
97	Framed-IPv6-Prefix	User IPv6 address	IPv6	Conditional Note 2~~8~~
96	Framed-Interface-Id	User IPv6 Interface Identifier	IPv6	Conditional Notes 1 and~~6,~~ ~~8~~2
44	Acct-Session-Id	User session identifier.	GGSN IP address (IPv4 or IPv6) and Charging-ID concatenated in a UTF-8 encoded hexadecimal.	Mandatory

			~~NOTE: The GGSN IP address is the same as that used in the GCDRs.~~(Note 3)	
NOTE 1~~6~~: Included if the prefix alone is not unique for the user. This may be the case, for example, if address is assigned using stateful address autoconfiguration or if a static IPv6 address. NOTE 2~~8~~: Either IPv4 or IPv6 address/prefix attribute shall be present. NOTE 3: The GGSN IP address is the same as that used in the GCDRs.				

Annex A (informative): Interworking PCS1900 with PSDNs

~~<VOID>~~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
06-2001	TSG#12	NP-010256	018		Clarifications on the non-transparent access mode	4.0.0	4.1.0
06-2001	TSG#12	NP-010256	020		Set the use of PPP between the MT and TE as an option when interworking with MIPv4	4.0.0	4.1.0
09-2001	TSG#13	NP-010530	021	5	Standard method for information delivery (MSISDN; IP address…) between GPRS and external PDN using RADIUS	4.1.0	4.2.0
12-2001	TSG#14	NP-010672	023	2	Standard method for information update between GPRS and external PDN using RADIUS	4.2.0	4.3.0
12-2001	TSG#14	NP-010672	024	2	Standard method for interworking between GPRS and external PDN using RADIUS	4.2.0	4.3.0
12-2001	TSG#14	NP-010572	028	1	Correction to the Calling-Station-Id attribute	4.2.0	4.3.0
12-2001	TSG#14	NP-010572	030	1	Correction to 3GPP Vendor specify attribute 3GPP-IMSI	4.2.0	4.3.0
12-2001	TSG#14	NP-010572	032		Correction to 3GPP vendor specific attributes containing MCC-MNC	4.2.0	4.3.0
03-2002	TSG#15	NP-020080	038		Change of associated attribute for 3GPP-NSAPI	4.3.0	4.4.0
06-2002	TSG#16	NP-020295	048	1	Corrections to the 3GPP RADIUS attributes	4.4.0	4.5.0
06-2002	TSG#16	NP-020295	055	3	Clarification on the Radius Flows	4.4.0	4.5.0
06-2002	TSG#16	NP-020171	060		Address autoconfiguration of IPv6 terminals and IPv6 update	4.4.0	4.5.0
12-2002	TSG#18	NP-020613	065		Correction of figure for Radius Accounting Update	4.5.0	4.6.0
12-2002	TSG#18	NP-020614	069		Corrections related to IPv6	4.5.0	4.6.0
12-2002	TSG#18	NP-020613	071		RADIUS enhancement for identification of VPLMN	4.5.0	4.6.0

3GPP TSG-CN WG3 Meeting #27
Dublin, Ireland, 10th - 14th February 2003.

Tdoc ⌘N3-030124

CR-Form-v7

CHANGE REQUEST

⌘ **29.061** **CR** **083** ⌘ **rev** **1** ⌘ Current version: **5.4.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	Correction of References and specification Corrections
Source:	⌘	TSG_CN WG3 *[Siemens AG, MCC]*
Work item code:	⌘	TEI
Date:	⌘	11/02/2003
Category:	⌘	**A**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Inconsistencies in the specification, Missing and incorrect references
Summary of change:	⌘	Correction of incorrect and missing reference and general specification clean-up
Consequences if not approved:	⌘	Inconsistencies and errors in the referencing. Possible misunderstanding when reading specification.

Clauses affected:	⌘	Most of the specification			
Other specs affected:	⌘	**Y**	**N**		
			X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

3GPP TS 29.061 V5.4.0 (2002-12)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Core Network;
~~Packet Domain;~~
Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and ~~Packet Data~~ Packet Data Networks (PDN)
(Release 5)

Keywords

UMTS, GSM, packet mode, interworking, PLMN, PDN

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

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.

The present document is valid for a PLMN in A/Gb mode as well as for a PLMN in Iu mode. If text applies only for one of these systems it is explicitly mentioned by using the terms "A/Gb mode" and "Iu mode". Please note, that the A interface does not play any role in the scope of ~~this document~~the present document although the term "A/Gb mode" is used.

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. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

~~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] Void.

[2] 3GPP TS 22.060: "General Packet Radio Service (GPRS); Service Description~~:~~; Stage 1 ~~Service Description~~".

[3] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service Description; Stage 2".

[4] Void.

[5] Void.

[6] Void.

[7] Void.

[8] Void.

[9] Void.

[10] 3GPP TS 27.060: "Packet Domain; Mobile Station (MS) supporting Packet Switched s~~S~~ervices".

[11] ITU-T Recommendation E.164: "The international public telecommunication numbering plan~~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~~ names ~~-~~ ~~Concepts~~ concepts and ~~Facilities~~facilities" (STD 7).

[20] Void.

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

[21b] IETF RFC 1662 (1994): "PPP in HDLC-like Framing".

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

[23] 3GPP TS 44.008: "Mobile radio interface layer 3 specification; Core Network ~~P~~protocols;~~ –~~ Stage 3".

[24] 3GPP TS 29.060: "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp i~~I~~nterface".

[25] IETF RFC 2794 (2000)~~, Pat R. Calhoun and Charles E. Perkins~~: "Mobile IP Network Address Identifier Extension for IPv4", P. Calhoun, C. Perkins~~, 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 RFC 2373 (1998): "IP ~~version~~ Version 6 Addressing Architecture".

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

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

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

[32] IETF RFC 1112 (1989)~~, S.E. Deering~~: "Host extensions for IP multicasting", S.E. Deering.

[33] IETF RFC 2236 (1997)~~, W. Fenner~~: "Internet Group Management Protocol, Version 2", W. Fenner.

[34] IETF RFC 2362 (1998)~~, D. Estrin and al~~: "Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification", D. Estrin, D. Farinacci, A. Helmy, D. Thaler, S. Deering, M. Handley, V. Jacobson, C. Liu, P. Sharma, L. Wei~~".~~

[35] IETF RFC 1075 (1988)~~, D. Waitzman and al~~: "Distance Vector Multicast Routing Protocol", D. Waitzman, C. Partridge, S.E. Deering.

[36] IETF RFC 1585 (1994)~~, J. Moy~~: "MOSPF: Analysis and Experience", J. Moy~~.~~.

[37] IETF RFC 2290 (1998)~~, J. Solomon, S. Glass~~: "Mobile-IPv4 Configuration Option for PPP IPCP ", J. Solomon, S. Glass.

[38] IETF RFC 2865 (2000)~~, C. Rigney, S. Willens, A. Rubens, W. Simpson~~: "Remote Authentication Dial In User Service (RADIUS)", C. Rigney, S. Willens, A. Rubens, W. Simpson.

[39] IETF RFC 2866 (2000)~~, C. Rigney, Livingston~~: "~~-~~RADIUS Accounting~~-~~", C. Rigney, Livingston.

[40] 3GPP TS 23.003: "~~3rd Generation Partnership Project; Technical Specification Group Core Network;~~ Numbering, addressing and identification".

[41] IETF RFC 2882 (2000)~~, D. Mitton~~: "Network Access Servers Requirements: Extended RADIUS Practices", D. Mitton.

[42] 3GPP TR 21.905: "-Vocabulary for 3GPP Specifications".

[43] IETF RFC 2472 (1998)~~, D. Haskins, E. Allen~~: ~~"~~"IP Version 6 over PPP~~"~~", D. Haskins, E. Allen.

[44] IETF RFC 2461 (1998)~~, T. Narten, E. Nordmark, W. Simpson~~: ~~"~~"Neighbor Discovery for IP Version 6 (IPv6)~~"~~", T. Narten, E. Nordmark, W. Simpson

[45] IETF RFC 3118 (2001)~~, R. Droms, W. Arbaugh~~: ~~"~~"Authentication for DHCP Messages~~"~~", R. Droms, W. Arbaugh.

[46] IETF Internet-Draft: ~~"~~"Dynamic Host Configuration Protocol for IPv6 (DHCPv6)~~"~~", draft-ietf-dhc-dhcpv6-~~24~~28.txt, work in progress.

[47] 3GPP TS 24.229: ~~"~~"IP Multimedia Call Control Protocol based on SIP and SDP~~"~~"

[48] IETF RFC 2710 (1999)~~, S. Deering, W. Fenner, B. Haberman~~: ~~"~~"Multicast Listener Discovery (MLD) for IPv6~~"~~", S. Deering, W. Fenner, B. Haberman.

[49] IETF RFC 2460 (1998)~~, S.Deering,, R.Hinden~~: ~~"~~"Internet Protocol, Version 6 (IPv6) Specification~~"~~", S.Deering, R.Hinden.

[50] IETF RFC 3162 (2001)~~, B. Adoba, G. Zorn, D. Mitton~~: ~~"~~"RADIUS and IPv6~~"~~", B. Adoba, G. Zorn, D. Mitton.

[51] IETF RFC 2548 (1999)~~, G.Zorn~~: ~~"~~"Microsoft Vendor-specific RADIUS Attributes~~"~~", G.Zorn.

[52] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2~~IP Multimedia Core Network Subsystem (IMS)~~".

[53] 3GPP TS 29.207: "Policy control over Go interface".

[54] 3GPP TS 24.008: "Mobile radio interface layer 3 specification; Core Network protocols; ~~-~~ ~~s~~Stage 3".

[55] ~~3GPP TS 24.229: "IP Multimedia Call Control Protocol based on SIP and SDP~~Void.~~".~~

[56] 3GPP TS 29.208: ~~"~~"End to end Quality of Service (QoS) signalling flows~~"~~".

[57] ~~IETF RFC 1034 (1987): "Domain Names - Concepts and Facilities" (STD 13).~~Void.

[58] IETF RFC 1035 (1987): "Domain ~~Names~~ names ~~-~~ ~~Implementation~~ implementation and ~~Specification~~specification" (STD 13).

[59] IETF RFC 1886 (1995): "DNS Extensions to support IP version 6".

[60] IETF RFC 1771 (1995): "A Border Gateway Protocol 4 (BGP-4)".

[61] IETF RFC 1825 (1995): "Security Architecture for the Internet Protocol".

[62] IETF RFC 1826 (1995): "IP Authentication Header".

[63] IETF RFC 1827 (1995): "IP Encapsulating Security Payload (ESP)".

3 Definitions, abbreviations and symbols

3.1 Definitions

For the purposes of the present document, the ~~following~~ terms and definitions given in 3GPP TS 22.060 [2] and 3GPP TS 23.060 [3] and the following apply:

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

A/Gb mode: indicates that the text applies only to a system or sub-system which operate in A/Gb mode of operation, i.e. with a functional division that is in accordance with the use of an A or a Gb interface between the radio access network and the core network.

Iu mode: indicates that the text applies only to a system or a sub-system which operates in Iu mode of operation, i.e. with a functional division that is in accordance with the use of an Iu-CS or Iu-PS interface between the radio access network and the core network.

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
DHCPv6	Dynamic Host Configuration Protocol version 6
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
IMS	IP Multimedia Core Network Subsystem
IP	Internet Protocol
IPCP	IP Control Protocol (PPP NCP for IPv4)
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPV6CP	IPv6 Control Protocol (PPP NCP for IPv6)
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
LAC	L2TP Access Concentrator
LAN	Local Area Network
LNS	L2TP Network Server
MIP	Mobile IP
MLD	Multicast Listener Discovery
MOSPF	Multicast Open Shortest Path First
MS	Mobile Station
MT	Mobile Terminal
MTU	Maximum Transfer Unit
NAI	Network Access Identifier
PAP	Password Authentication Protocol
PCF	Policy Control Function
PDCP	Packet Data Convergence Protocol

PDN	Packet Data Network
PDU	Protocol Data Unit
PEP	Policy Enforcement Point
PIM-SM	Protocol Independent Multicast – Sparse Mode
PPP	Point-to-Point Protocol
PS	Packet Switched
RADIUS	Remote Authentication Dial In User Service
SBLP	Service Based Local Policy
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.
Go	Interface between a GGSN and a PCF.
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 fixed network part in A/Gb mode. The Um interface is the A/Gb mode 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 fixed network part in Iu mode. The Uu interface is the Iu mode 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 3GPP technical specifications. The Packet Domain related key characteristics are found in 3GPP TS 22.060 [2] and 3GPP TS 23.060 [3].

4.2 Key characteristics of PSDN

~~<VOID>~~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 [40] 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 PLMN network in the overall Packet Domain environment.

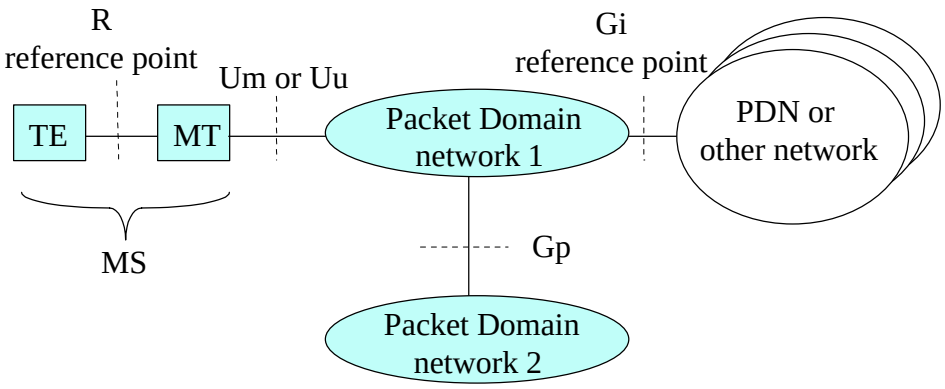


Figure 1: Packet Domain Access Interfaces and Reference Points

7 Interface to Packet Domain Bearer Services

7.1 A/Gb mode

~~The following f~~Figure 2a shows the relationship of the Packet Domain Bearer in A/Gb mode terminating at the SNDCP layer to the rest of the A/Gb mode Packet Domain environment. It is shown for reference purposes only and detailed information can be found in 3GPP TS 23.060 [3].

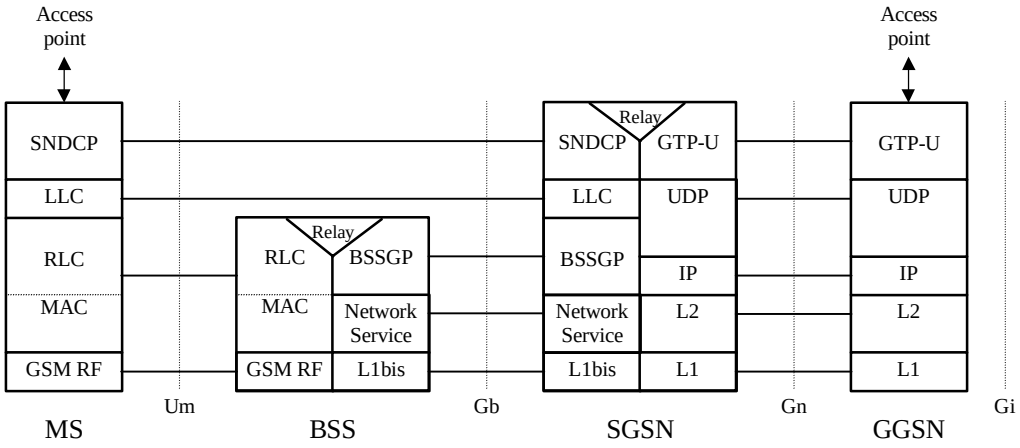


Figure 2a: User Plane for Packet Domain services in A/Gb mode

7.2 Iu mode

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

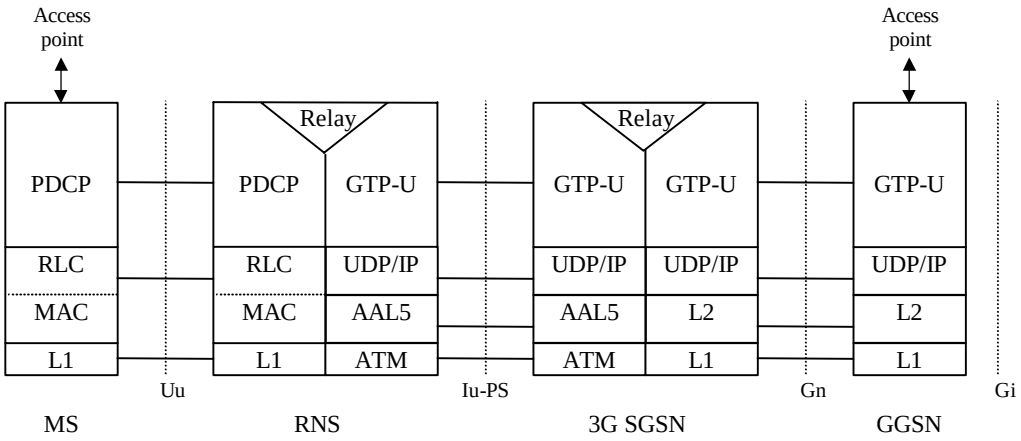


Figure 2b: User Plane for Packet Domain services in Iu mode

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 [3]. 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 [2] and 3GPP TS 23.060 [3]. 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>~~Figure 3: Void

Figure 4: Void

Figure 5: Void

Figure 6: 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~~IPv6. The interworking point with IP networks is at the Gi reference point as shown in figure 7.

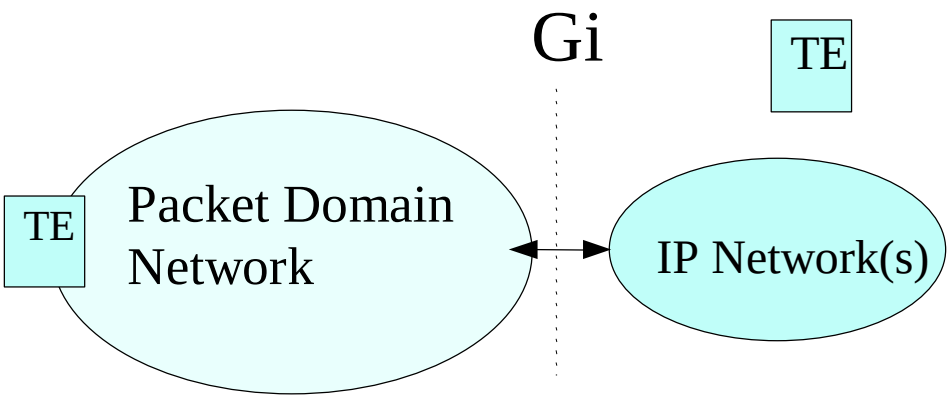


Figure 7: IP network interworking

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.

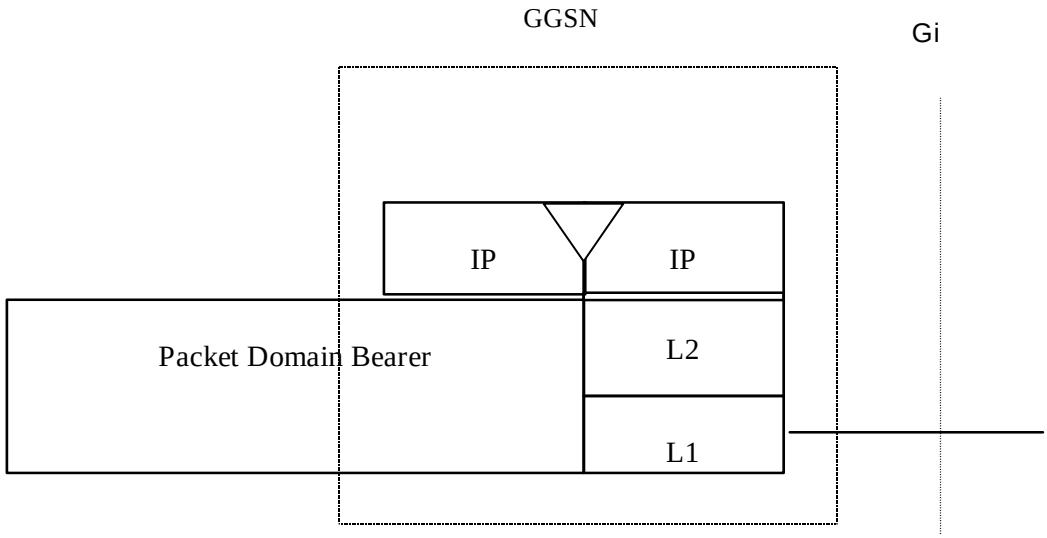


Figure 8: The protocol stacks for the IP / Gi reference point

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, IPv6 address autoconfiguration, 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.

The mechanisms for host configuration and user authentication described in this ~~section~~subclause and its sub-~~section~~clauses are only applicable to the activation of the first context activated for a specific PDP address (using the ~~"~~"PDP Context Activation Procedure~~"~~"). The activation of any subsequent PDP contexts for that PDP address, using the ~~"~~"Secondary PDP Context Activation Procedure~~"~~", as well as the use of TFTs, is described in 3GPP TS 23.060 [3].

11.2.1.1 Transparent access to the Internet

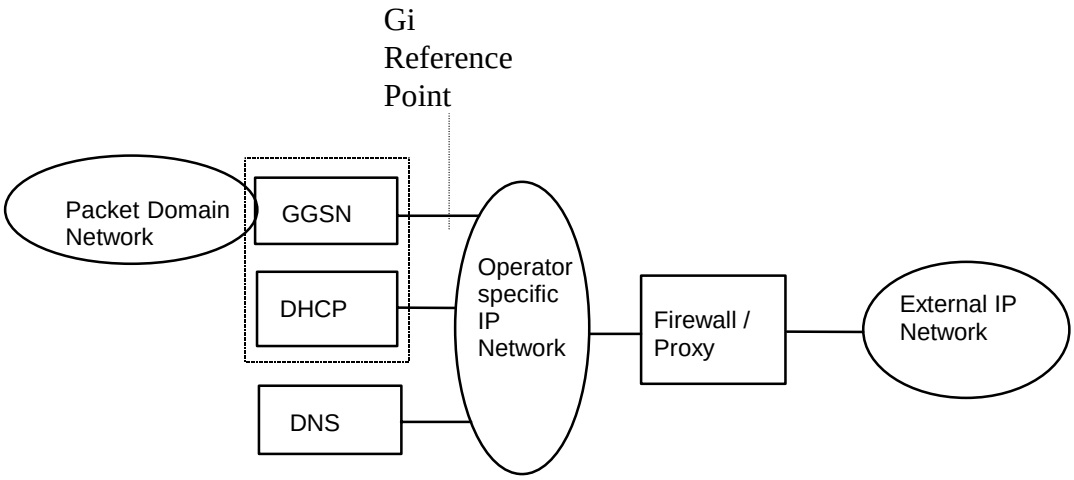


Figure 9: Example of the PDN Interworking Model, transparent case

In this case (see figure 9):

- the MS is given an address or IPv6 Prefix belonging to the operator addressing space. The address or IPv6 Prefix 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 or IPv6 Prefix is used for packet forwarding between the Internet and the GGSN and within the packet domain. With IPv6, either– Stateless or Stateful Address Autoconfiguration shall be used to assign an IPv6 address to the MS. These procedures are as described in the IPv6 non-transparent access case except that the addresses belong to the operator addressing space. The use of stateful or stateless is configured per APN.

- 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.

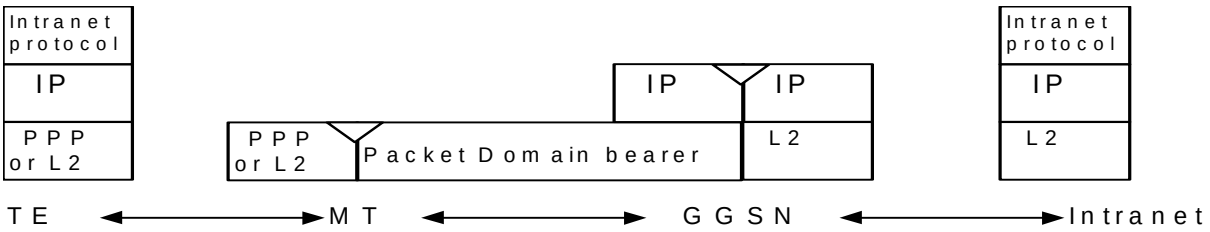


Figure 10: Transparent access to an Intranet

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 Pрrotocol»."."

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

An example of an «"Intranet Pprotocol»-" is IPsec (see RFC -1825 [61]). 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 [62] and RFC -1827 [63]). In this case private IP tunnelling within public IP takes place.

11.2.1.2 IPv4 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 AAA, 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 AAA, DHCP, …, belonging to the Intranet/ISP;

- the protocol configuration options are retrieved (if requested by the MS at PDP context activation) from some server (AAA 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.

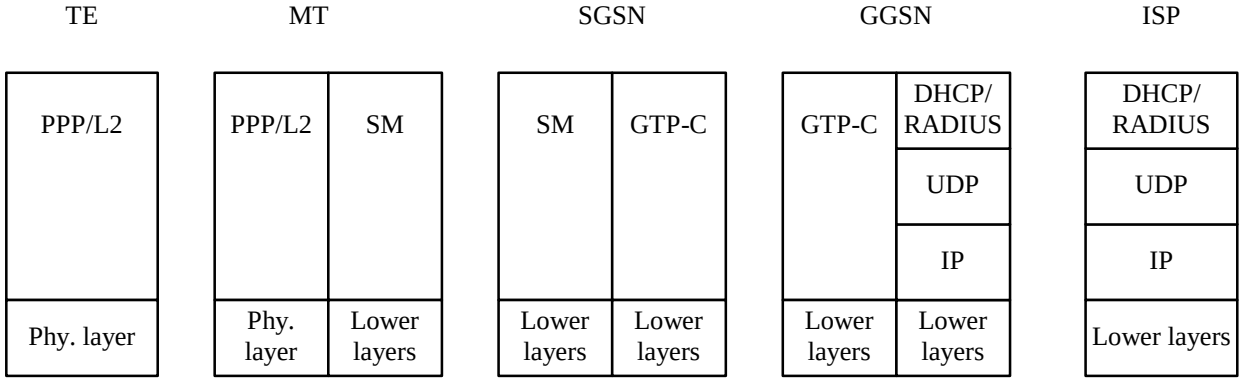


Figure 11a: Signalling plane of non transparent case

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 AAA 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 AAA 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 1661 [21a] and RFC 1662 [21b] 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.

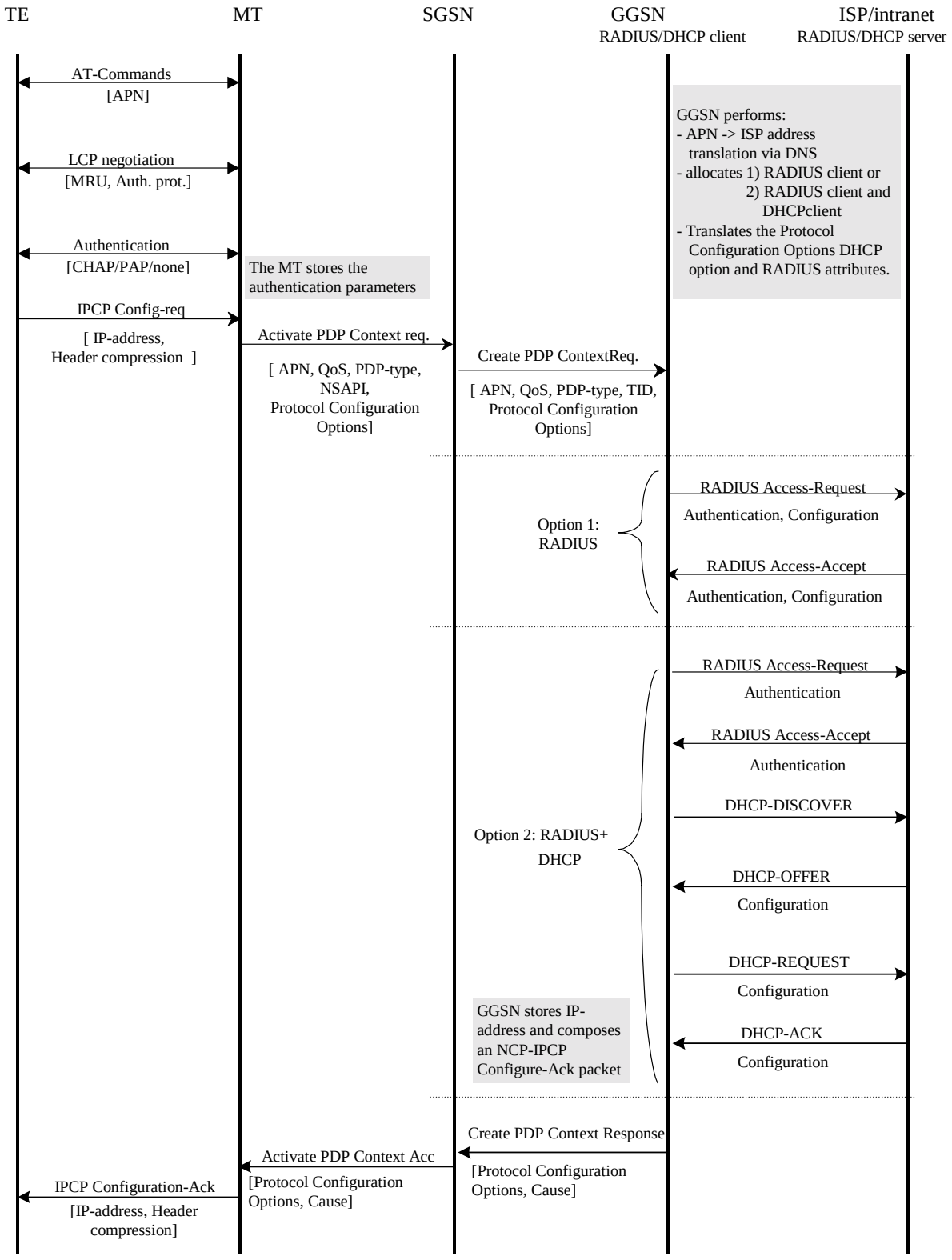


Figure 11b: PDP Context Activation for the IPv4 Non-transparent case

11.2.1.3 IPv6 Non Transparent access to an Intranet or ISP

When using IPv6 Address Autoconfiguration (either Stateless or Stateful), the process of setting up the access to an Intranet or ISP involves two signalling phases. The first signalling phase is done in the control plane and consists of the PDP context activation, followed by a second signalling phase done in the user plane.

The user plane signalling phase shall be either stateless or stateful. The stateless procedure, which involves only the MS and the GGSN, is described in subclause "IPv6 Stateless Address Autoconfiguration". The stateful procedure, which involves the MS, GGSN (as DHCP relay agent) and one or several DHCP servers on the Intranet or ISP, is described in subclause "IPv6 Stateful Address Autoconfiguration".

Whether to use stateless or stateful address autoconfiguration procedure is configured per APN in the GGSN. For APNs configured as stateless, the GGSN shall only use the Prefix part of the IPv6 address for forwarding of mobile terminated IP packets. The size of the prefix shall be according to the maximum prefix length for a global IPv6 address as specified in the IPv6 Addressing Architecture, see RFC 2373 [28].

Stateful and Stateless Autoconfiguration may also co-exist. In that case, the MS shall use Stateless to configure the address and Stateful to configure additional parameters only. The MS shall not use Stateless and Stateful Address Autoconfiguration simultaneously since GPRS only supports one prefix per PDP Context (see 3GPP TS 23.060 [3]).

The selection between Stateful and Stateless Autoconfiguration is dictated by the Router Advertisements sent by the GGSN as described in the corresponding subclauses below and according to the principles defined in RFC 2461 [44] and RFC 2462 [29].

For MS, IPv6 Stateless Address Autoconfiguration is mandatory, and IPv6 Stateful Address Autoconfiguration is optional.

11.2.1.3.1 IPv6 PDP Context Activation

In this case:

- The GGSN provides the MS with an IPv6 Prefix belonging to the Intranet/ISP addressing space. A dynamic IPv6 address shall be given using either stateless or stateful address autoconfiguration. This IPv6 address is used for packet forwarding within the packet domain and for packet forwarding on the Intranet/ISP;

- the MS may send an authentication request at PDP context activation and the GGSN may request user authentication from a server, e.g. AAA, …, belonging to the Intranet/ISP;

- the protocol configuration options are retrieved (if requested by the MS at PDP context activation) from some server, e.g. AAA, …, belonging to the Intranet/ISP;

- in order to avoid any conflict between the link-local address of the MS and that of the GGSN, the Interface-Identifier used by the MS to build its link-local address shall be assigned by the GGSN. The GGSN ensures the uniqueness of this interface-identifier. The MT shall then enforce the use of this Interface-Identifier by the TE. This is valid for both stateless and stateful address autoconfiguration.

- 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 over the insecure connection. This security protocol is defined by mutual agreement between PLMN operator and Intranet/ISP administrator.

- the MS may request for DNS server IPv6 addresses using the PCO IE in e.g. the PDP Context Request message. In that case the GGSN may return the IP address of one or more DNS servers in the PCO in the PDP Context Response message. The DNS address(es) shall be coded in the PCO as specified in 3GPP TS 24.008 [54]. If a list of servers is received, the MS shall adhere to the explicit prioritisation order of the list.

In the following signalling flow example, PPP is used as layer 2 protocol over the R reference point. The MT behaves 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 RADIUS authentication. The result of the host authentication is carried via GTP-C back to the SGSN, which then relays the result to the MT. The MT finalises the

IPV6CP negotiation by sending an IPV6CP Configure-Ack message to the TE with the appropriate options included, e.g., Interface-Identifier. The Interface-Identifier shall be used in the TE to create a link-local address to be able to perform the IPv6 address autoconfiguration (see subclauses 11.2.1.3.2 and 11.2.1.3.3).

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 IPv6 Interface-Identifier negotiation by sending the IPV6CP Configure-Request message to the MT.

5) The MT sends the Activate PDP Context Request message to the SGSN, including the Protocol Configuration Options. The Protocol Configuration Options IE may contain negotiated LCP options such as negotiated Authentication Protocol as well as any authentication data previously stored in the MT. It may also contain a request for dynamic configuration of DNS server IPv6 addresses. The MS shall for dynamic address allocation leave PDP Address empty and set PDP Type to IPv6. The SGSN sends the Create PDP context request message to the chosen GGSN including the unmodified Protocol Configuration Options.

6) The GGSN deduces from local configuration data associated with the APN:

   - IPv6 address allocation type (stateless or stateful);
   - the source of IPv6 Prefixes in the stateless case (GGSN internal prefix pool, or external address allocation server);
   - any server(s) to be used for address allocation, authentication and/or protocol configuration options retrieval (e.g. IMS related configuration, see 3GPP TS 24.229 [47]);
   - the protocol e.g. RADIUS, to be used with the server(s);
   - the communication and security feature needed to communicate with the server(s);

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

   - GGSN internal Prefix pool for IPv6 prefix allocation and no authentication;
   - GGSN internal Prefix pool for IPv6 prefix allocation and RADIUS for authentication. The AAA server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the GGSN;
   - RADIUS for authentication and IPv6 prefix allocation. The AAA server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the GGSN;

NOTE: DHCPv6 may be used for IPv6 prefix allocation when an appropriate RFC becomes available.

   IPv6 Prefixes in a GGSN internal Prefix pool shall be configurable and structured per APN.

   The GGSN shall in the PDP Address IE in the Create PDP Context Response return an IPv6 address composed of a Prefix and an Interface-Identifier. The Interface-Identifier may have any value and it does not need to be unique within or across APNs. It shall however not conflict with the Interface-Identifier the GGSN has selected for its own side of the MS-GGSN link. The Prefix assigned by the GGSN or the external AAA server shall be globally or site-local unique, if stateless address autoconfiguration is configured on this APN. If, on the other hand, stateful address autoconfiguration is configured on the APN, the Prefix part of the IPv6 address returned in the PDP Address IE shall be set to the link-local prefix (FE80::/64).

   The GGSN shall analyse the requested values of all the protocol options contained in the received Protocol Configurations Options IE. The contents of the Protocol Configurations Options IE sent in the GGSN response shall be in accordance with the relevant standards e.g. the PPP standard RFC 1661 [21a] and RFC 1662 [21b].

7) The GGSN sends back to the SGSN a Create PDP Context Response message, containing the PDP Address IE and the Protocol Configuration Options IE. The Protocol Configuration Options IE may contain configuration

data such as a list of DNS server IPv6 addresses. The cause value shall be set according to the outcome of the host authentication and configuration.

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

9) The MT extracts the Interface-Identifier from the address received in the PDP Address IE and ignores the Prefix part. If this Interface-Identifier is identical to the tentative Interface-Identifier indicated in the IPV6CP Configure-Request message sent from the TE, the MT sends an IPV6CP Configure Ack packet, indicating this Interface-Identifier, to the TE.

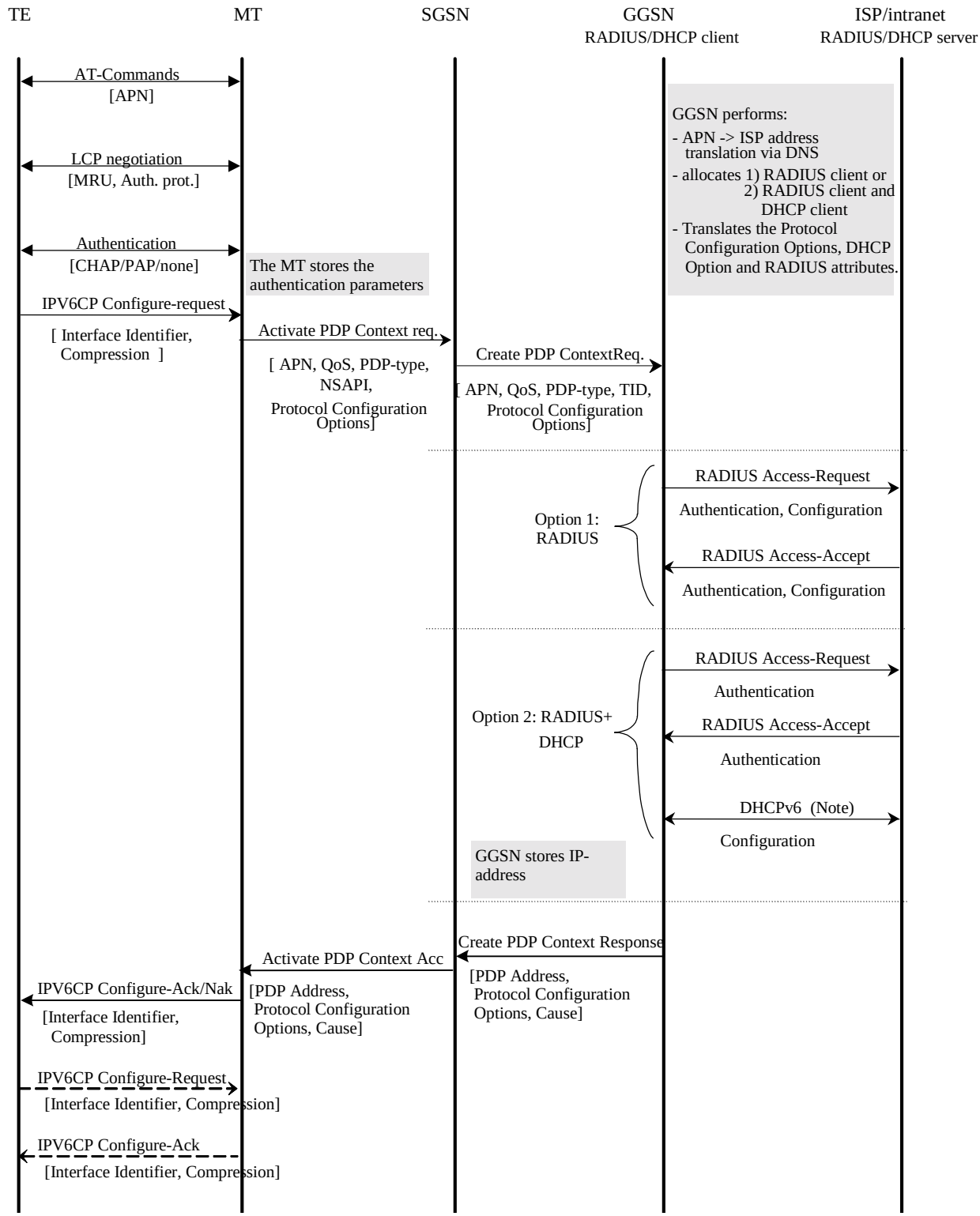
If the Interface-Identifier extracted from the address contained in the PDP Address IE is not identical to the tentative Interface-Identifier indicated in the IPV6CP Configure-Request message sent from the TE, the MT sends an IPV6CP Configure-Nak packet, indicating the Interface-Identifier extracted from the address contained in the PDP Address IE, to the TE. The TE then sends a new IPV6CP Configure-Request message to the MT, indicating the same Interface-Identifier as was indicated in the received IPV6CP Configure Nak (as indicated by the dotted IPV6CP Configure-Request and Configure-Ack in the figure below). Finally the MT responds with a IPV6CP Configure Ack packet.

In case a PDP Context Reject was sent to the MS the MT sends an LCP Terminate-Request to the TE.

10) When the TE has accepted the Interface-Identifier given by the MT, the user plane link from the TE to the GGSN and the external ISP/Intranet is established and the IPv6 address autoconfiguration may proceed.

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.

An LCP Terminate-request causes a PDP context deactivation.



Note 1OTE: DHCPv6 may be used for IPv6 prefix allocation when an appropriate RFC becomes available.

Figure 11ba: PDP Context Activation for the IPv6 Non-transparent case

Figure 11ba above is valid for both Stateless and Stateful Address Autoconfiguration case. In the Stateful case though, option 2 does not apply and option 1 may only be used for authentication. The use of DHCPv6 above is different and used in a different context than when used for Stateful Address Autoconfiguration as in subclause 11.2.1.3.3.

11.2.1.3.2 IPv6 Stateless Address Autoconfiguration

As described in 3GPP TS 23.060 [3], a PDP Context of PDP type IPv6 activated by means of the IPv6 Stateless Address Autoconfiguration Procedure is uniquely identified by the prefix part of the IPv6 address only. The MS may select any value for the Interface-Identifier part of the address. The only exception is the Interface-Identifier for the link-local address used by the MS (see RFC 2373 [28]). This Interface-Identifier shall be assigned by the GGSN to avoid any conflict between the link-local address of the MS and that of the GGSN itself. This is described in subclause "IPv6 PDP Context Activation" above.

For IPv6 the PDP Context Activation phase is followed by an address autoconfiguration phase. The procedure describing APNs configured to use Stateless Address Autoconfiguration, may be as follows:

1) After the first phase of setting up IPv6 access to an Intranet or ISP, the MS shall use the IPv6 Interface-Identifier, as provided by the GGSN, to create its IPv6 Link-Local Unicast Address according to RFC 2373 [28].

   Before the MS can communicate with other hosts or MSes on the Intranet/ISP, the MS must obtain an IPv6 Global or Site-Local Unicast Address. The simplest way is the IPv6 Stateless Address Autoconfiguration procedure described below and in 3GPP TS 23.060 [3]. The procedure is consistent with RFC 2462 [29].

   The procedure below takes place through signalling in the user plane. It is done on the link between the MS and the GGSN. From the MS perspective the GGSN is now the first router on the link.

2) After the GGSN has sent a Create PDP Context Response message to the SGSN, it shall start sending Router Advertisements periodically on the new MS-GGSN link established by the PDP Context. The MS may issue a Router Solicitation directly after the user plane establishment. This shall trigger the GGSN to send a Router Advertisement immediately.

   To indicate to the MS that stateless address autoconfiguration shall be performed, the GGSN shall leave the M-flag cleared in the Router Advertisement messages. An MS shall not perform stateless and stateful address autoconfiguration simultaneously, since multiple prefixes are not allowed in GPRS. The O-flag may be set though, since it does not result in additional addresses being acquired (see below).

   The Prefix sent in the Router Advertisements shall be identical to the Prefix returned in the Create PDP Context Response. The Prefix is contained in the Prefix Information Option of the Router Advertisements and shall have the A-flag set ("Autonomous address configuration flag") and the L-flag cleared (i.e. the prefix should not be used for on-link determination). The lifetime of the prefix shall be set to infinity. In practice, the lifetime of a Prefix will be the lifetime of its PDP Context. There shall be exactly one Prefix included in the Router Advertisements.

   The handling of Router Advertisements shall be consistent with what is specified in RFC 2461 [44]. For the MS-GGSN link however, some specific handling shall apply. The randomisation part to determine when Router Advertisements shall be sent may be omitted since the GGSN is the only router on the link. Furthermore, some 3GPP specific protocol constants and default values shall apply (see subclause "IPv6 Router Configuration Variables in the GGSN"). These relate to the periodicity of the Router Advertisements initially and during continued operation. The motivation for this is to have a faster user-plane set-up even in bad radio conditions and to minimize MS power consumption during long continued operation.

3) When creating a Global or Site-Local Unicast Address, the MS may use the Interface-Identifier received during the PDP Context Activation phase or it may generate a new Interface-Identifier. There is no restriction on the value of the Interface-Identifier of the Global or Site-Local Unicast Address, since the Prefix is unique. Interface-Identifiers shall in any case be 64-bit long.

   Since the GGSN guarantees that the Prefix is unique, the MS does not need to perform any Duplicate Address Detection on addresses it creates. That is, the 'DupAddrDetectTransmits' variable in the MS should have a value of zero. If the MS finds more than one Prefix in the Router Advertisement message, it shall only consider the first one and silently discard the others. The GGSN shall not generate any globally unique IPv6 addresses for itself using the Prefix assigned to the MS in the Router Advertisement.

If the O-flag ("Other stateful configuration flag") was set in the Router Advertisement, the MS may start a DHCP session to retrieve additional configuration parameters. See subclause 13.2.2 "Other configuration by the Intranet or ISP". If the MS is not DHCP capable, the O-flag may be ignored.

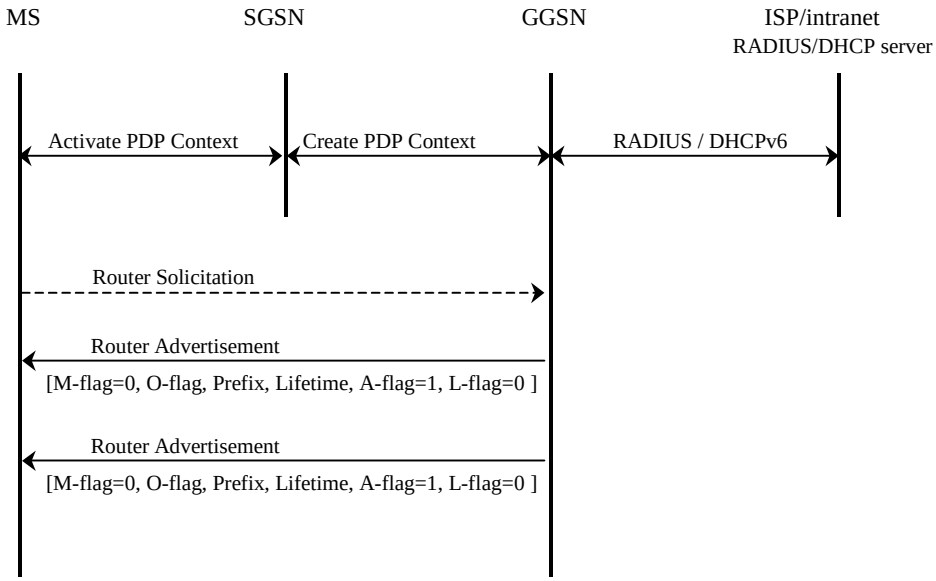


Figure 11bb: IPv6 Stateless Address Autoconfiguration

11.2.1.3.3 IPv6 Stateful Address Autoconfiguration

For IPv6 the PDP Context Activation phase is followed by an address autoconfiguration phase. For APNs configured to use Stateful Address Autoconfiguration, the procedure may for example look like below. A more detailed description of Stateful Address Autoconfiguration is described in clause "Interworking with PDN (DHCP)". Support of DHCP is not mandatory in the MS.

1) After the first phase of setting up IPv6 access to an Intranet or ISP, the MS shall use the IPv6 Interface Identifier, as provided by the GGSN, to create its IPv6 Link-Local Unicast Address according to RFC 2373 [28].

2) After the GGSN has sent a Create PDP Context Response message to the SGSN, it shall start sending Router Advertisements periodically on the new MS-GGSN link established by the PDP Context. The MS may issue a Router Solicitation directly after the user plane establishment. This shall trigger the GGSN to send a Router Advertisement immediately. This shall be consistent with what is specified in RFC 2461 [44]. For the MS-GGSN link however, some 3GPP specific protocol constants and default values shall apply (see subclause "IPv6 Router Configuration Variables in the GGSN").

   To indicate to the MS that Stateful Address Autoconfiguration shall be performed, the Router Advertisements shall not contain any Prefix-Information option and the M-flag ("Managed Address Configuration Flag") shall be set.

3) When the MS has received a Router Advertisement with the M-flag set, it shall start a DHCPv6 configuration as described in subclause "Address allocation using DHCPv6" including a request for an IPv6 address.

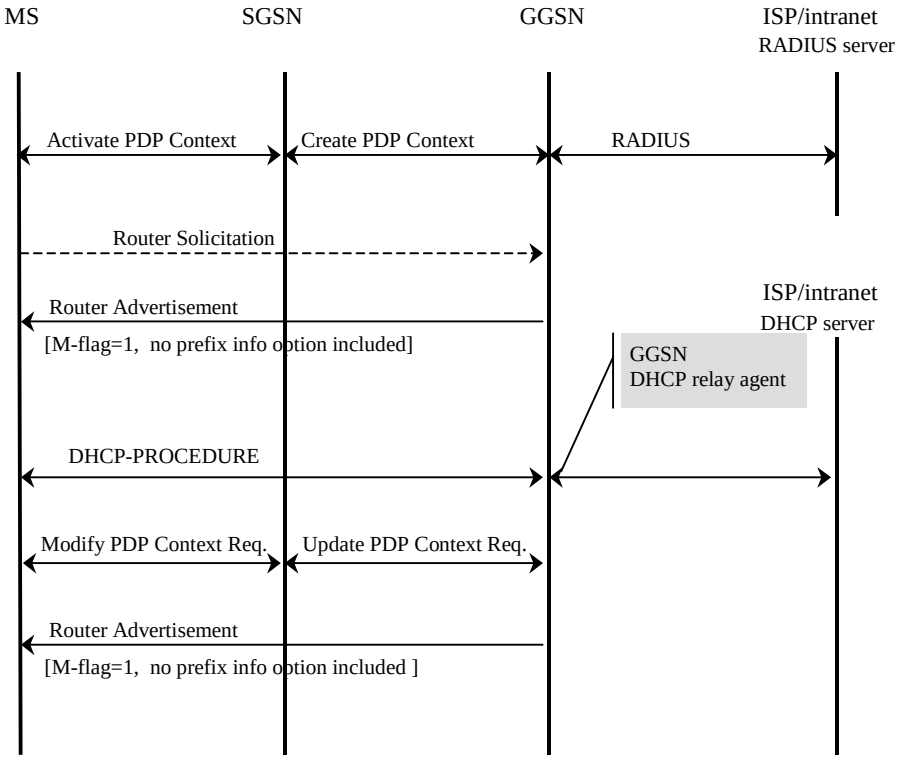


Figure 11bc: IPv6 Stateful Address Autoconfiguration

11.2.1.3.4 IPv6 Router Configuration Variables in the GGSN

For IPv6 Stateless and Stateful Address Autoconfiguration to work properly the GGSN shall behave as an IPv6 router towards the MS. In this respect the GGSN shall be consistent with the RFCs specifying this process (for example RFC 2462 [29] and RFC 2461 [44]), unless stated otherwise in this or other 3GPP specifications.

RFC 2461 [44] specifies a set of conceptual router configuration variables. Some of these variables require particular attention in GPRS in order to preserve radio resources and MS power consumption while still allowing for appropriate robustness and fast user-plane set-up time even in bad radio conditions, or simply because they have a particular meaning in GPRS. These particular variables are listed below with appropriate (default) values and shall be configurable per APN. The values specified hereafter are specific to GPRS and supersede those specified in ~~RFC~~ RFC 2461 [44].

MaxRtrAdvInterval

Shall have a default value of 21 600 s~~econds~~ (6 h).

MinRtrAdvInterval

Shall have a default value of 0.75 ×~~*~~ MaxRtrAdvInterval i.e.16 200 s~~econds~~ (4.5 h).

AdvValidLifetime

Shall have a value giving Prefixes infinite lifetime, i.e. 0xFFFFFFFF. The assigned prefix remains Preferred until PDP Context Deactivation.

AdvPreferredLifetime

Shall have a value giving Prefixes infinite lifetime, i.e. 0xFFFFFFFF. The assigned prefix remains Preferred until PDP Context Deactivation.

RFC 2461 [44] also specifies a number of protocol constants. The following shall have specific values for GPRS:

MAX_INITIAL_RTR_ADVERT_INTERVAL

This constant may be a variable within GPRS. It may have a value that gradually increases (exponentially or by some other means) with the number of initial Router Advertisements sent. This will enable a fast set-up of the MS-GGSN link in most cases, while still allowing the MS to receive a Router Advertisement within the initial phase, even in case of bad radio conditions or slow response time, without having to send a large number of initial Router Advertisements.

MAX_INITIAL_RTR_ADVERTISEMENTS

This is the number of Router Advertisements sent during the initial phase after the MS-GGSN link has been established. The value of this constant shall be chosen carefully, and in conjunction with MAX_INITIAL_RTR_ADVERT_INTERVAL, so as to not overload the radio interface while still allowing the MS to complete its configuration in a reasonable delay. For instance, the default value could be chosen so that initial Router Advertisements are sent for at least 30 s~~econds~~.

After the initial phase, the periodicity is controlled by the MaxRtrAdvInterval and the MinRtrAdvInterval constants.

11.2.1.4 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 RFC 2002 [30]. Mobile IP (MIP) is a mobility management protocol developed by IETF. The Mobile IP Foreign Agent (FA) RFC 2002 [30] is located in the Core Network in the GGSN. MIP also uses a Home Agent (HA) RFC 2002 [30] which may or may not be located in a PLMN 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 RFC 2002 [30] are sent with UDP.

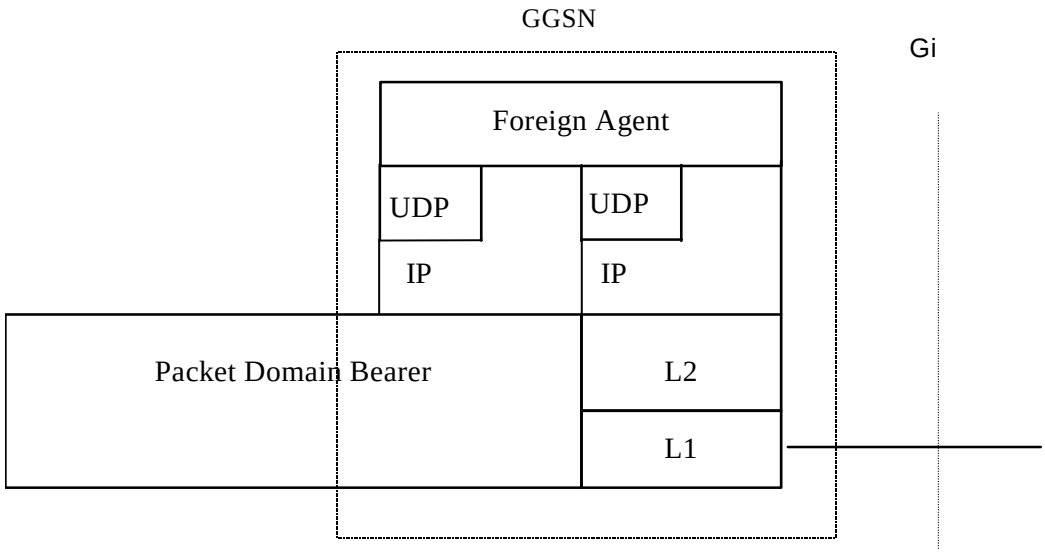


Figure 11c: The protocol stacks for the Gi IP reference point in the MIP signalling plane

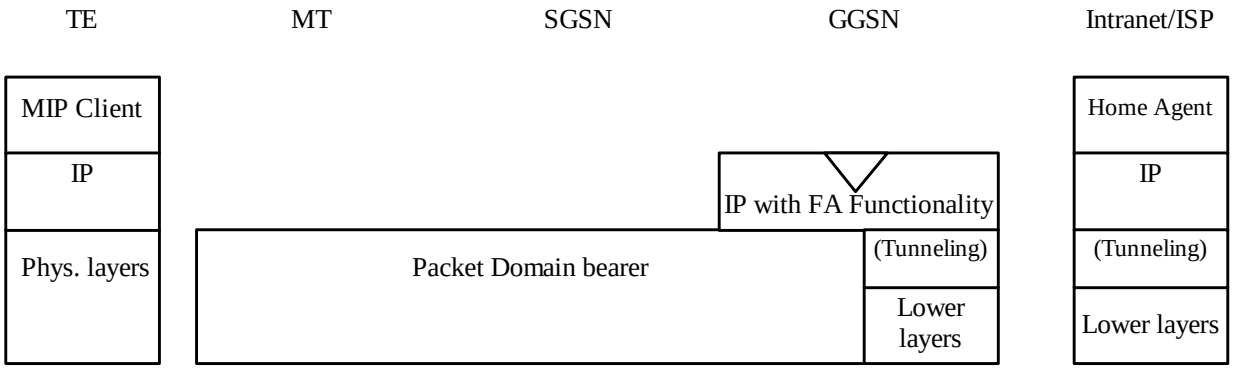


Figure 11d: Protocol stacks for user access with MIP

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 RFC 2794 [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. In this example the MS is separated into a TE and MT, with AT commands and PPP used in-between (see 3GPP TS 27.060 [10]). The PS attach procedures have been omitted for clarity.

IPv4 - Registration UMTS/GPRS + MIP , FA care-of address

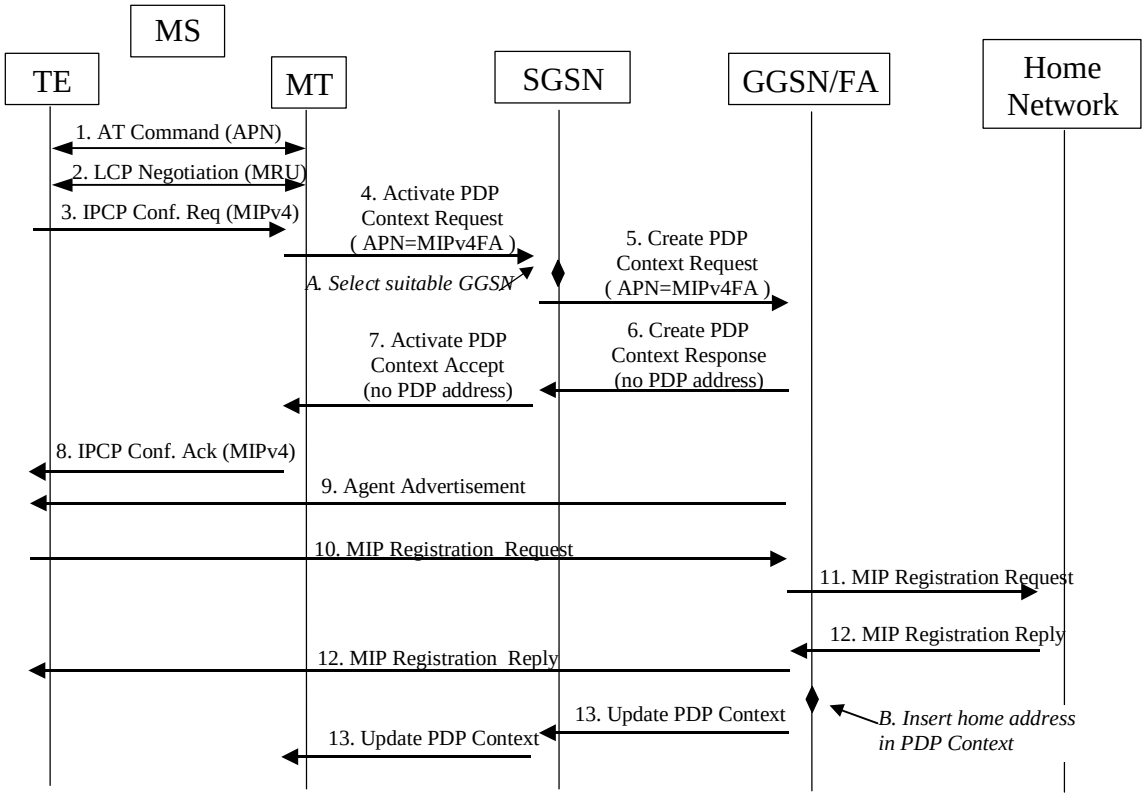


Figure 11e: Example of PDP Context activation with Mobile IP registration -(the PS attach procedure not included)

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 RFC 2290 [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 RFC 2794 [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 RFC 2002 [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 RFC 2002 [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 RFC 2794 [25] and~~,~~ RFC 2486 [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 case of IPv6, a global IPv6 prefix can be obtained from the same sources.

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

1. the GPRS operator manages internally the subnetwork addresses or IPv6 prefixes. Each private network is assigned a unique subnetwork address or IPv6 prefixes. 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 or IPv6 prefixes, is unique.

~~Note~~NOTE:~~-~~ In IPv6 ~~"~~"site-local addresses~~"~~" replace ~~"~~"private addresses~~"~~" in IPv4, see RFC 2373 [28]. Site-local addresses may be used when a site (e.g. a corporate network) requires local administration of its address space.

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

- The PLMN operator allocates a static IP (IPv4 or IPv6) 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 (IPv4 or IPv6) address or IPv6 prefix as described in 3GPP TS 23.060 [3].

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 [19] and RFC 1035 [58].~~)~~

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 (IPv4) and/or MLD (IPv6) and one or more Inter-Router Multicast protocols, such as DVMRP, MOSPF, or PIM-SM.

IGMP/MLD is an integral part of IP. All hosts wishing to receive IP multicasts are required to implement IGMP (or equivalent) and class-D IPv4 addresses or MLD and IPv6 multicast according to RFC 2710 [48]. IGMP/MLD 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/MLD 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 or MLD Report 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 f~~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.

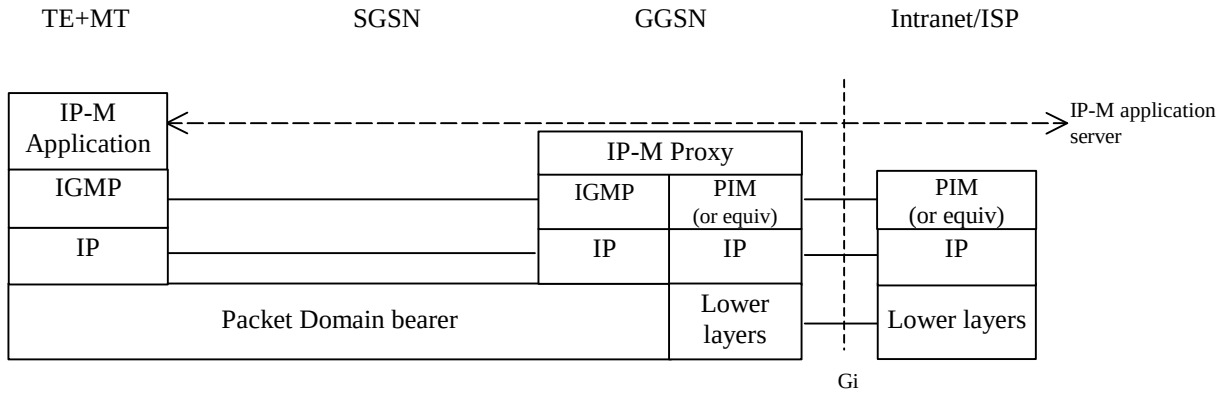


Figure 12: Protocol configuration for IP-Multicast handling (control plane)

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 RFC 1661 [21a] and RFC 1662 [21b]. 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.

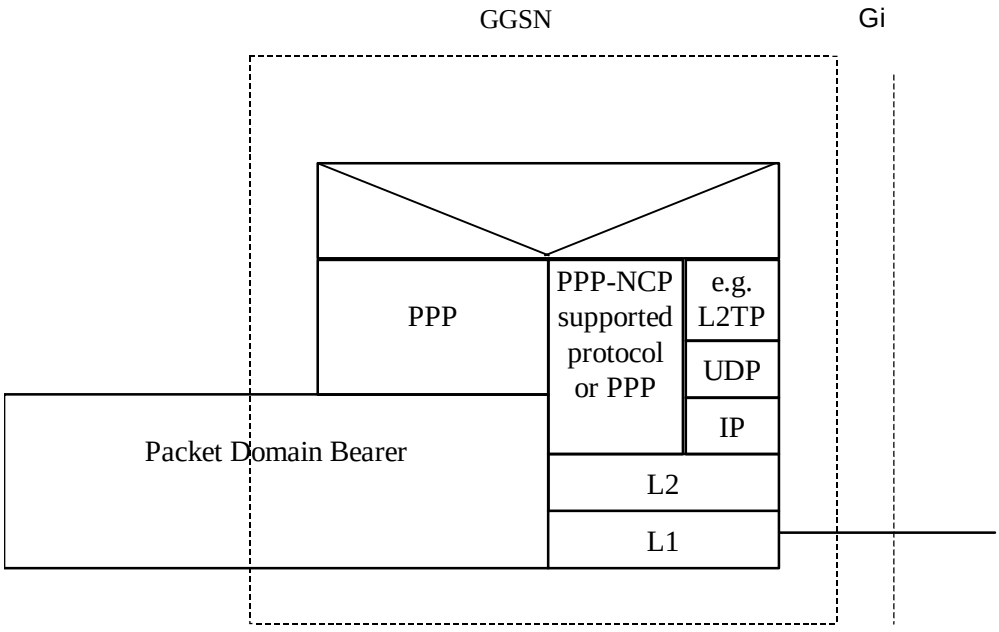


Figure 13: The protocol stacks for the Gi PPP reference point

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);

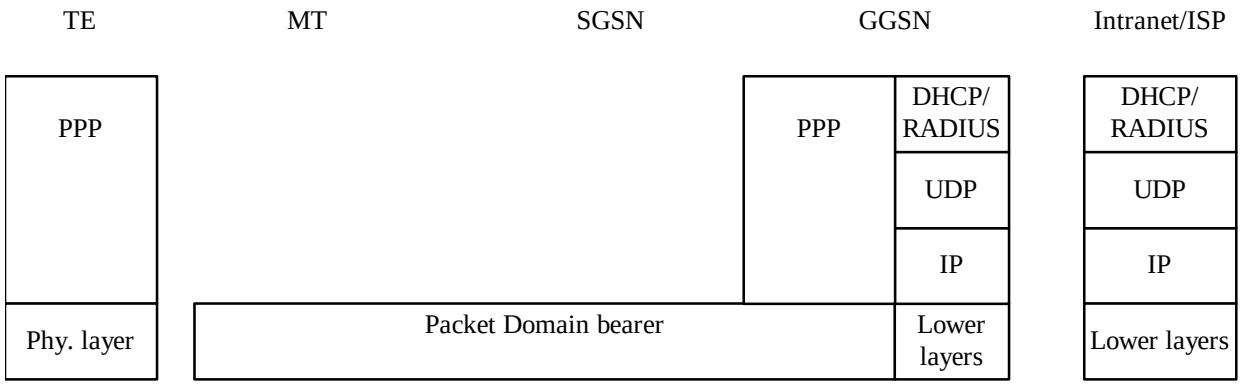


Figure 14: Protocol stack for direct access to IP-based Intranets/ISPs

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

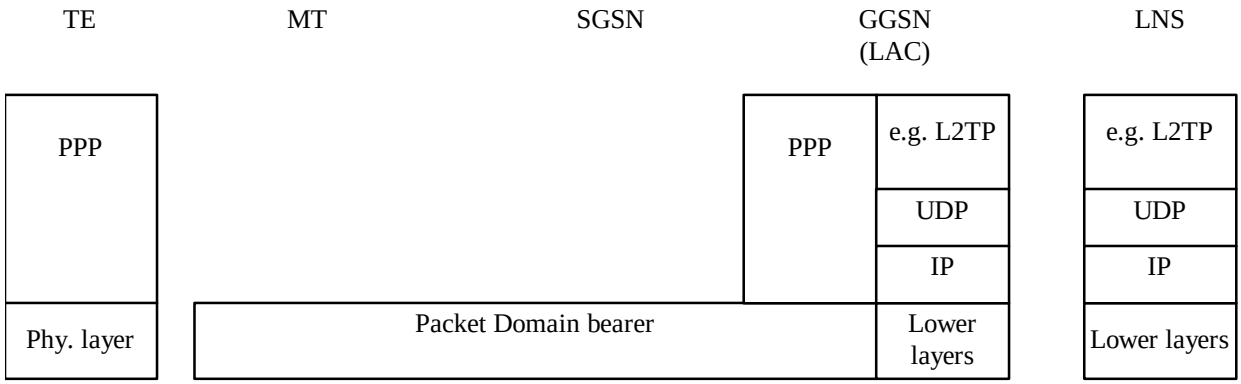


Figure 15: Protocol stack for virtual dial-up access with PPP frame tunnelling

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 AAA, 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 AAA 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 AAA 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 NCP 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.

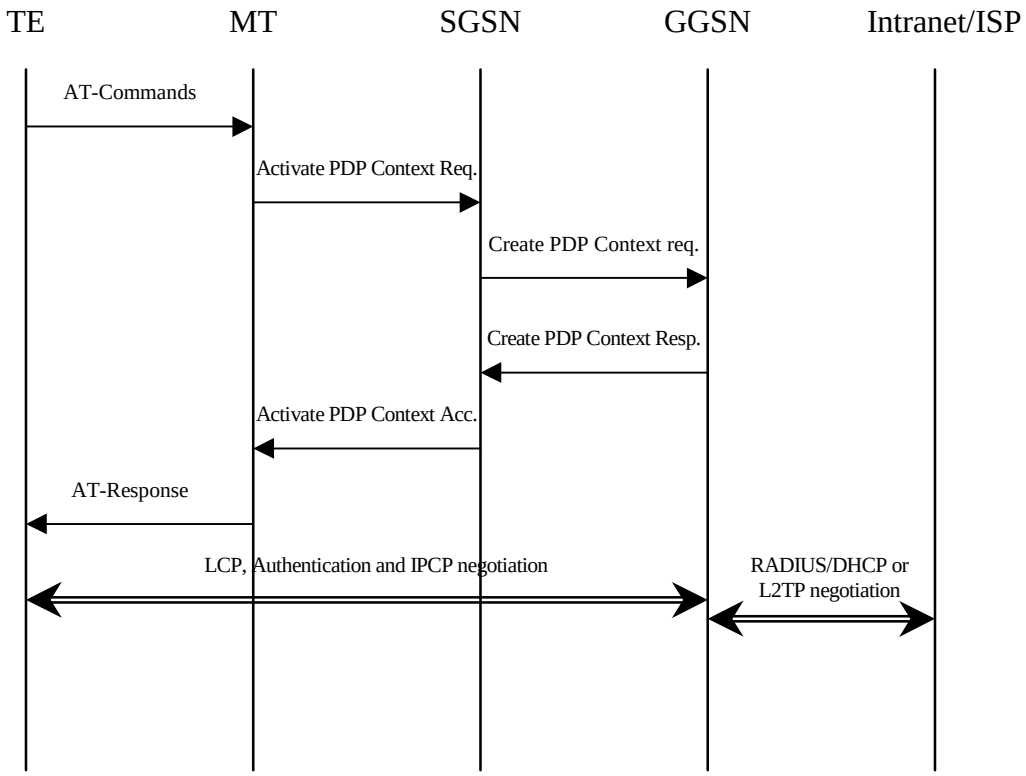

TE
MT
SGSN
GGSN
Intranet/ISP
AT-Commands
Activate PDP Context Req.
Create PDP Context req.
Create PDP Context Resp.
Activate PDP Context Acc.
AT-Response
LCP, Authentication and IPCP negotiation
RADIUS/DHCP or
L2TP negotiation

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, RFC 2131 [26]) and DHCPv6 when the DHCPv6 IETF Internet-Draft [46] ~~it~~ becomes an RFC standard ~~[46]~~. 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 present document.

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 RFC 1661 [21a] and RFC 1662 [21b] 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.

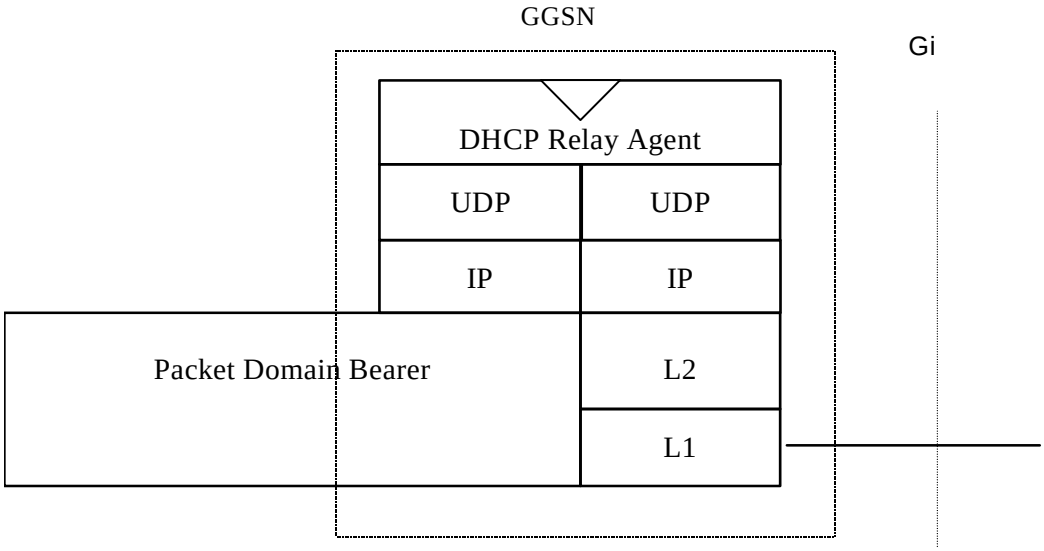


Figure 16b: The protocol stacks for the Gi IP reference point for DHCP

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 3GPP 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 (see RFC 3118 [45]).

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

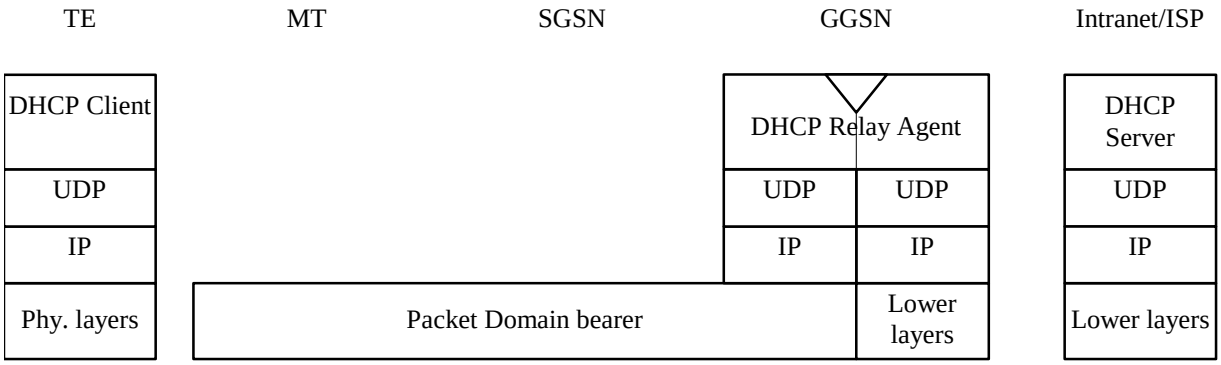


Figure 16c: Protocol stack for access with DHCP end-to-end

13.2.1.1 Address allocation using DHCPv4

The following description bullet items describe the DHCPv4 signal flow. For a detailed description of the DHCP messages refer to RFC 2131 [26] and RFC 1542, [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 3GPP 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.

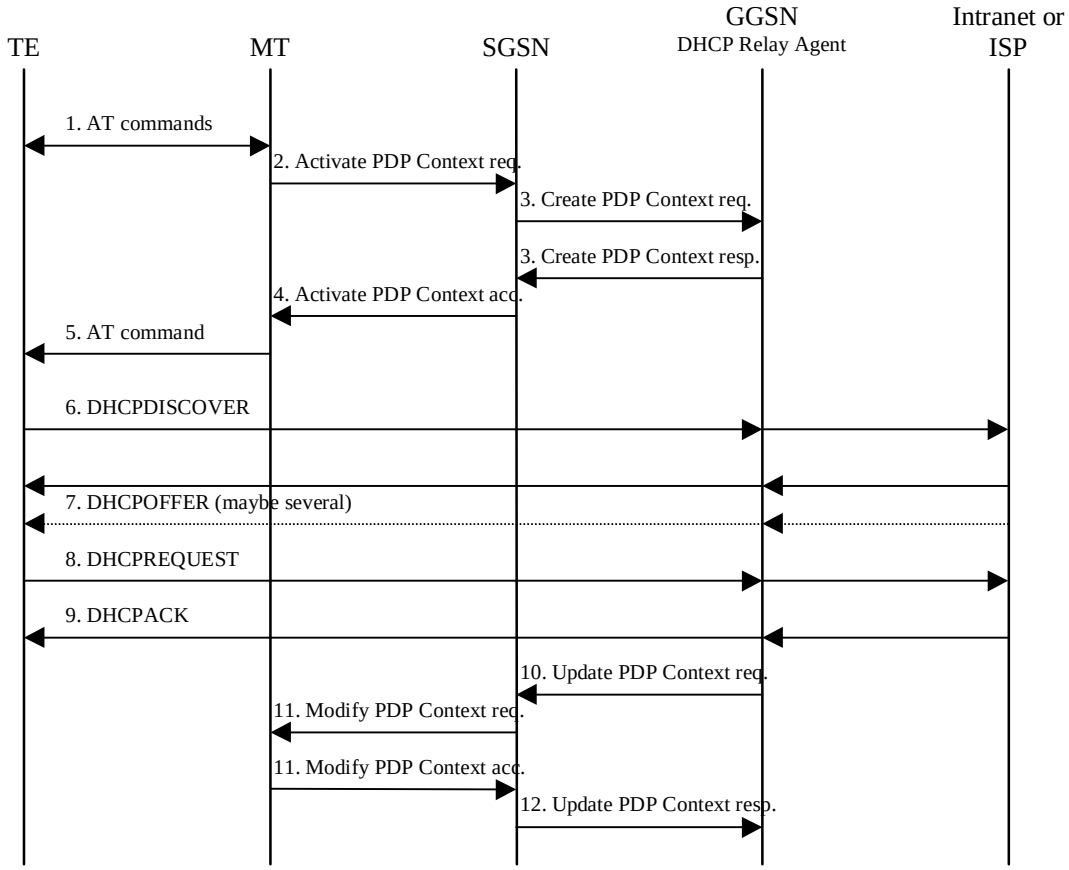


Figure16d: DHCPv4 signal flow

13.2.1.2 Address allocation using DHCPv6

The following description bullet items describe the signal flow. For a detailed description of the DHCPv6 messages refer to the DHCPv6 IETF Internet-Draft [46]. In the context of IPv6, address allocation through DHCP is also referred to as Stateful Address Autoconfiguration. The end-to-end protocol configuration is depicted in figure 16e.

The PDP Context activation part and the initial Router Advertisement that triggers the MS to do the Stateful Address Autoconfiguration is described in subclause "IPv6 Non Transparent access to an Intranet or ISP".

~~1)~~1) The TE sends a SOLICIT message with the IP destination address set to the All_DHCP_Relay_Agents_and_Servers multicast address defined in the DHCPv6 IETF Internet-Draft~~DHCPv6~~ [46]. The source address is the link local address created by the MS. The SOLICIT message shall contain one IA option.

~~2)~~2) The GGSN creates a RELAY-FORWARD message. The "Client-Message" option shall include the entire SOLICIT message. The GGSN sends the message to the DHCP server(s) configured for the APN using unicast addresses or All_DHCP_Servers multicast address. More details on the parameters for the RELAY-FORWARD are found in the DHCPv6 IETF Internet-Draft [46]. The GGSN may store a PDP Context ID in the Interface-Id option if this aids it in handling the Relay-Reply (the DHCP server will echo the Interface-Id option).

~~3)~~3) DHCP servers receiving the RELAY-FORWARD message including the SOLICIT request reply by sending a RELAY-REPLY message. The "Server-Message" option includes the ADVERTISE message with an offered IP address.

~~4)~~4) GGSN extracts the ADVERTISE messages and forwards the messages to the proper MS.

~~5)~~5) The TE chooses one of the possibly several ADVERTISE messages and sends a REQUEST confirming its choice and requesting additional configuration information.

~~6)~~6) GGSN embeds the REQUEST in the ~~"~~"Client-Message~~"~~" option of~~ ~~the RELAY-FORWARD and sends it as explained in step 2.

~~7)~~7) The selected DHCP server receives the RELAY-FORWARD and replies with a RELAY-REPLY. The ~~"~~"Server~~ ~~Message~~"~~" option includes the REPLY message containing the configuration information requested by the TE.

~~8)~~8) The GGSN extracts the REPLY message and forwards it to the proper MS. GGSN also extracts IA option information such as the allocated MS IPv6 address and its lifetime and stores it in the corresponding PDP context. The GGSN shall silently discard any Neighbour Solicitation message sent by the MS to perform Duplicate Address Detection (see 3GPP TS 23.060 [3]).

~~9)~~9) The GGSN 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 IPv6 address.

~~10)~~10) The SGSN sends a Modify PDP Context Request to the MT with the allocated IPv6 address in the PDP Address information element.

~~11)~~11) The MT acknowledges by sending a Modify PDP Context Accept to the SGSN.

~~12)~~12) The SGSN sends an Update PDP Context Response to the GGSN. The PDP context has been successfully updated with the allocated IPv6 address.

~~13)~~13) In the Stateful Address Autoconfiguration, Router Advertisements sent by GGSN on the MS-GGSN link shall not contain any Prefix Information option, even when GGSN has knowledge of the Prefix of the MS through the DHCP relay agent. The Prefix need not be advertised since the MS is the only host on the link and Stateless Address Autoconfiguration shall not be performed concurrently to Stateful Address Autoconfiguration.

EXAMPLE: In the following example a successful PDP context activation with use of DHCPv6 from end to end is shown.

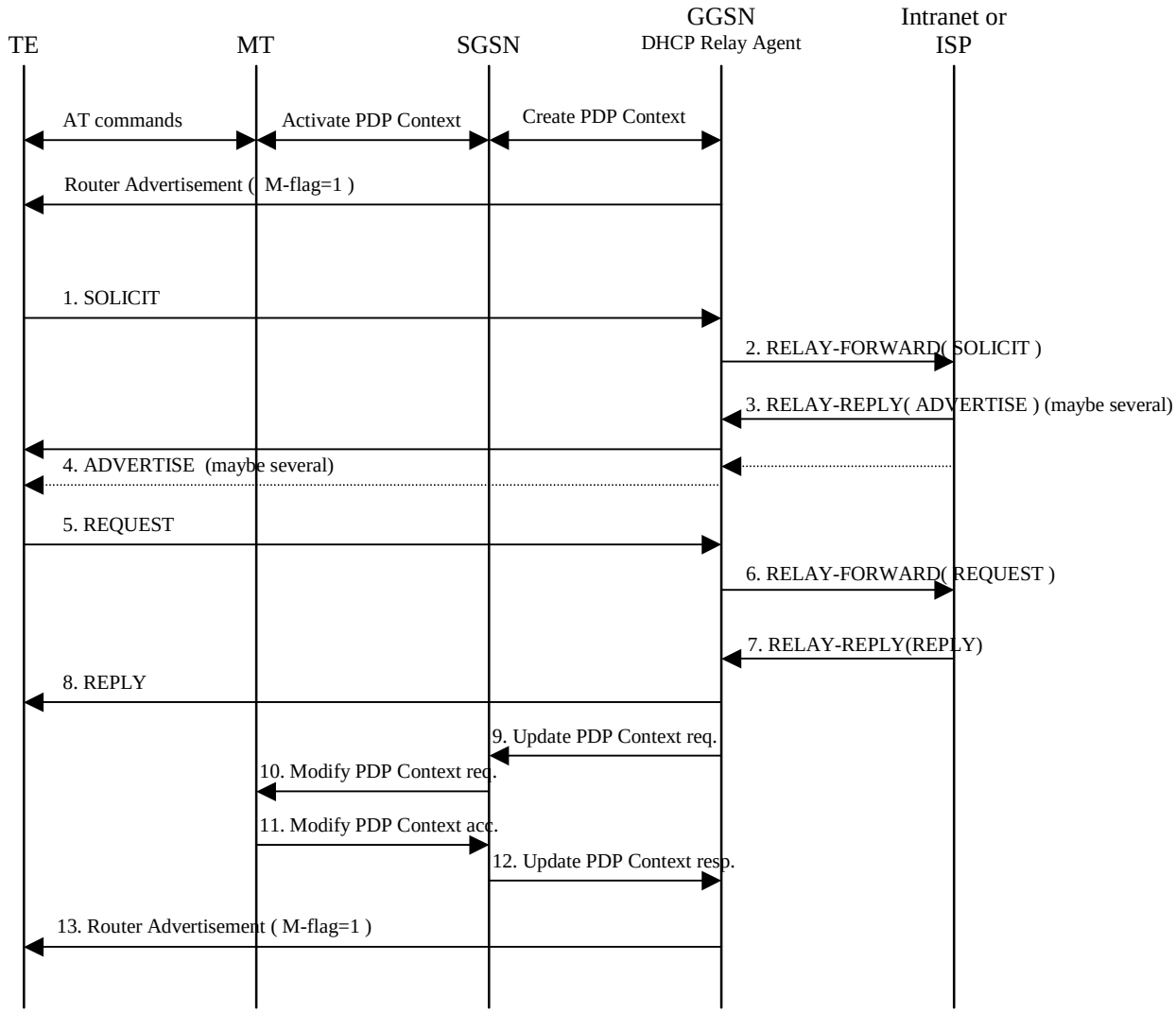


Figure 16e: DHCPv6 signal flow

13.2.2 Other configuration by the Intranet or ISP (IPv6 only)

When using IPv6, in some situations the MS may need additional configuration information from the Intranet or ISP besides the IP address. It may for example be IMS related configuration options (see 3GPP TS 24.229 [47]). If the MS is DHCP capable and the IPv6 address has been allocated using Stateless Address Autoconfiguration, the MS may use a procedure as in the example below to configure additional external network protocol parameters, or other parameters that apply to the Intranet or ISP. The GGSN shall in this case indicate to the MS that there is additional configuration information to retrieve by setting the O-flag in the Router Advertisements. This shall be configured per APN in the GGSN.

The following description bullet items describe an example of a signal flow, where the MS directs an Information-Request to the All_DHCP_Relay_Agents_and_Servers multicast address. The MS may also direct the message to a specific server instead of all servers. For a detailed description of the DHCPv6 messages refer to the DHCPv6 IETF Internet-Draft [46]. The sequence is depicted in figure 16f.

1) A Router Advertisement with the O-flag set, is sent from GGSN to TE to indicate to it to retrieve other configuration information.

2) The TE sends an INFORMATION-REQUEST message with the IP destination address set to the All_DHCP_Relay_Agents_and_Servers multicast address defined in the DHCPv6 IETF Internet-Draft DHCPv6 [46]. The source address shall be the link-local address of the MS. The DHCP relay agent in the GGSN shall forward the message.

3)3) DHCP servers receiving the forwarded INFORMATION-REQUEST message, reply by sending a RELAY-REPLY message, with the "server-message" option including a REPLY message with the requested configuration parameters.

- The TE chooses one of the possibly several REPLY messages and extracts the configuration information.

EXAMPLE: In the following example a request for information with use of DHCPv6 from end to end is shown.

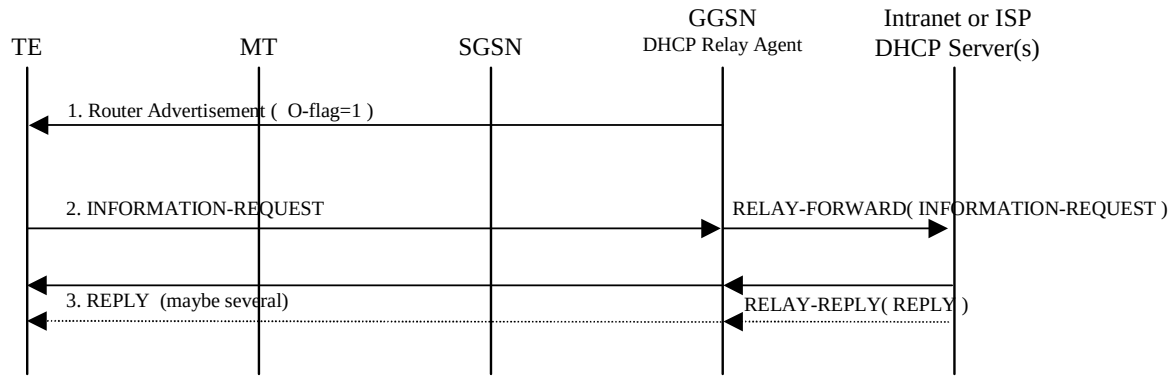


Figure 16f: DHCPv6 Other configuration signal flow

13a Interworking with IMS

13a.1 General

Interworking with the IP Multimedia Core Network Subsystem (IMS) puts additional requirements on the GGSN. When the MS connects to the IP Multimedia Core Network Subsystem (IMS), specific parameters in Session Management messages may be handled. The IMS specific parameters are: IMS signalling flag, P-CSCF address request, returned P-CSCF address(es), media authorization token(s) and flow identifier(s).

For interworking with the IMS, the Go interface (see 3GPP TS 29.207 [53]) is used to correlate the session (SIP/SDP) and the bearer (PDP Contexts).

The mechanisms in GGSN to support IMS shall be:

- P-CSCF discovery.
- Dedicated signalling PDP contexts; with associated static packet filters to permit signalling to/from designated servers.
- Go interface for charging correlation and policy control of PDP contexts for IMS media flows.

These mechanisms are however not restricted to the IMS and could be used for other services that could benefit from these mechanisms.

13a.2 IMS Interworking Model

The signalling interface between MS and P-CSCF is a logical interface, i.e. it is using GPRS as a bearer. The Go interface is used for network communication between the GGSN and the PCF. For a description of the IMS architecture, refer to 3GPP TS 23.228 [52]. For a more detailed view of GGSN IMS interworking, see 3GPP TS 29.207 [53].

13a.2.1 IMS Specific Configuration in the GGSN

The GGSN shall have a list of preconfigured addresses of signalling servers (P-CSCF servers). This list shall be provided to MSs on request. The list shall be possible to preconfigure per APN.

The GGSN shall have preconfigured static packet filters, to be applied on dedicated signalling PDP contexts. The static packet filters shall filter up-link and down-link packets and only allow traffic to/from the preconfigured signalling servers and to DNS and DHCP servers. The static packet filters shall be possible to pre-configure per APN.

It shall be possible to enable/disable the use of the Go interface per APN. The GGSN shall handle Create PDP Context Requests that include binding information as specified in 3GPP TS 29.207 [53].

The GGSN shall support IPv6 addresses and protocol for IMS signalling and IMS bearers.

The GGSN shall provide support for P-CSCF discovery in two different ways (see 3GPP TS 23.228 [52]):

- GPRS procedure for P-CSCF discovery, i.e. request and provision of P-CSCF address(es) within the PCO IE in GPRS Session Management procedures (see 3GPP TS 24.008 [54]).

- Via DHCPv6 servers i.e. the GGSN shall provide the functionality of a DHCPv6 relay agent

On APNs providing IMS services, the information advertised in Router Advertisements from GGSN to MSs shall be configured in the same manner as for other APNs prviding IPv6 services (see subclause 11.2.1.3.4), except that the "O-flag" shall be set even when the "M-flag" is cleared.

NOTE: When the "M-flag" is cleared, the "O- flag" shall be set in IPv6 Router Advertisement messages sent by the GGSN for APNs used for IMS services. This will trigger a DHCP capable MS to start a DHCPv6 session to retrieve server addresses and other configuration parameters. An MS which doesn't support DHCP will simply ignore the "O-flag". An MS may simultaneously use stateless address autoconfiguration for configuring its IPv6 address and stateful autoconfiguration for configuring IMS specific parameters. An MS which doesn't support DHCP, shall request IMS specific configuration (e.g. P-CSCF address) in the PCO IE in the Create PDP Context message.

The GGSN shall support a DHCPv6 relay agent.

13a.2.2 IMS Specific Procedures in the GGSN

13a.2.2.1 Request for Signalling Server Address

When an MS indicates a request for a P-CSCF address in the PCO IE in a Create PDP Context Request message, the GGSN shall respond with one or more P-CSCF server addresses if available for this APN. If the GGSN has no P-CSCF address available, the GGSN shall ignore the request. If the GGSN provides more than one P-CSCF IPv6 address in the response, the GGSN shall sort the addresses with the highest priority P-CSCF server first in the PCO IE. The GGSN may use different prioritisations for different MSes, e.g. for load sharing between the P-CSCF servers. The coding of the PCO IE is described in the 3GPP TS 24.008 [54]. This procedure shall be followed regardless of whether or not the MS uses a dedicated signalling PDP context, and irrespective of the Go status for the APN.

13a.2.2.2 Establishment of a PDP Context Dedicated for Signalling

The GGSN shall allow IMS signalling on a "general-purpose PDP context", in which case the IMS signalling shall be provided like any other transparent services provided by the packet domain.

The GGSN may (dependent on operator policy) also support dedicated signalling PDP Contexts for IMS services. An MS may request a dedicated signalling PDP context (see 3GPP TS 24.229 [5547]). The operator may provide special properties to dedicated signalling PDP contexts, e.g special charging and enhanced QoS. It is out of the current scope of this TS to further specify these properties.

For a PDP Context marked as a dedicated signalling PDP Context, the GGSN shall apply static packet filters, which shall only allow packets to be sent to and from a pre-configured set of signalling servers, such as P-CSCF(s), DHCP server(s) and DNS server(s). The static packet filters for down-link signalling traffic shall have the format of a TFT and be sorted so that they precede both the SBLP based filters and the UE specified TFT filters. This will secure the use of the correct PDP context for the signalling traffic, and that only authorized traffic uses the signalling PDP context. The

static packet filters shall be pre-configured in the GGSN by the operator. For dedicated signalling PDP Contexts, any TFT specified by the MS shall be replaced by the GGSN pre-configured static packet filters.

13a.2.2.3 Creation of a PDP Context for IMS Media Flows

For PDP Contexts used to carry IMS media flows, specific policies may be applied. The policy includes packet filtering, which enables a specific charging for these PDP Contexts, see 3GPP TS 29.207 [53].

The creation of a PDP Context to be used to carry media flows involves interaction between the MS and the GGSN and between the GGSN and the P-CSCF/PCF. The interaction between the GGSN and the P-CSCF/PCF, i.e. the Go interface, is described in detail in 3GPP TS 29.207 [53]. The interaction between the MS and GGSN is described in 3GPP TS 29.208 [56].

If binding information (media authorization token and flow identifiers) is included in a Create PDP Context Request message, the GGSN shall use the Go interface to authorize the request and retrieve a policy for filtering. If the Go interface is not enabled for the APN, the request may be rejected based on operator policy.

The GGSN identifies the PCF to interact with using a PCF identifier. The PCF identifier is part of the media authorization token in the binding information, and is a fully qualified domain name (see 3GPP TS 29.207 [53]). Inclusion of both binding information and an indication for a dedicated signalling PDP Context in the same Create PDP Context Request message is not permitted. If both are received together, the GGSN shall reject the PDP context request.

14 Internet Hosted Octet Stream Service (IHOSS)

~~Void.~~**Figure 17: Void**

Figure 18: Void

Figure 19: Void

Figure 20: Void

15 Interworking between Packet Domains

The primary reason for the interworking between Packet Domains is to support roaming subscribers as described in 3GPP TS 23.060 [3]. The general model for Packet Domain interworking is shown in figure 21.

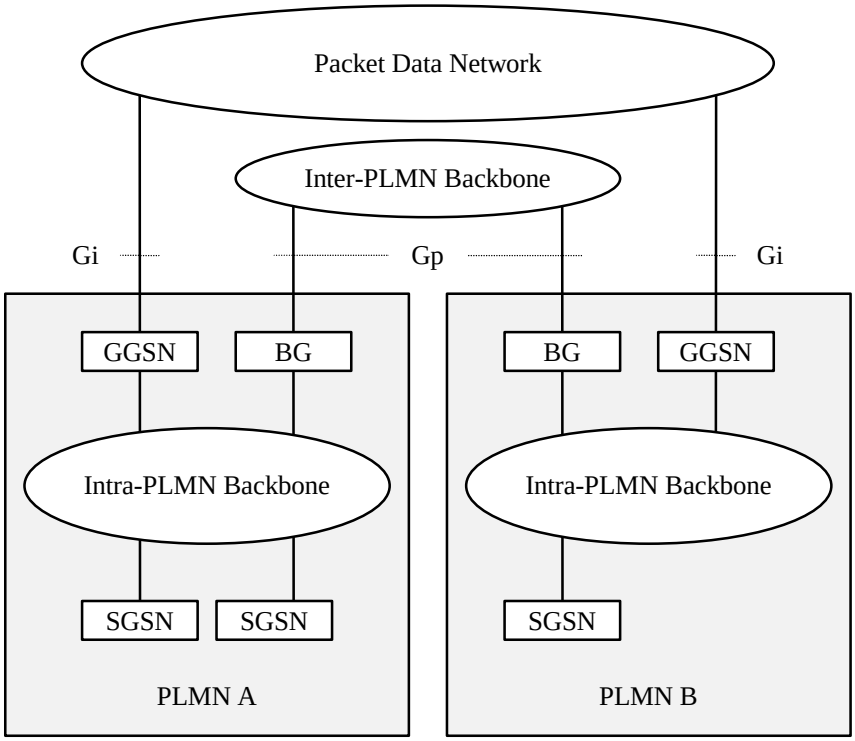


Figure 21: General interworking between Packet Domains to support roaming subscribers.

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 [3].

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 [3].

The inter-PLMN link may be any packet data network or dedicated link as described in 3GPP TS 23.060 [3]. 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 [61]) and accompanying specifications for authentication (RFC 1826 [62]) and encryption (RFC 1827 [63]) 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 [60]) 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.

16 Usage of RADIUS on Gi interface

A GGSN may, on a per APN basis, use RADIUS authentication to authenticate a user and RADIUS accounting to provide information to an AAA (Authentication, Authorization and Accounting) server.

16.1 RADIUS Authentication

RADIUS Authentication shall be used according to RFC 2865 [38] and RFC 3162 [50].

The RADIUS client function may reside in a GGSN. When the GGSN receives a Create PDP Context request message the RADIUS client function may send the authentication information to an authentication server, which is identified during the APN provisioning.

The authentication server checks that the user can be accepted. The response (when positive) may contain network information, such as an IP address or IPv6 prefix for the user.

The information delivered during the RADIUS authentication can be used to automatically correlate the users identity (the MSISDN or IMSI) to the IP-address or IPv6 prefix, assigned/confirmed by the GGSN or the authentication server respectively. The same procedure applies, in case of sending the authentication to a 'proxy' authentication server.

RADIUS Authentication is only applicable to the primary PDP context. When the GGSN receives an Access-Accept message from the authentication server it shall complete the PDP context activation procedure. If Access-Reject or no response is received, the GGSN shall reject the PDP Context Activation attempt with a suitable cause code, e.g. User Authentication failed.

16.2 RADIUS Accounting

RADIUS Accounting shall be used according to RFC 2866 [39] and RFC 3162 [50].

The RADIUS accounting client function may reside in a GGSN. The RADIUS accounting client may send information to an accounting server, which is identified during the APN provisioning. The accounting server may store this information and use it to automatically identify the user. This information can be trusted because the GPRS network has authenticated the subscriber (i.e. SIM card and possibly other authentication methods).

RADIUS Accounting-Request Start and Stop messages may be used during both primary and secondary PDP context activation and deactivation procedures respectively.

The use of Accounting-Request STOP and in addition the Accounting ON and Accounting OFF messages may be used to ensure that information stored in the accounting server is synchronised with the GGSN information.

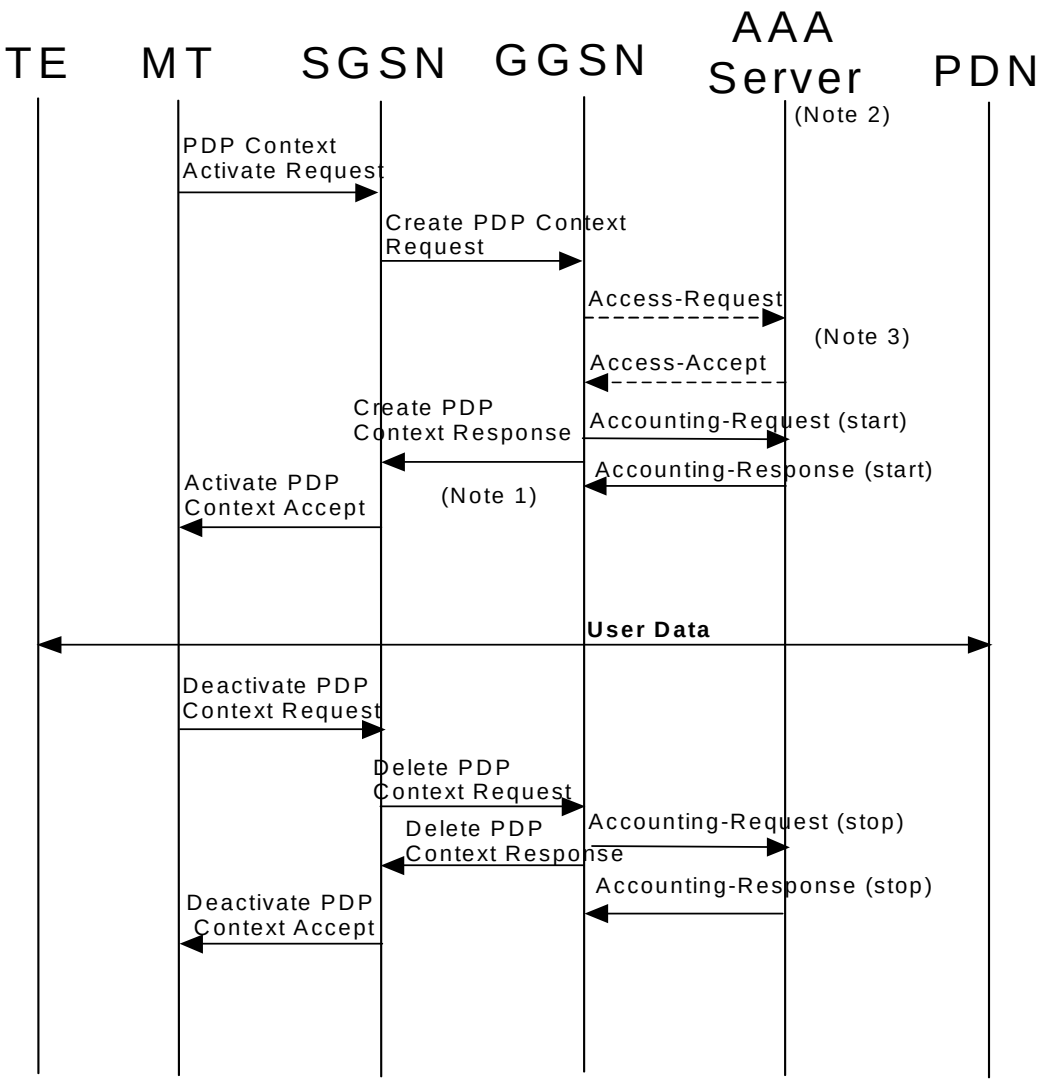
If the AAA server is used for IP address or IPv6 prefix assignment, then, upon reception of a RADIUS Accounting-Request STOP message for all PDP contexts associated to a session defined by APN and IMSI or MSISDN, the AAA server may make the associated IP address or IPv6 prefix available for assignment.

In order to avoid race conditions, the GGSN shall include a 3GPP Vendor-Specific sub-attribute "Session Stop indicator" when it sends the Accounting-Request STOP for the last PDP context of a PDP session and the PDP session is terminated~~.~~ (i.e. the IP address or IPv6 prefix and all GTP tunnels can be released). The AAA server shall not assume the PDP session terminated until an Accounting-Request STOP with the Session Stop indicator is received.

16.3 Authentication and accounting message flows

16.3.1 IP PDP type

~~The f~~Figure 22 represents the RADIUS message flows between a GGSN and an Authentication, Authorization and Accounting (AAA) server.



NOTE 1: If some external applications require RADIUS Accounting request (Start) information before they can process user packets, then the selected APN (GGSN) may be configured in such a way that the GGSN drops user data until the Accounting Response (START) is received from the AAA server. The GGSN may wait for the Accounting Response (START) before sending the CreatePDPContextResponse. The GGSN may reject the PDP context if the Accounting Response (START) is not received.
NOTE 2: Separate accounting and authentication servers may be used.
NOTE 3: The Access-Request message shall be used for primary PDP context only.
NOTE 4: The Accounting-Request (Start) message may be sent at a later stage, e.g. after IPv6 address has been assigned and PDP Context updated, in case of a stateful address autoconfiguration.

Figure 22: RADIUS message flow for PDP type IP (successful user authentication case)

When a GGSN receives a Create PDP Context Request message for a given APN, the GGSN may (depending on the configuration for this APN) send a RADIUS Access-Request to an AAA server. The AAA server authenticates and authorizes the user. If RADIUS is also responsible for IP address or IPv6 prefix allocation the AAA server shall return the allocated IP address or IPv6 prefix in the Access-Accept message.

Even if the GGSN was not involved in user authentication (e.g. transparent network access mode), it may send a RADIUS Accounting-Request START message to an AAA server. This message contains parameters, e.g. the tuple which includes the user-id and IP address or IPv6 prefix, to be used by application servers (e.g. WAP gateway) in order to identify the user. This message also indicates to the AAA server that the user session has started.

If some external applications require RADIUS Accounting request (Start) information before they can process user packets, then the selected APN (GGSN) may be configured in such a way that the GGSN drops user data until the Accounting Response (START) is received from the AAA server. The GGSN may wait for the Accounting Response (START) before sending the CreatePDPContextResponse. The GGSN may reject the PDP context if the Accounting Response (START) is not received. The authentication and accounting servers may be separately configured for each APN.

At a stateful address autoconfiguration, no IP address or IPv6 prefix is available at PDP context activation. In that case the GGSN may wait to send the Accounting-Request START message until the TE receives its IP address in a DHCP-REPLY.

When the GGSN receives a Delete PDP Context Request message and providing a RADIUS Accounting-Request START message was sent previously, the GGSN shall send a RADIUS Accounting-Request STOP message to the AAA server, which indicates the termination of this particular user session. The GGSN shall immediately send a Delete PDP context response, without waiting for an Accounting-Response STOP message from the AAA server.

The AAA server shall deallocate the IP address or IPv6 prefix (if any) initially allocated to the subscriber, if there is no session for the subscriber.

Accounting-Request ON and Accounting-Request OFF messages may be sent from the GGSN to the AAA server to ensure the correct synchronization of the session information in the GGSN and the AAA server.

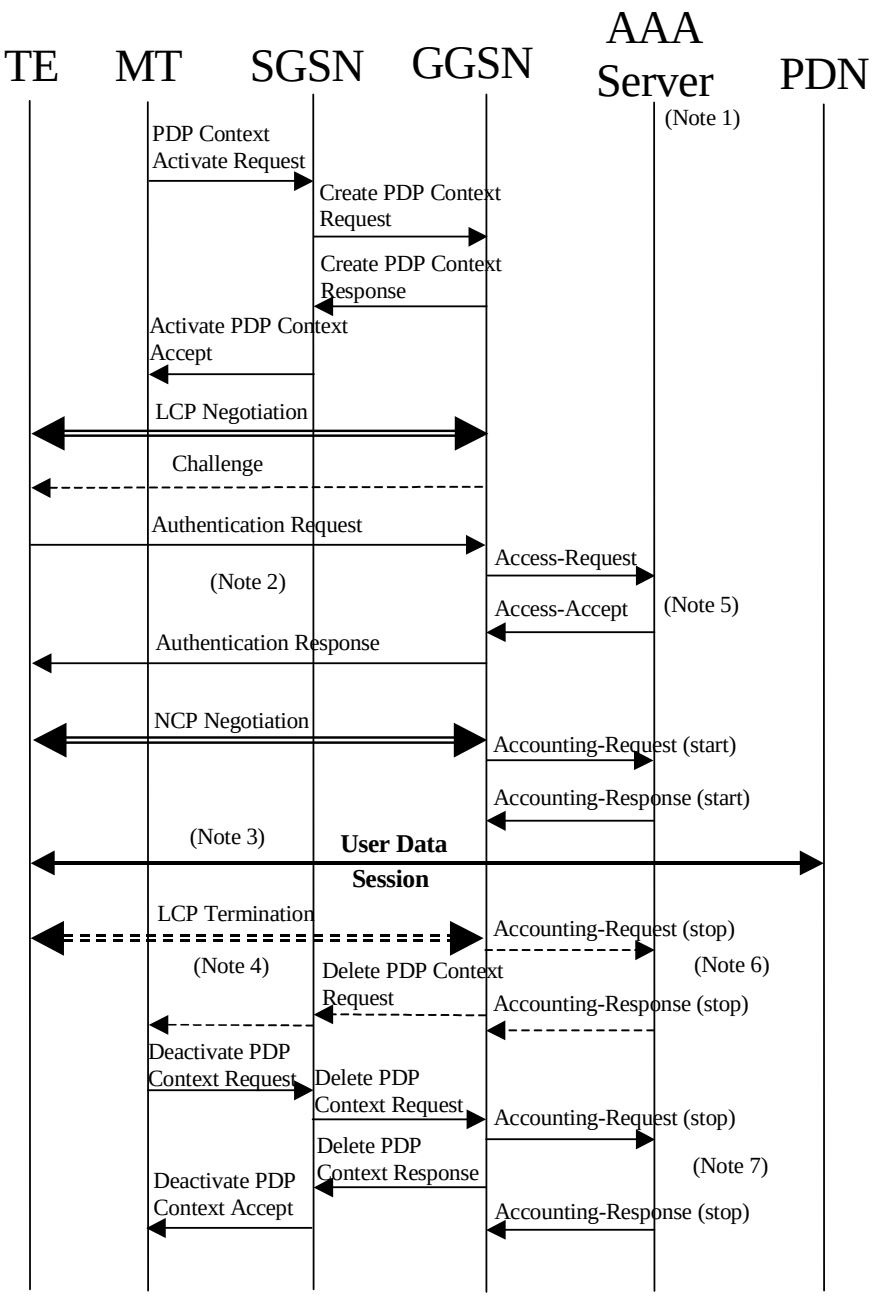
The GGSN may send an Accounting-Request ON message to the AAA server to indicate that a restart has occurred. The AAA server may then release the associated resources.

Prior to a scheduled restart, the GGSN may send Accounting-Request OFF message to the AAA server. The AAA server may then release the associated resources.

If an Access-Challenge is sent to the GGSN when an Access-Request message is pending and when IP PDP type is used, the GGSN shall silently discard the Access-Challenge message and it shall treat an Access-Challenge as though it had received an Access-Reject instead RFC 2865 [38].

16.3.2 PPP PDP type

~~The f~~Figure 23 describes the RADIUS message flows between a GGSN and an Authentication, Authorization and Accounting (AAA) server for the case where PPP is terminated at the GGSN. The case where PPP is relayed to an LNS is beyond the scope of ~~this specification~~the present document.



NOTE 1: Separate accounting and Authentication servers may be used.
NOTE 2: Actual messages depend on the used authentication protocol (e.g. PAP, CHAP).
NOTE 3: If some external applications require RADIUS Accounting request (Start) information before they can process user packets, then the selected APN (GGSN) may be configured in such a way that the GGSN drops user data until the Accounting Response (START) is received from the AAA server. The GGSN may delete the PDP context if the Accounting Response (START) is not received.
NOTE 4: An LCP termination procedure may be performed. Either the MS or the GGSN may initiate the context deactivation.
NOTE 5: The Access-Request message shall be used for primary PDP context only.
NOTE 6: Network Initiated deactivation.
NOTE 7: User Initiated deactivation.

Figure 23: RADIUS message flow for PDP type PPP (successful user authentication case)

When a GGSN receives a Create PDP Context Request message for a given APN, the GGSN shall immediately send a Create PDP context response back to the SGSN. After PPP link setup, the authentication phase may take place. During Authentication phase, the GGSN sends a RADIUS Access-Request to an AAA server. The AAA server authenticates

and authorizes the user. If RADIUS is also responsible for IP address allocation the AAA server shall return the allocated IP address or IPv6 prefix in the Access-Accept message (if the user was authenticated).

If the user is not authenticated, the GGSN shall send a Delete PDP context request to the SGSN.

Even if the GGSN was not involved in user authentication (e.g. for PPP no authentication may be selected), it may send a RADIUS Accounting-Request– START message to an AAA server. This message contains parameters, e.g. a tuple which includes the user-id and IP address or IPv6 prefix, to be used by application servers (e.g. WAP gateway) in order to identify the user. This message also indicates to the AAA server that the user session has started, and the QoS parameters associated to the session.

If some external applications require RADIUS Accounting request (Start) information before they can process user packets, then the selected APN (GGSN) may be configured in such a way that the GGSN drops user data until the Accounting Response (START) is received from the AAA server. The GGSN may delete the PDP context if the Accounting Response (START) is not received. The Authentication and Accounting servers may be separately configured for each APN.

When the GGSN receives a Delete PDP Context Request message and providing a RADIUS Accounting-Request START message was sent previously, the GGSN shall send a RADIUS Accounting-Request STOP message to the AAA server, which indicates the termination of this particular user session. The GGSN shall immediately send a Delete PDP context response, without waiting for an Accounting-Response STOP message from the AAA server.

The AAA server shall deallocate the IP address or IPv6 prefix (if any) initially allocated to the subscriber.

Accounting-Request ON and Accounting-Request OFF messages may be sent from the GGSN to the AAA server to ensure the correct synchronization of the session information in the GGSN and the AAA server.

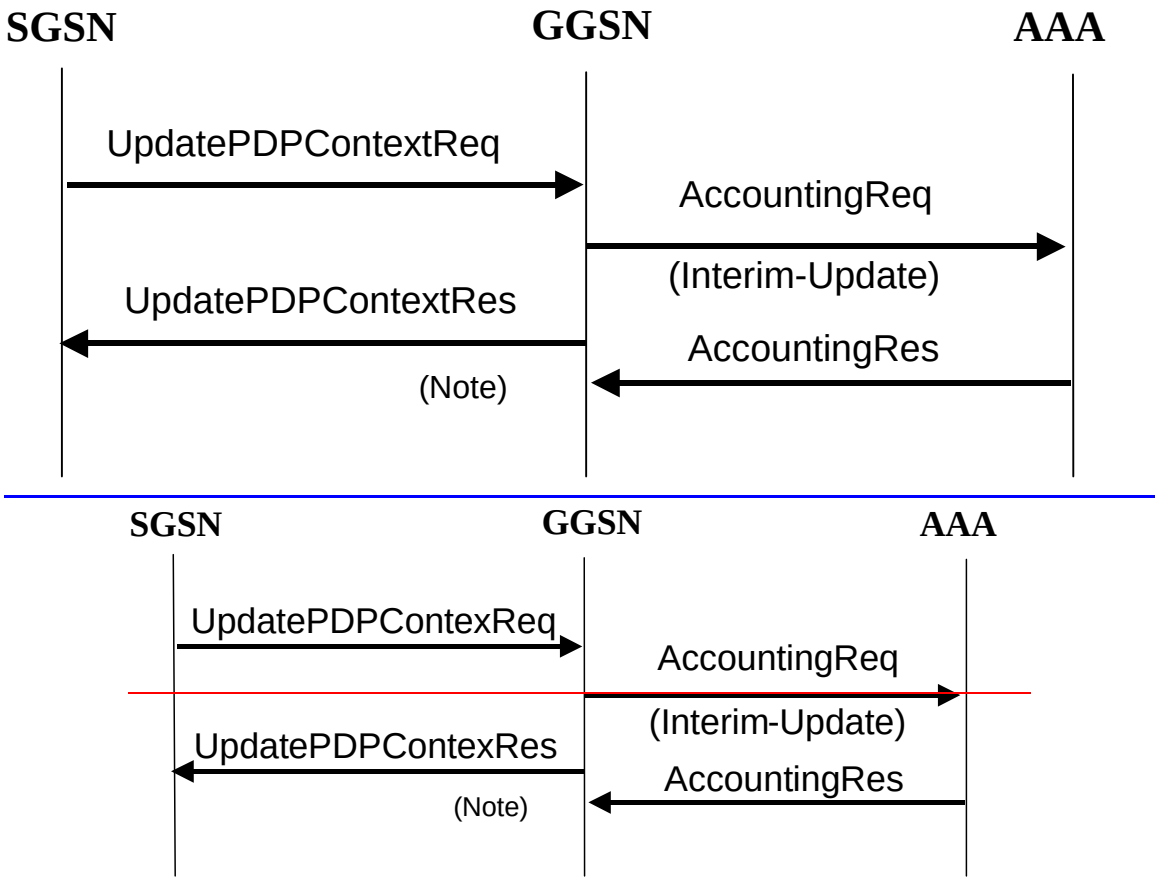
The GGSN may send an Accounting-Request ON message to the AAA server to indicate that a restart has occurred. The AAA server may then release the associated resources.

Prior to a scheduled restart, the GGSN may send Accounting-Request OFF message to the AAA server, the AAA server may then release the associated resources.

If an Access-Challenge is sent to the GGSN when using PPP PDP type, the GGSN shall handle it by PPP CHAP providing PPP CHAP was the selected Authentication protocol. If CHAP authentication was not selected, authentication shall fail RFC 2865 [38].

16.3.3 Accounting Update

During the life of a PDP context some information related to this PDP context may change (i.e. SGSN address if a Inter-SGSN RA update occurs). Upon reception of an UpdatePDPContextRequest from the SGSN, the GGSN may send an Accounting Request Interim-Update to the AAA server to update the necessary information related to this PDP context (~~S~~see ~~F~~figure 24). In such a case, the GGSN need not wait for the RADIUS AccountingResponse from the AAA server message before sending the UpdatePDPContextResponse to the SGSN. The GGSN may delete the PDP context if the AccountingResponse is not received from the AAA.

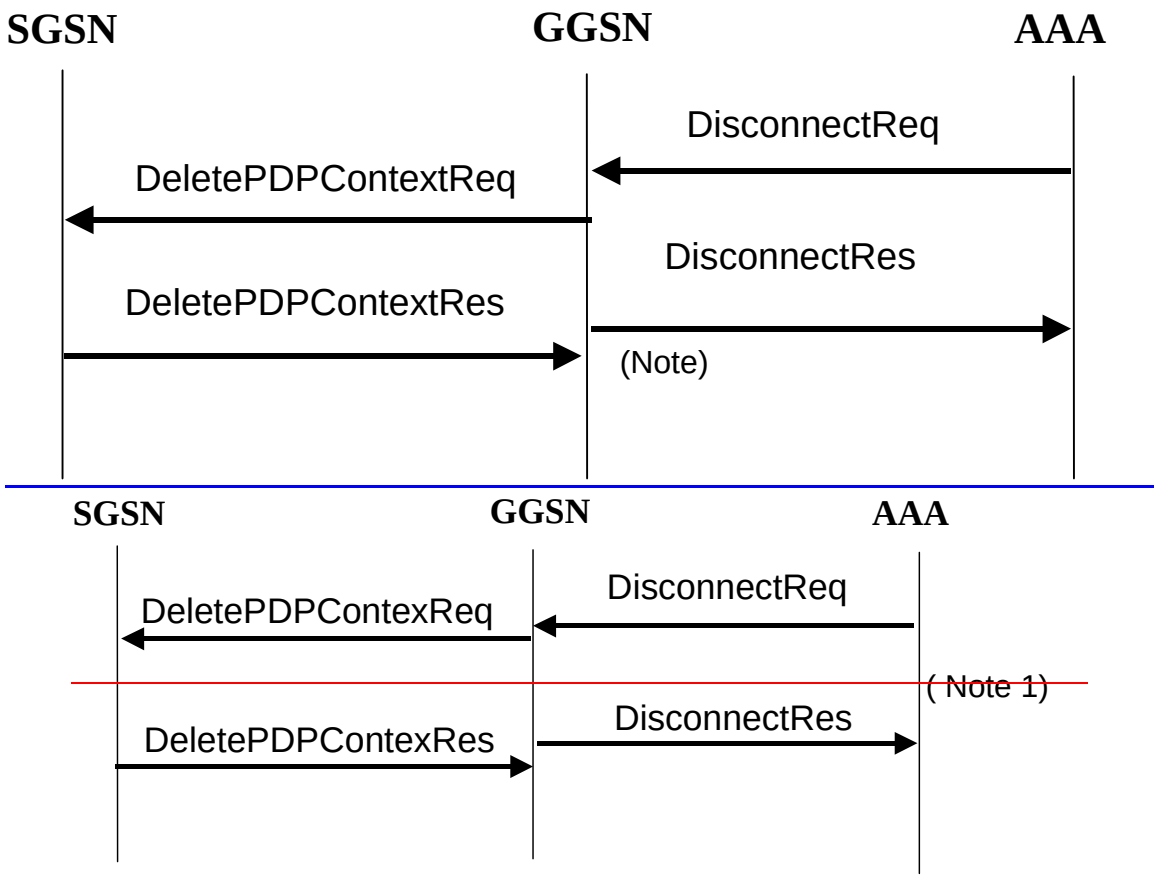


N~~ote 1~~OTE:- As shown the GGSN need not wait for the RADIUS AccountingResponse from the AAA server message to send the UpdatePDPContextResponse to the SGSN. The GGSN may delete the PDP context if the AccountingResponse is not received from the AAA.

Figure 24: RADIUS for PDP context Update

16.3.4 AAA-Initiated PDP context termination

RADIUS is used as the protocol between the GGSN and a AAA server or proxy for applications (e.g. MMS) to deliver information related to GPRS user session. However some IP applications could need to interwork with the GGSN to terminate a particular PDP context. For this purpose, the AAA server or proxy may send a RADIUS Disconnect Request to the GGSN. As depicted in ~~Figure~~ figure 25, the GGSN may react by deleting the corresponding PDP context or silently discard the Disconnect Request message. For more information on RADIUS Disconnect, see RFC 2882 [41]. If the GGSN deletes the corresponding PDP context, it need not wait for the DeletePDPContextResponse from the SGSN before sending the RADIUS DisconnectResponse to the AAA server.



Note 1OTE: As showed on fiFigure 25, the GGSN need not wait for the DeletePDPContextResponse from the SGSN to send the RADIUS DisconnectResponse to the AAA server.

Figure 25: PDP Context deletion with RADIUS

16.4 List of RADIUS attributes

The following tables describe the actual content of the RADIUS messages exchanged between the GGSN and the AAA server. Other RADIUS attributes may be used as defined in RADIUS RFC(s). Unless otherwise stated, when the encoding scheme of an attribute is specified as UTF-8 encoding, this shall be interpreted as UTF-8 hexadecimal encoding.

16.4.1 Access-Request message (sent from the GGSN to AAA server)

The table 1 describes the attributes of the Access-Request message.

Table 1: The attributes of the Access-Request message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username is provided by the user (extracted from the Protocol Configuration Options (PCO) field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used). If no username is available a generic username, configurable on a per APN basis, shall be present.	String	Mandatory
2	User-Password	User password provided by the user if PAP is used (extracted from the PCO field of the Create PDP Context Request message) or PPP	String	Conditional Note 1

Attr #	Attribute Name	Description	Content	Presence Requirement
		authentication phase (if PPP PDP type is used). If no password is available a generic password, configurable on a per APN basis, shall be present.		
3	CHAP-Password	User password provided by the user if CHAP is used (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used).	String	Conditional Note 2
4	NAS-IP-Address	IP address of the GGSN for communication with the AAA server.	IPv4	Conditional Note 45
95	NAS-IPv6-Address	IP address of the GGSN for communication with the AAA server.	IPv6	Conditional Note 3 and, 54
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 3
6	Service-Type	Indicates the type of service for this user	Framed	Optional
7	Framed-Protocol	Indicates the type of protocol for this user	7 (GPRS PDP Context)	Optional
8	Framed-IP-Address	IP address allocated for this user	IPv4	Conditional Note 45
9	Framed-IP-Netmask	Netmask for the user IP address	IPv4	Conditional Note 45
97	Framed-IPv6-Prefix	IPv6 address prefix allocated for this user	IPv6	Conditional Note 45
96	Framed-Interface-Id	User IPv6 Interface Identifier	IPv6	Conditional Notes 5, 64 and 5
30	Called-Station-Id	Identifier for the target network	APN (UTF-8 encoded)	Mandatory
31	Calling-Station-Id	This attribute is the identifier for the MS, and it shall be configurable on a per APN basis.	MSISDN in international format according to 3GPP TS 23.003 [40], UTF-8 encoded decimal. Note that there are no leading characters in front of the country code. (Note 6)	Optional
60	CHAP-Challenge	Challenge if CHAP is used (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used).	String	Conditional Note 2
61	NAS-Port-Type	Port type for the GGSN	As per RFC 2865 [38]	Optional
26/10415	3GPP Vendor-Specific	Sub-attributes according sub-clausesubclause 16.4.7	See sub-clausesubclause 16.4.7	Optional except sub-attribute 3 which is conditional

NOTE 1: Shall be present if PAP is used.
NOTE 2: Shall be present if CHAP is used.
NOTE 3: Either NAS-IP-Address or NAS-Identifier shall be present.
NOTE 54: Either IPv4 or IPv6 address/prefix attribute shall be present. The IP protocol version for end-user and network may be different.
NOTE 56: Included if the prefix alone is not unique for the user. This may be the case, for example, if address is assigned using stateful address autoconfiguration or if a static IPv6 address.
NOTE 6: There are no leading characters in front of the country code.

16.4.2 Access-Accept (sent from AAA server to GGSN)

T~~he t~~able 2 describes the attributes of the Access-Accept message. See RFC 2548 [51] for definition of MS specific attributes.

Table 2: The attributes of the Access-Accept message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username received in the Access-Request message or a substitute username provided by the AAA server. If the User-Name has been received in the Access-Accept message, this user-name shall be used in preference to the above	String	Optional
6	Service-Type	Indicates the type of service for this user	Framed	Optional
7	Framed-Protocol	Indicates the type of protocol for this user	7 (GPRS PDP Context)	Optional
8	Framed-IP-Address	IP address allocated for this user, if the AAA server is used to allocate IP address.	IPv4	Conditional Note 2~~5~~
9	Framed-IP-Netmask	Netmask for the user IP address, if the AAA server is used to allocate IP netmask.	IPv4	Conditional Note 2~~5~~
97	Framed-IPv6-Prefix	IPv6 address prefix allocated for this user, if the AAA server is used to allocate IP address prefixes.	IPv6	Conditional Note 2~~5~~
100	Framed-IPv6-Pool	Name of the prefix pool for the specific APN	IPv6	Optional Note 2~~5~~
12	Framed-IP-MTU	MTU for the user towards this particular APN, MTU shall be less or equal to 1500	String	Optional
25	Class	Identifier to be used in all subsequent accounting messages.	String	Optional (N~~OTE 4~~ote 1)
27	Session-Timeout	Indicates the timeout value (in seconds) for the user session	32 bit unsigned Integer	Optional
28	Idle-Timeout	Indicates the timeout value (in seconds) for idle user session	32 bit unsigned Integer	Optional
26/311	MS- primary-DNS-server	Contains the primary DNS server address for this APN	Ipv4	Optional Note 3~~7~~
26/311	MS-Secondary-DNS-Server	Contains the secondary DNS server address for this APN	IPv4	Optional Note 3~~7~~
26/311	MS-Primary-NBNS-Server	Contains the primary NetBios name server address for this APN	IPv4	Optional Note 3~~7~~
26/311	MS-Secondary-NBNS-Server	Contains the secondary NetBios server address for this APN	IPv4	Optional Note 3~~7~~
26/10415/17	3GPP-IPv6-DNS-Servers	List of IPv6 addresses of DNS servers for this APN	IPv6	Optional Note 3~~7~~

NOTE 1~~4~~: The presence of this attribute is conditional upon this attribute being received in the Access-Accept message
NOTE 2~~5~~: ~~-~~Either IPv4 or IPv6 address/prefix attribute shall be present. The IP protocol version for end-user and network may be different.
NOTE 3~~7~~: ~~-~~Either IPv4 or IPv6 address attribute shall be present

16.4.3 Accounting-Request START (sent from GGSN to AAA server)

T~~he t~~able 3 describes the attributes of the Accounting-Request START message.

Table 3: The attributes of the Accounting-Request START message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username provided by the user (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used). If no username is available a generic username, configurable on a per APN basis, shall be present. If the User-Name has been received in the Access-Accept message, this user-name shall be used in preference to the above	String	Optional
4	NAS-IP-Address	GGSN IP address for communication with the AAA server.	IPv4	Conditional Notes 1 and 3~~, 5~~
95	NAS-IPv6-Address	GGSN IPv6 address for communication with the AAA server.	IPv6	Conditional Notes 1 and 3~~, 5~~
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 1~~3~~
6	Service-Type	Indicates the type of service for this user	Framed	Optional
7	Framed Protocol	Indicates the type of protocol for this user	7 (GPRS PDP Context)	Optional
8	Framed-IP-Address	User IP address	IPv4	Conditional Note 3~~5~~
97	Framed-IPv6-Prefix	User IPv6 Prefix	IPv6	Conditional Note 3~~5~~
96	Framed-Interface-Id	User IPv6 Interface Identifier	IPv6	Conditional Notes 3 and 4~~5, 6~~
25	Class	Received in the access accept	String	Conditional (~~NOTE~~ Note 2~~4~~)
30	Called-Station-Id	Identifier for the target network	APN (UTF-8 encoded)	Mandatory
31	Calling-Station-Id	This attribute is the identifier for the MS, and it shall be configurable on a per APN basis.	MSISDN in international format according to 3GPP TS 23.003 [40], UTF-8 encoded decimal. ~~Note that there are no leading characters in front of the country code.~~ (Note 6)	Optional
40	Acct-Status-Type	Type of accounting message	START	Mandatory
41	Acct-Delay-Time	Indicates how many seconds the GGSN has been trying to send this record for, and can be subtracted from the time of arrival on the AAA server to find the approximate time (in seconds) of the event generating this Accounting-Request.	32 unsigned integer	Optional

Attr #	Attribute Name	Description	Content	Presence Requirement
44	Acct-Session-Id	User session identifier.	GGSN IP address (IPv4 or IPv6) and Charging-ID concatenated in a UTF-8 encoded hexadecimal. ~~NOTE: The GGSN IP address is the same as that used in the GCDRs.~~(Note 5)	Mandatory
45	Acct-Authentic	Authentication method	RADIUS or LOCAL	Optional
61	NAS-Port-Type	Port type for the GGSN	As per RFC 2865 [38]	Optional
26/10415	3GPP Vendor-Specific	Sub-attributes according ~~sub-clause~~subclause 16.4.7.	See ~~sub-clause~~subclause 16.4.7	Optional except sub-attribute 3 which is conditional

NOTE ~~3~~1: Either NAS-IP-Address or NAS-Identifier shall be present.
NOTE 2~~4~~: The presence of this attribute is conditional upon this attribute being received in the Access-Accept message
NOTE 3~~5~~: Either IPv4 or IPv6 address/prefix attribute shall be present. The IP protocol version for end-user and network may be different.
NOTE 4~~6~~: Included if the prefix alone is not unique for the user. This may be the case, for example, if address is assigned using stateful address autoconfiguration or if a static IPv6 address.
NOTE 5: The GGSN IP address is the same as that used in the GCDRs.
NOTE 6: There are no leading characters in front of the country code.

16.4.4 Accounting Request STOP (sent from GGSN to AAA server)

T~~he t~~able 4 describes the attributes of the Accounting-Request STOP message.

Table 4: The attributes of the Accounting-Request STOP message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username provided by the user (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used). If no username is available a generic username, configurable on a per APN basis, shall be present. If the User-Name has been received in the Access-Accept message, this user-name shall be used in preference to the above	String	Optional
4	NAS-IP-Address	IP address of the GGSN for communication with the AAA server.	IPv4	Conditional Notes 1 and 3~~,5~~
95	NAS-IPv6-Address	IP address of the GGSN for communication with the AAA server.	IPv6	Conditional Notes 1 and 3~~,~~ ~~5~~
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 1~~3~~
6	Service-Type	Indicates the type of service for this user	Framed	Optional
7	Framed Protocol	Indicates the type of protocol for this user	7 (GPRS PDP Context)	Optional
8	Framed-IP-Address	User IP address	IPv4	Conditional Note 3~~5~~
97	Framed-IPv6-Prefix	User IPv6 Prefix	IPv6	Conditional Note 3~~5~~
96	Framed-Interface-Id	User IPv6 Interface Identifier	IPv6	Conditional Notes 3 and 4~~5, 6~~
25	Class	Received in the access accept	String	Optional (N~~OTE 4~~ote 2)
30	Called-Station-Id	Identifier for the target network	APN (UTF-8 encoded)	Mandatory
31	Calling-Station-Id	This attribute is the identifier for the MS, and it shall be configurable on a per APN basis.	MSISDN in international format according to 3GPP TS 23.003 [40], UTF-8 encoded. (Note 6)~~Note that there are no leading characters in front of the country code.~~	Optional
40	Acct-Status-Type	Indicates the type of accounting request	STOP	Mandatory
41	Acct-Delay-Time	Indicates how many seconds the GGSN has been trying to send this record for, and can be subtracted from the time of arrival on the AAA server to find the approximate time of the event generating this Accounting-Request	Second	Optional
42	Acct-Input-Octets	GGSN counted number of octets sent by the user for the PDP context	32 bit unsigned integer	Optional
43	Acct-Output-Octets	GGSN counted number of octets received by the user for the PDP context	32 bit unsigned integer	Optional
44	Acct-Session-Id	User session identifier.	GGSN IP	Mandatory

Attr #	Attribute Name	Description	Content	Presence Requirement
			address (IPv4 or IPv6) and Charging-ID concatenated in a UTF-8 encoded hexadecimal. ~~NOTE: The GGSN IP address is the same as that used in the GCDRs.~~(Note 5)	
45	Acct-Authentic	Authentication method	RADIUS or LOCAL	Optional
46	Acct-Session-Time	Duration of the session	Second	Optional
47	Acct-Input-Packets	GGSN counted number of packets sent by the user	Packet	Optional
48	Acct-Output-Packets	GGSN counted number of packets received by the user	Packet	Optional
49	Acct-Terminate-Cause	Indicate how the session was terminated	See RFC 2866 [39]	Optional
61	NAS-Port-Type	Port type for the GGSN	As per RFC 2865 [38]	Optional
26/10415	3GPP Vendor-Specific	Sub-attributes according to ~~sub-clause~~subclause 16.4.7.	See ~~sub-clause~~subclause 16.4.7	Optional except sub-attribute 3 which is conditional
NOTE 1~~3~~: Either NAS-IP-Address or NAS-Identifier shall be present. NOTE 2~~4~~: The presence of this attribute is conditional upon this attribute being received in the Access-Accept message NOTE 3~~5~~: Either IPv4 or IPv6 address/prefix attribute shall be present. The IP protocol version for end-user and network may be different. NOTE 4~~6~~: Included if the prefix alone is not unique for the user. This may be the case, for example, if address is assigned using stateful address autoconfiguration or if a static IPv6 address. NOTE 5: The GGSN IP address is the same as that used in the GCDRs. NOTE 6: There are no leading characters in front of the country code.				

16.4.5 Accounting Request ON (optionally sent from GGSN to AAA server)

T~~he t~~able 5 describes the attributes of the Accounting-Request ON message.

Table 5: The attributes of the Accounting-Request ON message

Attr #	Attribute Name	Description	Content	Presence Requirement
4	NAS-IP-Address	IP address of the GGSN for communication with the AAA server.	IPv4	Conditional Notes ~~3, 7~~1 and 2
95	NAS-IPv6-Address	IP address of the GGSN for communication with the AAA server.	IPv6	Conditional Notes ~~3, 7~~1 and 2
30	Called-Station-ID	Identifier for the target network.	APN (UTF-8 encoded)	Optional
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 1~~3~~
NOTE 1~~3~~: Either NAS-IP-Address or NAS-Identifier shall be present. NOTE 2~~7~~: Either IPv4 or IPv6 address attribute shall be present.				

16.4.6 Accounting Request OFF (optionally sent from GGSN to AAA server)

The table 6 describes the attributes of the Accounting-Request OFF message.

Table 6: The attributes of the Accounting-Request OFF message

Attr #	Attribute Name	Description	Content	Presence Requirement
4	NAS-IP-Address	IP address of the GGSN for communication with the AAA server.	IPv4	Conditional Notes 3, 71 and 2
95	NAS-IPv6-Address	IP address of the GGSN for communication with the AAA server.	IPv6	Conditional Notes 13, 7 and 2
30	Called-Station-ID	Identifier for the target network.	APN (UTF-8 encoded)	Optional
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 13
NOTE 13: Either NAS-IP-Address or NAS-Identifier shall be present. NOTE 72: Either IPv4 or IPv6 address attribute shall be present.				

16.4.7 Sub-attributes of the 3GPP Vendor-Specific attribute

The table 7 describes the sub-attributes of the 3GPP Vendor-Specific attribute of the Access-Request, Accounting-Request START, Accounting-Request STOP and Accounting-Request Interim-Update messages.

Table 7: The sub-attributes of the 3GPP Vendor-Specific attribute of the Access-Request, Accounting-Request START, Accounting-Request STOP and Accounting-Request Interim-Update messages

Sub-attr #	Sub-attribute Name	Description	Presence Requirement	Associated attribute (Location of Sub-attr)
1	3GPP-IMSI	IMSI for this user	Optional	Access-Request, Accounting-Request START, Accounting-Request – STOP, Accounting-Request Interim-Update
2	3GPP-Charging-Id	Charging ID for this PDP Context (this together with the GGSN-Address constitutes a unique identifier for the PDP context).	Optional	Access-Request, Accounting-Request START, Accounting-Request -STOP, Accounting-Request Interim-Update
3	3GPP-PDP Type	Type of PDP context, e.g. IP or PPP	Conditional (mandatory if attribute 7 is present)	Access-Request Accounting-Request START, Accounting-Request -STOP, Accounting-Request Interim-Update
4	3GPP-CG-Address	Charging Gateway IP address	Optional	Access-Request, Accounting-Request START, Accounting-Request -STOP, Accounting-Request

Sub-attr #	Sub-attribute Name	Description	Presence Requirement	Associated attribute (Location of Sub-attr)
				Interim-Update
5	3GPP-GPRS-Negotiated-QoS-Profile	QoS profile applied by GGSN	Optional	Access-Request, Accounting-Request START, Accounting-Request -STOP, Accounting-Request Interim-Update
6	3GPP-SGSN-Address	SGSN IP address that is used by the GTP control plane for the handling of control messages. It may be used to identify the PLMN to which the user is attached.	Optional	Access-Request, Accounting-Request START, Accounting-Request -STOP, Accounting-Request Interim-Update
7	3GPP-GGSN-Address	GGSN IP address that is used by the GTP control plane for the context establishment. -It is the same as the GGSN IP address used in the GCDRs.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
8	3GPP-IMSI-MCC-MNC	MCC and MNC extracted from the user-''s IMSI (first 5 or 6 digits, as applicable from the presented IMSI).	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
9	3GPP-GGSN- MCC-MNC	MCC-MNC of the network the GGSN belongs to.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
10	3GPP-NSAPI	Identifies a particular PDP context for the associated PDN and MSISDN/IMSI from creation to deletion.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP Accounting-Request Interim-Update
11	3GPP- Session-Stop-Indicator	Indicates to the AAA server that the last PDP context of a session is released and that the PDP session has been terminated.	Optional	Accounting Request STOP
12	3GPP- Selection-Mode	Contains the Selection mode for this PDP Context received in the Create PDP Context Request Message	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
13	3GPP-Charging-Characteristics	Contains the charging characteristics for this PDP Context received in the	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request

Sub-attr #	Sub-attribute Name	Description	Presence Requirement	Associated attribute (Location of Sub-attr)
		Create PDP Context Request Message (only available in R99 and later releases)		Interim-Update
14	3GPP-CG-IPv6-Address	Charging Gateway IPv6 address	Optional	Access-Request, Accounting-Request START, Accounting-Request– STOP, Accounting-Request Interim-Update
15	3GPP-SGSN-IPv6-Address	SGSN IPv6 address that is used by the GTP control plane for the handling of control messages. It may be used to identify the PLMN to which the user is attached.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
16	3GPP-GGSN-IPv6-Address	GGSN IPv6 address that is used by the GTP control plane for the context establishment.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
17	3GPP- IPv6-DNS-Servers	List of IPv6 addresses of DNS servers for an APN	Optional	Access-Accept
18	3GPP-SGSN-MCC-MNC	MCC and MNC extracted from the RAI within the Create PDP Context Request or Update PDP Context Request message.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update

The RADIUS vendor Attribute is encoded as follows (as per RFC 2865 [38])

Octets	Bits 8 7 6 5 4 3 2 1
1	Type = 26
2	Length = n
3	Vendor id octet 1
4	Vendor id octet 2
5	Vendor id octet 3
6	Vendor id octet 4
7-n	String

n ≥ ~~>=~~7

3GPP Vendor Id = 10415

The string part is encoded as follows:

Octets	Bits 8	7	6	5	4	3	2	1
1	3GPP type =							
2	3GPP Length = m							
3 –m	3GPP value							

m ≥~~>=~~ 2 and m ≤~~<=~~ 248

The 3GPP specific attributes encoding is clarified below.

1 -~~-~~ 3GPP-***IMSI***

Octets	Bits 8	7	6	5	4	3	2	1
1	3GPP type = 1							
2	3GPP Length= m							
3-m	IMSI digits 1-n (UTF-8 encoded)							

3GPP Type: 1

n ≤~~<=~~15

Length: m = 17

IMSI value: Text:

This is the UTF-8 encoded IMSI; The definition of IMSI shall be in accordance with 3GPP TS 23.003 [40] and 3GPP TS 29.060 [24]~~ and [41]~~. There shall be no padding characters between the MCC and MNC, and between the MNC and MSIN. If the IMSI is less than 15 digits, the padding in the GTP information element shall be removed by the GGSN and not encoded in this sub-attribute.

2 - 3GPP-***Charging ID***

Octets	Bits 8	7	6	5	4	3	2	1
1	3GPP type = 2							
2	3GPP Length= 6							
3	Charging ID value Octet 1							
4	Charging ID value Octet 2							
5	Charging ID value Octet 3							
6	Charging ID value Octet 4							

3GPP Type: 2

Length: 6

Charging ID value: 32 bits unsigned integer

3 - 3GPP-***PDP type***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 3							
2	3GPP Length= 6							
3	PDP type octet 1							
4	PDP type octet 2							
5	PDP type octet 3							
6	PDP type octet 4							

3GPP Type: 3

Length: 6

PDP type value: Unsigned 32 bits integer

PDP type octet possible values:

0 = IPv4

1 = PPP

2 = IPv6

4 - 3GPP-***Charging Gateway address***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 4							
2	3GPP Length= 6							
3	Charging GW addr Octet 1							
4	Charging GW addr Octet 2							
5	Charging GW addr Octet 3							
6	Charging GW addr Octet 4							

3GPP Type: 4

Length: 6

Charging GW address value: -Address

5 - 3GPP-***GPRS Negotiated QoS profile***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 5							
2	3GPP Length= L							
3 -L	UTF-8 encoded QoS profile							

3GPP Type: 5

Length: -27 (release 99) or 11 (release 98)

QoS profile value:- Text

UTF-8 encoded QoS profile syntax:

"<Release indicator> – <release specific QoS IE UTF-8 encoding>"

<Release indicator> = UTF-8 encoded number :

"98" = Release 98

"99"= Release 99

<release specific QoS profile UTF-8 encoding> = UTF-8 encoded QoS profile for the release indicated by the release indicator.

The UTF-8 encoding of a QoS IE is defined as follows: each octet is described by 2 UTF-8 encoded digits, defining its hexadecimal representation. The QoS profile definition is in 3GPP TS 24.008 [54].

The release 98 QoS profile data is 3 octets long, which then results in a 6 octets UTF-8 encoded string.

The release 99 QoS profile data is 11 octets long, which results in a 22 octets UTF-8 encoded string.

6 - 3GPP-***SGSN address***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 6							
2	3GPP Length= 6							
3	SGSN addr Octet 1							
4	SGSN addr Octet 2							
5	SGSN addr Octet 3							
6	SGSN addr Octet 4							

3GPP Type: 6

Length: 6

SGSN address value:- Address

7 - 3GPP-***GGSN address***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 7							
2	3GPP Length= 6							
3	GGSN addr Octet 1							
4	GGSN addr Octet 2							
5	GGSN addr Octet 3							
6	GGSN addr Octet 4							

3GPP Type: 7

Length: 6

GGSN address value: Address

8 - 3GPP-***IMSI MCC-MNC***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 8							
2	3GPP Length= n							
3	MCC digit1 (UTF-8 encoded)							
4	MCC digit2 (UTF-8 encoded)							
5	MCC digit3 (UTF-8 encoded)							
6	MNC digit1 (UTF-8 encoded)							
7	MNC digit2 (UTF-8 encoded)							
8	MNC digit3 if present (UTF-8 encoded)							

3GPP Type: 8

Length: n shall be 7 or 8 octets depending on the presence of MNC digit 3

MS address value: text

This is the UTF-8 encoding of the MS MCC-MNC values. In accordance with 3GPP TS 23.003 [40] and 3GPP TS 29.060 [24] ~~and [41]~~ the MCC shall be 3 digits and the MNC shall be either 2 or 3 digits. There shall be no padding characters between the MCC and MNC.

9 - 3GPP-***GGSN MCC-MNC***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 9							
2	3GPP Length= n							
3	MCC digit1 (UTF-8 encoded)							
4	MCC digit2 (UTF-8 encoded)							
5	MCC digit3 (UTF-8 encoded)							
6	MNC digit1 (UTF-8 encoded)							
7	MNC digit2 (UTF-8 encoded)							
8	MNC digit3 if present (UTF-8 encoded)							

3GPP Type: 9

Length: n shall be 7 or 8 octets depending on the presence of MNC digit 3

GGSN address value: -text

This is the UTF-8 encoding of the GGSN MCC-MNC values. In accordance with 3GPP TS 23.003 [40] and 3GPP TS 29.060 [24] ~~and [41]~~ the MCC shall be 3 digits and the MNC shall be either 2 or 3 digits. There shall be no padding characters between the MCC and MNC.

10 - 3GPP-***NSAPI***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 10							
2	3GPP Length= 3							
3	NSAPI							

3GPP Type: 10

Length: 3

NSAPI value: text

It is the value of the NSAPI of the PDP context the RADIUS message is related to. It is encoded as its hexadecimal representation, using 1UTF-8 encoded digit.

11 - 3GPP-***Session Stop Indicator***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 11							
2	3GPP Length= 3							
3	1 1 1 1 1 1 1 1							

3GPP Type: 11

Length: -3

-Value is set to all 1.

12 - 3GPP-***Selection-Mode***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 12							
2	3GPP Length= 1							
3	UTF-8 encoded Selection mode string							

3GPP Type: 12

Length:- 3

Selection mode value: Text

The format of this attribute shall be a character string consisting of a single digit, mapping from the binary value of the selection mode in the Create PDP Context message (3GPP TS 29.060 [24]). Where 3GPP TS 29.060 [24] provides for interpretation of the value, e.g. map "3" to "2", this shall be done by the GGSN.

13 - 3GPP-***Charging-Characteristics***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 13							
2	3GPP Length= 6							
3-6	UTF-8 encoded Charging Characteristics value							

3GPP Type: 13

Length: -6

Charging characteristics value: -Text

The charging characteristics is value is the value of the 2 octets value field taken from the GTP IE described in 3GPP TS 29.060 [24], subclausesection 7.7.23.

Each octet of this IE field value is represented via 2 UTF-8 encoded digits, defining its hexadecimal representation.

14 - 3GPP-***Charging Gateway IPv6 address***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 14							
2	3GPP Length= 18							
3	Charging GW IPv6 addr Octet 1							
4	Charging GW IPv6 addr Octet 2							
5-18	Charging GW IPv6 addr Octet 3-16							

3GPP Type: 14

Length: 18

Charging GW IPv6 address value:- IPv6 Address

15 - 3GPP-***SGSN IPv6 address***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 15							
2	3GPP Length= 18							
3	SGSN IPv6 addr Octet 1							
4	SGSN IPv6 addr Octet 2							
5-18	SGSN IPv6 addr Octet 3-16							

3GPP Type: 15

Length: 18

SGSN IPv6 address value: IPv6 Address

16 - 3GPP-***GGSN IPv6 address***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 16							
2	3GPP Length= 18							
3	GGSN IPv6 addr Octet 1							
4	GGSN IPv6 addr Octet 2							
5-18	GGSN IPv6 addr Octet 3-16							

3GPP Type: 16

Length: 18

GGSN IPv6 address value: IPv6 Address

17 – 3GPP-***IPv6-DNS-Servers***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 17							
2	3GPP Length= m							
3-18	(1st) DNS IPv6 addr Octet 1-16							
19-34	(2nd) DNS IPv6 addr Octet 1-16							
k-m	(n-th) DNS IPv6 addr Octet 1-16							

3GPP Type: 17

Length: m = n × *16 + 2; –n ≥ >=1 and n ≤ <=15;— k = m-15

IPv6 DNS Server value:- IPv6 AddressThe 3GPP- IPv6-DNS-Servers Attribute provides a list of one or more ('n') IPv6 addresses of Domain Name Server (DNS) servers for an APN. The DNS servers are listed in the order of preference for use by a client resolver, i.e. the first is 'Primary DNS Server', the second is 'Secondary DNS Server' etc. The attribute may be included in Access-Accept packets.

18 - 3GPP-***SGSN MCC-MNC***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 18							
2	3GPP Length= n							
3	MCC digit1 (UTF-8 encoded)							
4	MCC digit2 (UTF-8 encoded)							
5	MCC digit3 (UTF-8 encoded)							
6	MNC digit1 (UTF-8 encoded)							
7	MNC digit2 (UTF-8 encoded)							
8	MNC digit3 if present (UTF-8 encoded)							

3GPP Type: 18

Length: n shall be 7 or 8 octets depending on the presence of MNC digit 3

SGSN address value: ~~-~~text

This is the UTF-8 encoding of the RAI MCC-MNC values. In accordance with 3GPP TS 23.003 [40] and 3GPP TS 29.060 [24] ~~and [41]~~ the MCC shall be 3 digits and the MNC shall be either 2 or 3 digits. There shall be no padding characters between the MCC and MNC.

16.4.8 Accounting Request Interim-Update (sent from GGSN to AAA server)

T~~he t~~able 8 describes the attributes of the Accounting-Request Interim-Update message.

Table 8: The attributes of the Accounting-Request Interim-Update message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username provided by the user (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used). If no username is available a generic username, configurable on a per APN basis, shall be present. If the User-Name has been received in the Access-Accept message, this user-name shall be used in preference to the above	String	Optional
4	NAS-IP-Address	IP address of the GGSN for communication with the AAA server.	IPv4	Conditional Notes ~~3, 5~~1 and 3
95	NAS-IPv6-Address	IP address of the GGSN for communication with the AAA server.	IPv6	Conditional Notes 1 and 3~~, 5~~
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 1~~3~~
6	Service-Type	Indicates the type of service for this user	Framed	Optional
7	Framed Protocol	Indicates the type of protocol for this user	7 (GPRS PDP Context)	Optional
8	Framed-IP-Address	User IP address	IPv4	Conditional Note 3~~5~~

Attr #	Attribute Name	Description	Content	Presence Requirement
97	Framed-IPv6-Prefix	User IPv6 address	IPv6	Conditional Note 3~~5~~
96	Framed-Interface-Id	User IPv6 Interface Identifier	IPv6	Conditional Note~~5, 6~~s 3 and 4
25	Class	Received in the access accept	String	Optional (N~~OTE 4~~ote 2)
30	Called-Station-Id	Identifier for the target network	APN (UTF-8 encoded)	Mandatory
31	Calling-Station-Id	This attribute is the identifier for the MS, and it shall be configurable on a per APN basis.	MSISDN in international format according to 3GPP TS 23.003 [40], UTF-8 encoded. ~~Note that there are no leading characters in front of the country code.~~ (Note 6)	Optional
40	Acct-Status-Type	Indicates the type of accounting request	Interim-Update	Mandatory
41	Acct-Delay-Time	Indicates how many seconds the GGSN has been trying to send this record for, and can be subtracted from the time of arrival on the AAA server to find the approximate time of the event generating this Accounting-Request	Second	Optional
42	Acct-Input-Octets	GGSN counted number of octets sent by the user for the PDP context	32 bit unsigned integer	Optional
43	Acct-Output-Octets	GGSN counted number of octets received by the user for the PDP context	32 bit unsigned integer	Optional
44	Acct-Session-Id	User session identifier.	GGSN IP address (IPv4 or IPv6) and Charging-ID concatenated in a UTF-8 encoded hexadecimal. ~~NOTE: The GGSN IP address is the same as that used in the GCDRs.~~(Note 5)	Mandatory
45	Acct-Authentic	Authentication method	RADIUS or LOCAL	Optional
46	Acct-Session-Time	Duration of the session	Second	Optional
47	Acct-Input-Packets	GGSN counted number of packets sent by the user	Packet	Optional
48	Acct-Output-Packets	GGSN counted number of packets received by the user	Packet	Optional
61	NAS-Port-Type	Port type for the GGSN	As per RFC 2865 [38]	Optional
26/10415	3GPP Vendor-Specific	Sub-attributes according to ~~sub-clause~~subclause 16.4.7.	See ~~sub-clause~~subclause 16.4.7	Optional except sub-attribute 3 which is conditional

Attr #	Attribute Name	Description	Content	Presence Requirement
NOTE 1~~3~~: Either NAS-IP-Address or NAS-Identifier shall be present. NOTE 2~~4~~: The presence of this attribute is conditional upon this attribute being received in the Access-Accept message NOTE 3~~5~~: Either IPv4 or IPv6 address/prefix attribute shall be present. The IP protocol version for end-user and network may be different. NOTE 4~~6~~: Included if the prefix alone is not unique for the user. This may be the case, for example, if address is assigned using stateful address autoconfiguration or if a static IPv6 address. NOTE 5: The GGSN IP address is the same as that used in the GCDRs. NOTE 6: There are no leading characters in front of the country code.				

16.4.9 Disconnect Request (optionally sent from AAA server to GGSN)

T~~he t~~able 9 describes the attributes of the Disconnect-Request message.

Table 9: The attributes of the Disconnect-Request message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username provided by the user (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used). If no username is available a generic username, configurable on a per APN basis, shall be present. If the User-Name has been sent in the Access-Accept message, this user-name shall be used in preference to the above	String	Optional
8	Framed-IP-Address	User IP address	IPv4	Conditional Note 2~~8~~
97	Framed-IPv6-Prefix	User IPv6 address	IPv6	Conditional Note 2~~8~~
96	Framed-Interface-Id	User IPv6 Interface Identifier	IPv6	Conditional Note ~~6, 8~~s 1and 2
44	Acct-Session-Id	User session identifier.	GGSN IP address (IPv4 or IPv6) and Charging-ID concatenated in a UTF-8 encoded hexadecimal. ~~NOTE: The GGSN IP address is the same as that used in the GCDRs.~~(Note 3)	Mandatory
NOTE ~~6~~1: Included if the prefix alone is not unique for the user. This may be the case, for example, if address is assigned using stateful address autoconfiguration or if a static IPv6 address. NOTE ~~8~~2: Either IPv4 or IPv6 address/prefix attribute shall be present. NOTE 3: The GGSN IP address is the same as that used in the GCDRs.				

Annex A (informative): Interworking PCS1900 with PSDNs

~~<VOID>~~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
06-2001	TSG#12	NP-010256	018		Clarifications on the non-transparent access mode	4.0.0	4.1.0
06-2001	TSG#12	NP-010256	020		Set the use of PPP between the MT and TE as an option when interworking with MIPv4	4.0.0	4.1.0
09-2001	TSG#13	NP-010530	021	5	Standard method for information delivery (MSISDN; IP address…) between GPRS and external PDN using RADIUS	4.1.0	4.2.0
12-2001	TSG#14	NP-010672	023	2	Standard method for information update between GPRS and external PDN using RADIUS	4.2.0	4.3.0
12-2001	TSG#14	NP-010672	024	2	Standard method for interworking between GPRS and external PDN using RADIUS	4.2.0	4.3.0
12-2001	TSG#14	NP-010572	028	1	Correction to the Calling-Station-Id attribute	4.2.0	4.3.0
12-2001	TSG#14	NP-010572	030	1	Correction to 3GPP Vendor specify attribute 3GPP-IMSI	4.2.0	4.3.0
12-2001	TSG#14	NP-010572	032		Correction to 3GPP vendor specific attributes containing MCC-MNC	4.2.0	4.3.0
12-2001	TSG#14	NP-010604	035	2	New terminology required by GERAN	4.3.0	5.0.0
03-2002	TSG#15	NP-020080	039		Change of associated attribute for 3GPP-NSAPI	5.0.0	5.1.0
06-2002	TSG#16	NP-020171	044	4	Address autoconfiguration of IPv6 terminals and IPv6 update	5.1.0	5.2.0
06-2002	TSG#16	NP-020295	054		Corrections to the 3GPP RADIUS attributes	5.1.0	5.2.0
06-2002	TSG#16	NP-020295	056	1	Clarification on the Radius Flows	5.1.0	5.2.0
07-2002					Editorial - to correct minor error in Change History box	5.2.0	5.2.1
09-2002	TSG#17	NP-020417	057	8	Actions within the GGSN for IMS parameters sent in PDP context activation	5.2.1	5.3.0
09-2002	TSG#17	NP-020408	061	2	Configuration of Domain Name System (DNS) server IPV6 addresses	5.2.1	5.3.0
12-2002	TSG#18	NP-020613	066		Correction of figure for Radius Accounting Update	5.3.0	5.4.0
12-2002	TSG#18	NP-020623	067	3	Handling of binding information by GGSN	5.3.0	5.4.0
12-2002	TSG#18	NP-020613	072		RADIUS enhancement for identification of VPLMN	5.3.0	5.4.0

3GPP TSG-CN WG3 Meeting #27
Dublin, Ireland, 10th - 14th February 2003.

Tdoc ⌘N3-030125

CR-Form-v7

CHANGE REQUEST

⌘ **24.022** **CR** **008** ⌘**rev** **1** ⌘ Current version: **5.1.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Correction of an incorrect Reference
Source:	⌘	TSG_CN WG3 *[MCC]*
Work item code:	⌘	TEI
Date:	⌘	10/02/2003
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Inconsistencies in the specification, Missing and incorrect references
Summary of change:	⌘	Correction of an incorrect reference, and additional editorial corrections to the specification.
Consequences if not approved:	⌘	Inconsitencies and errors in the referencing. Possible mis-understanfing when reading specification.

Clauses affected:	⌘	5.6.1 corrected reference, and editorials to most parts of the specification

	Y	N		
Other specs affected: ⌘		X	Other core specifications	⌘
		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

3GPP TS 24.022 V5.1.0 (2002-12)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Core Network; Radio Link Protocol (RLP) for circuit switched bearer and teleservices (Release 5)

Keywords
UMTS, network, radio, circuit mode

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

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

The present document specifies the Radio Link Protocol (RLP) for circuit switched data transmission 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 specifies the Radio Link Protocol (RLP) for circuit switched data transmission within a PLMN. RLP covers the Layer 2 functionality of the ISO OSI Reference Model (ISO/IEC 7498 [22]). It is based on ideas contained in ISO/IEC 3309 [21], ISO/IEC 4335 [20] and ISO/IEC 7809 [26] (HDLC of ISO) as well as ITU-T Recommendation X.25 [30] and Q.92x (LAP-B and LAP-D of ITU, respectively.) RLP has been tailored to the special needs of digital radio transmission. RLP provides to its users the OSI Data Link Service (ISO/IEC 8886 [24]).

RLP is intended for use with non-transparent data-transfer. Protocol conversion may be provided for a variety of protocol configurations. Those foreseen immediately are:

- character-mode protocols using start-stop transmission (IA5);
- X.25 LAP-B.

For reasons of better presentation, material about protocol conversion has been placed within those Specifications concerned with the relevant Terminal Adapters, i.e. 3GPP TS 27.002 [10] for the asynchronous case and 3GPP TS 27.003 [11] for the synchronous case. Care must be taken that that material also applies to Interworking Functions; see 3GPP TS 29.007 [13].

The present document is valid for a PLMN in A/Gb mode as well as in Iu mode. If text applies only for one of these systems it is explicitly mentioned by using the terms "A/Gb mode" and "Iu mode". Please note, that the Gb interface does not play any role in the scope of ~~this document~~the present document although the term "A/Gb mode" is used.

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. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

~~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] Void.

[2] 3GPP TS 44.021: "Rate adaption on the Mobile Station - Base Station System (MS - BSS) interface".

[3] 3GPP TS 48.004: "Base Station System - Mobile services Switching Centre (BSS - MSC) interface Layer 1 specification".

[4] 3GPP TS 48.020: "Rate adaption on the Base Station System - Mobile services Switching Centre (BSS - MSC) interface".

[5] 3GPP TS 25.410: "UTRAN Iu ~~Interface~~interface: General Aspects and Principles".

[6] 3GPP TS 25.411: "UTRAN Iu ~~Interface~~ interface Layer 1".

[7] 3GPP TS 25.414: "UTRAN Iu ~~I~~interface ~~Data~~ data ~~Transport~~ transport and ~~Transport~~ transport ~~Signalling~~signalling".

[8] 3GPP TS 25.415: "UTRAN Iu interface user plane protocols~~Iu Interface CN-UTRAN User Plane Protocols~~".

[9] 3GPP TS 27.001: "General on Terminal Adaptation Functions (TAF) for Mobile Stations (MS)".

[10] 3GPP TS 27.002: "Terminal Adaptation Functions (TAF) for services using ~~asynchronous~~ Asynchronous bearer capabilities".

[11] 3GPP TS 27.003: "Terminal Adaptation Functions (TAF) for services using ~~synchronous~~ Synchronous bearer capabilities".

[12] Void.

[13] 3GPP TS 29.007: "General requirements on interworking between the Public Land Mobile Network (PLMN) and the Integrated Services Digital Network (ISDN) or Public Switched Telephone Network (PSTN)".

[14] ITU-T Recommendation Q.920: "ISDN user-network interface data link layer - General aspects".

[15] ITU-T Recommendation Q.921: "ISDN user-network interface - ~~data~~ Data link layer specification".

[16] ITU-T Recommendation Q.921bis: "Abstract test suite~~s~~ for LAPD conformance testing~~s~~".

[17] ITU-T Recommendation Q.922: "ISDN data link layer specification for frame mode bearer services".

[18] ITU-T Recommendation V.42bis: "Data compression procedures for Data Circuit-terminating Equipment (DCE) using error correction procedures~~Data Compression for Data Circuit Terminating Equipment (DCE) using Error Correction Procedures~~".

[19] ITU-T Recommendation X.25: "Interface between Data Terminal Equipment (DTE) and Data Circuit ~~-t~~Terminating Equipment (DCE) for terminals operating in ~~Packet~~ packet m~~M~~ode and connected to ~~Public~~ public ~~Data~~ data ~~Networks~~ networks by dedicated Circuit".

[20] ISO/IEC ~~Recommendation~~ 4335: "Information technology - Telecommunications and information exchange between systems - ~~High~~ High-level ~~data~~ Data ~~link~~ Link C~~c~~ontrol (HDLC) procedures - Elements of procedures".

[21] ISO/IEC ~~Recommendation~~ 3309: "Information technology - Telecommunications and information exchange between systems - ~~High~~ High-level ~~data~~ Data ~~l~~Link ~~c~~Control (HDLC) procedures - Frame structure".

[22] ISO ~~Recommendation~~/IEC 7498: "Information ~~processing systems~~technology - Open Systems Interconnection - Basic Reference Model".

[23] ISO ~~Recommendation~~/IEC 8885: "Information technology - Telecommunication and information exchange between systems - High-level ~~data~~ Data ~~l~~Link ~~c~~Control (HDLC) procedures - General purpose XID frame information field content and format".

[24] ISO ~~Recommendation~~/IEC 8886: "Information technology - Open Systems Interconnection - Data link service definition~~Telecommunication and information exchange between systems - Data link service definitions for Open Systems interconnection~~".

[25] ISO ~~Recommendation~~/TR 8509: "Information processing systems - Open Systems Interconnection - Service conventions".

[26] ISO/IEC ~~Recommendation~~ 7809: "Information technology - Telecommunications and information exchange between systems - High-level ~~data~~ Data ~~link~~ Link ~~c~~Control (HDLC) procedures - Classes of procedures".

[27] ISO Recommendation/IEC 7776: "Information technology - Telecommunications and information exchange between systems - High-level data link control procedures - Description of the X.25 LAPB-compatible DTE data link procedures Information processing systems - High-level data link control procedures - Description of the X.25 LAPB-compatible DTE data link procedures".

[28] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[29] 3GPP TS 43.051: "GSM/EDGE Radio Access Network (GERAN) overall description; Stage 2".

[30] ITU-T 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".

2.1 Definitions and abbreviations

2.1.1 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [28] and the following apply:

In addition to the following, abbreviations used in the present document are listed in 3GPP TR 21.905 [28].

ABM	Asynchronous Balanced Mode
ADM	Asynchronous Disconnected Mode
ATM	Asynchronous Transfer Mode.
C/R	Command/Response bit
DISC	Disconnect frame
DM	Disconnected Mode frame
DTX	Discontinuous Transmission
FCS	Frame Check Sequence
L2R	Layer 2 Relay function
N(R)	Receive sequence number
N(S)	Send sequence number
NULL	Null information frame
P/F	Poll/Final bit
REJ	Reject frame
REMAP	Remap frame
RLP	Radio Link Protocol
RNR	Receive Nor ready frame
RR	Receive Ready frame
SABM	Set Asynchronous Balanced Mode frame
SREJ	Selected reject frame
STM	Synchronous Transfer Mode
TEST	Test frame
UA	Unnumbered Acknowledge frame
UI	Unnumbered Information frame
XID	Exchange Identification frame

2.1.2 Definitions

For the purposes of the present document, the following terms and definitions apply:

A/Gb mode: A system or a subsystem operates in A/Gb mode if an A or Gb interface is used between the radio access network and the core network.

backwards compatibility: RLP defines several backwards-compatible versions. That means that a newer version can interwork with an older one without changing the older one. This is realized by a fall back mechanism during XID exchange.

command: instruction represented in the RLP header, causing the receiving RLP entity to execute a specific function.

frame check sequence: field of redundant information based on a cyclic code, used for error detection.

I + S frame: RLP frame that is used for user information transfer, carrying supervisory information piggyback.

improper frame: RLP frame having an FCS error or having a header the contents of which is inconsistent with ~~this Specification~~the present document.

Iu mode: ~~A~~ system or a subsystem operates in Iu mode if an Iu-CS or Iu-PS interface is used between the radio access network and the core network. It operates in UTRAN Iu mode if UTRAN is used as radio access network. It operates in GERAN Iu mode if GERAN is used as radio access network.

non-transparent: in PLMN data transmission, a configuration where at layer 2, protocol information of the fixed network is mapped on RLP elements, and vice versa.

piggybacking: means by which one and the same frame can carry both user information and RLP related supervisory information.

response: reply represented in the RLP-header, by which the sending RLP entity reports back about its status.

RLP frame: sequence of contiguous bits, representing an RLP procedural element.

RLP header: that part of an RLP frame that encodes either a command or a response, located at the beginning of the RLP frame.

S frame: RLP frame that contains supervisory information in the absence of user information.

transparent: in PLMN data transmission, a configuration where at layer 2 (and also at the layers above) no protocol conversion takes place.

U frame: RLP frame that contains unnumbered protocol control information.

3 Introduction

Three versions of RLP are defined:

- RLP version 0: single-link basic version;
- RLP version 1: single-link extended version (e.g. extended by data compression);
- RLP version 2: multi-link version.

RLP uses one physical link (single-link) or from 1 up to 4 (multi-link) substreams on one or more physical links. However, the RLP multi-link version is designed to be able to support up to 8 physical links. If, in the call set-up signalling, either end indicates that it cannot support multi-link operation, neither end shall require usage of RLP ~~-~~versions higher than 1. If the BC negotiation during call set-up results in a possibility for multi-link operation during the call, both ends shall require and accept RLP version 2 only.

If the BC-IE sent by the UE in the SETUP or CALL CONFIRM message indicates negotiation during call set-up results in "maximum number of traffic channels" = "1 TCH" and WAIUR ≤ 14~~,~~4 kbit/s and the BC-IE sent by the UE in the CALL CONFIRM message (MT case) or by the MSC in the CALL PROCEEDING message (MO case) indicates UIMI ~~-~~= "not required/not allowed" or "up to 1 TCH/F allowed/may be requested/allowed", this is shall be interpreted as if at least one end does not support multi-link operation, and neither end shall require RLP version higher than 1.

RLP makes use of an underlying FEC (Forward Error Correction) mechanism. For RLP to perform adequately it is assumed that the basic radio channel together with FEC provides for a block error rate of less than 10 %, where a block consists of 240 bits or 576 bits (Further study on the BLER for 576-bit blocks is needed). Furthermore, it is assumed that in case of multi-link RLP the difference of the delay between all physical links is less than timer T4.

In A/Gb mode and in GERAN Iu mode, RLP frames are of a fixed size of 240 (TCH/F4~~,~~8 and TCH/F9~~,~~6 channel codings) or 576 bits (TCH/F14~~,~~4, TCH/F28~~,~~8 and TCH/F43~~,~~2 channel codings). In UTRAN Iu mode, the RLP frame size does not depend on the channel coding, only 576 bit frames are used.

RLP entities running only in an UTRAN Iu mode environment need only to support the 576 bit frame length. The REMAP function is not necessary. RLP entities running in both of the systems have to support the REMAP function. In a handover from UTRAN Iu mode to A/Gb mode or GERAN Iu mode the frame either stays 576 bits long or changes from 576 bits to 240 bits incurring a REMAP. In a handover from A/Gb mode or GERAN Iu mode to UTRAN Iu mode the frame either stays 576 bits long or changes from 240 bits to 576 bits incurring a REMAP.

In A/Gb mode, RLP frames are sent in strict alignment with the radio transmission. (For details, see 3GPP -TS 44.021 ([2]). Whenever a frame is to be sent, the RLP entity has to provide the necessary protocol information to be contained in it.

Provision is made for ~~discontinuous~~ Discontinuous ~~transmission~~ Transmission (DTX).

RLP spans from the User Equipment (UE) to the interworking function (IWF), located at the nearest Mobile Switching Centre (MSC), or beyond. Depending on the exact location of the IWF, handover of the UE may result in link-reset or even total loss of the connection.

The UE shall initiate the RLP link. In addition the MSC/IWF may initiate the RLP link.

In the terminology of HDLC, RLP is used in a balanced configuration, employing asynchronous operation, i.e. either station has the right to set-up, reset, or disconnect a link at any time. Procedural means are provided for to deal with contentious situations, should they ever occur.

RLP is full-duplex in the sense that it allows for information to be transferred in both directions simultaneously.

4 Frame structure

4.1 Basic frame structure

In A/Gb mode and GERAN Iu mode, an RLP-frame has a fixed length of either 240 bits, used when the channel coding is TCH/F4~~.~~,8 or TCH/F9~~.~~,6, or 576 bits, used when the channel coding is TCH/F14~~.~~,4, TCH/F28~~.~~,8 or TCH/F43~~.~~,2. In UTRAN Iu mode, the RLP-frame has a fixed length of 576 bits.

A frame consists of a header, an information field, and an FCS (frame check sequence) field. The size of the components depends on the radio channel type, RLP version and on the RLP frame. As a benefit of using strict alignment with underlying radio transmission there is no need for frame delimiters (like flags etc.) in RLP. In consequence, there is no "bit-stuffing" necessary in order to achieve code transparency.

a) 240 bit frame size

	Header	Information	FCS
version 0 and 1, version 2 (U frames only)	16 bit	200 bit	24 bit
version 2 (S and I+S frames only)	24 bit	192 bit	24 bit

b) 576 bit frame size

	Header	Information	FCS
version 0, 1, and version 2 (U frames only)	16 bit	536 bit	24 bit
version 2 (S and I+S frames only)	24 bit	528 bit	24 bit

Figure 1: Frame structure

4.2 RLP header

An RLP-header carries one of three types of control information, the first being unnumbered protocol control information (U frames), the second being supervisory information (S frames), the third being user information carrying supervisory information piggybacked (I + S frames).

4.3 Order of transmission

The header, as defined in subclause 5.2, shall be transmitted from left to right. The FCS shall be transmitted commencing with the highest order term. The order of bit transmission for the information field is from left to right.

4.4 Frame check sequence

The FCS shall be the ones complement of the modulo 2 sum of:

a) the remainder of:

For 240 bit frames:

$x^{216}(x^{23} + x^{22} + x^{21} + x^{20} + x^{19} + x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$

For 576 bit frames:

$x^{552}(x^{23} + x^{22} + x^{21} + x^{20} + x^{19} + x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

divided modulo 2 by the generator polynomial:

$x^{24} + x^{23} + x^{21} + x^{20} + x^{19} + x^{17} + x^{16} + x^{15} + x^{13} + x^8 + x^7 + x^5 + x^4 + x^2 + 1$

and

b) the remainder of the division modulo 2 by the generator polynomial:

$x^{24} + x^{23} + x^{21} + x^{20} + x^{19} + x^{17} + x^{16} + x^{15} + x^{13} + x^8 + x^7 + x^5 + x^4 + x^2 + 1$

of the product of x^{24} by the content of the frame, excluding the FCS field. (The first bit transmitted corresponds to the highest order term.)

Implementation note: As a typical implementation, at the transmitter, the initial content of the register of the device computing the remainder of the division is pre-set to all ones and is then modified by division by the generator polynomial (as described above) of the header and information field; the ones complement of the resulting remainder is transmitted as the 24 bit FCS sequence.

At the receiver, the initial content of the register of the device computing the remainder is pre-set to all ones. The final remainder after multiplication by x^{24} and then division (modulo 2) by the generator polynomial:

$$x^{24} + x^{23} + x^{21} + x^{20} + x^{19} + x^{17} + x^{16} + x^{15} + x^{13} + x^8 + x^7 + x^5 + x^4 + x^2 + 1$$

of the serial incoming protected bits and the FCS will be:

0 1 1 0 1 1 0 1 1 0 0 0 1 0 0 1 0 0 1 1 0 0 0 0 (x^{23} to x^0, resp.)

in the absence of transmission errors.

5 Elements and procedure

5.1 Modes

An RLP entity can be in one of two modes:

- Asynchronous Balanced Mode (ABM);
- Asynchronous Disconnected Mode (ADM).

5.1.1 Asynchronous Balanced Mode (ABM)

In ABM, which is the data link operational mode, either RLP entity may send commands at any time and may initiate response frame transmission without receiving explicit permission to do so from the other RLP-station. In ABM, frames shall be used for information field transfer and/or to indicate status changes in the RLP-station.

5.1.2 Asynchronous Disconnected Mode (ADM)

In ADM, which is the data-link non-operational mode, the RLP entity shall be logically disconnected from the data link and shall, therefore, neither transmit nor accept numbered information frames.

The RLP entity shall, however, be permitted to transmit and accept NULL, DM, UI, TEST and XID frames. Either RLP entity can issue an SABM command at any time, in order to terminate the ADM state. In that case, entrance of the ABM state will be indicated by a UA response from the opposite station. If the opposite station is not able to enter ABM, it will indicate this by a DM response. All commands other than those mentioned above and any unsolicited response will be ignored in ADM under all circumstances.

5.2 Header and parameters

The formats defined for the header are listed in figure 2.

5.2.1 Generally used bits

NOTE 1S: C/R = COMMAND/RESPONSE BIT
P/F = POLL/FINAL BIT
X = DON'T CARES

S_1	S_2	
0	0	R R
0	1	R E J
1	0	R N R
1	1	S R E J

$M_1M_2M_3M_4M_5$	
1 1 1 0 0	S A B M
0 0 1 1 0	U A
0 0 0 1 0	D I S C
1 1 0 0 0	D M
1 1 1 1 0	NULL
0 0 0 0 0	U I
1 1 1 0 1	X I D
0 0 1 1 1	T E S T
1 0 0 0 1	REMAP

Versions 0 and 1:

NOTE 2S: N(S) : Bit 4 low order bit
N(R) : Bit 11 low order bit

U	C/R	X	X	1	1	1	1	1	1	P/F	M1	M2	M3	M4	M5	X
S	C/R	S1	S2	0	1	1	1	1	1	P/F	N (R)					
I+S	C/R	S1	S2	N (S)						P/F	N (R)					
bit	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Version 2:

NOTES 3: S = L2R Status Bit
N(S) : Bit 1 low order bit
N(R) : Bit 14 low order bit
UP : UP bit (only if negotiated, "don't care" otherwise)

	bit 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
U	C/R	X	X	1	1	1	1	1	1	P/F	M1	M2	M3	M4	M5	X								
S	X	X	X	0	1	1	1	1	1	P/F	C/R	S1	S2	N(R)									X	UP
I+S	N(S)									P/F	C/R	S1	S2	N(R)									S	UP

Figure 2: Header formats

5.2.1.1 Command/response bit, C/R

The C/R-bit is used to indicate whether the frame is a command or response frame and whether the P/F-bit is to be interpreted as a poll or final bit, resp. For commands, the C/R bit shall be set to "1", for responses it shall be set to "0".

5.2.1.2 Poll/Final bit, P/F

The P/F-bit is used to mark a special instance of command/response exchange. With a command, it is called the P-bit, with a response, it is called the F-bit. In any one direction, only one P/F-bit exchange may be outstanding at any time. A response with the F-bit set to "1" shall always reflect the latest receive status of the RLP entity.

A P/F-bit exchange always starts with a command frame with the P-bit set to "1", which shall be answered by a response frame with the F-bit set to "1" at the earliest response opportunity.

No unsolicited F-bit = "1" is allowed. Such a frame shall be considered "improper" (see subclause 5.3.1). In ABM, the use of the P/F-bit with numbered information exchange is only allowed for checkpoint-recovery (see subclause 5.3.3).

5.2.2 Unnumbered frames, U

5.2.2.1 Set asynchronous balanced mode SABM (11100)

The SABM encoding is used as a command only. It is always used with the P-bit set to "1".

The SABM command is used either to initiate a link for numbered information transfer, i.e. to go from ADM to ABM, or to reset a link already established for numbered information transfer. With an SABM command, no information transfer is allowed.

When issuing an SABM, the RLP entity has set to zero its internal variables for sending and receiving numbered information. The other RLP entity, on receiving an SABM command, will either confirm it by setting to zero its internal variables for sending and receiving numbered information and then issuing an UA (unnumbered acknowledgement) response or reject it by sending a DM (disconnected mode) response. In the former case, both entities have entered ABM and numbered information transfer may commence. In the latter case, both entities are in ADM.

When an SABM command is issued, a loss of information may occur. Appropriate action is in the responsibility of the layers above.

5.2.2.2 Unnumbered Acknowledge. UA (00110)

The UA encoding is used as a response only. It is used to positively acknowledge an SABM or DISC command. With the UA response, no information transfer is allowed. In version 2, the UA response is sent no sooner than T4 (see subclause 5.5.6) after the last information frame sent. Information frames received within a period of T4 after reception of the SABM are discarded.

5.2.2.3 Disconnect, DISC (00010)

The DISC encoding is used as a command only. It is used to disestablish a link, previously established for numbered information transfer, i.e. to terminate ABM and go into ADM. With the DISC command, no information transfer is allowed.

The other RLP-entity shall answer with a UA response before actioning the DISC command. When a DISC command is actioned, loss of information may occur. It is the responsibility of the layers above, to provide for a "graceful" disconnect.

5.2.2.4 Disconnected Mode, DM (11000)

The DM encoding is used as a response only. It is used by RLP entity to report that it is in ADM and, as an answer to SABM, that it is (possibly temporary) unable to action a mode setting command. With the DM response, no information transfer is allowed.

5.2.2.5 Unnumbered Information, UI (00000)

The information field is to be interpreted as unnumbered information. Unnumbered Information (UI) frames can be sent in both ADM and ABM. There is no acknowledgement of receipt of UI-frames within RLP.

5.2.2.6 Exchange Identification, XID (11101)

The information field is to be interpreted as exchange identification. This frame is used to negotiate and renegotiate parameters of RLP and layer 2 Relay function. XID frames can be sent in both ADM and ABM.

The negotiation procedure is one step i.e. one side will start the process by sending an XID command, offering a certain set of parameters from the applicable parameter repertoire (see table 1) the sending entity wants to negotiate proposing values within the allowed range. In return, the other side will send an XID response, either confirming these parameter values by returning the requested values, or offering higher or lower ones in their place (see table 1 for sense of negotiation), except when the indicated RLP version is a lower one where a limited set of those parameters presented in the XID command may be answered according to the negotiated version. In RLP versions higher than "0", any unrecognisable parameters will be ignored. Default values will apply to those parameters which are not commented upon by the responding side (see subclause 5.4 for default values). This normally will end the negotiation process. XID frames are always used with the P/F-bit set to "1".

Without any prior XID exchange, default values will apply (see subclause 5.4). A negotiation of data compression parameters (see table 1) is only allowed in ADM. In addition, in RLP version 2, negotiation of RLP version N°(see table 1) is only allowed in ADM.

In the case of a collision of XID commands, all XID commands shall be ignored. The UE shall restart the parameter negotiation on expiry of T1, while the Interworking Function shall do so on expiry of twice the value of T1. An unsuccessful XID exchange shall be repeated on expiry of T1. After N2 times of unsuccessful repetition, the link shall be disconnected.

In table 1 a list of parameters is given which constitute the parameter repertoire. In addition, the format of the XID information field is given.

Table 1: XID parameters

Parameter Name	Type	Length	Format (87654321)	Units	Sense of Negotiation	Valid in Versions
RLP version N°	1	1	bbbbbbbb (note 1)	./.	down	≥ 0
IWF to UE window size	2	1	00bbbbbb	./.	down	0..1
IWF to UE window size	2	1	00bbbbbb	8	down	≥ 2
UE to IWF window size	3	1	00bbbbbb	./.	down	0..1
UE to IWF window size	3	1	00bbbbbb	8	down	≥ 2
Acknowledgement Timer(T1)	4	1	bbbbbbbb	10ms	up	≥ 0
Retransmission attempts (N2)	5	1	bbbbbbbb	./.	up	≥ 0
Reply delay (T2) (note 2)	6	1	bbbbbbbb	10ms	up	≥ 0
Compression P_T P_0 P_1 low P_1 high P_2	7	4	aaaa 00bb cccccccc cccccccc dddddddd	./. ./. ./. ./.	none see ITU-T Q.921 [15] down down	≥ 1
Re-sequencing timer (T4) (note 2)**	8	1	bbbbbbbb	10 ms	up	≥ 2
Optional features	9	1	bbbbbbbb	./.	down	≥ 2
NOTE 1: Characters "a", "b", "c" and "d" indicate a bit which is part of the parameter value in question. Parameters indicated by "a" are not negotiable. NOTE 2: In case of negotiation of this parameter it may be necessary to negotiate also the other timer values (e.g. "Acknowledgement timer" (T1)).						

The type and length are encoded within one octet, the type field occupying bits 8 to 5 and the length field occupying bits 4 to 1; 1 resp. 5 being the least significant bit. The least significant bit shall always be transmitted first.

A parameter item consists of the type/length-octet followed by the value of that parameter, where the length-indicator gives the number of octets the value actually occupies. Such parameter items may be arranged in arbitrary order, with the exception of the RLP version number, which shall be sent first in RLP versions higher than "0". The parameter items must begin in the first octet of the XID-information field and follow on contiguously. The parameter list is delimited by parameter type zero.

5.2.2.7 Test, TEST (00111)

The information field of that frame is to be interpreted as test information. Test frames can be sent in both ADM and ABM. A test sequence is always initiated by sending a TEST command in one direction and completed by sending a TEST response in the other direction.

5.2.2.8 Null information, NULL (11110)

In ADM, null-frames shall be sent each time there is a send opportunity but no UI, TEST or XID frame is awaiting transmission.

In ABM, null-frames shall be sent in reset state if there is a send opportunity and no unnumbered frames are to be sent.

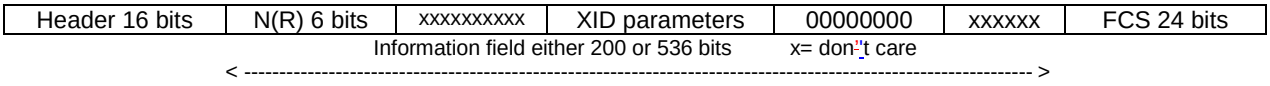
The information field is to be interpreted as null information i.e. the information field is not used and its contents may be arbitrary.

5.2.2.9 REMAP (10001)

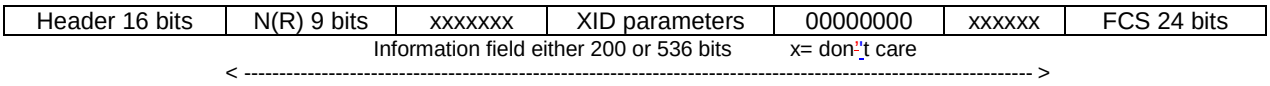
A REMAP-exchange can only take place in ABM following a change of channel coding. REMAP frames are always used with the P/F-bit set to "0". The exchange is started by the mobile-end which sends a REMAP command U-frame in the information field of which the RLP-entity indicates the N(R) of the frame - according to the 'old' frame format - from which the network-end should resend the information mapped into a frame format corresponding to the new channel coding. The mobile-end sends a REMAP-frame on every sending opportunity until a responding REMAP-frame is received from the network-end. The network-end answers by sending a REMAP U-frame with the C/R-bit set to 'Response'. In the information-field the network-end indicates the N(R)-number of the frame from which the mobile-end should remap the information into the new frame format. The network-end responds to all REMAP-commands it receives as long as it is in the REMAP synchronisation state. The network sends a numbered S -frame with poll bit P=1 or an I+S frame after the first REMAP frame to the user equipment to compel it to acknowledge the end of the REMAP condition. This frame is guarded by T1. Upon reception of an I+S frame or an S frame with the final bit F=1 from the UE, the IWF exists the REMAP synchronisation state. Any REMAP-acknowledgement that may arrive at the mobile-end after one of them has been received is discarded by the mobile-end. The RLP shall supervise the synchronisation state by a timer with the value of N2*T1. If the network-end does not receive an appropriate U-frame within N2*T1, it enters ADM. If the mobile-end does not receive a response within N2×T1 measured from the transmission of the first command, it enters ADM.

In addition to the N(R)-information the REMAP-frame information field can include any XID-parameters that should be renegotiated because of the change of channel coding. The procedures concerning these XID-parameters are as defined in subclause 5.2.2.6 ~~(Exchange Identification)~~ except that the mobile-end always starts the negotiation. Also the mapping of the parameters is as defined in subclause 5.2.2.6 ~~(Exchange Identification)~~ except that the first two octets in the REMAP information field are occupied by the N(R)-number (The LSB is transmitted first). The information field shall always include parameter type zero, which delimits the XID-parameter list.

After the change of channel coding, default values according to the new channel coding apply until new values have been negotiated by the REMAP or XID procedure. Default values according to the new channel coding also apply for those XID parameters that are not included in the REMAP information field. Values for XID parameters whose negotiation is only allowed in ADM remain valid after change of channel coding.



a) version 0 and 1



b) version 2

Figure 3: REMAP U-frame format

5.2.3 Supervisory frames, S, and numbered information transfer and supervisory frames combined, I+S

In ABM, there are cases where there is no user information pending transmission. In consequence, supervisory (S) frames alone must be conveyed. In such cases, the information field is to be interpreted as null information, i.e. the information field is not used and may be of arbitrary contents.

For reasons of optimization in the special situation of digital radio transmission, numbered information transfer frames carry also supervisory type information ("piggy-backing"). Numbered information can be exchanged only in ABM.

NOTE: The extent to which piggy-backing is used by the sending RLP entity is optional. An RLP entity receiving any of allowed piggy-backed formats, however, shall take the appropriate actions. Implementers should be aware that not using the full capability of piggy-backing could, in certain circumstances, result in a less than optimal performance.

5.2.3.1 Numbering

Each I frame is sequentially numbered and may have the value 0 through M-1, where M is the modulus. The modulus M is 62 (single-link) or 496 (multi-link).

5.2.3.2 Send Sequence number, N(S)

The send sequence number contains the number of the I frame. With the exception of SREJ conditions, information frames are transmitted in numerical order of their N(S). If multiple substreams are used, the frames may arrive at the receiver in another order. Normal information transfer is halted, when the number of outstanding, unacknowledged frames is equal to the currently established window size (see subclause 5.4).

5.2.3.3 Receive sequence number, N(R)

The N(R) field is used in ABM to designate the next information frame to be sent by the other RLP entity and to confirm that all frames up to and including N(R) - 1 have been received properly. As an exception to this, in the case of SREJ (selective reject), N(R) designates the information frame that is selectively rejected and thus requested for retransmission. In this case, no previously received frames are confirmed.

5.2.3.4 L2R Status bit

The L2R status bit set to "1" indicates that the L2R PDU transported in the information field of the RLP PDU contains at least a status octet. Otherwise, the L2R PDU contains only user data. The bit is only used for RLP-version 2.

5.2.3.5 Receive ready, RR (00)

The RR encoding can be used either as command or response. In ABM, it is used by an RLP entity to confirm all information frames up to and including N(R)-1. In doing so, the RLP-station allows the other station to transmit up to k additional information frames, counting from N(R) onwards. The issue of an RR command/response clears any previous busy condition in that direction.

5.2.3.6 Reject, REJ (01)

The REJ encoding can be used either as command or response. It is used by an RLP entity to indicate that in numbered information transfer one or more out-of sequence frames have been received. Frames up to and including N(R)-1 have been received correctly, frames N(R) and following are requested to be retransmitted. Following retransmission of those frames, further frames awaiting initial transmission may be sent. With respect to each direction of transmission, only one REJ condition may exist at any given time.

A REJ condition is cleared:

- on receipt of the frame numbered N(R);
- on time-out;
- or on reset (SABM).

An REJ shall be sent at the earliest opportunity. On time-out, REJ frames shall not be repeated. An RLP-entity receiving an REJ frame with the same N(R), which has already been the starting frame of a retransmission sequence due to P/F-bit checkpointing, shall inhibit the retransmission due to that particular REJ frame.

5.2.3.7 Receive not ready, RNR (10)

The RNR encoding can be used either as command or response. It is used by an RLP entity to indicate that it is temporarily not ready to receive numbered information frames. In that case, the RLP entity is said to be in the busy condition. All frames up to and including N(R)-1 shall be considered acknowledged. Subsequent frames, if any, shall not be considered confirmed. The acceptance status of those is a matter of further status exchange.

5.2.3.8 Selective reject, SREJ (11)

The SREJ encoding can be used either as command or response. The SREJ command/response is used to request retransmission of a single frame, thus, under certain circumstances, providing for more efficient error recovery than by REJ. No acknowledgement of received I frames is indicated by an SREJ frame, thus allowing an RLP entity to transmit one or more SREJ frames with a different N(R) before earlier SREJ conditions have been cleared.

An SREJ condition shall be cleared:

- on receipt of an information frame with N(S) equal N(R) of the SREJ;
- on time out;
- on reset (SABM).

No SREJ shall be issued during a pending REJ condition. For each frame, only one SREJ condition may exist at any time.

SREJ frames shall be sent at the earliest possibility. On time-out, SREJ frames may be repeated.

NOTE: Sending SREJ commands/responses is not mandatory.

5.2.3.9 Upgrading Proposal bit, UP bit

In version 2, the UP bit in the S and I+S frame headers may be used by the IWF to indicate to the UE that a service level upgrading will increase the throughput, and is used in accordance with 3GPP TS 27.001 [9] and 3GPP TS 29.007 [13]. The usage of the UP bit is negotiated by XID exchange.

5.3 Error Recovery

5.3.1 Improper frames

Frames containing an FCS error or having a control field the contents of which is not implemented or inconsistent with those defined in ~~this Specification~~the present document are called improper frames. Improper frames shall be ignored, i.e. the receiving RLP station shall not make any use of their contents.

5.3.2 N(S) sequence error

In numbered information transfer, any information frame with an N(S) out of the normal sequence shall lead to an N(S) sequence error condition, unless that frame is requested for retransmission by an SREJ, sent at an earlier time. In case multiple substreams make up a connection when the multi-link version is used the received frames must be re-sequenced. For that a timer T4 defines a re-sequencing period (see subclause 5.4) during which frames may be out-of-order. An N(S) sequence error condition only occurs if the N(S) arrives after the expiry of T4. There are three mechanisms to deal with N(S) sequence errors:

- REJ recovery;
- SREJ recovery;
- P/F-bit recovery (checkpointing).

The first two being the responsibility of the receiving station, the last being the responsibility of the sending station. There are no strict rules as to whether REJ or SREJ recovery shall be applied, however, if a station decides to initiate REJ or SREJ recovery, it shall do so at the earliest opportunity. The information part of out-of sequence frames shall be discarded, unless the receiving station intends to initiate SREJ recovery.

5.3.3 N(R) error

Any confirming N(R) that is not in the range of the window size shall be ignored.

5.3.4 Time-out and checkpointing

All frames requiring a response or acknowledgement shall be guarded by time-out (timer T1). In detail, those frames are:

- SABM;
- DISC;
- REJ;
- SREJ;
- numbered information frames (see note);
- any frame with the P-bit set to "1" in ABM, i.e. checkpointing.

NOTE: T1 started, or restarted if already running, on the transmission of every numbered information frame.

5.3.4.1 Treatment of errors during link establishment, link reset and link disconnect

An SABM, which is not answered by either UA or DM within the timer period, shall be repeated up to N2 times.

A DISC, which is not answered by UA within the timer period, shall be repeated up to N2 times.

If the SABM or DISC, respectively, is finally unanswered, the RLP station will go into ADM in any case. For this reason, it is the responsibility of the management of any RLP entity to put the RLP entity into ADM, should there be an indication of a permanent outage, i.e. a loss of connectivity longer than N2 times the timer value.

5.3.4.2 Treatment of errors during numbered information transfer

The last frame of a sequence of numbered information frames shall also be guarded by time-out. If neither a positive acknowledgement nor a REJ is received, the RLP entity will start checkpoint recovery, i.e. the station will send a frame with the P-bit set to "1", requesting the latest status information from the other entity, indicated by the F-bit set to "1". In that case, status information is carried either by RR or RNR responses and all frames currently held by the responding RLP entity which are not delivered because of missing frames shall be discarded. A P-bit set to "1" shall only be sent with a Supervisory Frame.

Awaiting the latest status information from the other RLP entity, the sending entity does not react on REJ and SREJ frames received during this time. If such status information is received, retransmission from N(R) onwards will be performed if appropriate. However, no frame sequence starting with a given N(R) shall be retransmitted more than N2 times. If there is a frame sequence that cannot be transmitted successfully after N2 repetitions, the RLP link shall be reset or disconnected.

If no status information is received during the time-out period, this request will be repeated up to N2 times. If still there is no valid status reported back, the RLP link shall be reset or disconnected.

5.3.5 Contentious situations

Due to the asynchronous procedure, various contentious situations may arise. A contention of SABMs shall result into both entities be set into ABM or be reset. A contention of DISC's shall result into both entities be disconnected. A contention of SABM and DISC shall result into both entities be disconnected.

5.4 Transitions between 240 bit and 576 bit frame lengths

The RLP has to change the supported frame length due to transitions between different channel codings. The RLP entities have to be re-synchronised after a change of the channel coding.

Any change of the channel coding is indicated to the RLP- entity by an external event. The RLP-entity at the mobile--end enters the synchronisation state when it receives a relevant Radio Resource Management message, and it starts sending the REMAP-messages at the earliest possible time. The RLP-entity at the network-end enters the synchronisation state when the network-end detects Layer 1 synchronisation after a change of channel coding. The change of channel coding is eventually confirmed by an outband signalling message.

On entering the synchronisation state timers are halted and zeroed, and the TX- and RX-windows are frozen. When the RLP entity enters the synchronisation state it clears all SREJ or REJ conditions, discards all out-of-sequence frames received and clears all previous re-transmission requests received by any SREJ.

After this the mobile-end starts a REMAP-exchange (subclause 5.2.2.9). When an RLP-entity receives a REMAP--frame, it moves the user information contained by the frames to be remapped from the TX-window to a transition buffer between the RLP- and L2R-entities. The L2R uses the information in this buffer before mapping new data into the PDUs. The network-end regards the REMAP-procedure as completed when it has received an I+S-frame, an S-frame or an SABM U-frame from the mobile-end, whereas the mobile-end leaves the synchronisation state after receiving a responding REMAP-frame or an SABM U-frame. The data in the transition buffer at the network-end must not be deleted before an I+S-, or an S-frame is received from the mobile-end.

Supervisory or Information transfer frames or XID U frames are discarded by the receiving entity while in REMAP synchronisation state. If the RLP entity receives another U-frame, it reacts according to the defined procedures. That is, if the frame is an SABM frame it performs a reset procedure and leaves the synchronisation state. If the frame is NULL, UI or TEST frame, RLP performs the defined procedure and remains in the synchronisation state. In the case of a DISC frame RLP terminates ABM and goes into ADM.

After the REMAP-procedure is completed, the RLP-entities leave the synchronisation state and normal operation is resumed. On resuming the normal operation, the TX- and RX- windows are emptied. The N(S)-numbering resumes from the value indicated in the REMAP-message by the N(R)-number.

Abortion of the transition or another transition taking place during the REMAP-procedure restarts the REMAP-procedure in order to resume operation using the channel coding corresponding to the latest transition.

5.5 List of system parameters

The system parameters are as follows.

Table 2: RLP parameter values

Name	Range of values	Default value	Recommended value
Version N°	0 – 2	0	2
k UE ⇒ IWF (for N° = 0/1)	0 – 61	61	61
k UE ⇒ IWF (for N° = 2)	0 - k_{max} (note 3)	480	240 (note 2)
k IWF ⇒ UE (for N° = 0/1)	0 – 61	61	61
k IWF ⇒ UE (for N° = 2)	0 - k_{max} (note 3)	480	240 (note 2)
T1 (note 1)	> 420 ms (version2) > 380 ms > 440 ms > 600 ms	520 ms (fullrate on 14, 5 kbit/s, 29,0 kbit/s or 43,5 kbit/s) 480 ms (fullrate on 12 kbit/s) 540 ms (fullrate on 6 kbit/s) 780 ms (halfrate)	520 ms (fullrate on 14, 5 kbit/s, 29,0 kbit/s or 43,5 kbit/s) 480 ms (fullrate on 12 kbit/s) 540 ms (fullrate on 6 kbit/s) 780 ms (halfrate)
T2 (note 1)		< 80 ms (fullrate on 14,5 kbit/s, 29,0 kbit/s or 43,5 kbit/s) < 80 ms (fulrate on 12 kbit/s) < 80 ms (fullrate on 6 kbit/s) < 80 ms (halfrate)	< 80 ms (fullrate on 14,5 kbit/s, 29,0 kbit/s or 43,5 kbit/s) < 80 ms (fullrate on 12 kbit/s) < 80 ms (fullrate on 6 kbit/s) < 80 ms (halfrate)
N2	> 0	6	6
P_T	0	0	0
P_0	0 – 3	0	3
P_1	512 – 65535	512	2048
P_2	6 – 250	6	20
T4 (note 1)	> 25 ms	30 ms 50 ms -(fullrate on 14,5 kbit/s, 29,0 kbit/s or 43,5 kbit/s)	30 ms 50 ms (fullrate on 14,5 kbit/s, 29,0 kbit/s or 43,5 kbit/s)
Optional feature, Up signalling	0 – 1	0	1

NOTE 1: The timer values shall fulfil the formula:
- T1 > T2 + T4 + (2 * transmission delay) for multi-link operation;
- T1 > T2 + (2 * transmission delay) for single link operation.

For A/Gb and GERAN Iu mode mode the values apply according to indicated channel types, for UTRAN Iu mode the values apply according to ""fullrate on 14.5"" Timer T4 is ignored in UTRAN Iu mode and in single-link operation.

NOTE 2: This value is recommended in the case of 4 physical links.

NOTE 3: The maximum window size shall fulfil the formula:
- kmax < 496 - n x* (1 + T4 / 20 ms), where n denotes the number of channels.

Any value k within the given range may be chosen.
However, to avoid transmission delay the value k should be:
- k > n x* (2 x* transmission delay) / 20 ms.

5.5.1 RLP Version N°

The current version of RLP is "2". "0" is the default value for the version N°. RLP-versions are backwards compatible. It is assumed that future versions of RLP will be backwards-compatible with former ones. Backwards-compatible refers to the signalling, i.e. the handling of the parameters in the XID frame. The parameters are defined as specified by the RLP version with the lower number.

5.5.2 Maximum number of outstanding I frames k (Window size)

The window size is the maximum number (k) of sequentially numbered I frames that may be outstanding (i.e. unacknowledged) at any given time. It shall be agreed for a period of time.

In case of a single-link version the value can never exceed 61. In the case of a multi-link version it is necessary to use a window size that is less than the sequence number space to avoid misinterpretations of the confirming N(R). Therefore, a guard section is defined and the value k must not exceed the value k_{max} defined in table 2. On mutual agreement between the communication parties, a smaller window size may be established. For the support of 4 physical links, a value of 240 is recommended.

5.5.3 Timer T1

The period of Timer T1 is regarded to start at the beginning of the transmission of the relevant frame.

The negotiation (or default) value is defined to be the earliest instant to enter recovery.

The period of Timer T1 at the end of which retransmission of a frame may be initiated according to the procedures described in subclause 5.3 ~~above~~, is a system parameter agreed for a period of time.

The proper operation of the procedure requires that Timer T1 be greater than the maximum time between transmission of frames (SABM, DM, DISC, I or supervisory commands) and the reception of the corresponding frame returned as a response to this frame (UA, DM or acknowledging frame). Therefore, the RLP entity should not delay the response or acknowledging frame returned to the above frame by more than a value T2. T2 is a system parameter, which is less than T1. T1 is influenced by the value of T4 and shall fulfil the formula in table 2.

5.5.4 Maximum number of retransmissions N2

The value of the maximum number of retransmissions N2 of a frame following the running out of Timer T1 is a system parameter agreed for a period of time.

5.5.5 Data Compression Parameters

If the Layer 2 Relay function supports a data compression function and its use is desired the needed data compression parameters have to be negotiated. The parameter P_T is not negotiable. In case of V.42 bis the parameters P_0, P_1 and P_2 have to be negotiated. The parameters are defined as follows:

- P_T: Type of data compression:
  - 0 V.42 bis;
  - other values are reserved.
- P_0: V.42bis data compression request:
  - 0 compress in neither direction;
  - 1 compress in initiator-responder direction only;
  - 2 compress in responder-initiator direction only;
  - 3 compress in both directions.
- P_1: V.42bis number of possible codewords in the algorithm;
- P_2: V.42bis maximum encodable data string length.

The initiator is the sender of XID command, the responder is the sender of XID response.

5.5.6 Re-sequencing period (Timer T4)

In the case of a multi-link version frames may be received out of sequence due to different transmission delays. The period of timer T4 guards the re-sequencing period. During this time frames may be out of sequence.

T4 is a system parameter agreed for a period of time. The proper operation of the procedure requires that the timer T4 shall be greater than the re-sequencing period and it shall fullfil the formula in table 2. A change of the timer T4 has impact on the usable maximum window size as defined in table 2.

5.5.7 Optional features

The format of the optional features parameters is an octet where each bit position represents an optional feature that can be negotiated. The optional features are:

Bit position	Optional feature name
1	Up signalling
2	(Not yet assigned)
3	(Not yet assigned)
4	(Not yet assigned)
5	(Not yet assigned)
6	(Not yet assigned)
7	(Not yet assigned)
8	(Not yet assigned)

The "Optional Features" parameter is negotiated bitwise in the downward sense, meaning that the value of bit *i* in the XID response shall be less or equal to the value of bit *i* in the XID command.

Up signalling: If the negotiated value of the "Up signalling" feature is 1, then the UP bit in the S and I+S frame header is used for indicating an upgrading proposal to the UE, otherwise the UP bit is ignored (don't care). This optional feature is only applicable for A/Gb mode and GERAN Iu mode.

5.6 Support for discontinuous transmission (DTX)

In both ADM and ABM, whenever the RLP entity has no numbered or unnumbered supervisory commands/responses and no information transfer frames pending transmission, the RLP entity shall indicate to the lower layer that the DTX function may be invoked.

5.6.1 In case of A/Gb mode

Protocol of lower layer conforms to 3GPP TS 48.004 [3], 3GPP TS 48.020 [25] and 3GPP TS ~~24.021~~44.021 [2]. A/Gb mode specification assumes STM for lower layer protocol. Even if there is no data to be sent, some transmission is needed on STM. RLP acts as follows in case of DTX.

In case DTX is invoked, in ADM a NULL-frame will be sent, and in ABM a RR or RNR S-frame will be sent.

5.6.2 In case of Iu mode

Protocol of lower layer conforms to 3GPP TS 25.410 [5], 3GPP TS 25.411 [6], 3GPP TS 25.414 [7], 3GPP TS 25.415 [8] and 3GPP TS 43.051 [29]. Iu mode specification assumes ATM for lower layer protocol. When there is no data to be sent, no transmission is available on ATM. In consideration of transmission efficiency, no transmission is suitable. RLP acts as follows in case of DTX.

In case DTX is invoked, in ADM and ABM no frame will be sent.

6 Service definitions

6.1 Introduction

This subclause defines the service provided by the RLP-sublayer to the L2R-sublayer at the boundary between the RLP-sublayer and the L2R-sublayer.

The relationships between RLP-sublayer, L2R-sublayer and RLP-protocol are shown in figure 4.

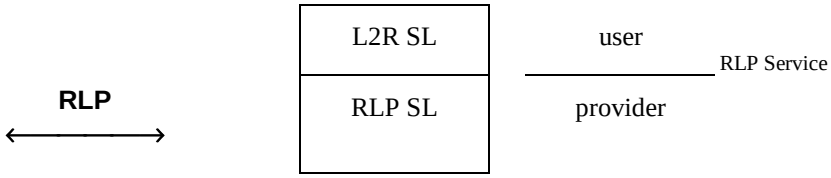


Figure 4: Basic relationship between RLP and L2R

The RLP service is defined in terms of:

- the primitive actions and events of the service;
- the parameters associated with each primitive action and event;
- the inter-relationship between, and the valid sequence of, these actions and events.

6.2 Conventions

For the description of the Data Link Service, the following conventions are used with time-sequence diagrams:

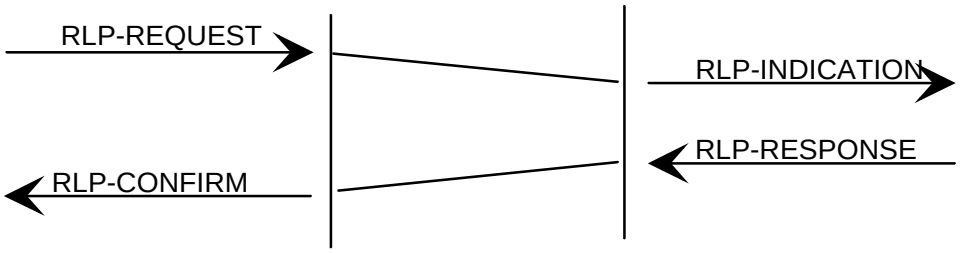


Figure 5: Confirmed service with acknowledgement

Figure 6: Unconfirmed service

In time-sequence diagrams, time moves from top to bottom. Arrows indicate the flow of information. Such flow of information may be subject to implicit flow-control. Skewed lines indicate a logical relationship between arrows. For clarity, the absence of such a relation may be marked by the symbol "~" (tilde).

6.3 Queue model

Between the two endpoints of an RLP-connection, there exists a flow control function. As a means of specifying this flow control feature and its relationship with other capabilities of the RLP, the following queue model is provided.

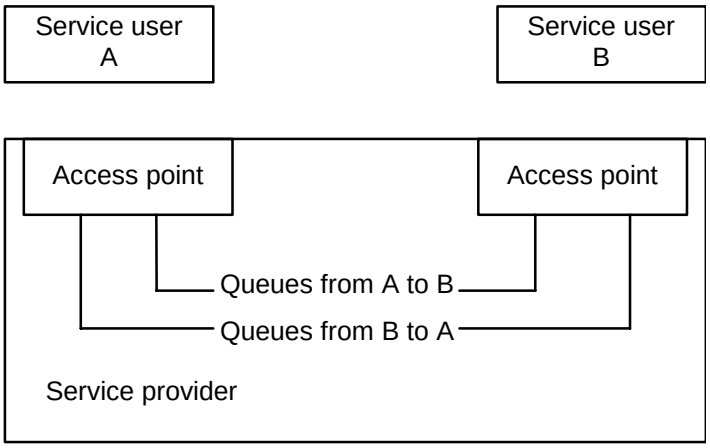


Figure 7: Queue Model

The following objects may be placed in a queue by a service user:

a) connect;

b) connection-mode data (numbered information);

c) reset;

d) disconnect.

The following objects may be placed in a queue by a service provider:

a) reset;

b) synchronization mark;

c) disconnect.

NOTE: Other possible objects (i.e. unnumbered information, identification, test) are irrelevant (-) to the queue model and for reasons of simplicity are not shown.

Following / Preceding	Connect	Data	Reset	Sync Mark	Disconnect
Connect	NA	----	-----	NA	DES
Data	NA	----	DES	NA	DES
Reset	NA	----	DES	----	DES
Synchronization Mark	NA	----	DES	NA	DES
Disconnect	NA	NA	NA	NA	DES
Legend: NA: Not applicable. --: not destructive, not able to advance ahead of the preceding object. DES: Destructive to the preceding object.					

6.4 List of Primitives

Link establishment:

RLP-CONNECT-REQUEST

RLP-CONNECT-INDICATION

RLP-CONNECT-RESPONSE (-NEG)

RLP-CONNECT-CONFIRM (-NEG)

Normal Data Transfer:

RLP-DATA-REQUEST (S, INF)

RLP-DATA-INDICATION (S, INF)

NOTE: The parameter S (L2R status bit) is only relevant for RLP-version 2.

Reset:

RLP-RESET-REQUEST

RLP-RESET-INDICATION

RLP-RESET-RESPONSE

RLP-RESET-CONFIRM

Release:

RLP-DISCONNECT-REQUEST

RLP-DISCONNECT-INDICATION

Miscellaneous:

unnumbered information

RLP-UNITDATA-REQUEST (INF)

RLP-UNITDATA-INDICATION (INF)

Exchange Identification:

RLP-XIDDATA-REQUEST (INF)

RLP-XIDDATA-INDICATION (INF)

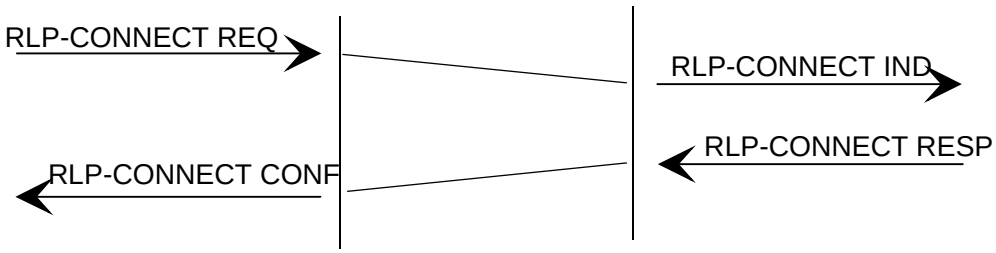
Test:

RLP-TESTDATA-REQUEST (INF)

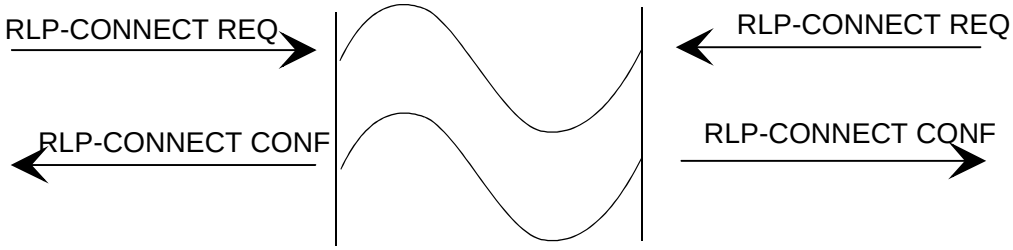
RLP-TESTDATA-CONFIRM (-NEG) (INF)

6.5 Possible RLP time sequence diagrams

a) Connection establishment (without collision)

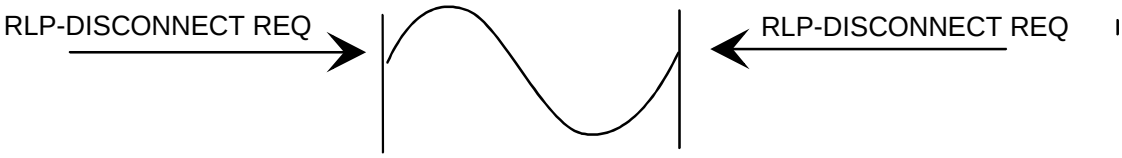


b) Connection establishment (with collision)

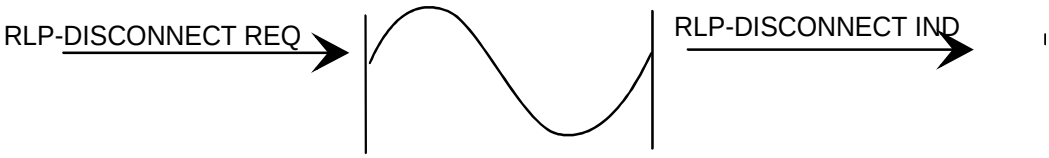


c) User invoked release (without collision)

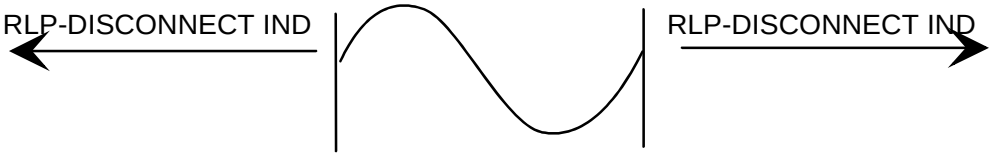
d) Collision of user invoked releases



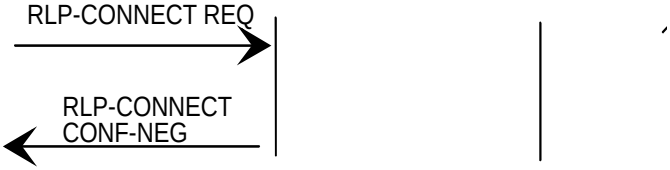
e) Simultaneous user and provider invoked release



f) Provider invoked release

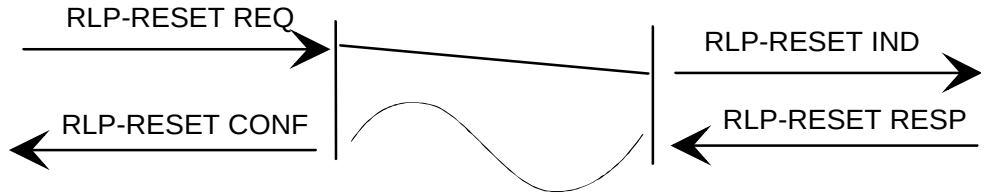


g) Provider rejection of establishment

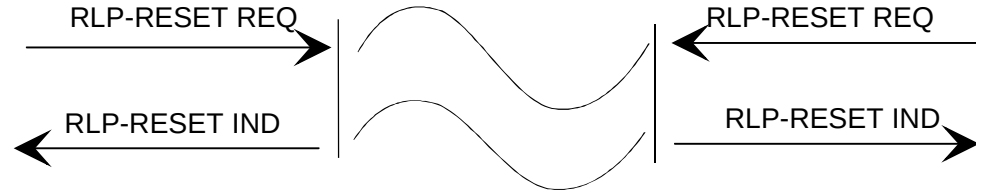


h) Normal data transfer

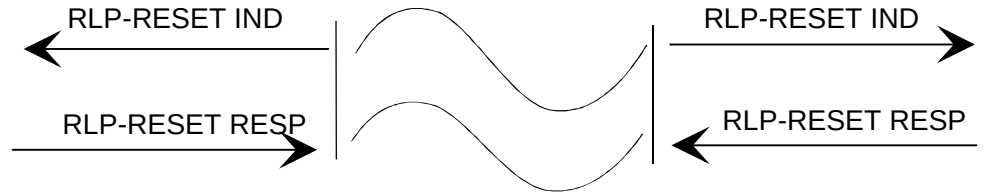
I) User invoked reset



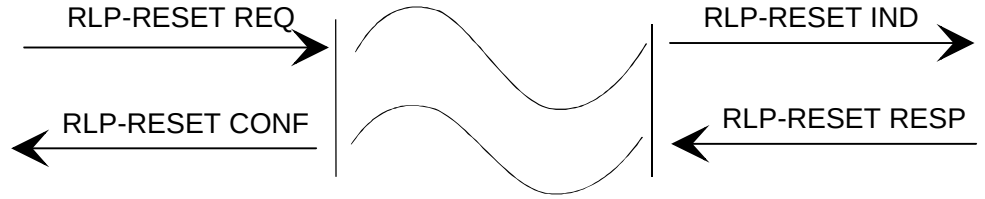
j) Collision of user invoked resets



k) provider invoked reset



l) simultaneous user and provider invoked reset



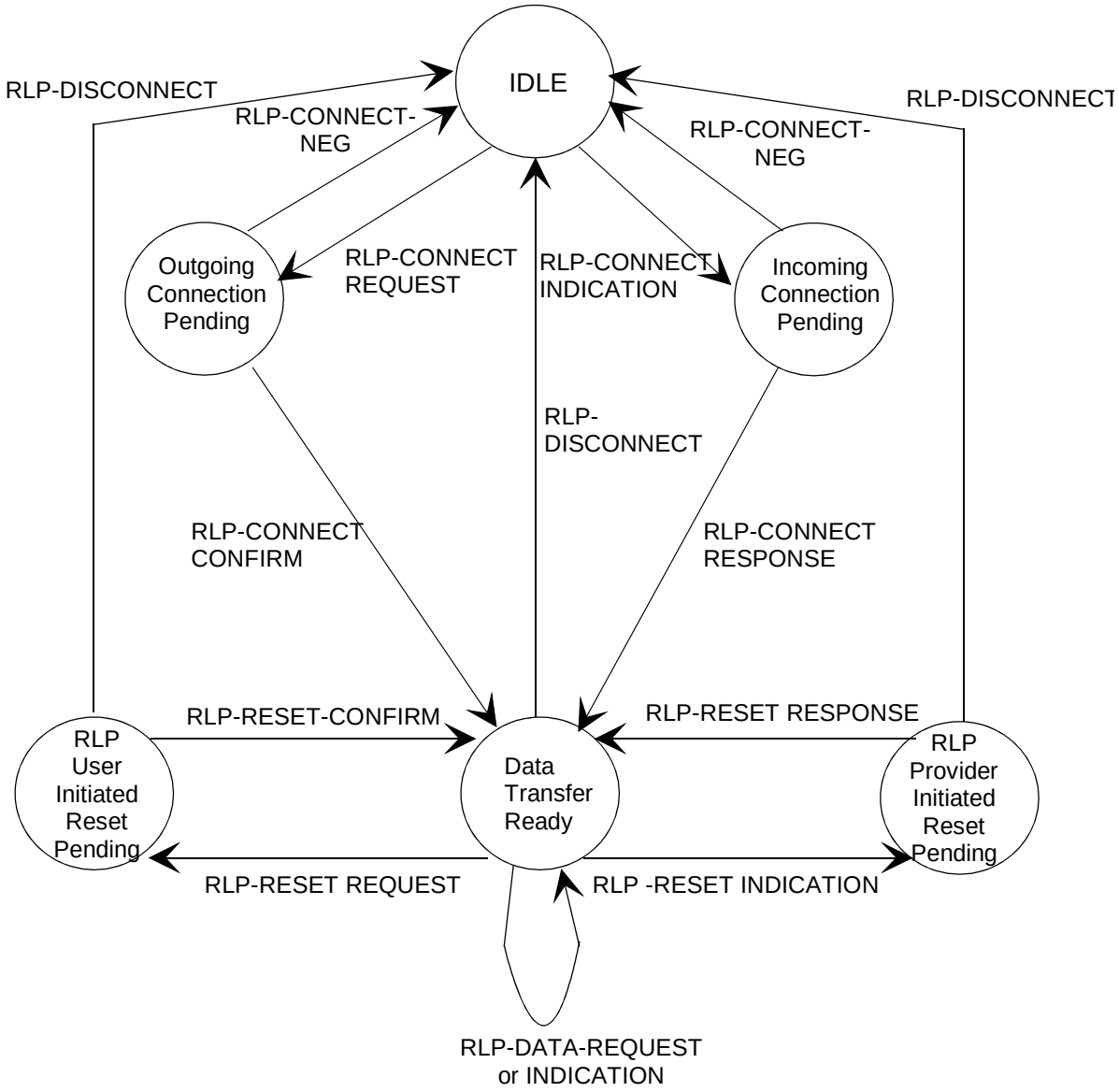


Figure 8: State transition diagram for sequence of RLP connection-mode service primitives

Annex A (informative): RLP SDL Diagrams

This annex describes a model implementation of an RLP entity for RLP version "0".

The description should help to clarify ~~this Specification~~the present document, the RLP service and protocol definition.

However, it is not intended to restrict any implementation of an RLP entity in any way, on condition the implementation shows the correct behaviour at the RLP protocol level.

The model implementation consists of three processes. Process "SEND_PDU" adds the CRC to a given PDU and hands it to the lower layer entity for transmission. Process "RECEIVE_PDU" gets a received PDU block, checks the value of the CRC and the bits of the PDU header. If the CRC has the right value and if the header is syntactically correct, the receipt event is signalled to the "RLP_KERNEL" process, which is the protocol handling automaton.

Each process is described as an extended finite state machine (using SDL-Diagrams).

Each state of the automaton is described by a (main-)state number and a corresponding (main-)state name. The state may further be distinguished by the value of other state variables. This scheme is used because not every state variable needs to be defined in every state. The states are defined in clause A.1.

The RLP machine reacts on events, which may be classified as:

- lower layer interface events;
- upper layer interface events; and
- station management or internal events.

The events of the RLP-Kernel are described in clause A.2.

A.1 List of RLP entity states

A.1.1 (main) states

state number	state symbol	state name
–0	S0	ADM and Detached
–1	S1	ADM and Attached
–2	S2	Pending Connect Request
–3	S3	Pending Connect Indication
–4	S4	ABM and Connection Established
–5	S5	Disconnect Initiated
–6	S6	Pending Reset Request
–7	S7	Pending Reset Indication

A.1.2 state variables

The main states are further distinguished by the values of the state variables. However, not every state variable is used (evaluated/ defined) in every state.

First some constants need to be defined:

M = 62 number of different sequence numbers (modulus).

Nmin = 0 smallest sequence number.

Nmax = 61 largest sequence number (= M - 1).

N2 = 6 maximum number of retransmissions.

variable name	variable type and range	semantic
Ackn_FBit	(0, 1)	Value of the F-Bit used in the next acknowledging PDU.
Ackn_State	(idle, send)	Ackn_State = send means, an acknowledging PDU (Supervisory or Data) has to be sent.
C	(0, 1)	to store the C/R-Bit value of a received S- or I-frames
Data	char[25]	to store temporarily the information part (user data) of a received I-frame.
DISC_Count	(0, 1,..., N2)	to count the transmissions of DISC.
DISC_PBit	(0, 1)	The value of the P-bit in the next DISC command PDU.
DISC_State	(idle, send, wait)	if (DISC_State = send) the DISC command PDU has to be sent at the next possible opportunity.
		if (DISC_State = wait) the RLP entity waits for the corresponding response.
DM_FBit	(0, 1)	Value of the F-Bit used in the next DM response PDU.
DM_State	(idle, send)	if (DM_State = send) the PDU DM has to be sent.
DTX_SF	(N, RR, RNR)	to store the last Supervisory frame for DTX (only RR or RNR can be suppressed)
DTX_VR	(0, 1,.., Nmax)	to store the last transmitted value of VR (used to decide the DTX condition)
F	(0, 1)	to store temporarily the F-bit of a received response PDU.
NR	(0, 1,..., Nmax)	to store temporarily the receive sequence number of a received S- or I-frame
NS	(0, 1,..., Nmax)	to store temporarily the send sequence number of a received I-frame
P	(0, 1)	to store temporarily the P-bit of a received command PDU
P_F	(0, 1)	to store temporarily the P- or F-bit of received command or response PDUs
Poll_Count	(0, 1,..., N2)	to count the transmissions of poll requests
Poll_State	(idle, send, wait)	(Poll_State = send) means, a supervisory PDU with P-bit set to one has to be sent
		(Poll_State = wait) means, the RLP entity waits for the response with F-bit set to one
Poll_xchg	(idle, wait)	(Poll_xchg = idle) means, sending of a frame with P-bit set is allowed
		(Poll_xchg = wait) means, an acknowledgement of a previous P-bit is outstanding
R[M]	record array	Receiver slots (M slots, numbered 0 to M-1)
R[n].Data	char[25]	to store user information
R[n].State	(idle, rcvd, ackn, srej, wait)	(R[n].State = rcvd) means, data has been received (with sequence number n).
		(R[n].State = ackn) means, data has been received and acknowledged
		(R[n].State = srej) means, the retransmission of data has to be requested using srej(n).
		(R[n].State = wait) means, the entity waits for the requested retransmitted data
REJ_State	(idle, send, wait)	The REJ_State is send if and only if a REJ PDU has to be sent
returncode	Integer	used in procedures to report a result
RRReady	Boolean	Remote Receiver Ready

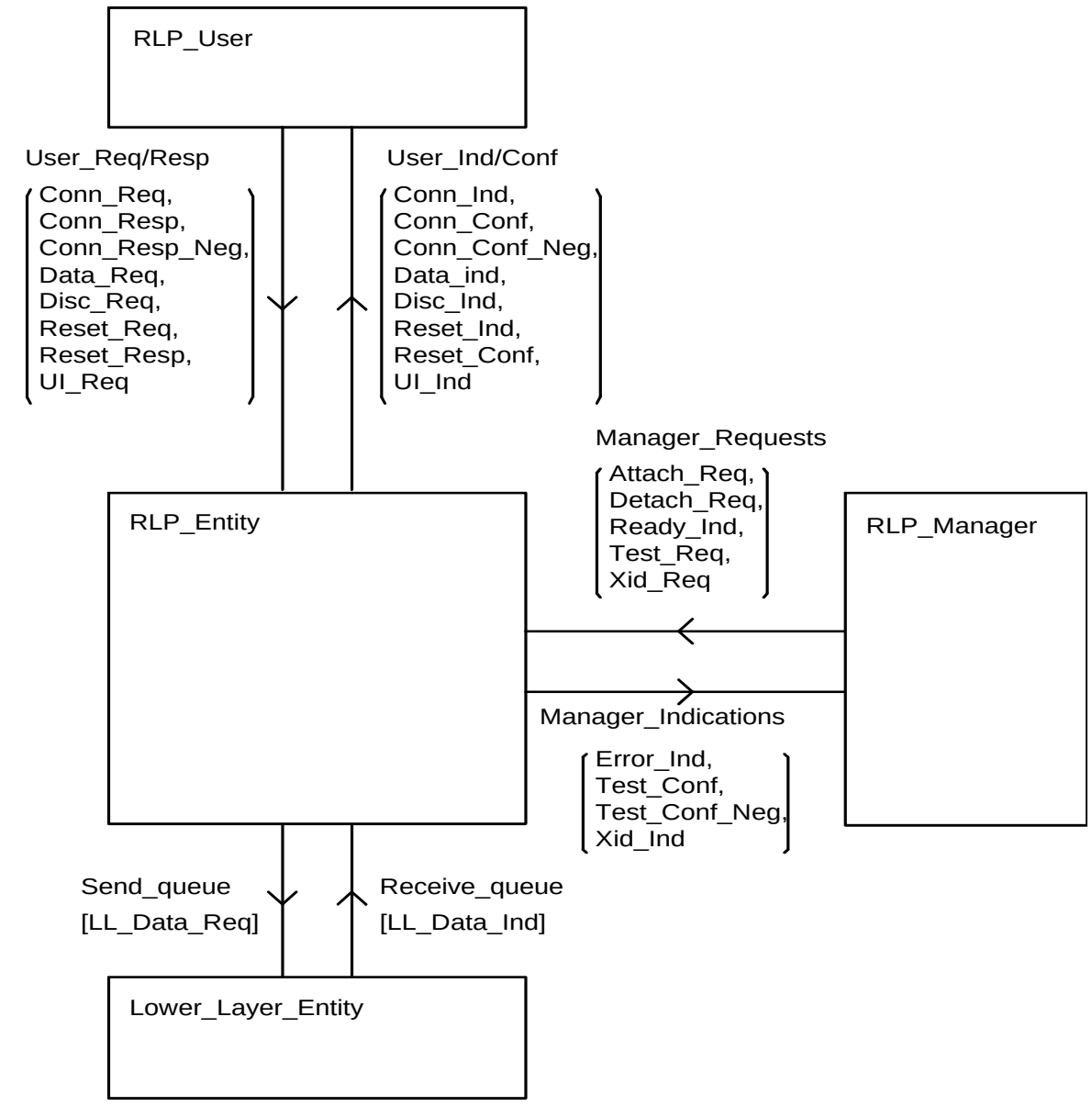
variable name	variable type and range	semantic
SABM_Count	(0, 1,..., N2)	to count the transmissions of SABM
SABM_State	(idle, send, wait)	if (.._State = send) the SABM PDU has to be sent if (.._State = wait) the RLP entity waits for the UA response
S[M]	record array	Sender Slots (M slots, numbered 0 to M-1)
S[n].Data	char[25]	user information to be sent
S[n].State	(idle, send, wait)	(S[n].State = send) means, data has to be sent (with sequence# n).
SF	(RR, RNR, REJ, SREJ)	to store the last superv. PDU type
T	Timer	used by the data sender if waiting for I-frame acknowledgements or F-bits
TEST_Count	(0, 1,...,N2)	to count the transmissions of TEST
TEST_C_Data	char [25]	data to be sent in the next TEST command PDU
TEST_C_PBit	(0, 1)	value of the P-Bit used in the next TEST command PDU
TEST_C_State	(idle, send, wait)	if (.._State = send) the TEST command PDU has to be sent if (.._State = wait) the RLP entity waits for the next TEST response
TEST_R_Data	char[25]	data to be sent in the next TEST response PDU
TEST_R_FBit	(0, 1)	value of the P-Bit used in the next TEST response PDU
TEST_R_State	(idle, send)	if (.._State = send) the TEST response PDU has to be sent
T_RCVR	Timer	used by the receiver to timeout a REJ condition
T_RCVS(n)	Timer	used by the receiver to timeout a SREJ condition for Slot n
T_TEST	Timer	used by the sender of a TEST frame if waiting for a TEST response
T_XID	Timer	used by the sender of a XID frame if waiting for the XID response
UA_FBit	(0, 1)	value of the F-Bit used in the next UA response
UA_State	(idle, send)	if (UA_State = send) an UA PDU has to be sent
UI_Data	char[25]	data to be sent in the next UI PDU
UI_PBit	(0, 1)	value of the P-Bit used in the next UI PDU
UI_State	(idle, send)	if (UI_State = send) a UI PDU has to be sent
VA	(0, 1,..., Nmax)	frame sequence number of oldest not yet acknowledged I-frame (if VA = VS then there are no unacknowledged frames)
VD	(0, 1, ..., Nmax)	slot number used in the next Data_Req
VR	(0, 1, ..., Nmax)	receiver sequence number (the next received I-frame is expected to carry this sequence number)
VS	(0, 1, ..., Nmax)	sender sequence number (under normal operating conditions the next I-frame is assigned this number)
XID_Count	(0, 1,...,N2)	to count the transmissions of XID commands
XID_C_Data	char [25]	data to be sent in the next XID command PDU
XID_C_PBit	(0, 1)	value of the P-Bit used in the next XID command PDU
XID_C_State	(idle, send, wait)	if (.._State = send) the XID command PDU has to be sent if (.._State = wait) the RLP entity waits for the next XID response
XID_R_FBit	(0, 1)	value of the P-Bit used in the next XID response PDU
XID_R_State	(idle, send)	if (.._State = send) the XID response PDU has to be sent

A.2 List of RLP entity events

The interface is indicated by l:lower, u:upper and m:management. From the formal definition point of view this distinction of course is unnecessary.

event#	name	semantic	interface
1	Attach_Req	Switch to "ADM and Attached"	m
2	Conn_Ind	Connect indication	u
3	Conn_Conf	Connect confirm	u
4	Conn_Conf_Neg	Connect confirm negative	u
5	Conn_Req	Connect request	u
6	Conn_Resp	Connect response	u
7	Conn_Resp_Neg	Connect response negative	u
8	Data_Ind(Data)	Data transfer indication (user data in Data)	u
9	Data_Req(Data)	Data transfer request (user data in Data)	u
10	Detach_Req	Switch to "ADM and Detached"	m
11	Disc_Ind	Disconnection indication	u
12	Disc_Req	Disconnect request	u
13	DISC(P)	PDU DISC received (P-bit in P)	l
14	DM(F)	PDU DM received (F-bit in F)	l
15	Error_Ind	Error Indication	u
16	LL_Data_Req	Data request to lower layer	l
17	LL_Data_Ind	Data indication from lower layer	l
18	NULL	PDU NULL received	l
19	Ready_Ind	Indication that a new PDU may be sent	m
20	Reset_Conf	Reset confirm	u
21	Reset_Ind	Reset indication	u
22	Reset_Req	Reset request	u
23	Reset_Resp	Reset response	u
24	RR_I(C, P_F, NR, NS, Data)	I-frame RR received	l
25	RNR_I(C, P_F, NR, NS, Data)	I-frame RNR received	l
26	REJ_I(C, P_F, NR, NS, Data)	I-frame REJ received	l
27	SREJ_I(C, P_F, NR, NS, Data)	I-frame SREJ received	l
28	RR(C, P_F, NR)	S-frame RR received	l
29	RNR(C, P_F, NR)	S-frame RNR received	l
30	REJ(C, P_F, NR)	S-frame REJ received	l
31	SREJ(C, P_F, NR)	S-frame SREJ received	l
32	SABM(P)	PDU SABM received	l
33	UA(F)	PDU UA received (F-bit in F)	l
34	UI_Req(Data)	Unnumbered Information transfer request	u
35	UI(C, P_F, Data)	UI PDU received	l
36	T	Timeout (Timer of the sender expired)	m
37	Test_Conf(Data)	Test confirm (received data in Data)	u
38	Test_Conf_Neg(Data)	Test confirm negative (received data in Data)	u
39	T_RCVR	Timeout (Timer of the receiver for REJ expired)	m
40	T_RCVS(n)	Timeout (Timer of the receiver for SREJ expired)	m
41	T_TEST	Timeout (Test timer expired)	m
42	T_XID	Timeout (Xid timer expired)	m
43	Test_Req(Data)	Test request (Test data in Data)	m
44	TEST(C, P_F, Data)	TEST command/response PDU received (C/R-bit in C, P/F-bit in P_F, Data in Data)	l
45	XID_Req(Data)	Exchange ID request	m
46	XID_Ind(Data)	Exchange ID indication	m
47	XID(C, P_F, Data)	XID command/response PDU received	l

System RLP - Overview



0422AF01.DRW 93-03-01

Figure A.1

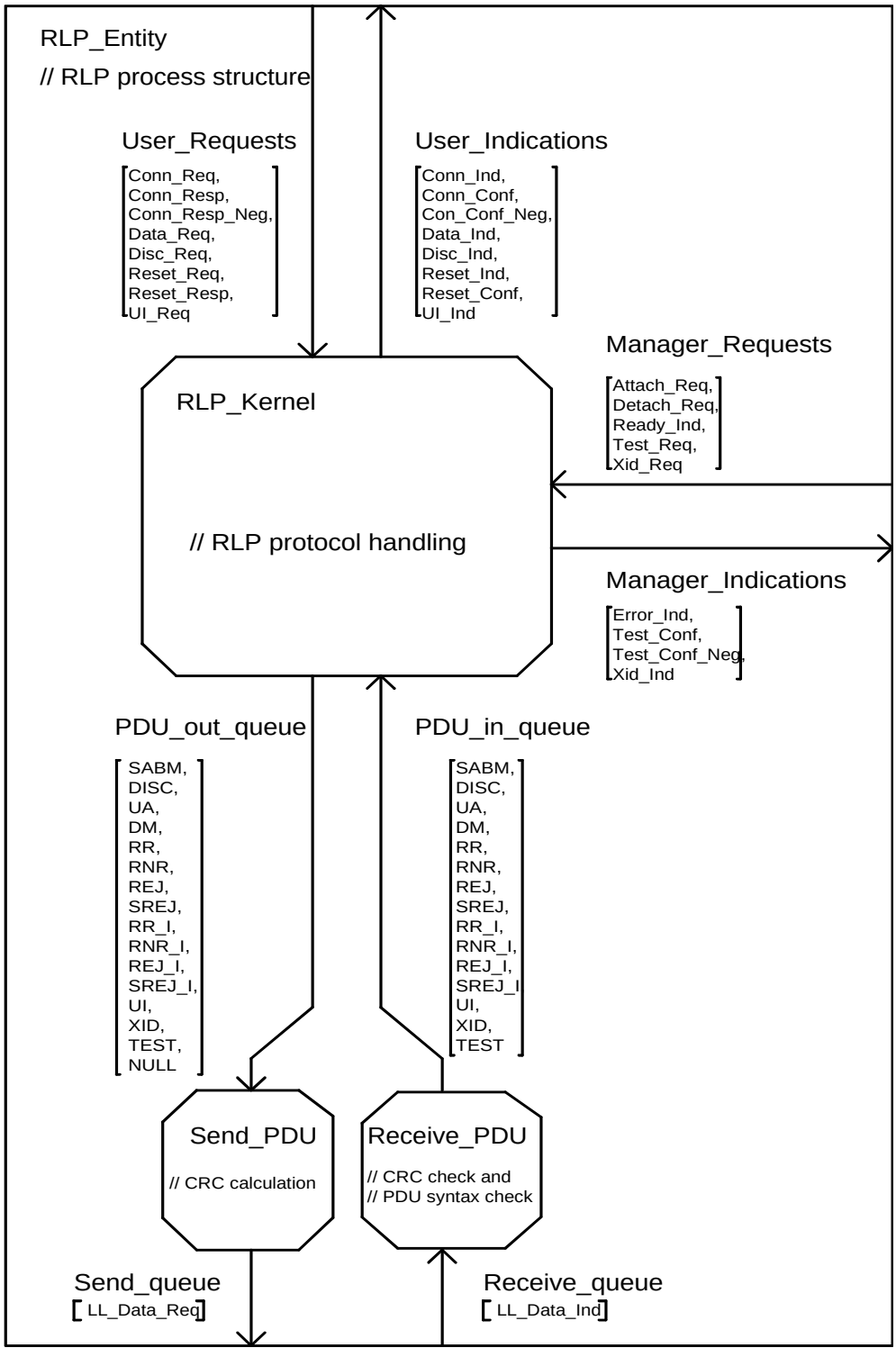

RLP_Entity
// RLP process structure
User_Requests
Conn_Req,
Conn_Resp,
Conn_Resp_Neg,
Data_Req,
Disc_Req,
Reset_Req,
Reset_Resp,
UI_Req
User_Indications
Conn_Ind,
Conn_Conf,
Con_Conf_Neg,
Data_Ind,
Disc_Ind,
Reset_Ind,
Reset_Conf,
UI_Ind
Manager_Requests
Attach_Req,
Detach_Req,
Ready_Ind,
Test_Req,
Xid_Req
RLP_Kernel
// RLP protocol handling
Manager_Indications
Error_Ind,
Test_Conf,
Test_Conf_Neg,
Xid_Ind
PDU_out_queue
SABM,
DISC,
UA,
DM,
RR,
RNR,
REJ,
SREJ,
RR_I,
RNR_I,
REJ_I,
SREJ_I,
UI,
XID,
TEST,
NULL
PDU_in_queue
SABM,
DISC,
UA,
DM,
RR,
RNR,
REJ,
SREJ,
RR_I,
RNR_I,
REJ_I,
SREJ_I
UI,
XID,
TEST
Send_PDU
// CRC calculation
Receive_PDU
// CRC check and
// PDU syntax check
Send_queue
[LL_Data_Req]
Receive_queue
[LL_Data_Ind]
0422AF02.DRW 93-05-25

Figure A.2

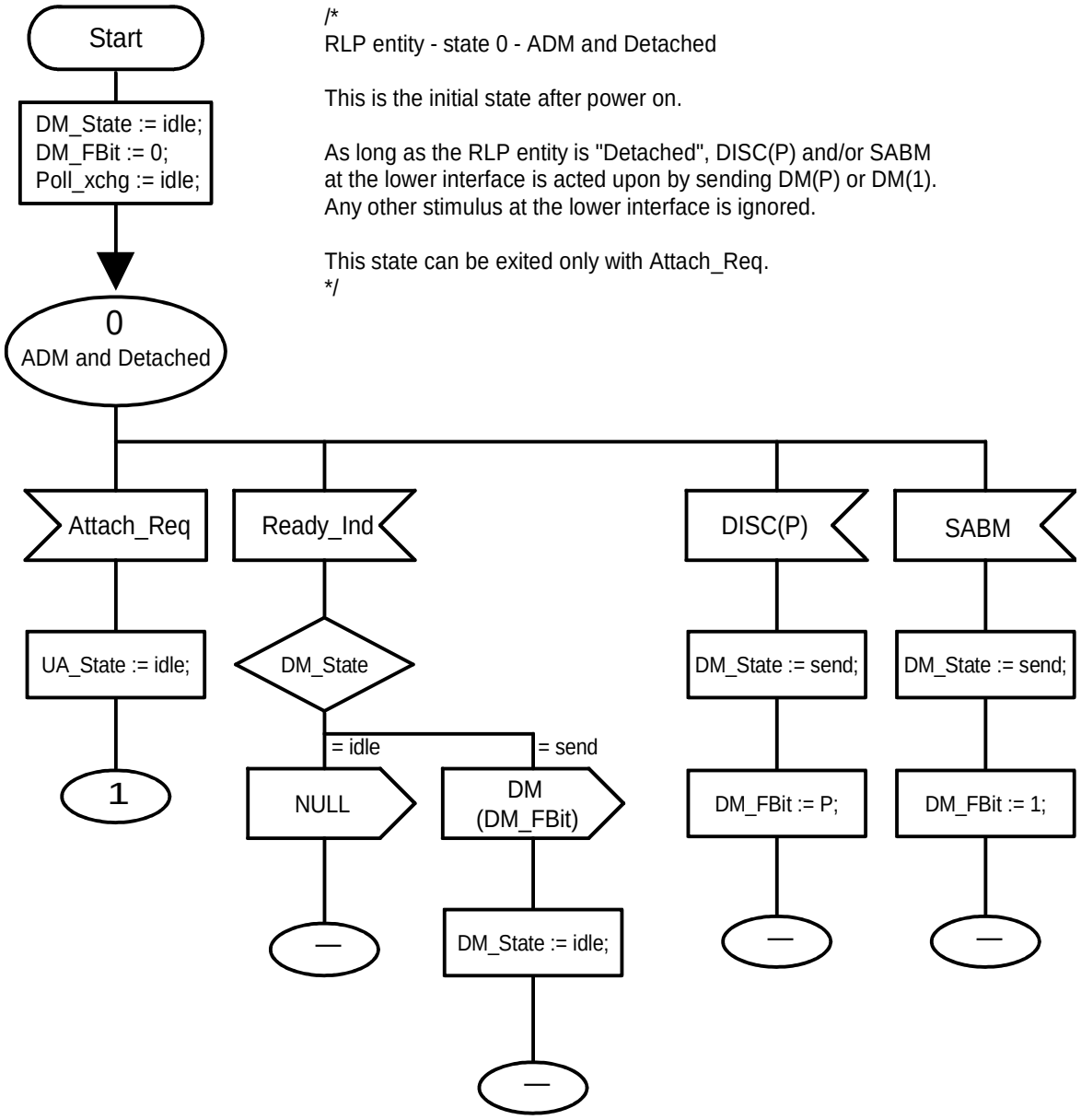

Start
DM_State := idle;
DM_FBit := 0;
Poll_xchg := idle;
0
ADM and Detached
/*
RLP entity - state 0 - ADM and Detached
This is the initial state after power on.
As long as the RLP entity is "Detached", DISC(P) and/or SABM
at the lower interface is acted upon by sending DM(P) or DM(1).
Any other stimulus at the lower interface is ignored.
This state can be exited only with Attach_Req.
*/
Attach_Req
Ready_Ind
DISC(P)
SABM
UA_State := idle;
DM_State
DM_State := send;
DM_State := send;
= idle
= send
1
NULL
DM
(DM_FBit)
DM_FBit := P;
DM_FBit := 1;
—
DM_State := idle;
—
—
—
0422AF03.DRW 93-02-26

Figure A.3

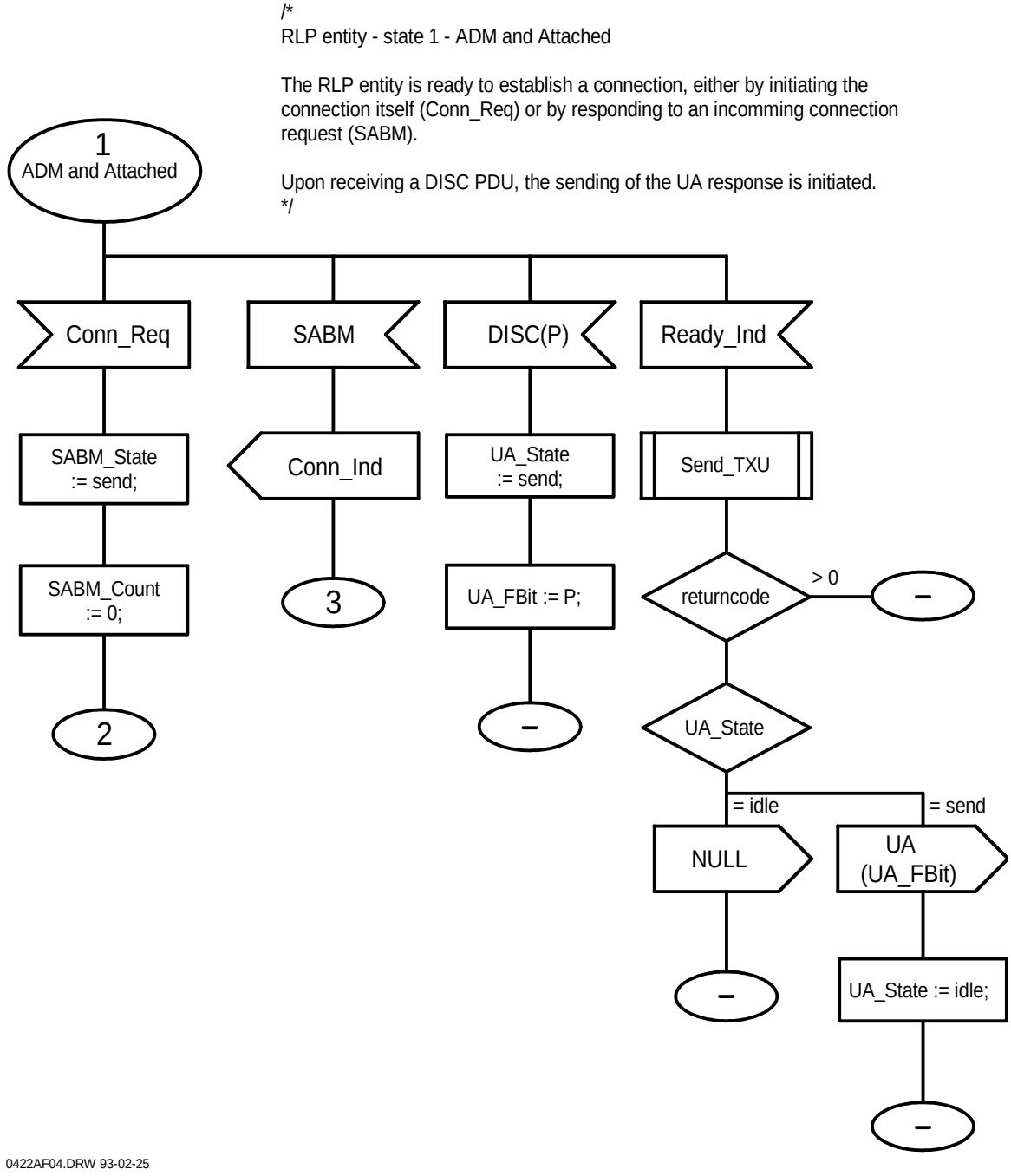

/*
RLP entity - state 1 - ADM and Attached
The RLP entity is ready to establish a connection, either by initiating the connection itself (Conn_Req) or by responding to an incomming connection request (SABM).
Upon receiving a DISC PDU, the sending of the UA response is initiated.
*/
1
ADM and Attached
Conn_Req
SABM
DISC(P)
Ready_Ind
SABM_State := send;
Conn_Ind
UA_State := send;
Send_TXU
SABM_Count := 0;
3
UA_FBit := P;
returncode
> 0
2
UA_State
= idle
= send
NULL
UA (UA_FBit)
UA_State := idle;
0422AF04.DRW 93-02-25

Figure A.4

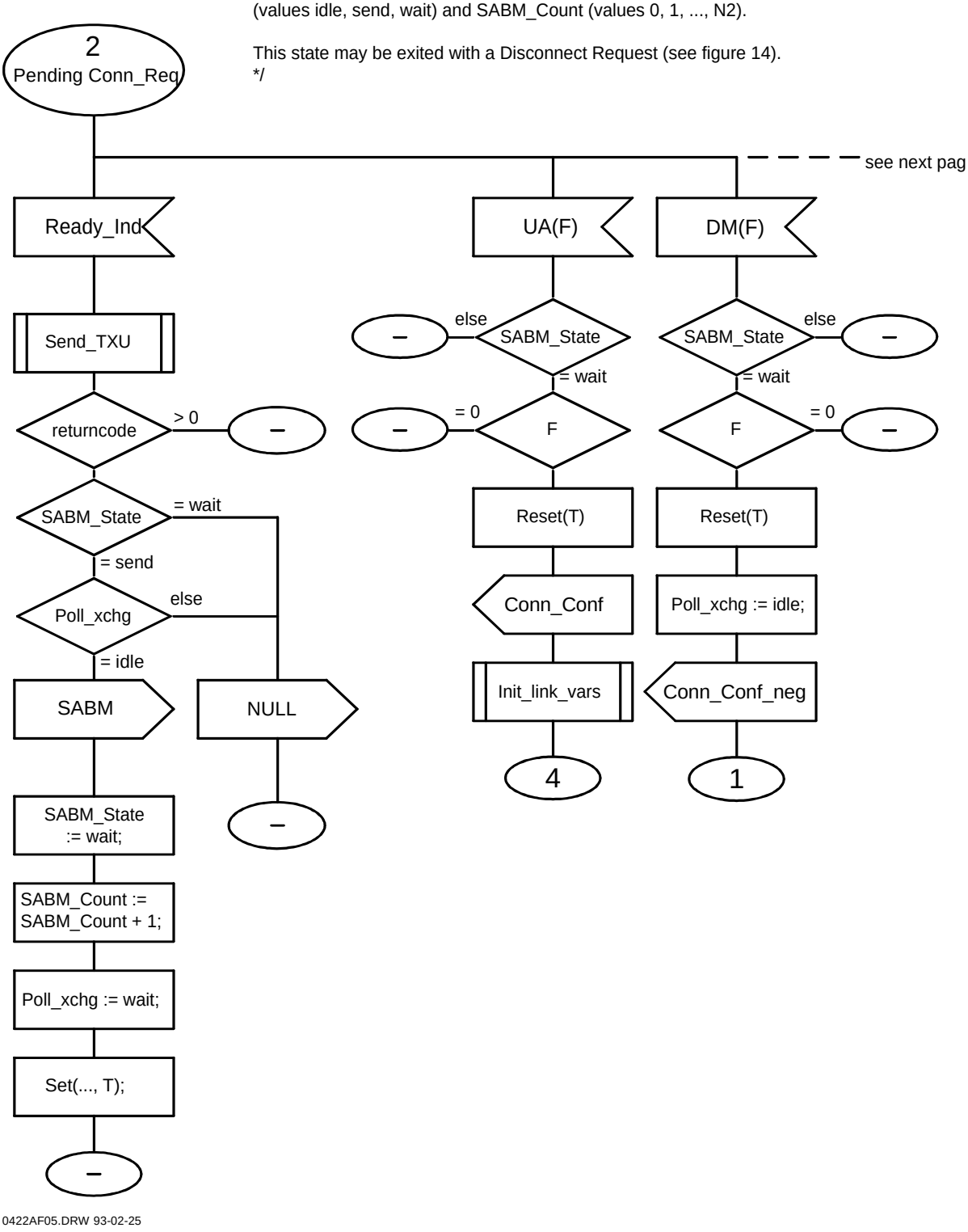

/*
RLP entity - state 2 - Pending connect request
Send (up to N2 repetitions) SABM and wait for the corresponding
UA with FBit = 1.
The (sub)state is controlled by the variable SABM_State
(values idle, send, wait) and SABM_Count (values 0, 1, ..., N2).
This state may be exited with a Disconnect Request (see figure 14).
*/
2
Pending Conn_Req
see next pag
Ready_Ind
Send_TXU
returncode
> 0
SABM_State
= wait
= send
Poll_xchg
else
= idle
SABM
NULL
SABM_State
:= wait;
SABM_Count :=
SABM_Count + 1;
Poll_xchg := wait;
Set(..., T);
UA(F)
else
SABM_State
= wait
= 0
F
Reset(T)
Conn_Conf
Init_link_vars
4
DM(F)
else
SABM_State
= wait
= 0
F
Reset(T)
Poll_xchg := idle;
Conn_Conf_neg
1
0422AF05.DRW 93-02-25

Figure A.5

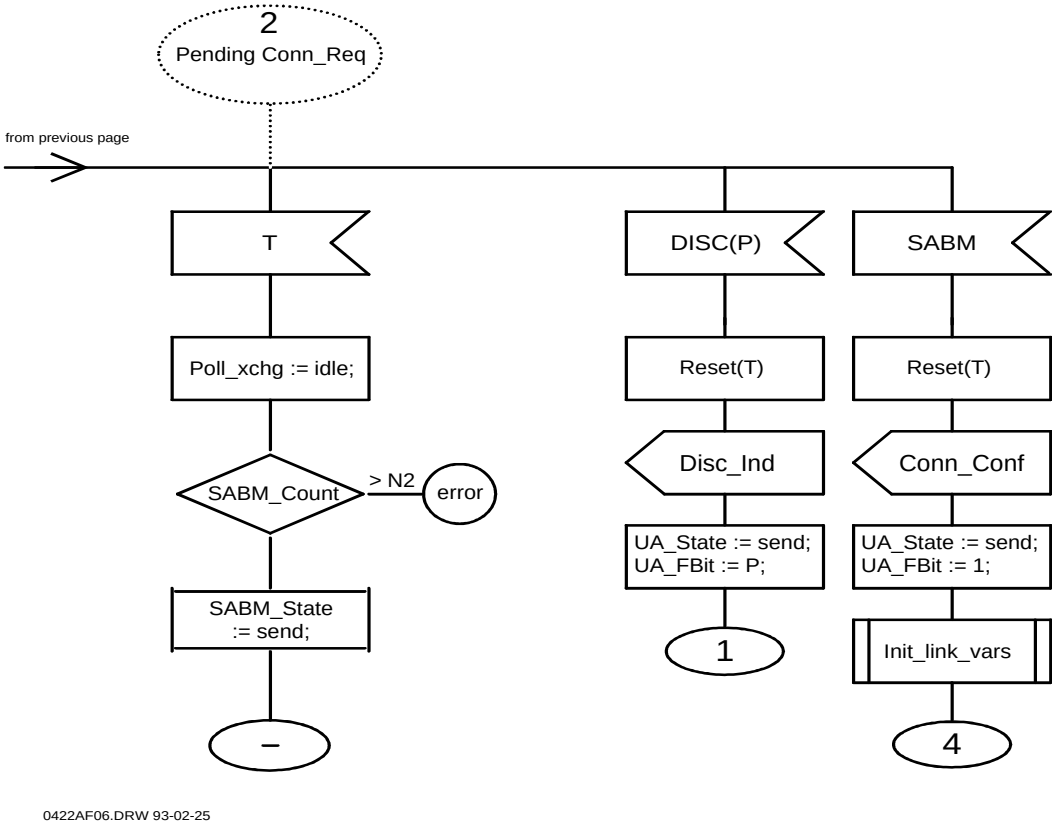

/*
RLP entity - state 2 - Pending connect request
This figure allowes up to N2 repetitions of SABM and
describes the disconnect and the SABM contention case.
*/
2
Pending Conn_Req
from previous page
T
Poll_xchg := idle;
SABM_Count
> N2
error
SABM_State
:= send;
–
DISC(P)
Reset(T)
Disc_Ind
UA_State := send;
UA_FBit := P;
1
SABM
Reset(T)
Conn_Conf
UA_State := send;
UA_FBit := 1;
Init_link_vars
4
0422AF06.DRW 93-02-25

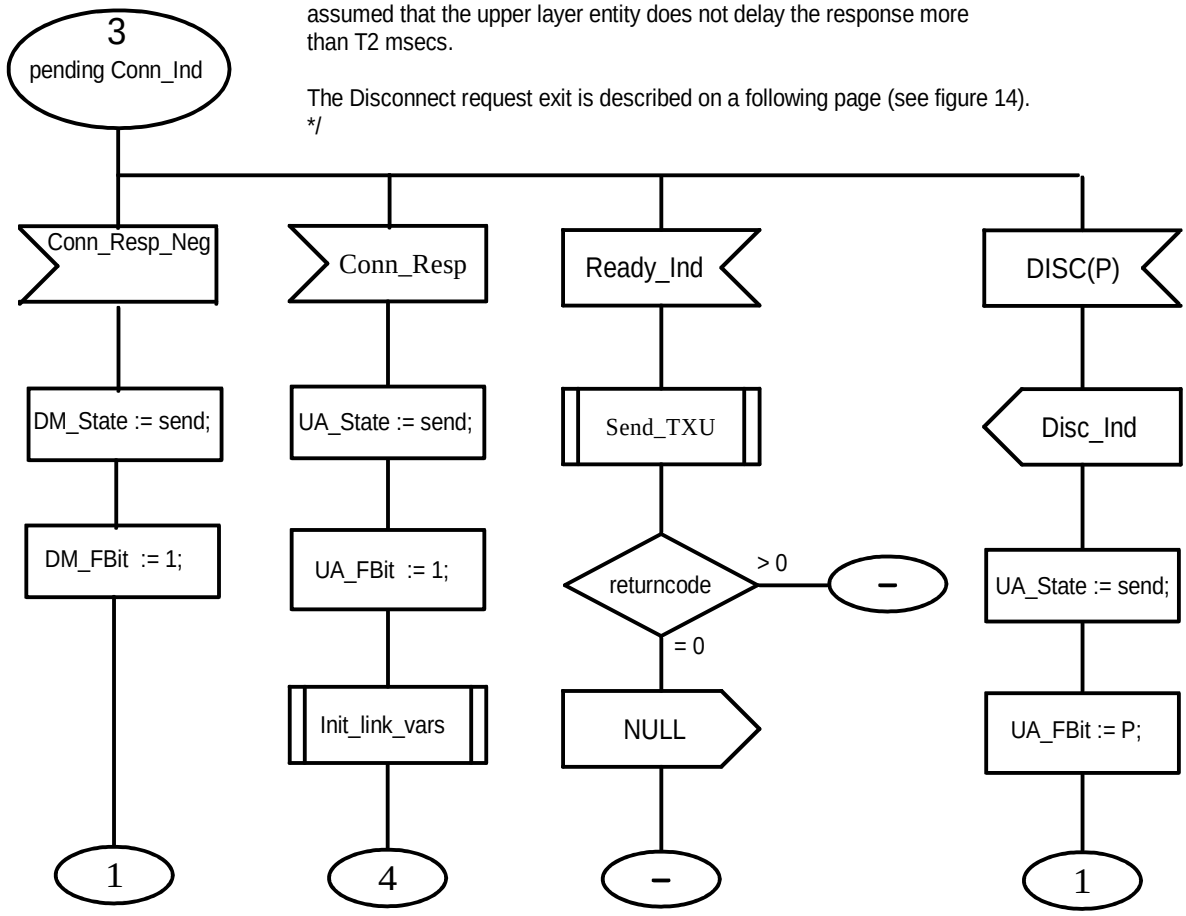
Figure A.6

/*
RLP entity - state 3 - pending Connect indication

After having received SABM, the RLP entity is waiting for the Connect response.

The upper layer entity may respond with Conn_Resp or Disc_Req. It is assumed that the upper layer entity does not delay the response more than T2 msecs.

The Disconnect request exit is described on a following page (see figure 14).
*/



0422AF07.DRW 94-09-15

Figure A.7

/*
RLP entity - state 4 - Connection established

This is the data transfer state. The user entity may transmit data by fireing Data_Requests. However, he is allowed to do so only if there are idle sender slots.

The data stored in the send slots will be transmitted at the next possible opportunity.

This state may be exited by a Disconnect Request (see Figure 14).
*/

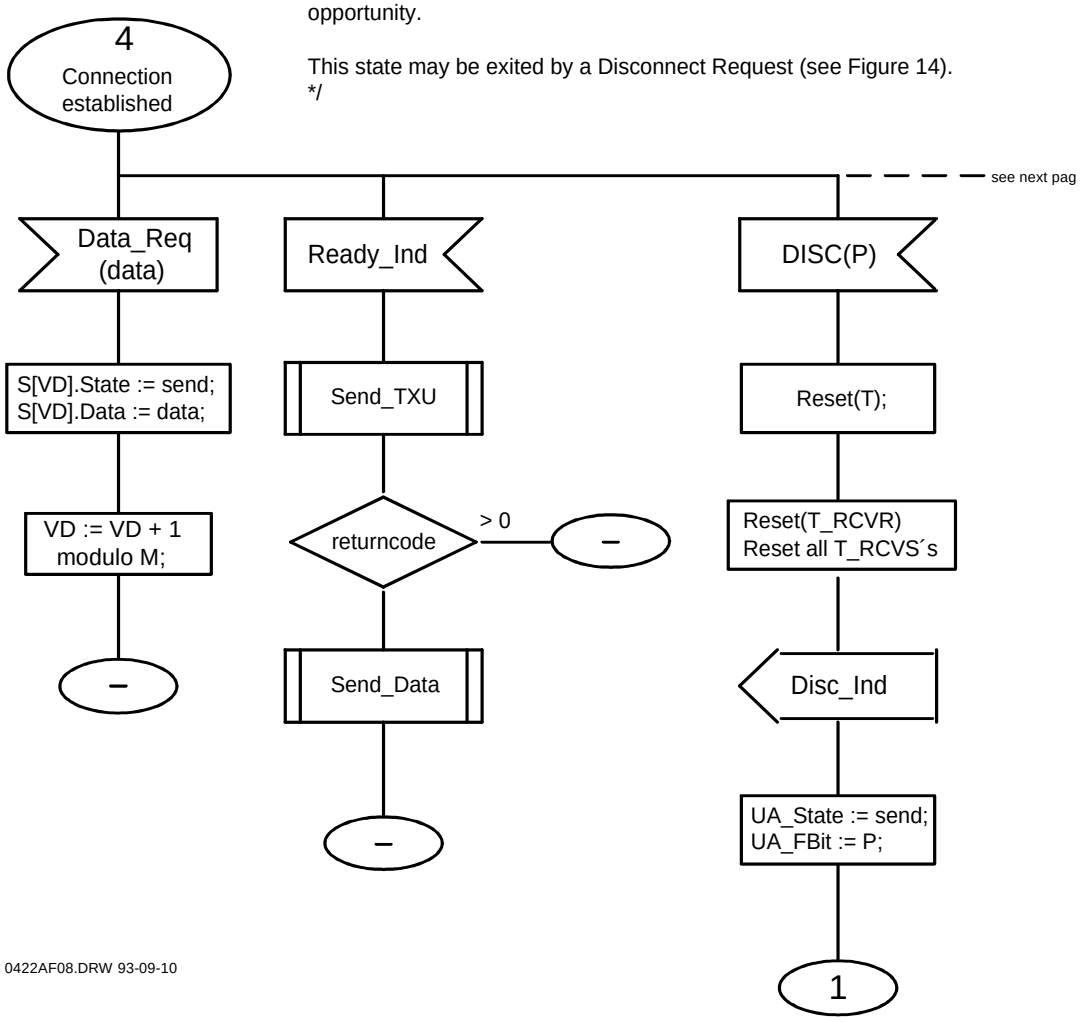


Figure A.8

/*
RLP entity - state 4 - Connection established

This dagram describes RESET and the Timeout-handling.

A timeout leads to error recovery by polling. This is controlled by
the Poll_State variable. The Poll_State transitions are:

idle -> send <-> wait -> idle

Zero up to N2 transitions wait->send may occur.
*/

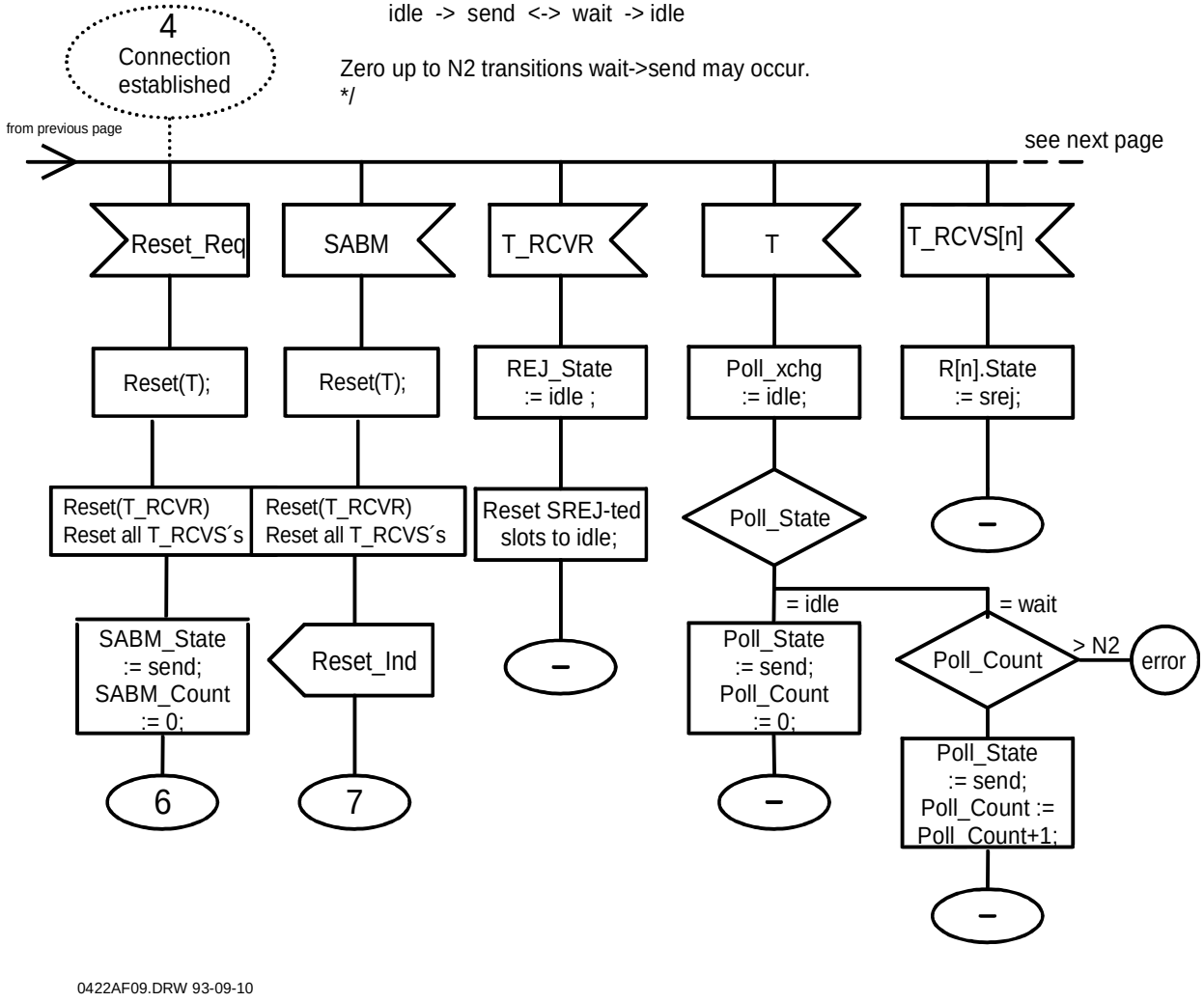


Figure A.9

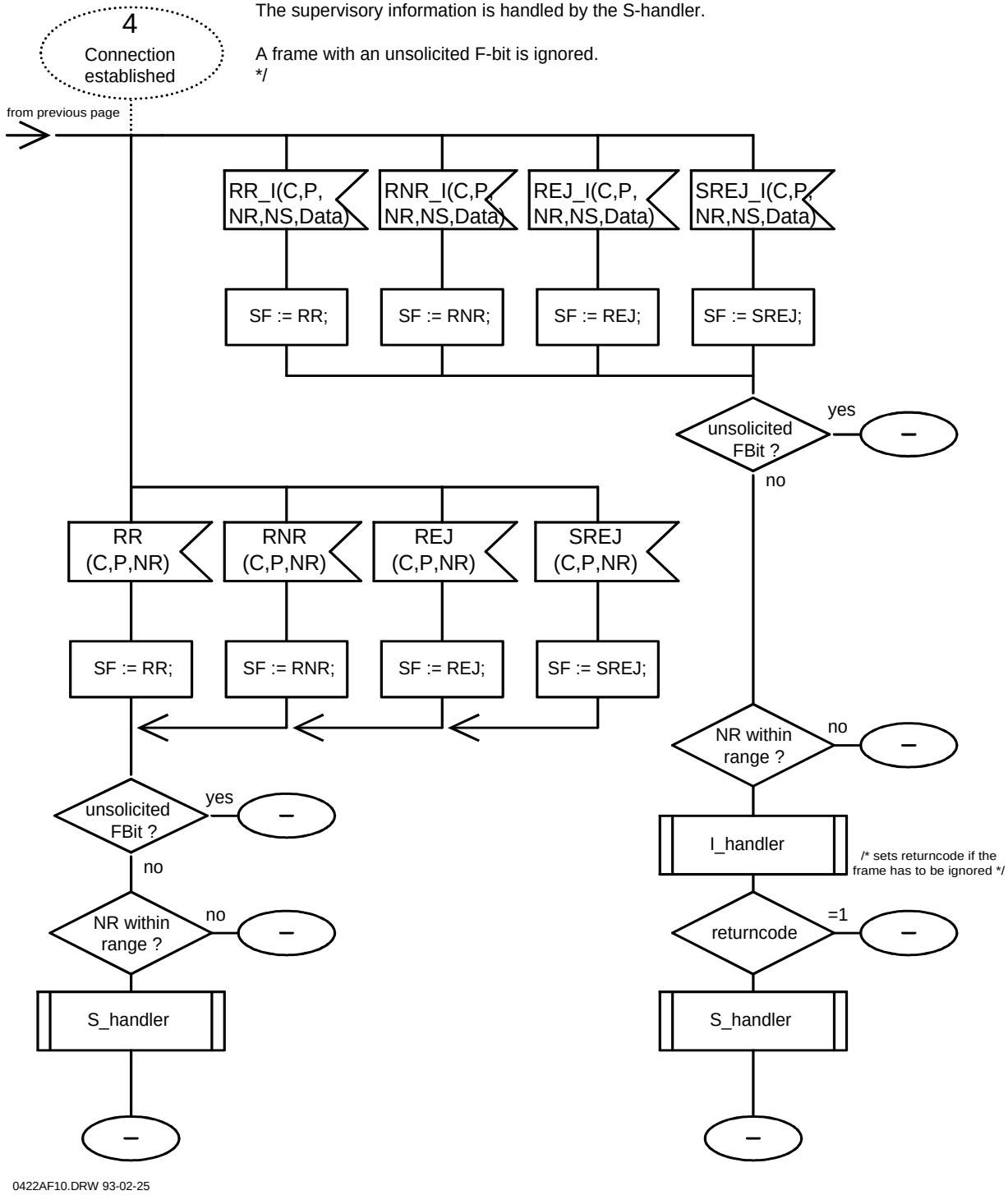

/*
RLP entity - state 4 - Connection established
This diagram describes the handling of I-frames and S-frames
(PDUs RR, RNR, REJ, SREJ and RR_I, RNR_I, REJ_I, SREJ_I).
If the frame contains user information, this is handled by the I-Handler.
The supervisory information is handled by the S-handler.
A frame with an unsolicited F-bit is ignored.
*/
4
Connection established
from previous page
RR_I(C,P, NR,NS,Data)
RNR_I(C,P, NR,NS,Data)
REJ_I(C,P, NR,NS,Data)
SREJ_I(C,P, NR,NS,Data)
SF := RR;
SF := RNR;
SF := REJ;
SF := SREJ;
unsolicited FBit ?
yes
no
RR (C,P,NR)
RNR (C,P,NR)
REJ (C,P,NR)
SREJ (C,P,NR)
SF := RR;
SF := RNR;
SF := REJ;
SF := SREJ;
NR within range ?
no
unsolicited FBit ?
yes
I_handler
/* sets returncode if the frame has to be ignored */
no
NR within range ?
no
returncode
=1
S_handler
S_handler
0422AF10.DRW 93-02-25

Figure A.10

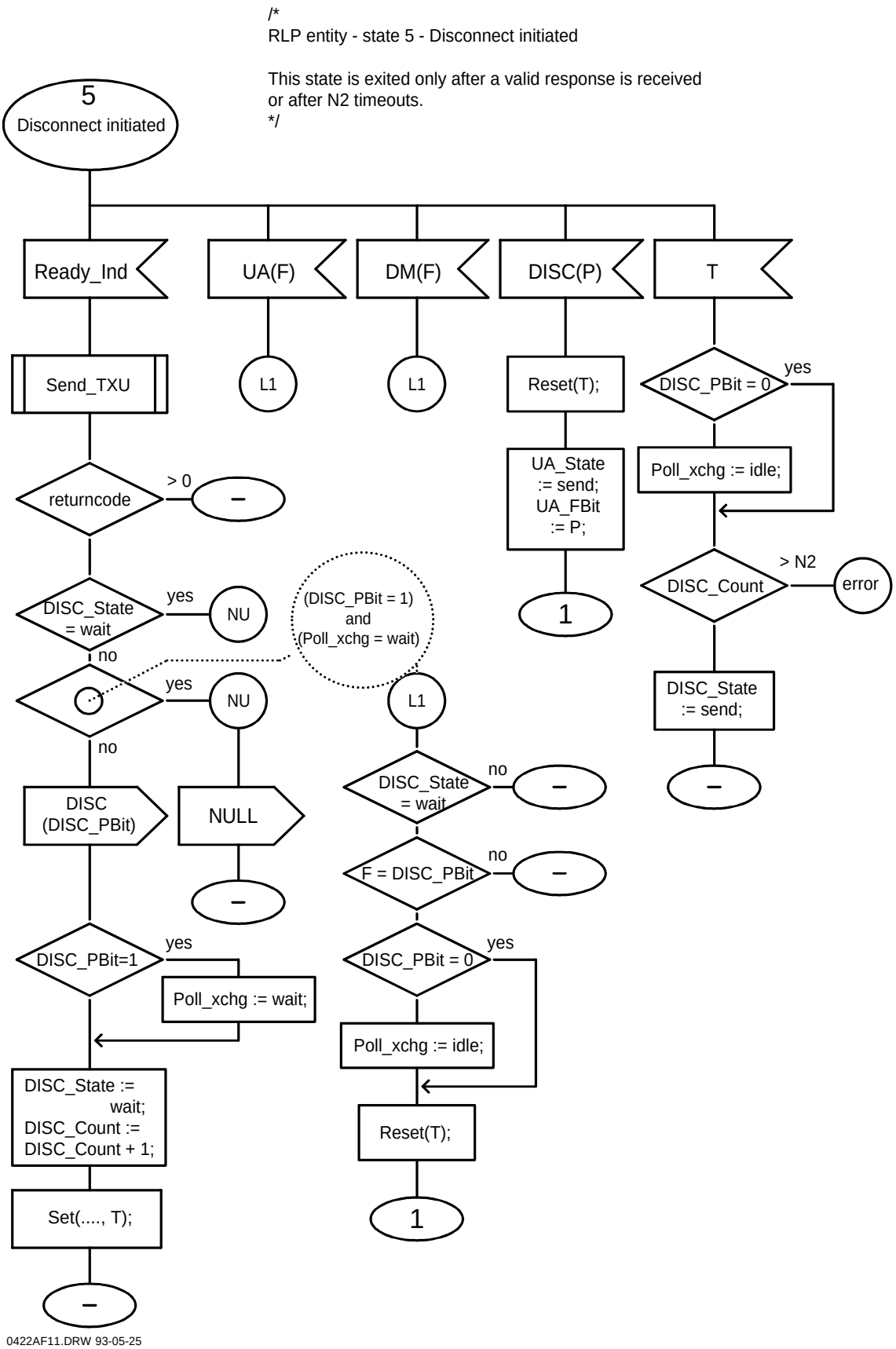

/*
RLP entity - state 5 - Disconnect initiated
This state is exited only after a valid response is received
or after N2 timeouts.
*/
5
Disconnect initiated
Ready_Ind
UA(F)
DM(F)
DISC(P)
T
Send_TXU
L1
L1
Reset(T);
DISC_PBit = 0
yes
UA_State := send; UA_FBit := P;
Poll_xchg := idle;
returncode
> 0
DISC_State = wait
yes
NU
(DISC_PBit = 1) and (Poll_xchg = wait)
DISC_Count
> N2
error
1
no
yes
NU
L1
DISC_State := send;
no
DISC_State = wait
DISC (DISC_PBit)
NULL
F = DISC_PBit
DISC_PBit=1
yes
DISC_PBit = 0
Poll_xchg := wait;
Poll_xchg := idle;
DISC_State := wait;
DISC_Count := DISC_Count + 1;
Reset(T);
Set(...., T);
1
0422AF11.DRW 93-05-25

Figure A.11

/*
RLP entity - state 6 - pending Reset Request

Send (up to N2 repetitions) SABM and wait for the responding UA with FBit=1.

The substate is controlled by the variable SABM_State (values idle, send, wait)
and SABM_Count (values 0..N2).

This state may be exited with a Disconnect Request (see Figure 14).
*/

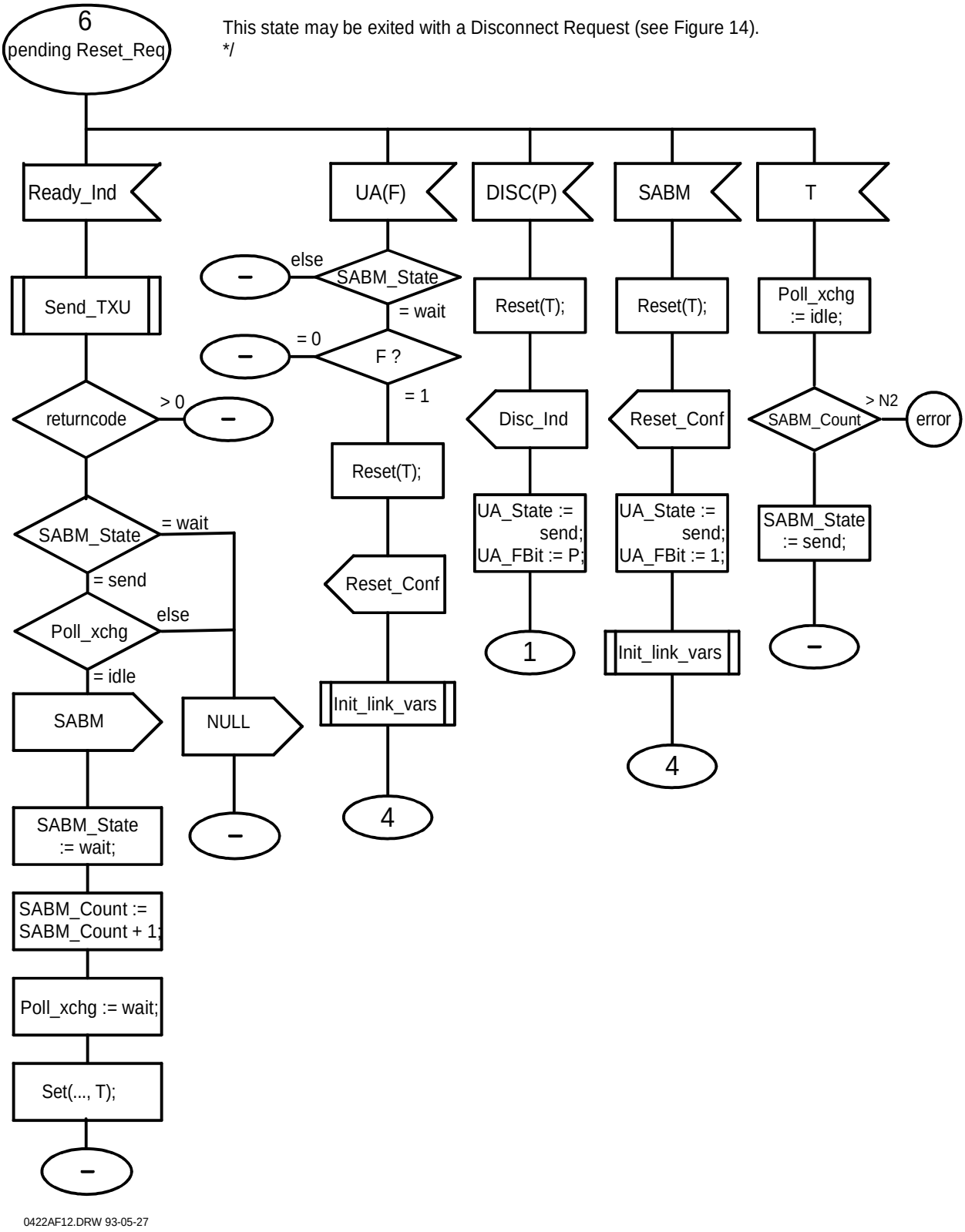


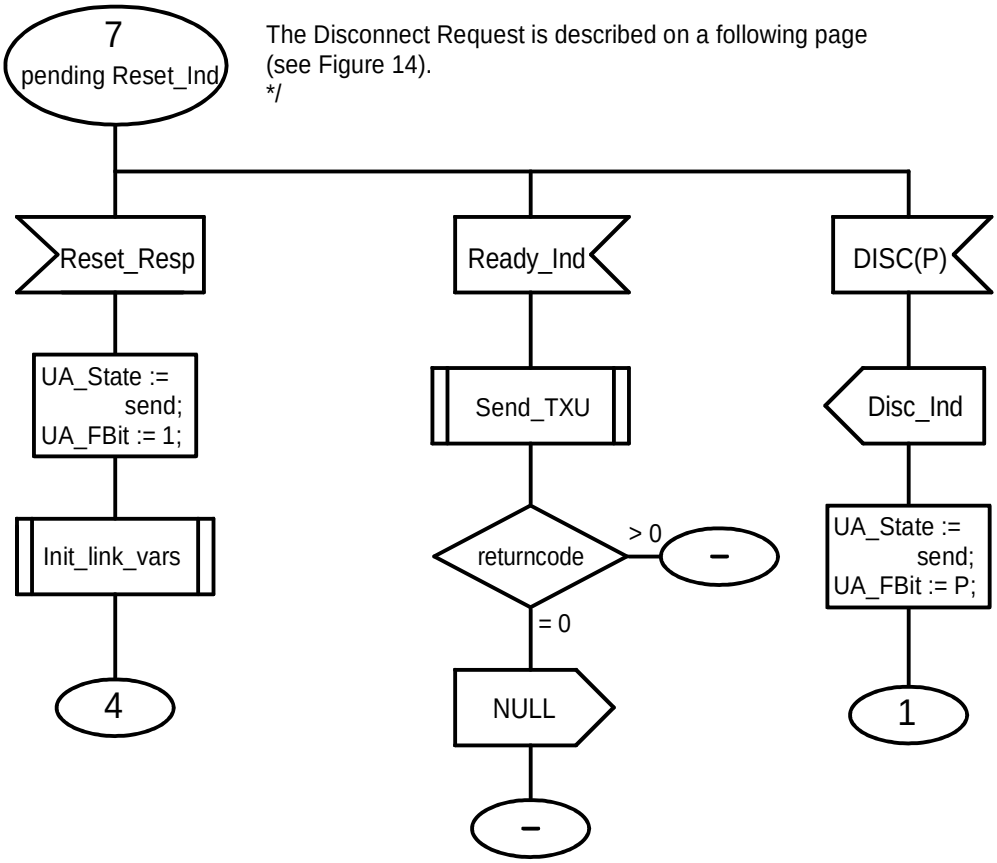
Figure A.12

/*
RLP entity - state 7 - pending Reset Indication

After having received SABM and having indicated Reset, the RLP entity is waiting for the Reset_Response.

The upper layer entity may respond with Reset_Resp or Disc_Req. It is assumed, that the upper layer entity does not delay the response more than T2 msecs.

The Disconnect Request is described on a following page (see Figure 14).
*/



0422AF13.DRW 93-03-01

Figure A.13

/*
This is the error handling
when there is no action
from the remote end
after N2 repetitions.
The error handling
and the state transition
depends on the situation
e.g. ADM in case of DISC
*/

/*
Detach Request

Detach is allowed at
any time.

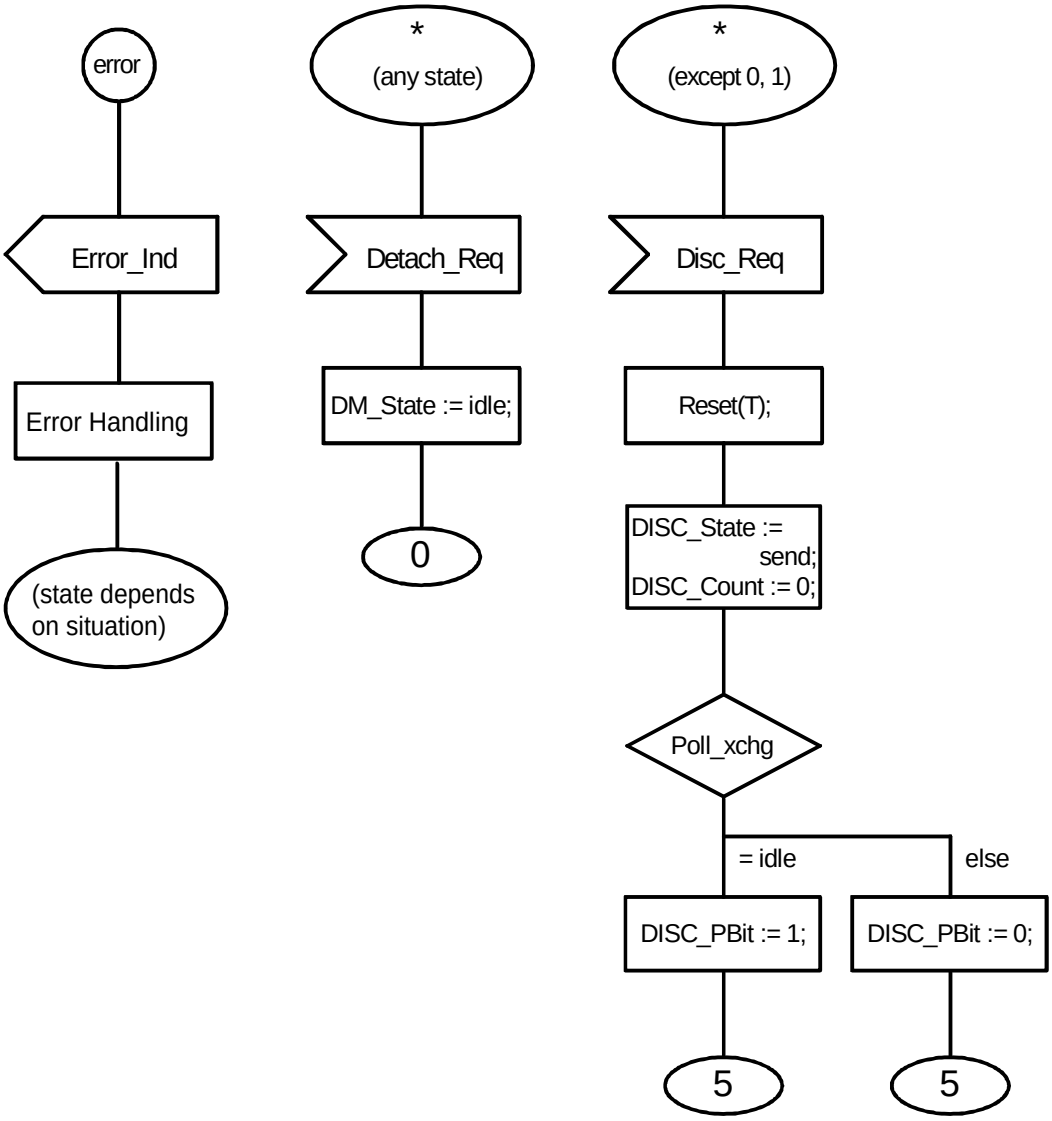
The Detach Request
is used to reset the RLP
entity to state 0, e.g. if
the physical connection
is lost.
*/

/*
Disconnect Request

Disconnect is used to release a connection.

The actions to be executed in these cases are:
reset the timer, activate sending of the DISC PDU.

The P-bit in the DISC command is set to
one or zero, depending on the Poll_xchg state.
*/



0422AF14.DRW 93-02-25

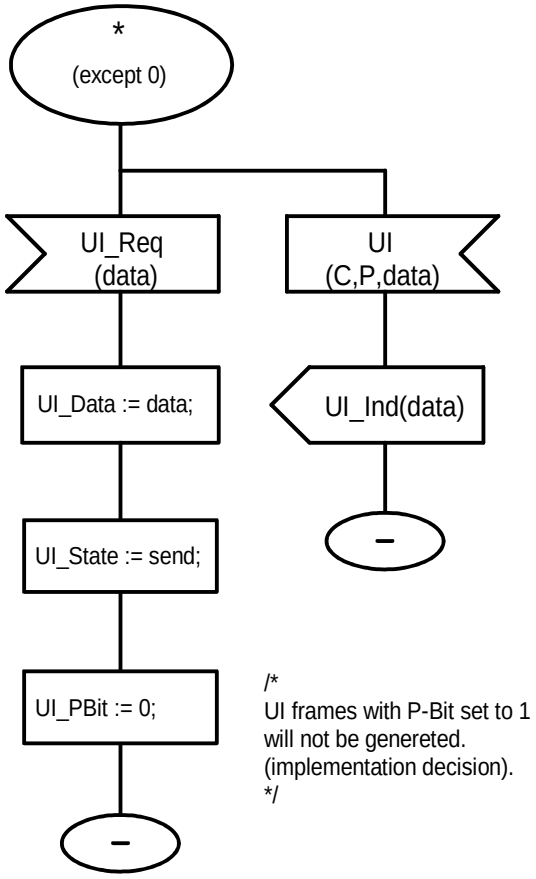
Figure A.14

/*
UI handling (UI_Req, UI)

UI_Requests are controlled using the state variable UI_State. The values (state transitions) are: idle -> send -> idle

It is assumed that the upper layer entity issues an UI_Req only if the RLP entity's UI_State is idle. The UI data is stored in the variable UI_Data.

The UI_PDU is generated at the next possible opportunity, i.e. after the higher priviledged PDUs (TEST PDUs, XID PDUs, if any) have been transmitted.
*/



0422AF15.DRW 93-02-26

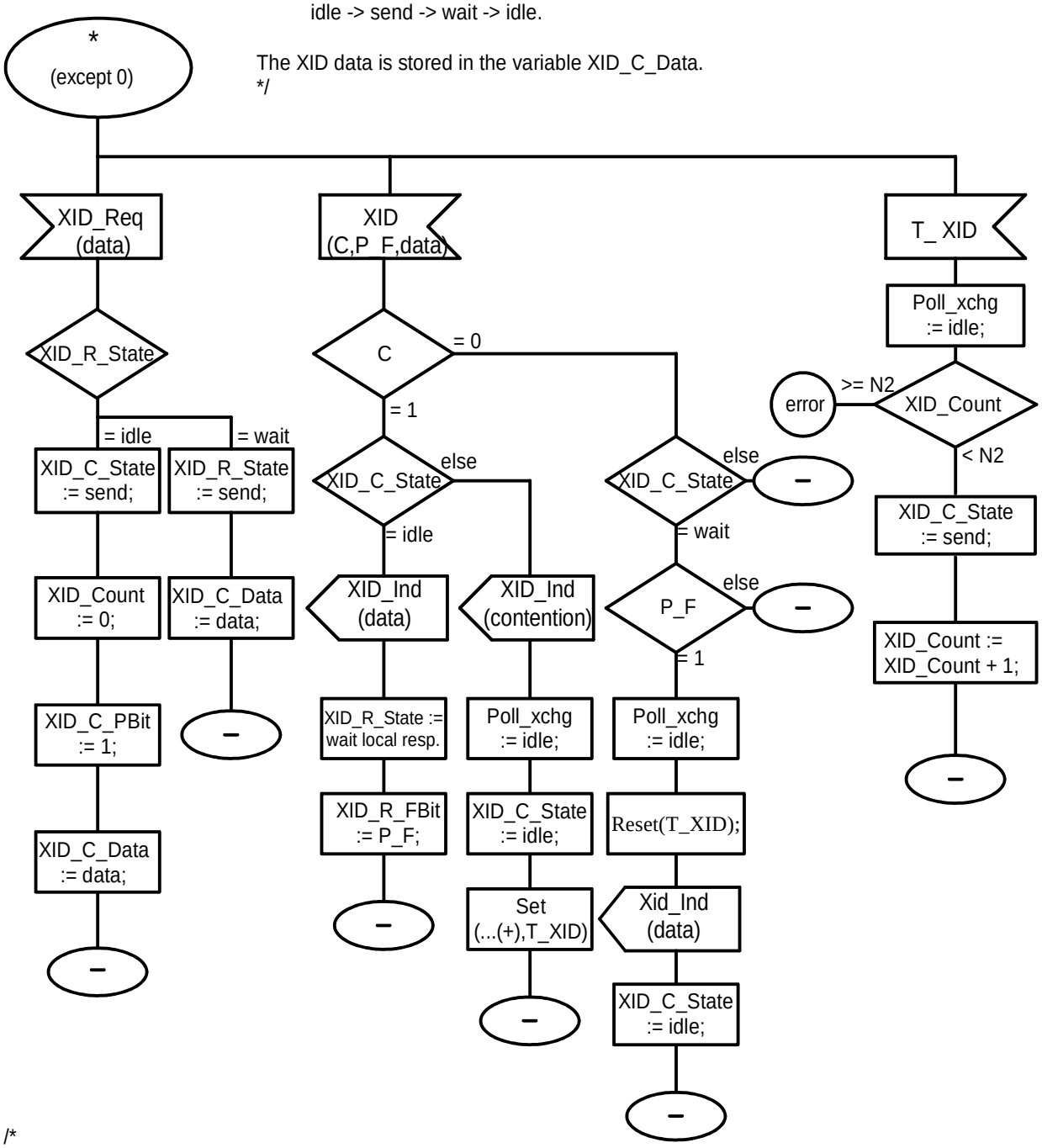
Figure A.15

/*
XID handling (XID_Req, XID)

XID requests are controlled using the state variable XID_C_State and XID_R_State. The state transitions being used are:

idle -> send -> wait -> idle.

The XID data is stored in the variable XID_C_Data.
*/



/*
The action on a received XID command PDU depends on the state variable XID_C_State. In the contation case the XID Command is sent again after a certain delay, depending on the 'location' of the RLP entity.

The XID command/response PDU is sent at the earliest possible opportunity, next after a possible pending TEST PDU (see procedure SEND_TXU) The value of the timer should be T1 ms in the Mobile Station, it should be twice this value in the Interworking Unit. This scheme is used to avoid repetinion of contentions.
*/

0422AF16.DRW 93-05-25

Figure A.16

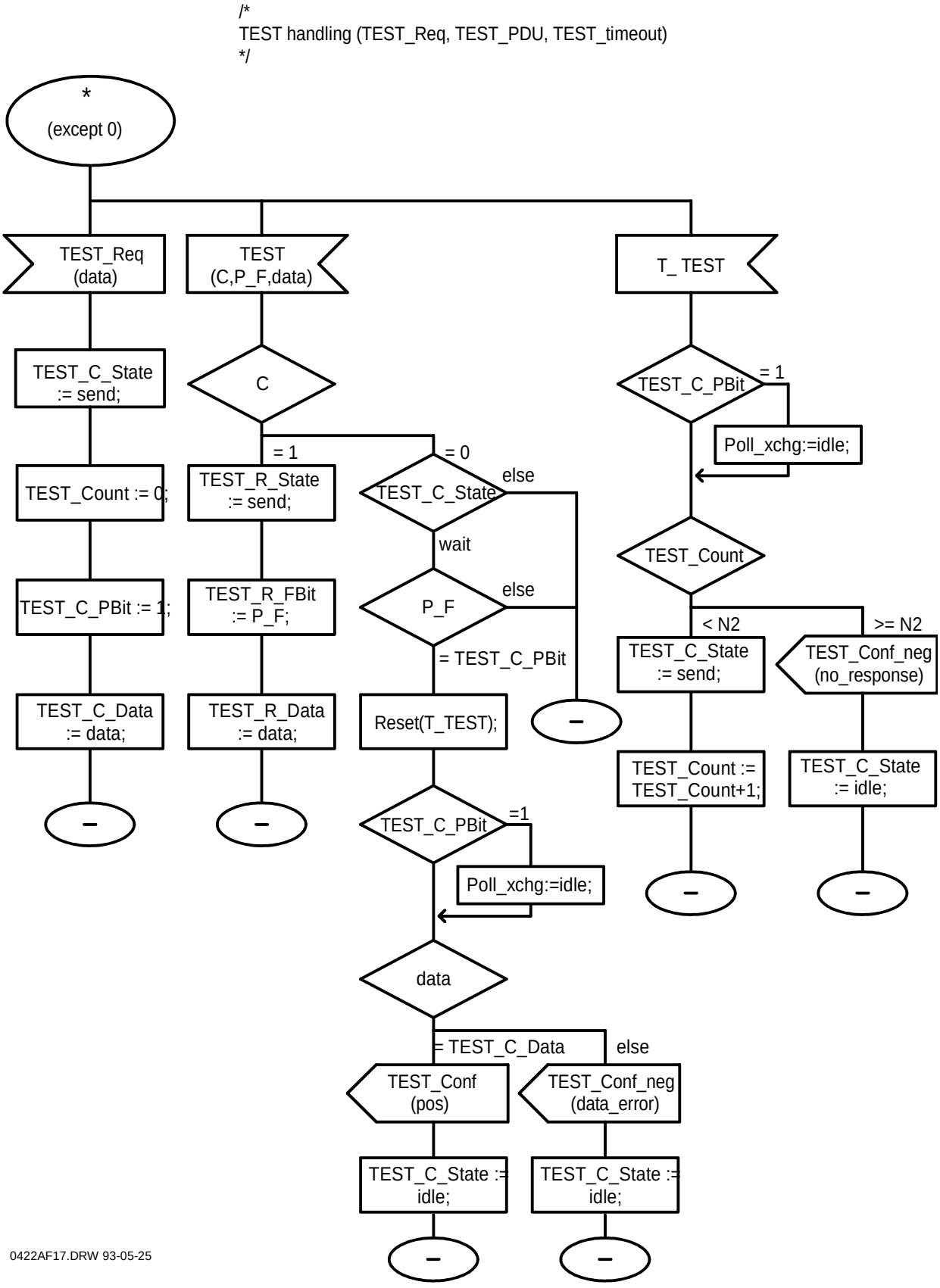

/*
TEST handling (TEST_Req, TEST_PDU, TEST_timeout)
*/
*
(except 0)
TEST_Req
(data)
TEST
(C,P_F,data)
T_ TEST
TEST_C_State
:= send;
C
TEST_C_PBit
= 1
Poll_xchg:=idle;
= 1
= 0
TEST_Count := 0;
TEST_R_State
:= send;
TEST_C_State
else
wait
TEST_Count
TEST_C_PBit := 1;
TEST_R_FBit
:= P_F;
P_F
else
< N2
>= N2
= TEST_C_PBit
TEST_C_State
:= send;
TEST_Conf_neg
(no_response)
TEST_C_Data
:= data;
TEST_R_Data
:= data;
Reset(T_TEST);
TEST_Count :=
TEST_Count+1;
TEST_C_State
:= idle;
TEST_C_PBit
=1
Poll_xchg:=idle;
data
= TEST_C_Data
else
TEST_Conf
(pos)
TEST_Conf_neg
(data_error)
TEST_C_State :=
idle;
TEST_C_State :=
idle;
0422AF17.DRW 93-05-25

Figure A.17

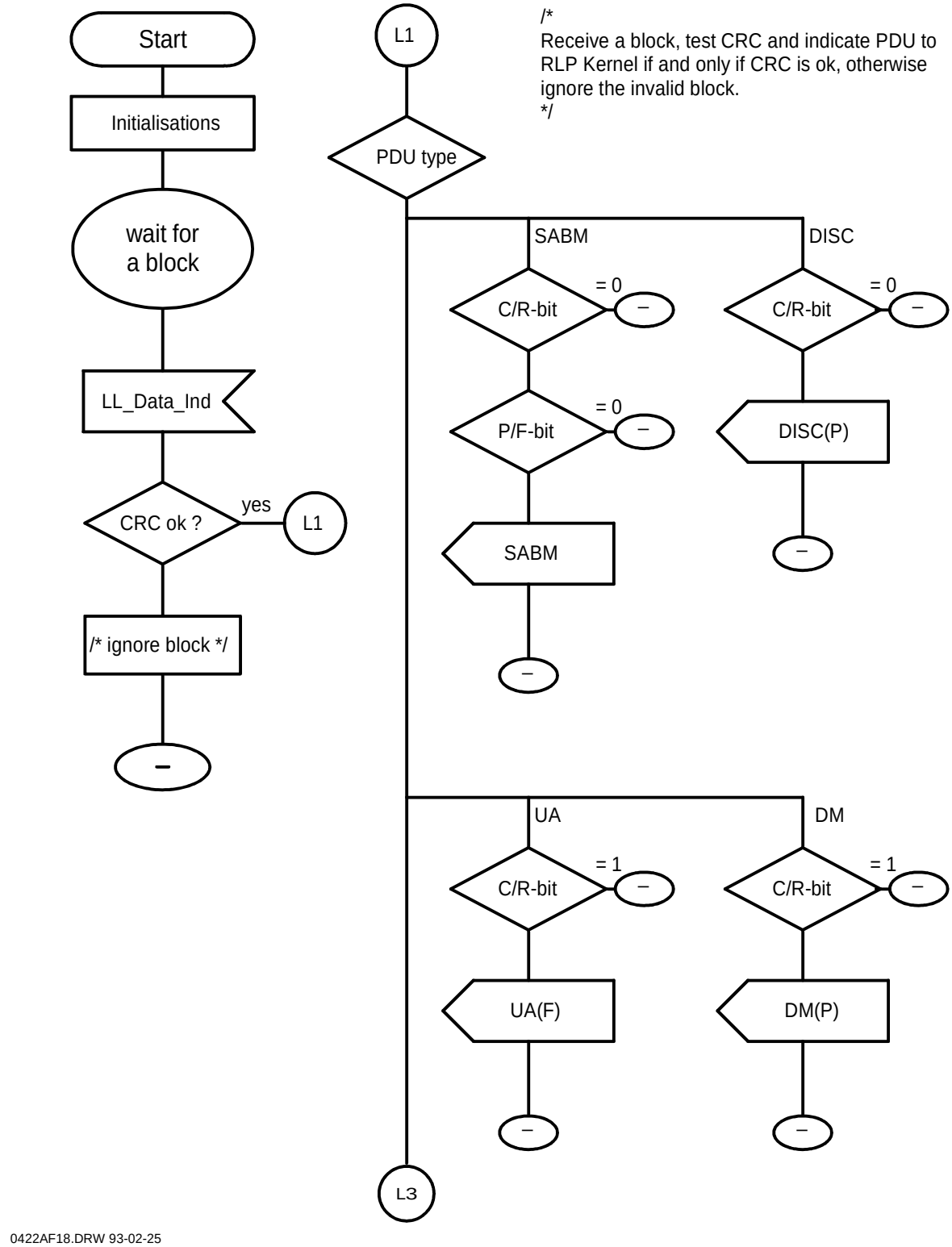
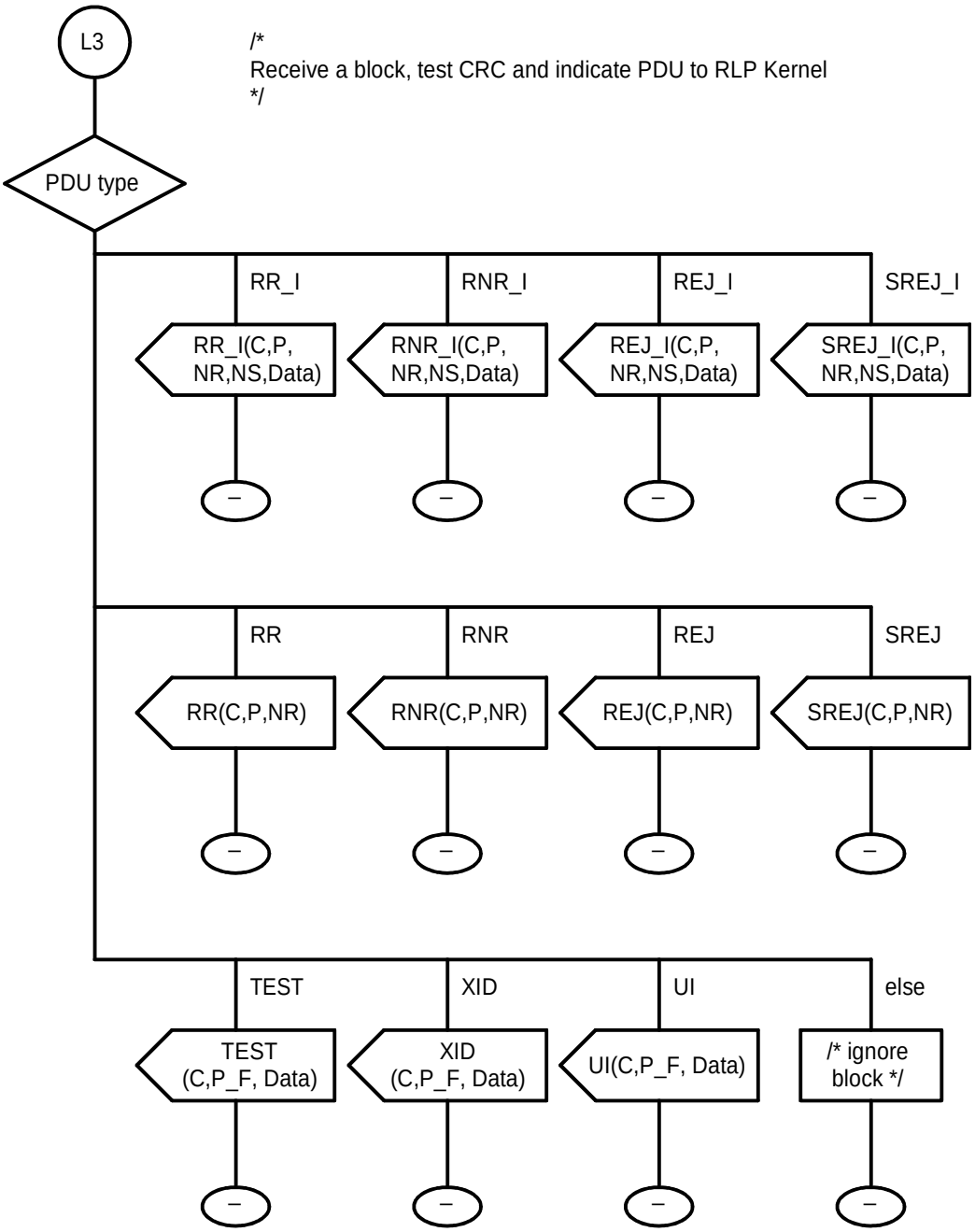

Process Receive_PDU
Start
Initialisations
wait for a block
LL_Data_Ind
CRC ok ?
yes
L1
/* ignore block */
L1
PDU type
/*
Receive a block, test CRC and indicate PDU to RLP Kernel if and only if CRC is ok, otherwise ignore the invalid block.
*/
SABM
DISC
C/R-bit
= 0
P/F-bit
= 0
SABM
C/R-bit
= 0
DISC(P)
UA
DM
C/R-bit
= 1
UA(F)
C/R-bit
= 1
DM(P)
L3
0422AF18.DRW 93-02-25

Figure A.18



0422AF19.DRW 93-02-25

Figure A.19

Process Send_PDU

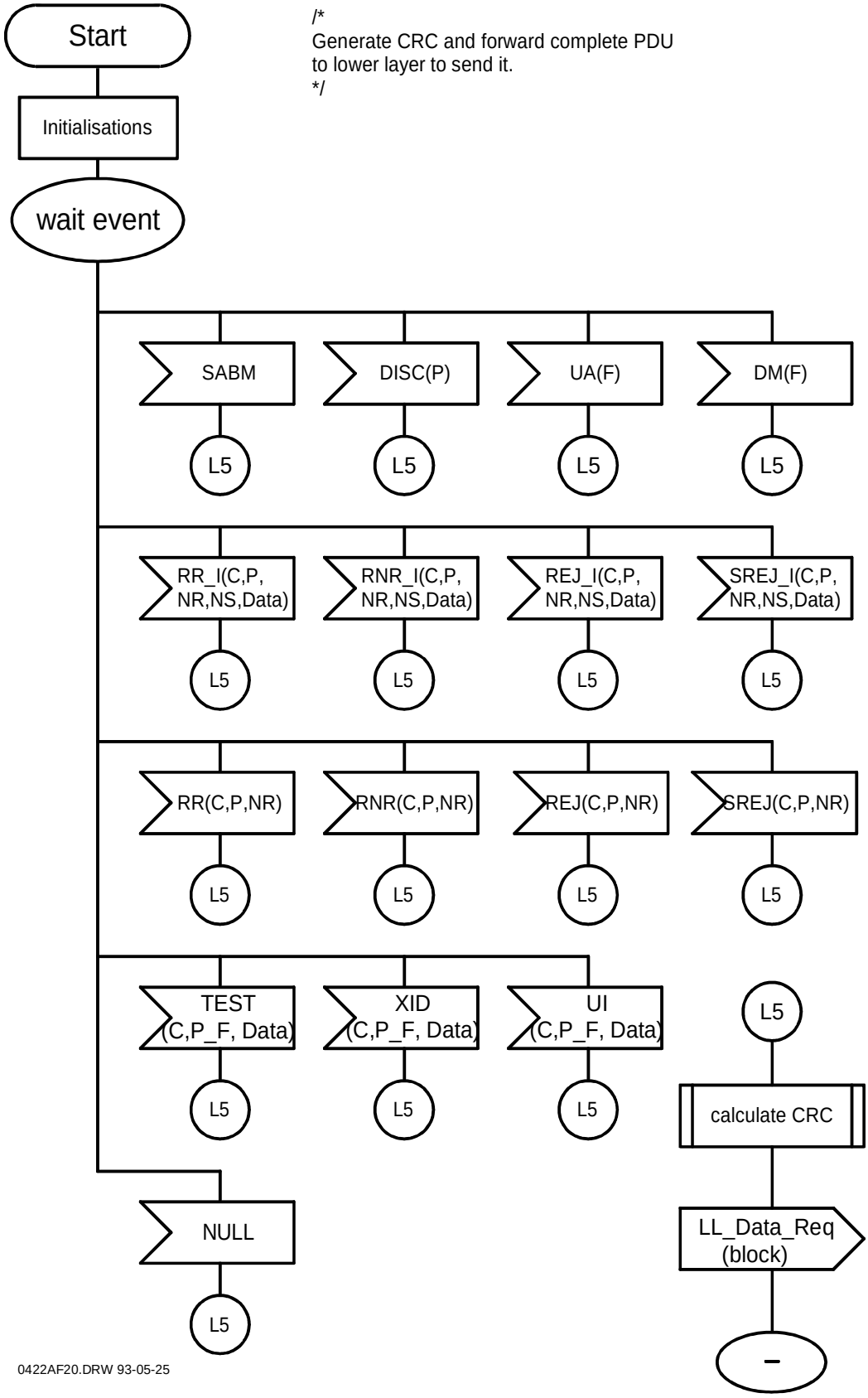
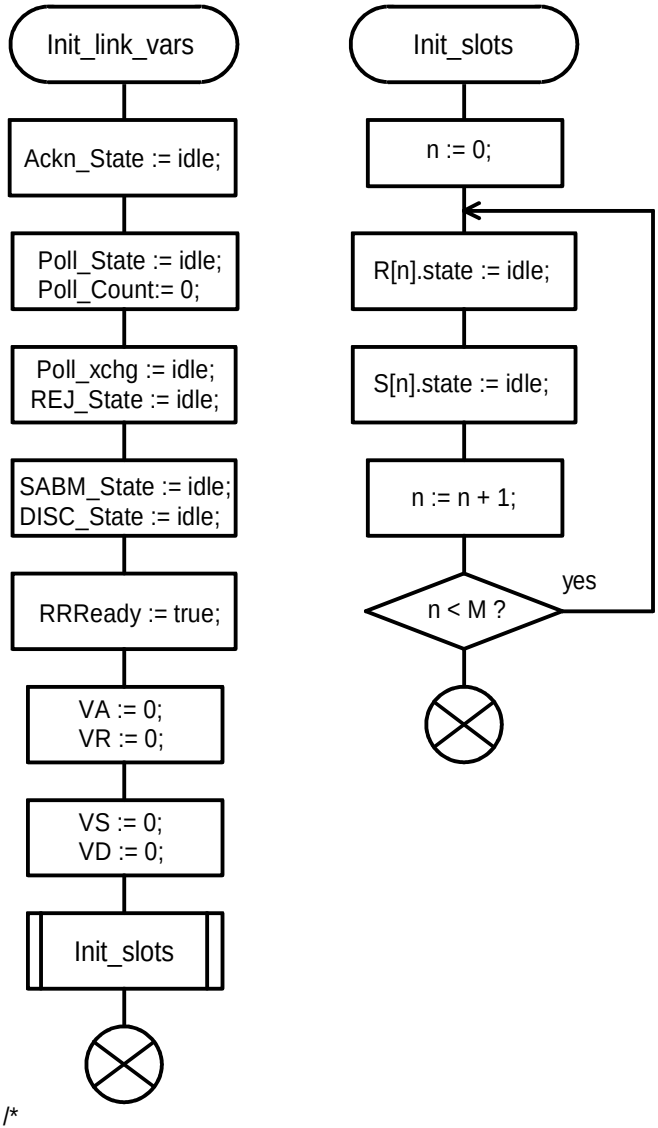


Figure A.20

/*
Initialise link variables - This procedure is called if the link is established or the link is reset.
*/



/*
There are M data receiver slots and M data sender slots (M <= 62).

The receiver states are: idle, rcvd, send, wait.

State = idle means: nothing received (with this number),
State = rcvd means: data received, to be delivered and acknowledged only if in sequence.
If delivered, the state becomes idle again.
State = send means: pending retransmission request for this block,
State = wait means : waiting for receiption of requested block.

The sender slot states are: idle, send, wait.

State = idle means: nothing to do, slot may be used (again).
State = send means: send data at the next possible opportunity.
State = wait means: wait for the acknowledgement
*/

0422AF21.DRW 93-03-01

Figure A.21

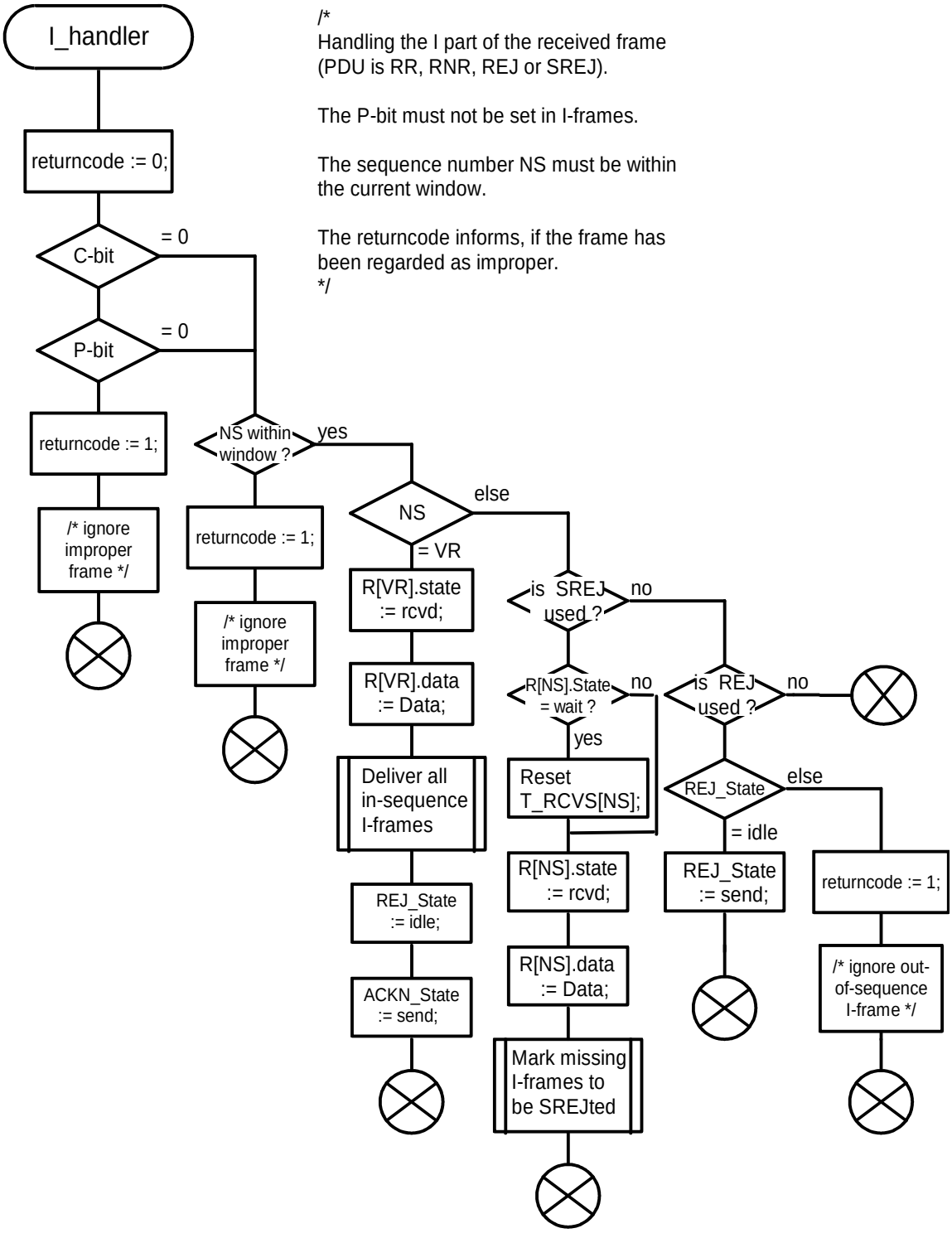

I_handler
/*
Handling the I part of the received frame
(PDU is RR, RNR, REJ or SREJ).
The P-bit must not be set in I-frames.
The sequence number NS must be within
the current window.
The returncode informs, if the frame has
been regarded as improper.
*/
returncode := 0;
C-bit
= 0
P-bit
= 0
returncode := 1;
/* ignore improper frame */
NS within window ?
yes
returncode := 1;
/* ignore improper frame */
NS
else
= VR
R[VR].state := rcvd;
R[VR].data := Data;
Deliver all in-sequence I-frames
REJ_State := idle;
ACKN_State := send;
is SREJ used ?
no
R[NS].State = wait ?
no
yes
Reset T_RCVS[NS];
R[NS].state := rcvd;
R[NS].data := Data;
Mark missing I-frames to be SREJted
is REJ used ?
no
REJ_State
else
= idle
REJ_State := send;
returncode := 1;
/* ignore out-of-sequence I-frame */
0422AF22.DRW 93-09-10

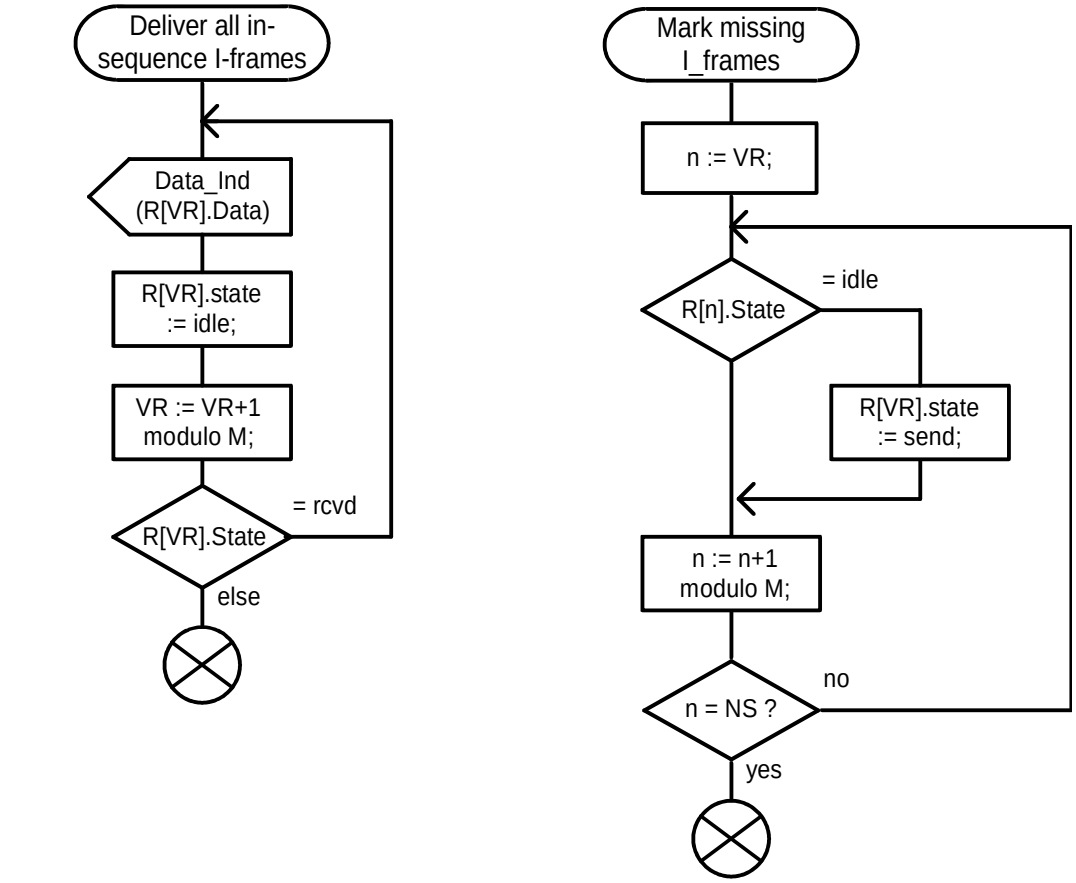
Figure A.22

/*
Deliver all in-sequence I-frames

Indicate all already received in-sequence information blocks. There may be more than one block which has to be indicated due to successful selective recovery.
*/

/*
mark all missing I-frames

All missing I-frames "between" VR an NS have to be marked if their state is idle.
*/



0422AF23.DRW 93-05-25

Figure A.23

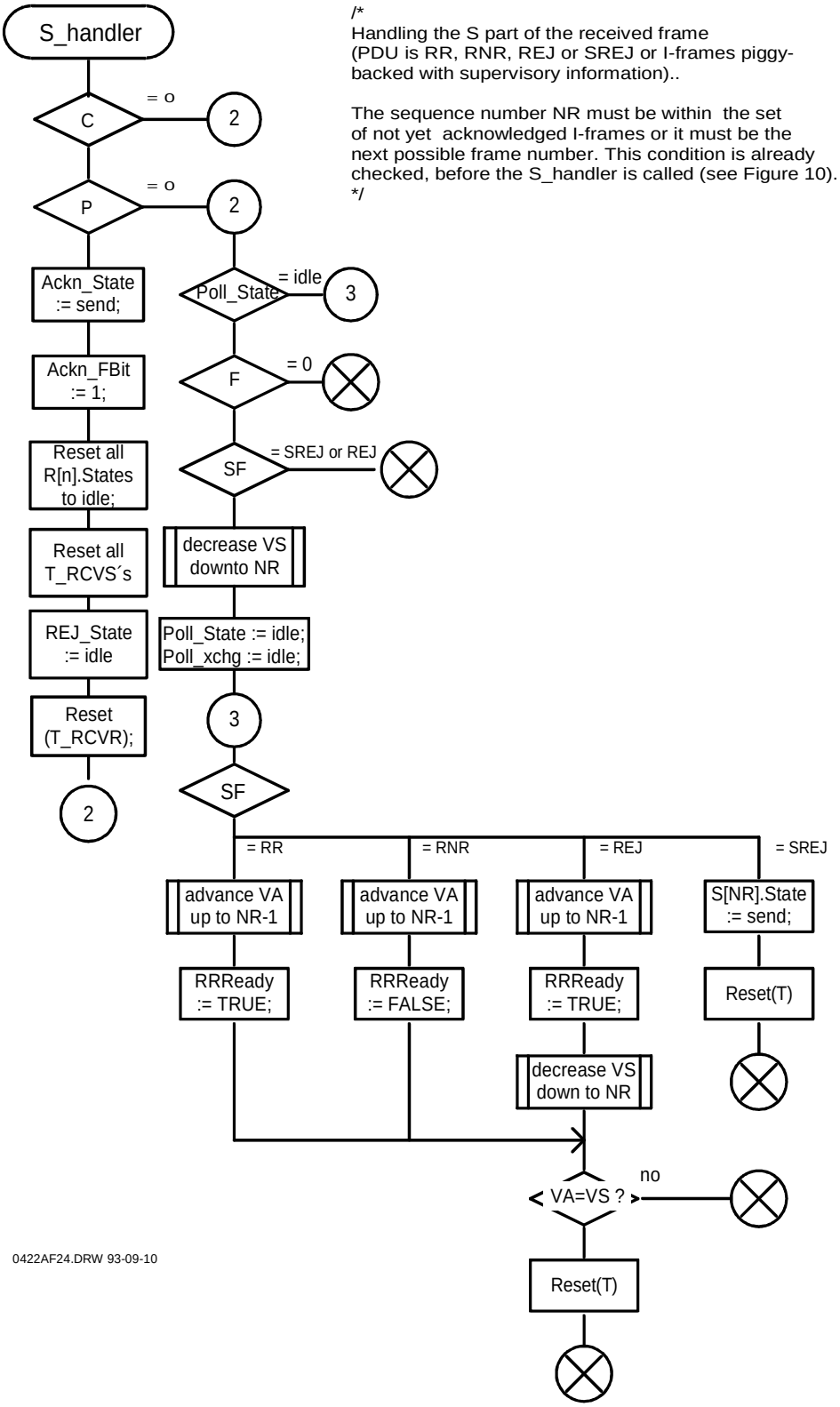
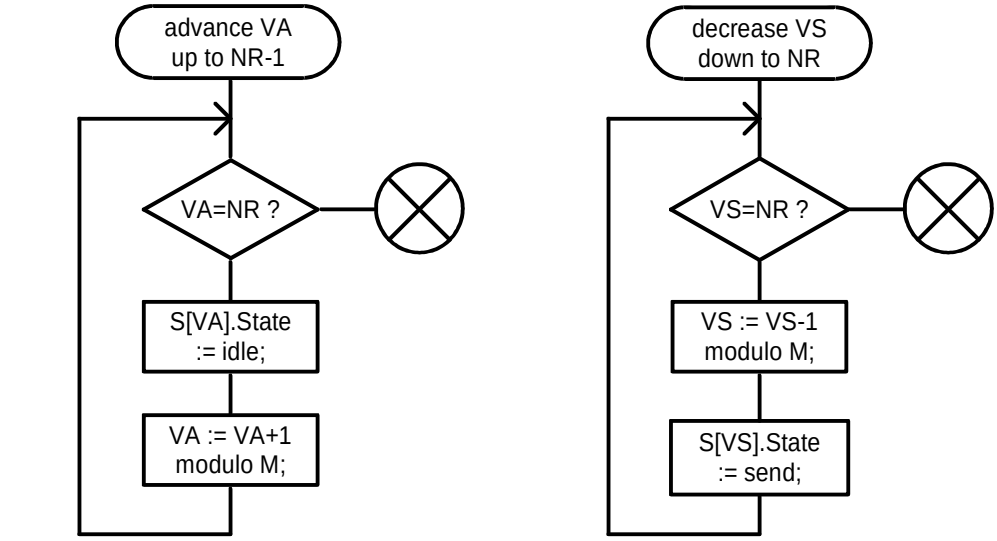

S_handler
/*
Handling the S part of the received frame
(PDU is RR, RNR, REJ or SREJ or I-frames piggy-backed with supervisory information)..
The sequence number NR must be within the set of not yet acknowledged I-frames or it must be the next possible frame number. This condition is already checked, before the S_handler is called (see Figure 10).
*/
C
= 0
2
P
= 0
2
Ackn_State := send;
Poll_State
= idle
3
Ackn_FBit := 1;
F
= 0
Reset all R[n].States to idle;
SF
= SREJ or REJ
Reset all T_RCVS´s
decrease VS downto NR
REJ_State := idle
Poll_State := idle;
Poll_xchg := idle;
Reset (T_RCVR);
3
2
SF
= RR
= RNR
= REJ
= SREJ
advance VA up to NR-1
advance VA up to NR-1
advance VA up to NR-1
S[NR].State := send;
RRReady := TRUE;
RRReady := FALSE;
RRReady := TRUE;
Reset(T)
decrease VS down to NR
VA=VS ?
no
Reset(T)
0422AF24.DRW 93-09-10

Figure A.24

/*
Advance the lower
window edge
*/

/*
Set the sender slot
states to send again
*/



0422AF25.DRW 93-03-01

Figure A.25

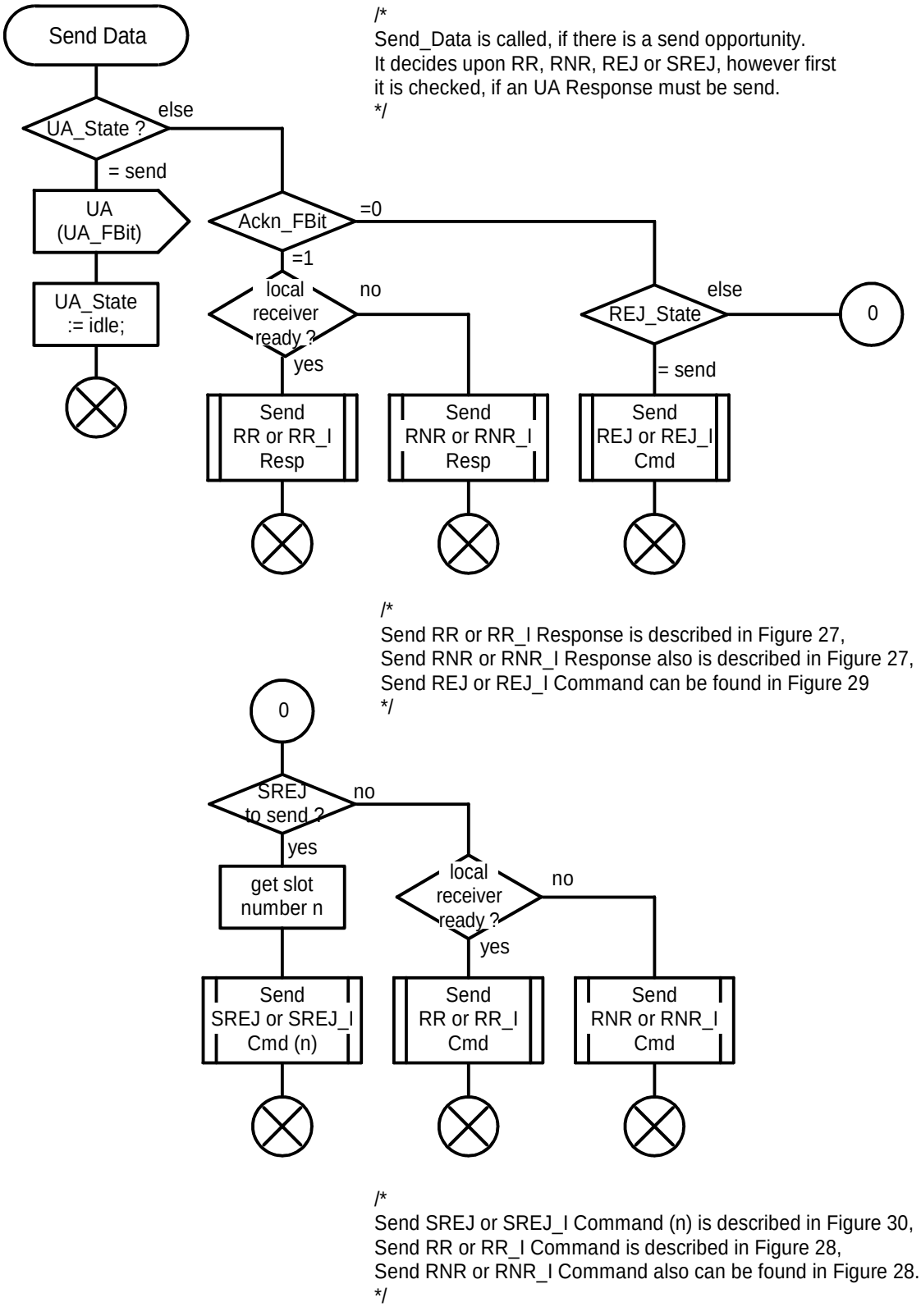
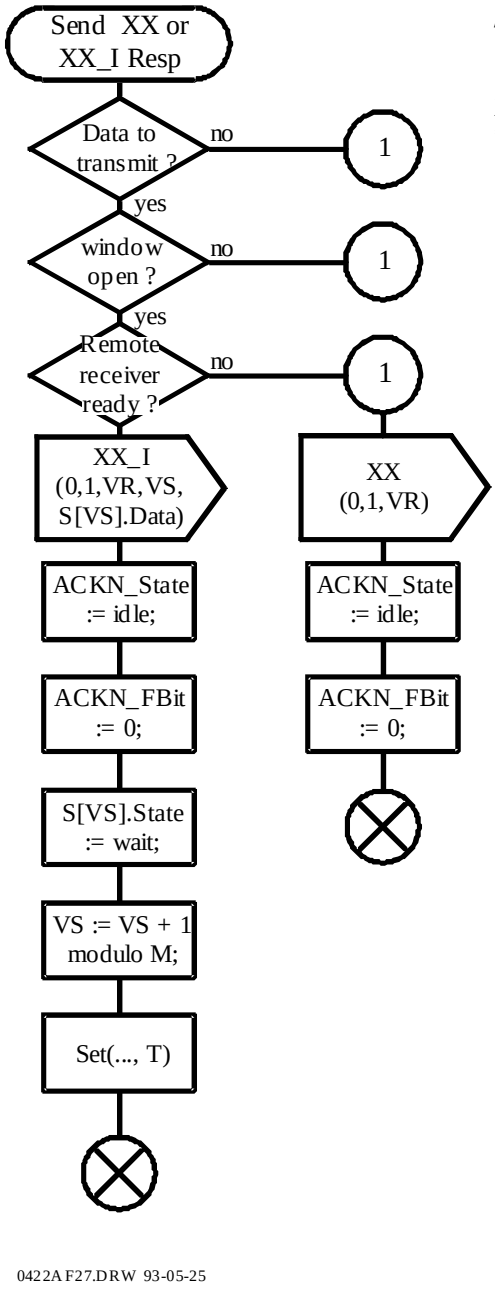

Send Data
/*
Send_Data is called, if there is a send opportunity.
It decides upon RR, RNR, REJ or SREJ, however first
it is checked, if an UA Response must be send.
*/
UA_State ?
else
= send
UA
(UA_FBit)
Ackn_FBit
=0
=1
UA_State
:= idle;
local
receiver
ready ?
no
yes
REJ_State
else
0
= send
Send
RR or RR_I
Resp
Send
RNR or RNR_I
Resp
Send
REJ or REJ_I
Cmd
/*
Send RR or RR_I Response is described in Figure 27,
Send RNR or RNR_I Response also is described in Figure 27,
Send REJ or REJ_I Command can be found in Figure 29
*/
0
SREJ
to send ?
no
yes
get slot
number n
local
receiver
ready ?
no
yes
Send
SREJ or SREJ_I
Cmd (n)
Send
RR or RR_I
Cmd
Send
RNR or RNR_I
Cmd
/*
Send SREJ or SREJ_I Command (n) is described in Figure 30,
Send RR or RR_I Command is described in Figure 28,
Send RNR or RNR_I Command also can be found in Figure 28.
*/
0422AF26.DRW 93-05-25

Figure A.26



/*
Send XX or XX_I response PDU with F-Bit set to one.

XX may be RR or RNR.
*/

Figure A.27

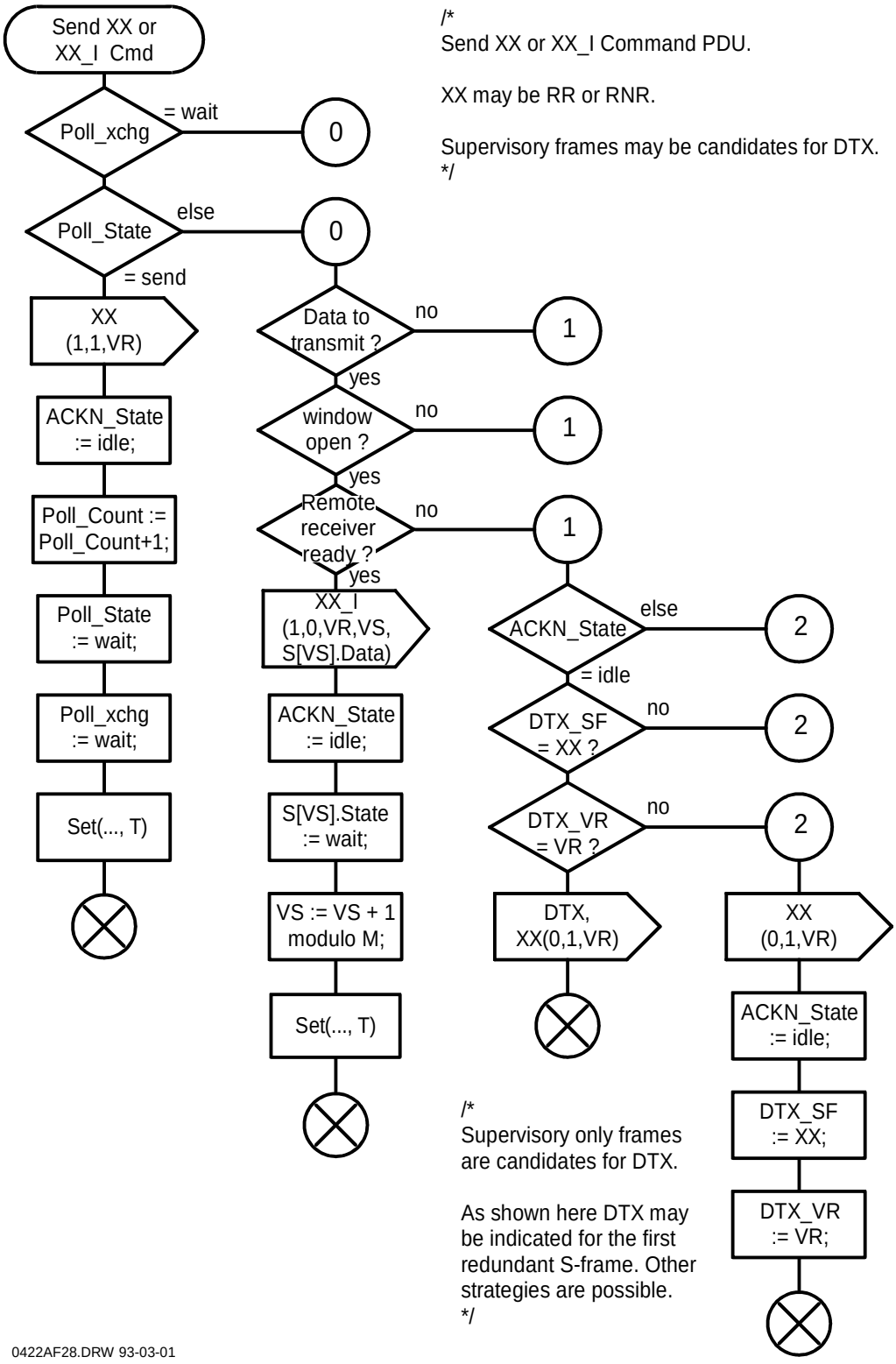

Send XX or XX_I Cmd
Poll_xchg
= wait
0
Poll_State
else
0
= send
XX (1,1,VR)
ACKN_State := idle;
Poll_Count := Poll_Count+1;
Poll_State := wait;
Poll_xchg := wait;
Set(..., T)
Data to transmit ?
no
1
yes
window open ?
no
1
yes
Remote receiver ready ?
no
1
yes
XX_I (1,0,VR,VS, S[VS].Data)
ACKN_State := idle;
S[VS].State := wait;
VS := VS + 1 modulo M;
Set(..., T)
ACKN_State
else
2
= idle
DTX_SF = XX ?
no
2
DTX_VR = VR ?
no
2
DTX, XX(0,1,VR)
XX (0,1,VR)
ACKN_State := idle;
DTX_SF := XX;
DTX_VR := VR;
/*
Send XX or XX_I Command PDU.
XX may be RR or RNR.
Supervisory frames may be candidates for DTX.
*/
/*
Supervisory only frames are candidates for DTX.
As shown here DTX may be indicated for the first redundant S-frame. Other strategies are possible.
*/
0422AF28.DRW 93-03-01

Figure A.28

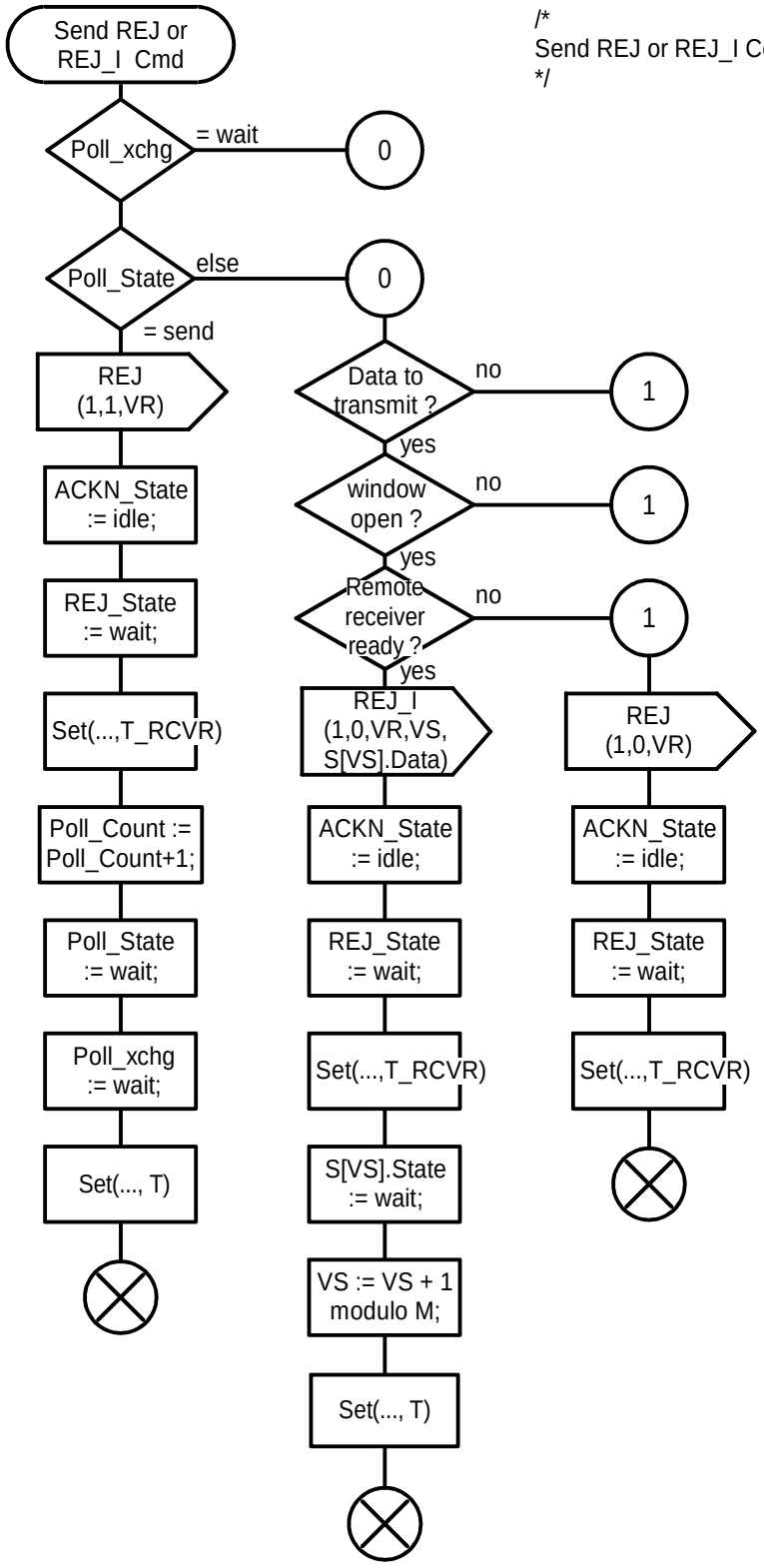

Send REJ or REJ_I Cmd
/*
Send REJ or REJ_I Command PDU.
*/
Poll_xchg
= wait
0
Poll_State
else
0
= send
REJ (1,1,VR)
ACKN_State := idle;
REJ_State := wait;
Set(...,T_RCVR)
Poll_Count := Poll_Count+1;
Poll_State := wait;
Poll_xchg := wait;
Set(..., T)
Data to transmit ?
no
1
yes
window open ?
no
1
yes
Remote receiver ready ?
no
1
yes
REJ_I (1,0,VR,VS, S[VS].Data)
ACKN_State := idle;
REJ_State := wait;
Set(...,T_RCVR)
S[VS].State := wait;
VS := VS + 1 modulo M;
Set(..., T)
REJ (1,0,VR)
ACKN_State := idle;
REJ_State := wait;
Set(...,T_RCVR)
0422AF29.DRW 93-03-01

Figure A.29

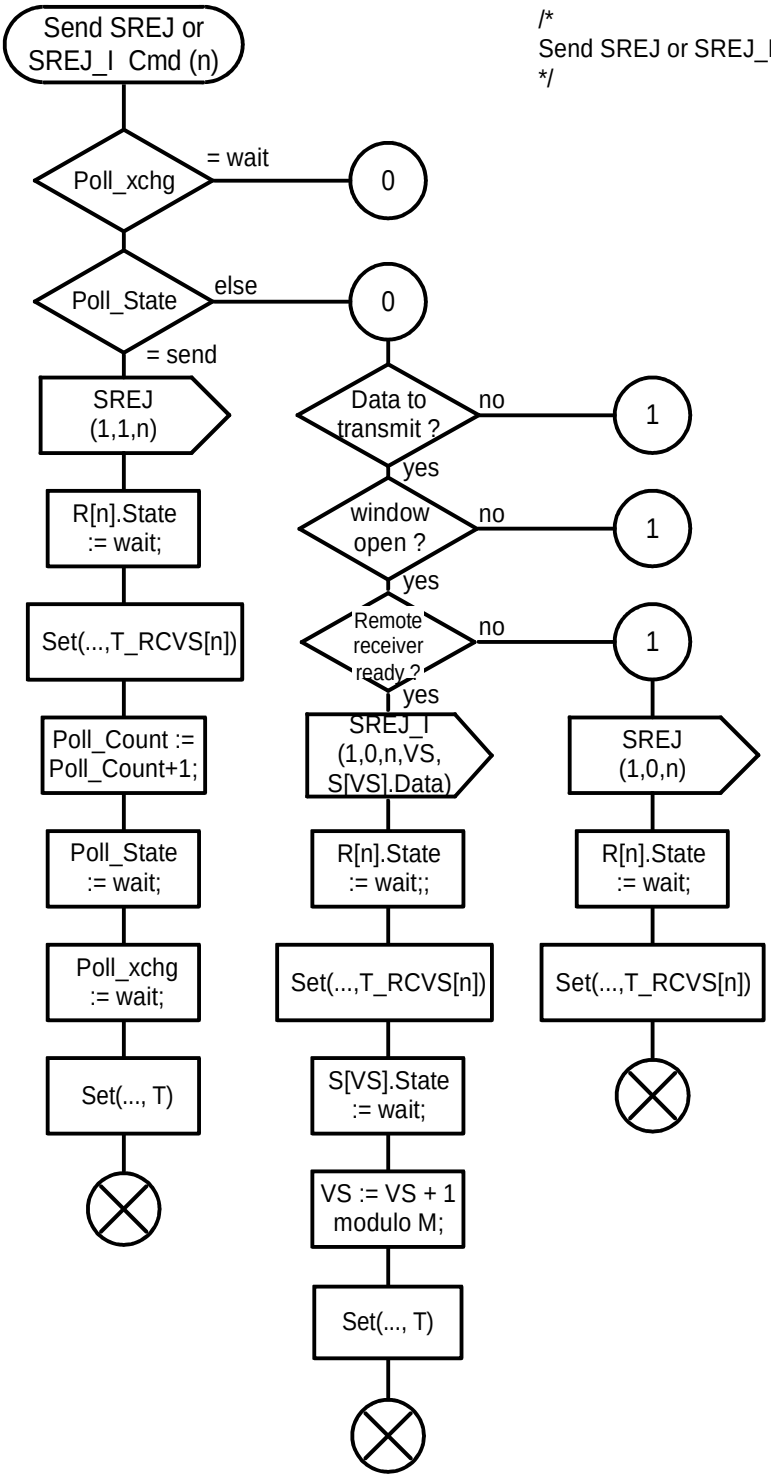

Send SREJ or SREJ_I Cmd (n)
/*
Send SREJ or SREJ_I Command PDU.
*/
Poll_xchg
= wait
0
Poll_State
else
0
= send
SREJ (1,1,n)
Data to transmit ?
no
1
yes
R[n].State := wait;
window open ?
no
1
yes
Set(...,T_RCVS[n])
Remote receiver ready ?
no
1
yes
Poll_Count := Poll_Count+1;
SREJ_I (1,0,n,VS, S[VS].Data)
SREJ (1,0,n)
Poll_State := wait;
R[n].State := wait;;
R[n].State := wait;
Poll_xchg := wait;
Set(...,T_RCVS[n])
Set(...,T_RCVS[n])
Set(..., T)
S[VS].State := wait;
VS := VS + 1 modulo M;
Set(..., T)
0422AF30.DRW 93-09-10

Figure A.30

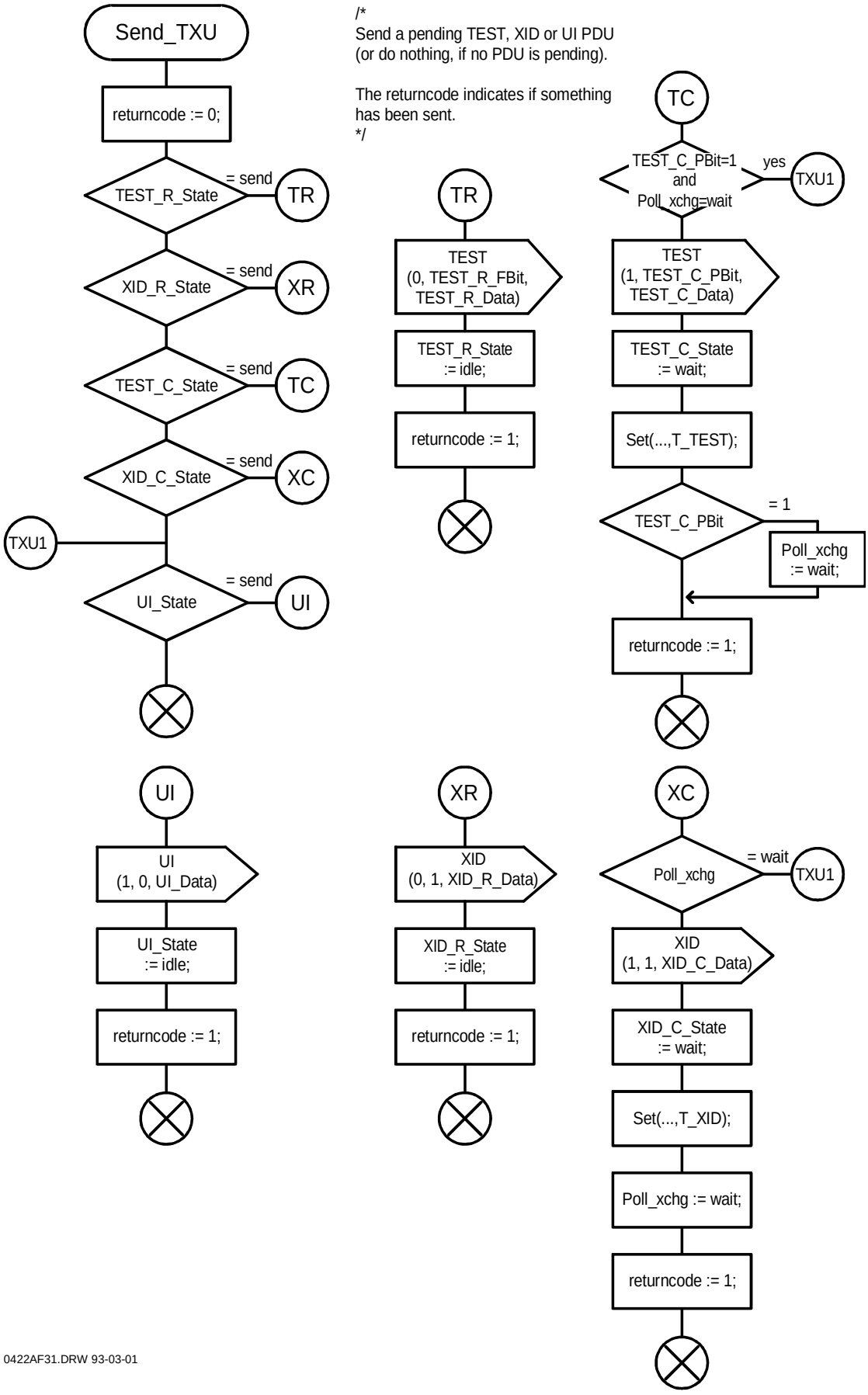

Send_TXU
/*
Send a pending TEST, XID or UI PDU
(or do nothing, if no PDU is pending).
The returncode indicates if something
has been sent.
*/
returncode := 0;
TEST_R_State
= send
TR
XID_R_State
= send
XR
TEST_C_State
= send
TC
XID_C_State
= send
XC
TXU1
UI_State
= send
UI
TR
TEST
(0, TEST_R_FBit,
TEST_R_Data)
TEST_R_State
:= idle;
returncode := 1;
TC
TEST_C_PBit=1
and
Poll_xchg=wait
yes
TXU1
TEST
(1, TEST_C_PBit,
TEST_C_Data)
TEST_C_State
:= wait;
Set(...,T_TEST);
TEST_C_PBit
= 1
Poll_xchg
:= wait;
returncode := 1;
UI
UI
(1, 0, UI_Data)
UI_State
:= idle;
returncode := 1;
XR
XID
(0, 1, XID_R_Data)
XID_R_State
:= idle;
returncode := 1;
XC
Poll_xchg
= wait
TXU1
XID
(1, 1, XID_C_Data)
XID_C_State
:= wait;
Set(...,T_XID);
Poll_xchg := wait;
returncode := 1;
0422AF31.DRW 93-03-01

Figure A.31

Annex B (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
	05-1999				Transferred to 3GPP CN1	7.0.0	
03-1999	TSG#03				Approved at CN#03		3.0.0
06-1999	TSG#04		001		Introduction of EDGE channel codings into the specifications	3.0.0	3.1.0
12-1999	TSG#06		002	1	Correction to REMAP procedure in RLP	3.1.0	3.2.0
12-1999	TSG#06		003		Updates to RLP and DTX for UMTS	3.1.0	3.2.0
06-2000	TSG#08		004		RLP timer for T4 in UMTS	3.2.0	3.3.0
	-		-		MCC Editorial update to make figures visible	3.3.0	3.3.1
09-2000	TSG#09		005	1	Relevance of GSM specific BC-IE parameters for negotiating RLP version in UMTS	3.3.1	3.4.0
03-2001	TSG#11				Upgraded to Release 4	3.4.0	4.0.0
12-2001	TSG#14	NP-010604	006	3	New terminology required by TSG GERAN	4.0.0	5.0.0
12-2002	TSG#18	NP-020617	007	1	CS Data Services (including HSCSD and EDGE) for GERAN Iu mode	5.0.0	5.1.0