ETSI TS 129 061 V6.8.0 (2006-06)

Technical Specification

**Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
Interworking between the Public Land Mobile Network (PLMN)
supporting packet based services and
Packet Data Networks (PDN)
(3GPP TS 29.061 version 6.8.0 Release 6)**

Reference
RTS/TSGC-0329061v680

Keywords
GSM, UMTS

ETSI

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

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

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

Intellectual Property Rights

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

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

Foreword

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

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

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp .

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 the present document although the term "A/Gb mode" is used.

The present document also defines, in clause 17, the protocol for the Gmb interface.

The present document also defines, in clause 18, the usage of Radius at the Pk Reference Point between the GGSN and the Presence Network Agent.

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] Void.

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

[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 services".

[11] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

[12] Void.

[13] Void.

[14] Void.

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

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

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

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

[19] IETF RFC 1034 (1987): "Domain names - concepts and facilities" (STD 7).

[20] Void.

[21a] IETF RFC 1661 (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).

[23] 3GPP TS 44.008: "Mobile radio interface layer 3 specification; Core Network protocols; Stage 3".

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

[25] IETF RFC 2794 (2000): "Mobile IP Network Address Identifier Extension for IPv4", P. Calhoun, C. Perkins.

[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 6 Addressing Architecture".

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

[30] IETF RFC 3344 (2002): "IP Mobility Support", C. Perkins.

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

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

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

[34] IETF RFC 2362 (1998): "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): "Distance Vector Multicast Routing Protocol", D. Waitzman, C. Partridge, S.E. Deering.

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

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

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

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

[40] 3GPP TS 23.003: "Numbering, addressing and identification".

[41] IETF RFC 3576 (2003): "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", M.Chiba, M.Eklund, D.Mitton, B.Aboba.

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

[43] Void.

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

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

[46] IETF RFC 3315 (2003) "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney.

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

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

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

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

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

[52] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[53] 3GPP TS 29.207: "Policy control over Go interface".

[54] 3GPP TS 24.008: "Mobile radio interface layer 3 specification; Core Network protocols; Stage 3".

[55] Void.

[56] 3GPP TS 29.208: "End to end Quality of Service (QoS) signalling flows".

[57] Void.

[58] IETF RFC 1035 (1987): "Domain names - implementation and specification" (STD 13).

[59] Void.

[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)".

[64] IETF RFC 2044 (1996): "UTF-8, a transformation format of Unicode and ISO 10646".

[65] 3GPP TS 23.246: "Multimedia Broadcast/Multicast Service (MBMS) Architecture and Functional Description".

[66] IETF RFC 3588: "Diameter Base Protocol".

[67] IETF RFC 4005 (2005): "Diameter Network Access Server Application".

[68] 3GPP TS 23.141: "Presence Service; Architecture and functional description".

[69] 3GPP TS 32.422: " Subscriber and equipment trace: Trace Control and Configuration Management".

[70] 3GPP TS 48.018: "Base Station System (BSS) - Serving GPRS Support Node (SGSN); BSS GPRS Protocol (BSSGP)".

3 Definitions, abbreviations and symbols

3.1 Definitions

For the purposes of the present document, the 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

Abbreviations used in the present document are listed in 3GPP TS 21.905 [42]. For the purposes of the present document, the following additional abbreviations apply:

APN	Access Point Name
ATM	Asynchronous Transfer Mode
BG	Border Gateway
BM-SC	Broadcast/Multicast Service Centre
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
MBMS	Multimedia Broadcast/Multicast Service
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
PDF	Policy Decision 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.
Gmb	Reference point between GGSN and BM-SC.
Gn	Interface between two GSNs within the same PLMN.
Go	Interface between a GGSN and a PDF.
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.
Pk	Reference Point between GGSN and Presence Network Agent.
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.

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.

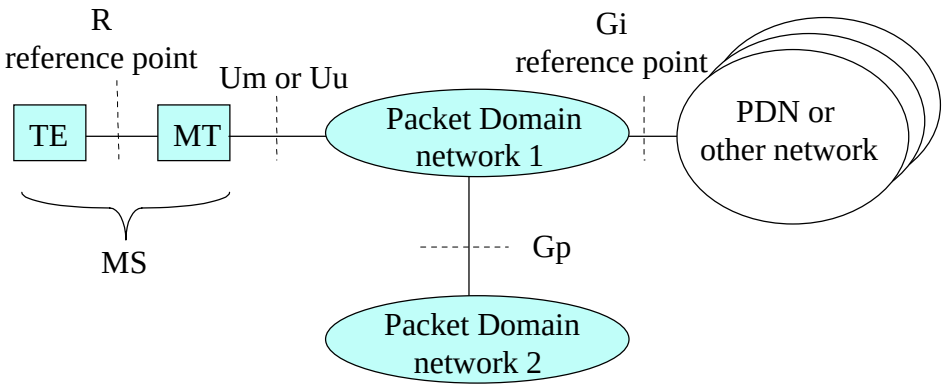


Figure 1: Packet Domain Access Interfaces and Reference Points

7 Interface to Packet Domain Bearer Services

7.1 A/Gb mode

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].

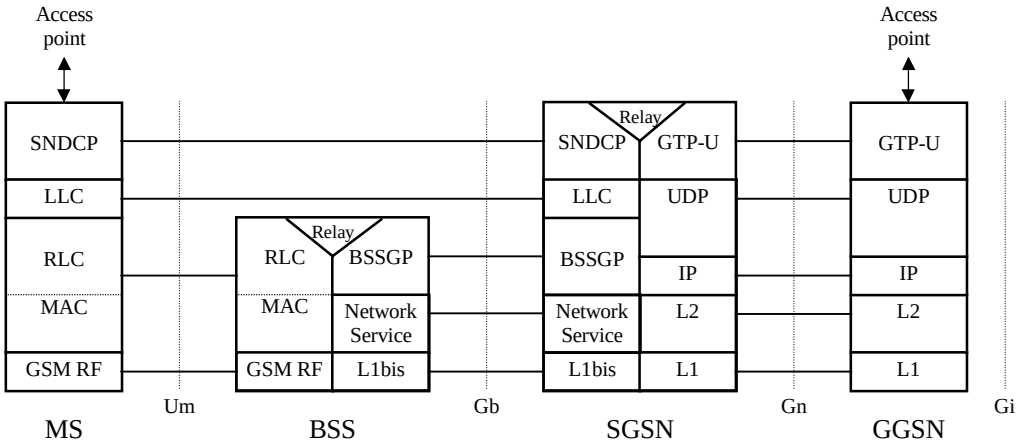


Figure 2a: User Plane for Packet Domain services in A/Gb mode

7.2 Iu mode

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].

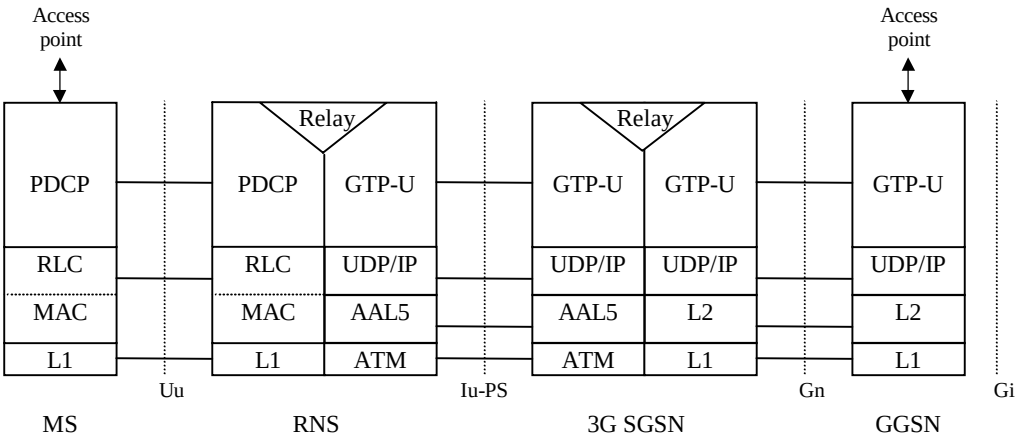


Figure 2b: User Plane for Packet Domain services in Iu mode

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.

8A Prevention of IP spoofing

If IP spoofing has to be prevented, the GGSN shall verify the source IP address of the IP packets issued by the UE and compare it against the address assigned during the PDP context activation procedure. If the verification fails the GGSN shall discard the packets and shall be capable to log the event in the security log against the subscriber information (IMSI/MSISDN).

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

11 Interworking with PDN (IP)

11.1 General

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

11.2 PDN Interworking Model

When interworking with the IP networks, the Packet Domain can operate IPv4 or IPv6. The interworking point with IP networks is at the Gi reference point as shown in figure 7.

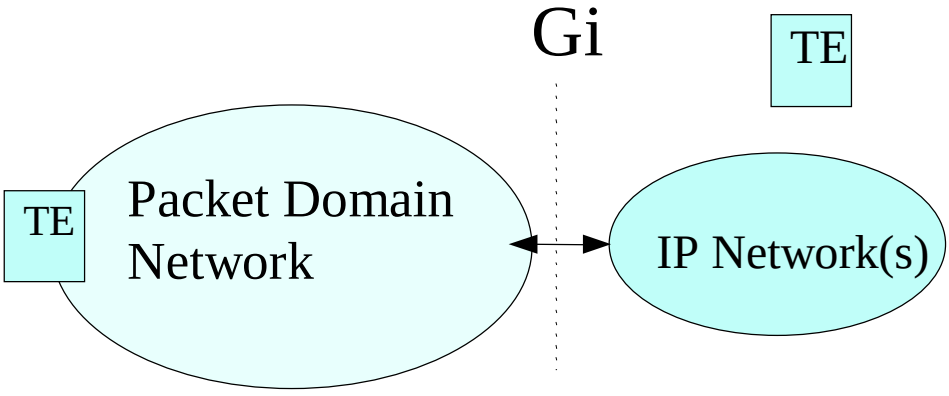


Figure 7: IP network interworking

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

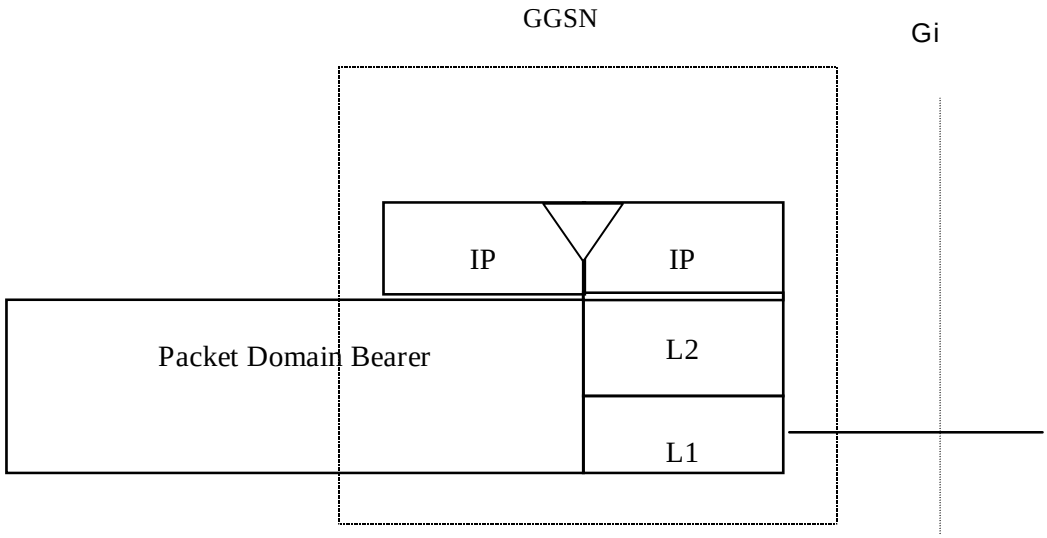


Figure 8: The protocol stacks for the IP / Gi reference point

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

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

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

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

11.2.1 Access to Internet, Intranet or ISP through Packet Domain

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

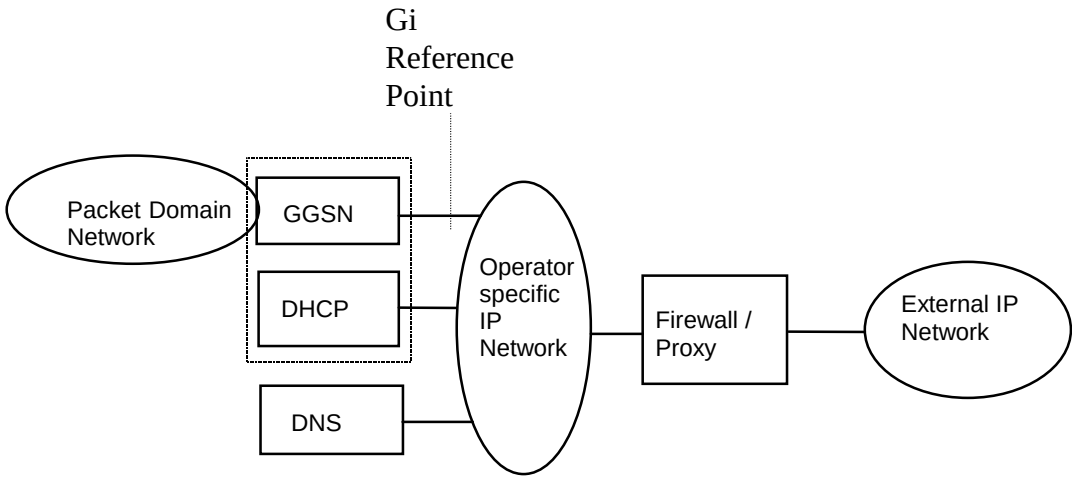


Figure 9: Example of the PDN Interworking Model, transparent case

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.

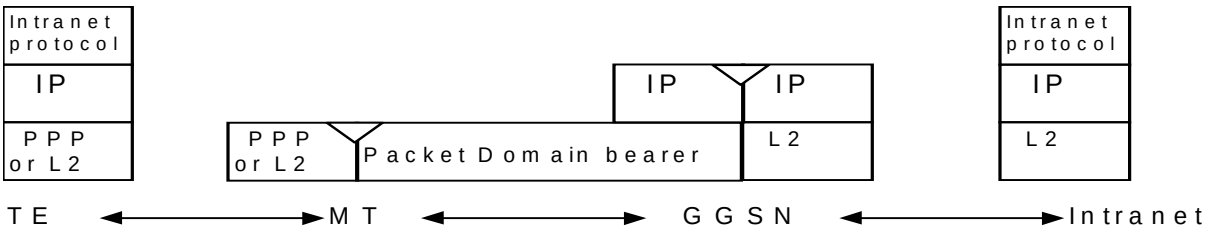


Figure 10: Transparent access to an Intranet

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 Protocol".

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

An example of an "Intranet Protocol" is IPsec (see RFC 1825 [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.

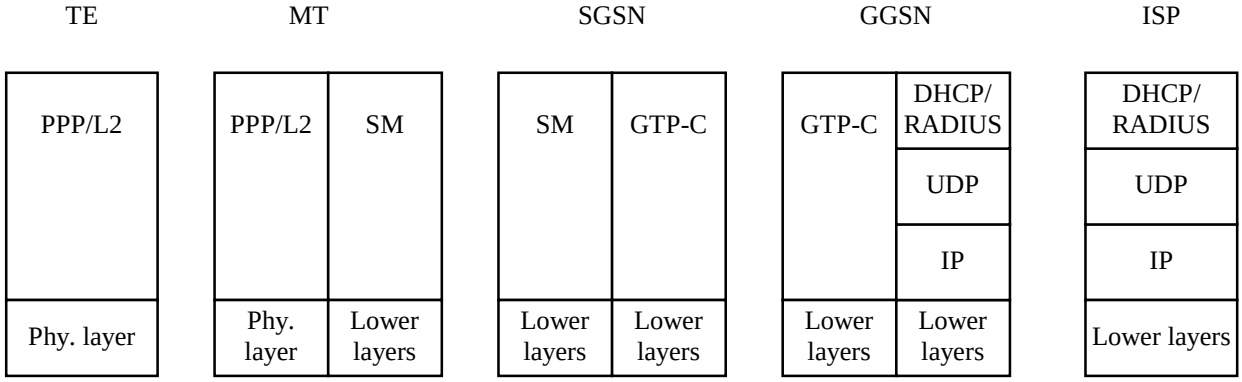


Figure 11a: Signalling plane of non transparent case

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.

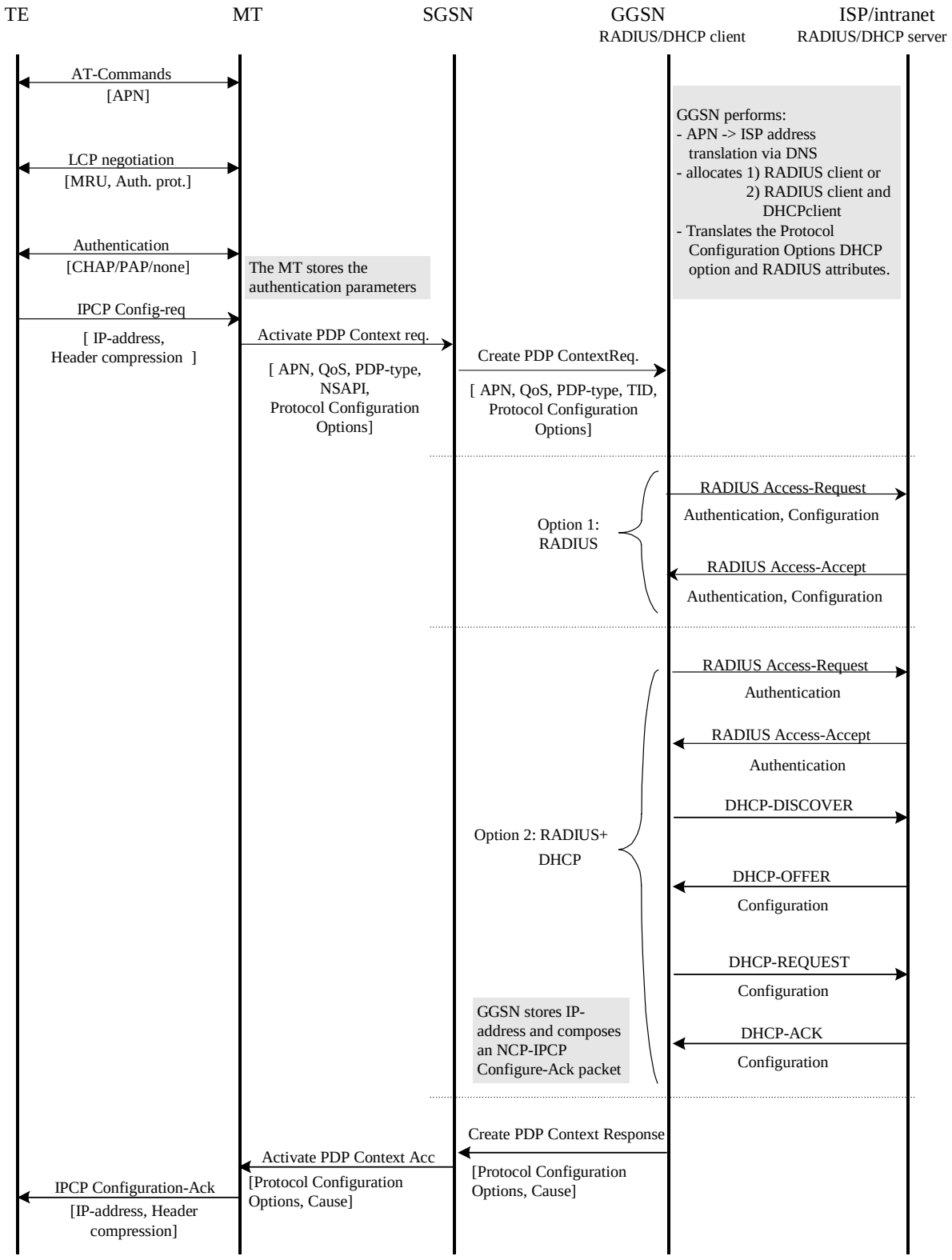


Figure 11b: PDP Context Activation for the IPv4 Non-transparent case

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.

   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.

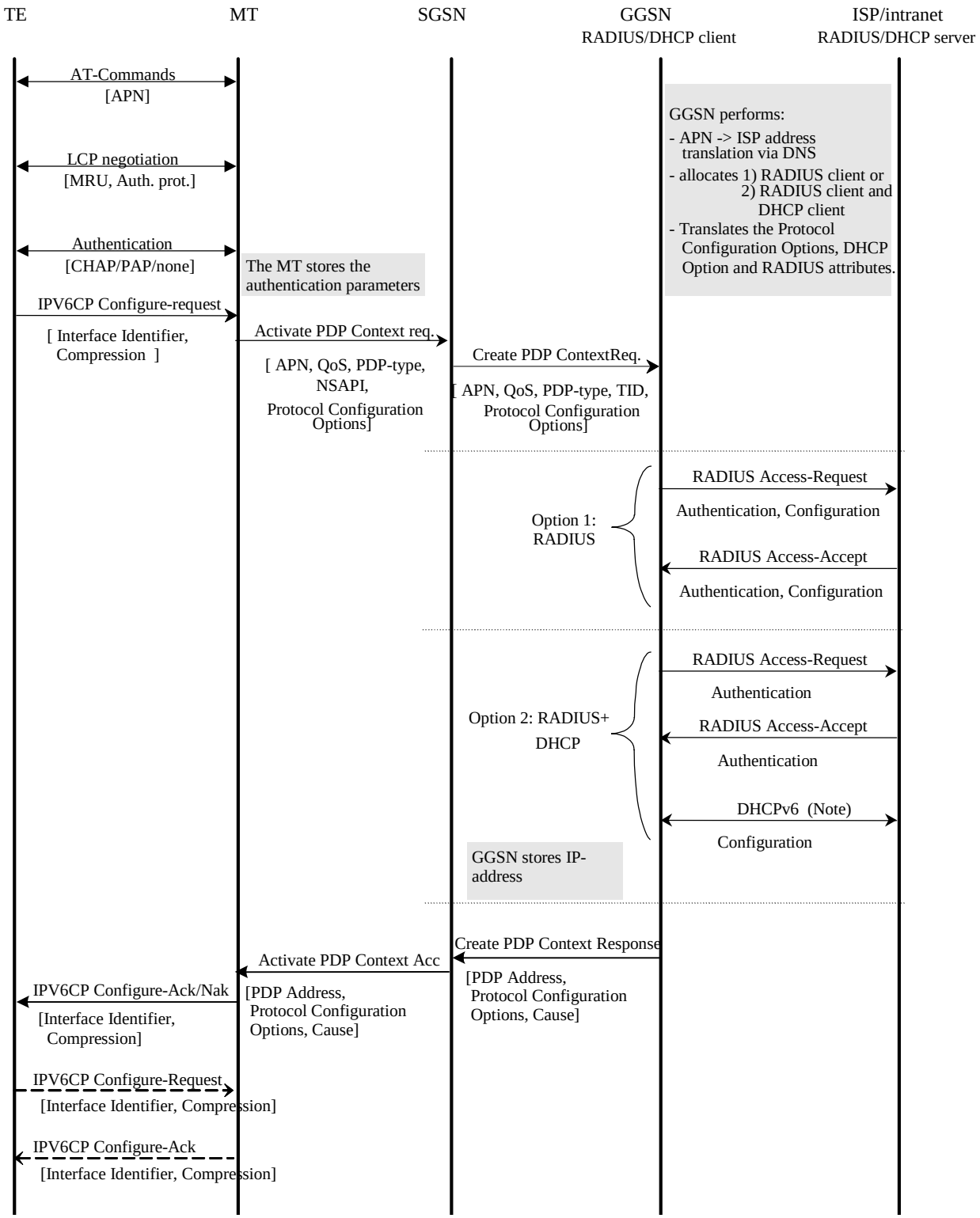
   If the Interface-Identifier extracted from the address contained in the PDP Address IE is not identical to the tentative Interface-Identifier indicated in the IPV6CP Configure-Request message sent from the TE, the MT sends an IPV6CP Configure-Nak packet, indicating the Interface-Identifier extracted 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: DHCPv6 may be used for IPv6 prefix allocation.

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

Figure 11ba 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.

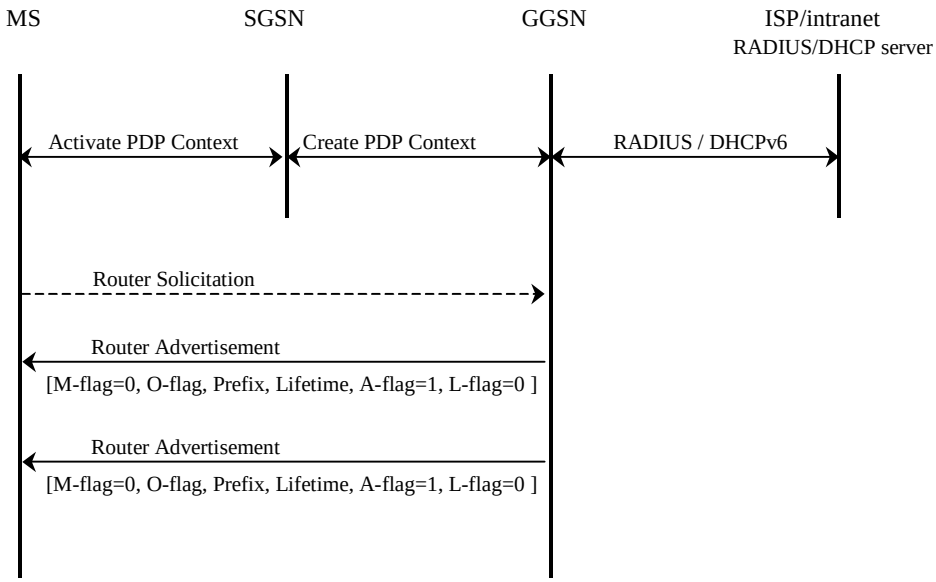


Figure 11bb: IPv6 Stateless Address Autoconfiguration

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.

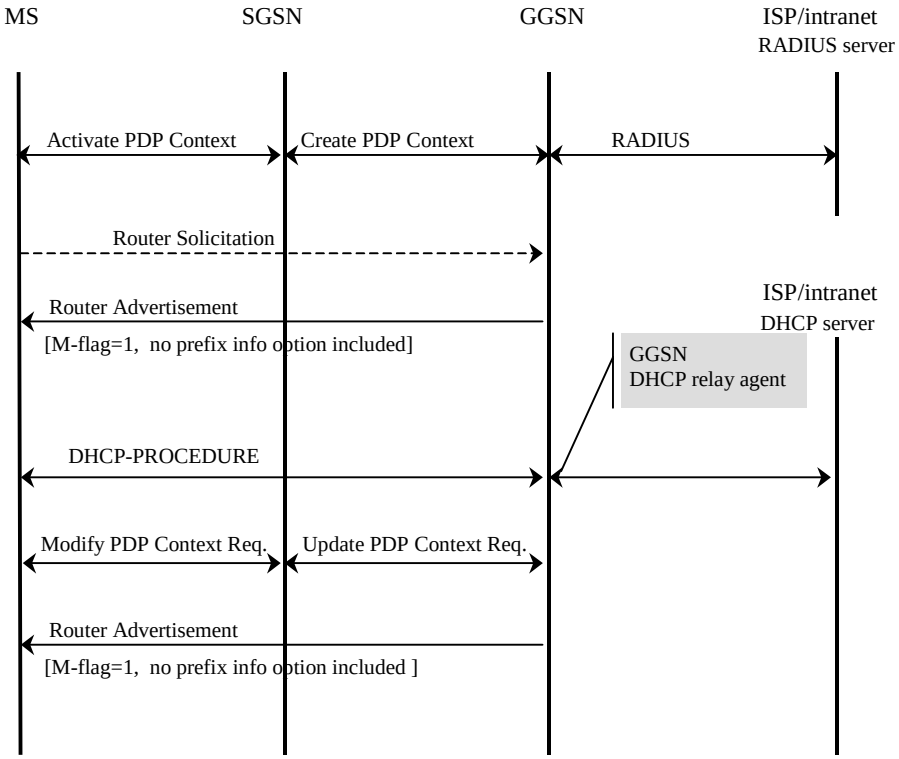


Figure 11bc: IPv6 Stateful Address Autoconfiguration

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 s (6 h).

MinRtrAdvInterval

Shall have a default value of 0,75 × MaxRtrAdvInterval i.e.16 200 s (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.

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 3344 [30]. Mobile IP (MIP) is a mobility management protocol developed by IETF. The Mobile IP Foreign Agent (FA) RFC 3344 [30] is located in the Core Network in the GGSN. MIP also uses a Home Agent (HA) RFC 3344 [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 3344 [30] are sent with UDP.

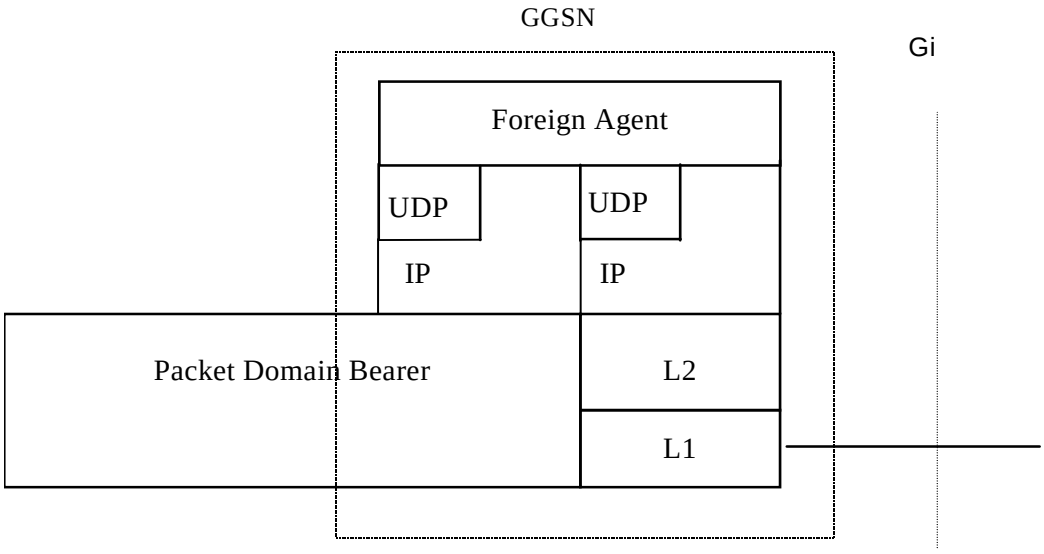


Figure 11c: The protocol stacks for the Gi IP reference point in the MIP signalling plane

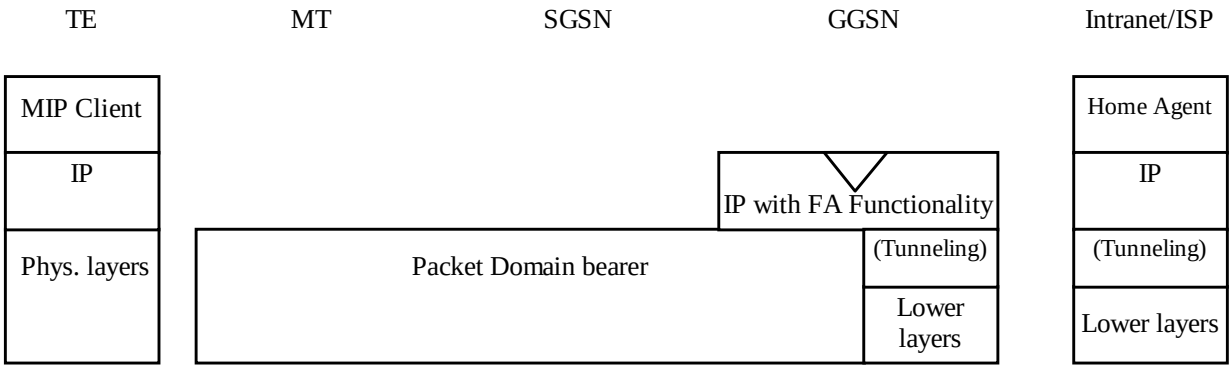


Figure 11d: Protocol stacks for user access with MIP

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

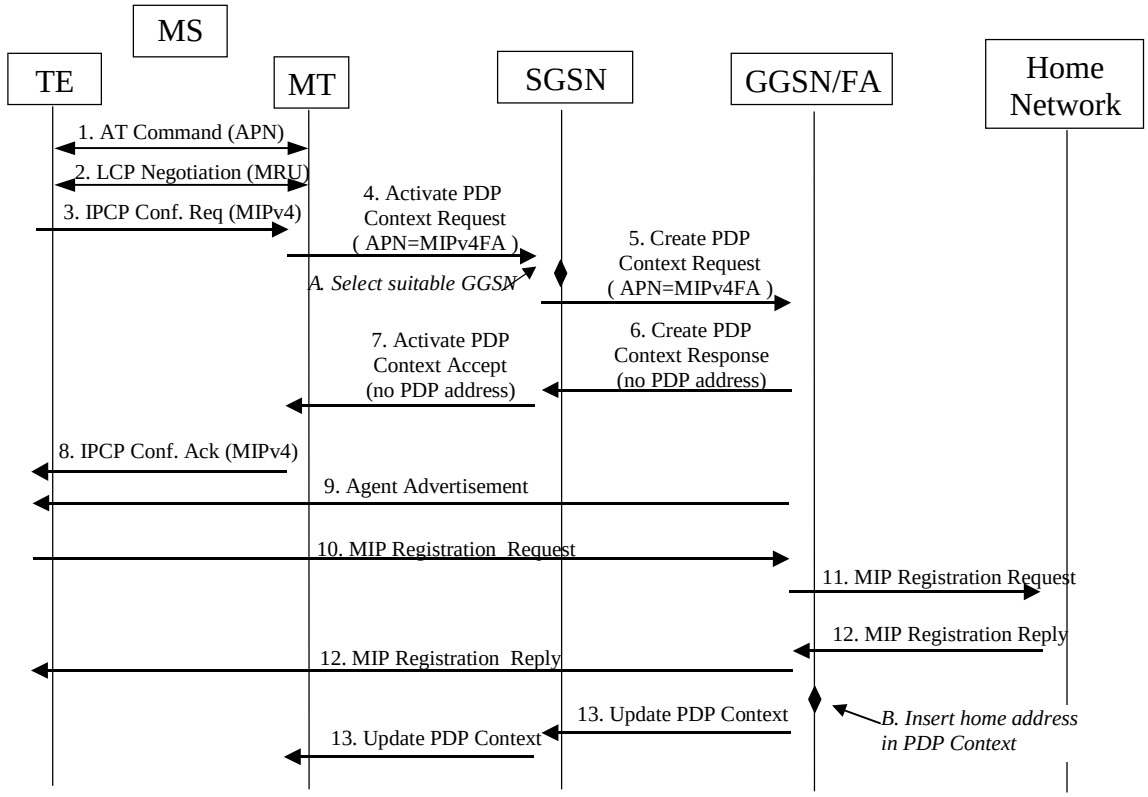


Figure 11e: Example of PDP Context activation with Mobile IP registration (the PS attach procedure not included)

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 MSs 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 3344 [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 3344 [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: 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.

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.

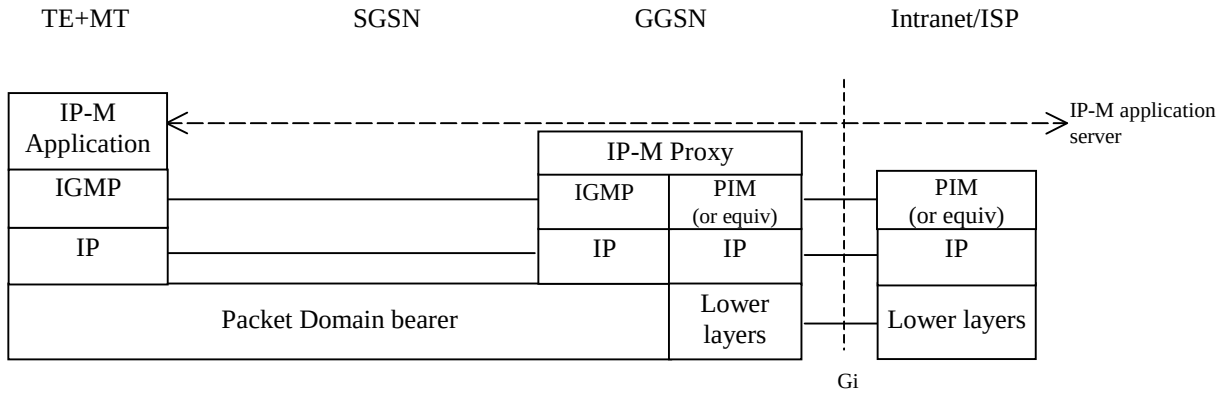


Figure 12: Protocol configuration for IP-Multicast handling (control plane)

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 NCPs 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.

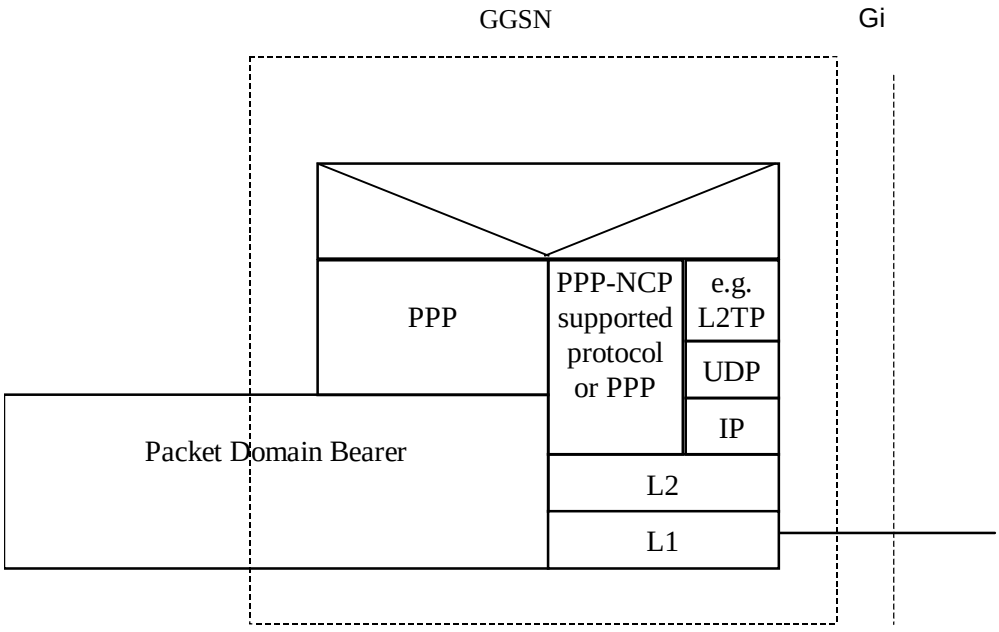


Figure 13: The protocol stacks for the Gi PPP reference point

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);

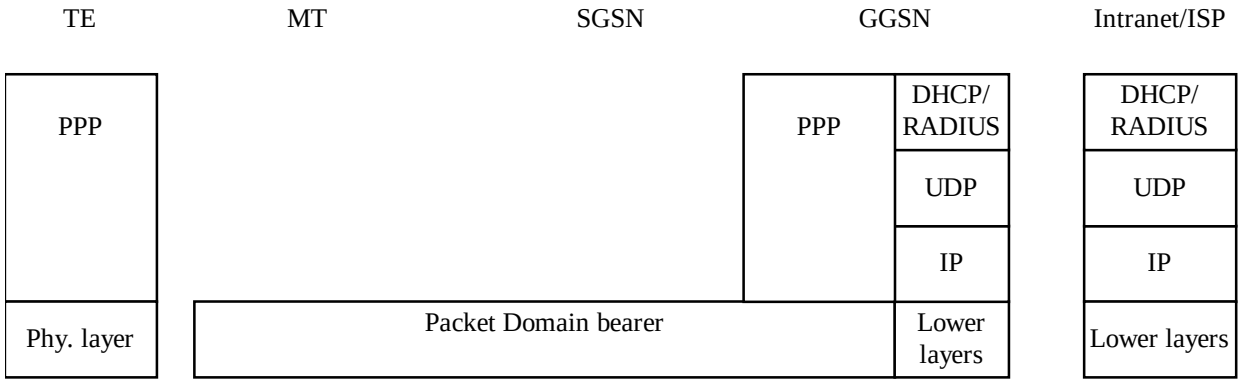


Figure 14: Protocol stack for direct access to IP-based Intranets/ISPs

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

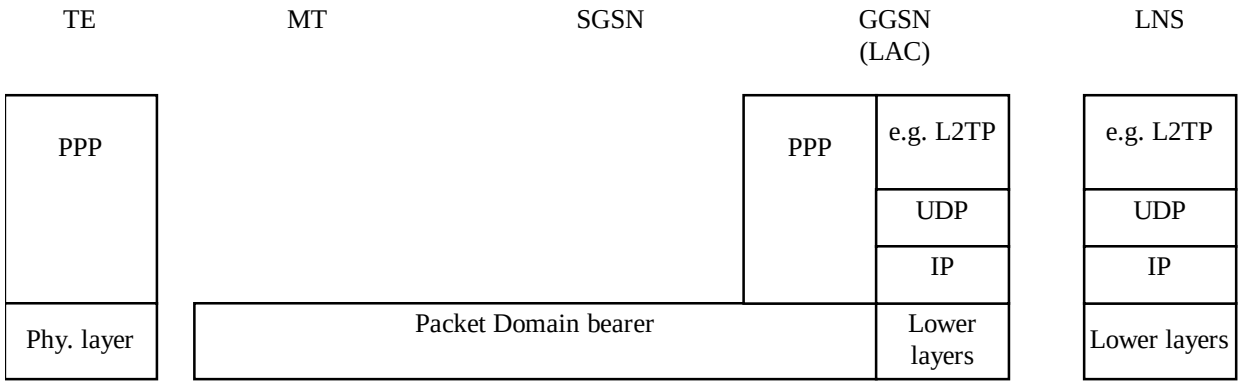


Figure 15: Protocol stack for virtual dial-up access with PPP frame tunnelling

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.

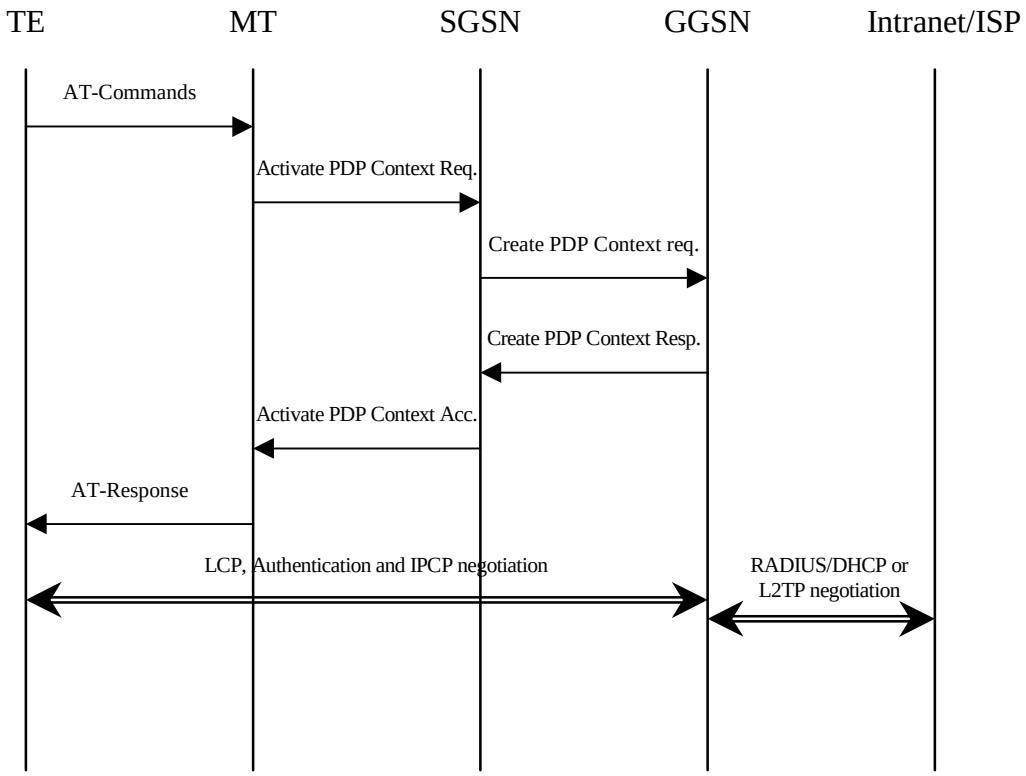


Figure 16a

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 (Dynamic Host Configuration Protocol for IPv6, IETF RFC 3315 [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 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.

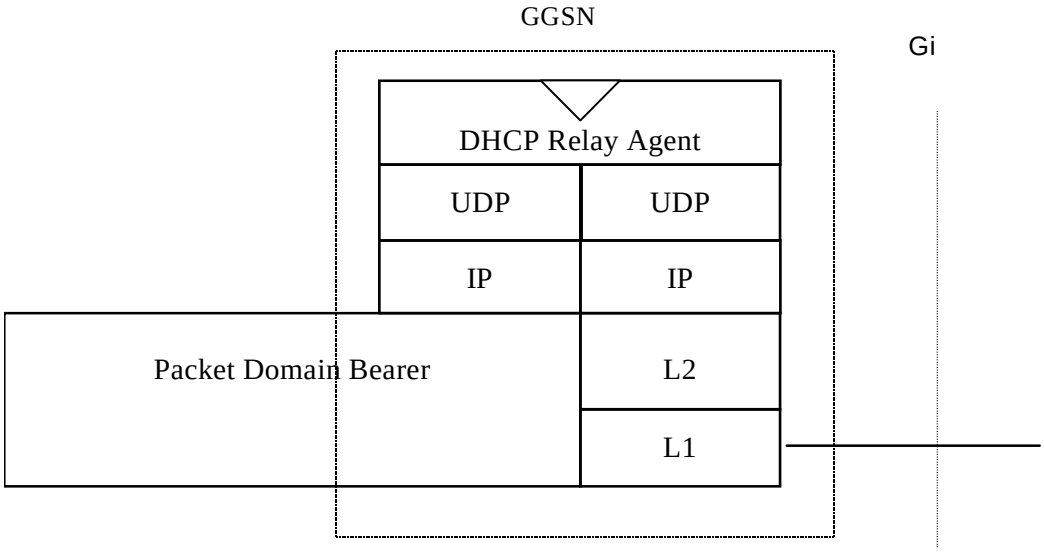


Figure 16b: The protocol stacks for the Gi IP reference point for DHCP

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.

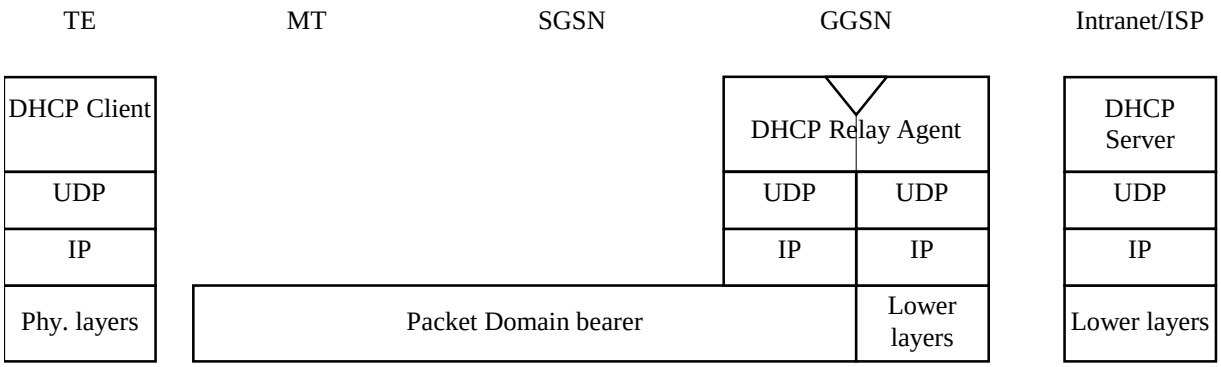


Figure 16c: Protocol stack for access with DHCP end-to-end

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.

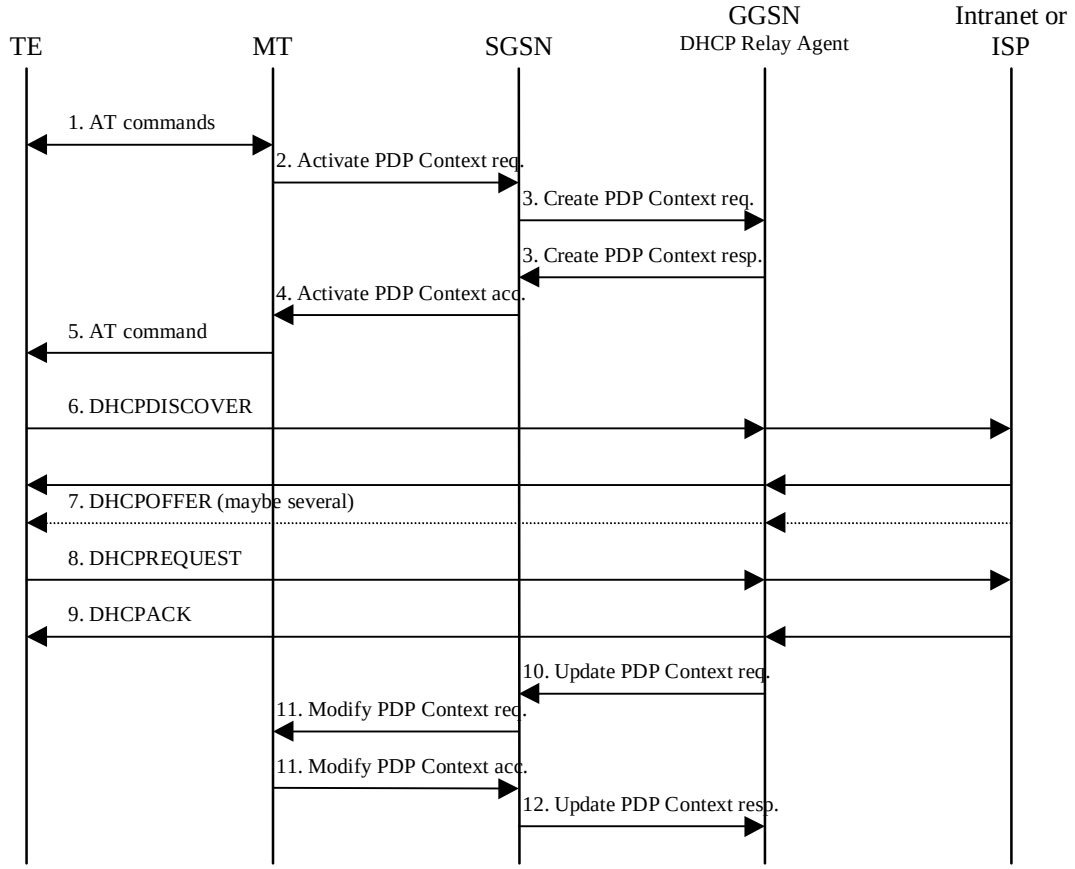


Figure16d: DHCPv4 signal flow

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 RFC 3315 [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) 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 RFC 3315 [46]. The source address is the link local address created by the MS. The SOLICIT message shall contain exactly one IA option.

2) The GGSN creates a RELAY-FORWARD message. The "Relay 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 RFC 3315 [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) DHCP servers receiving the RELAY-FORWARD message including the SOLICIT request reply by sending a RELAY-REPLY message. The "Relay Message" option includes the ADVERTISE message with an offered IP address.

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

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

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

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

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

11) 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 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.

The DHCPv6 server shall be configured to return exactly one address per IA option. If the request from the MS contains more than one IA option or if an MS sends additional REQUESTs for a PDP context that already has an address, the GGSN shall reject the request and return the status code " UnspecFail " (see IETF RFC3315 [46]) to the MS.

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

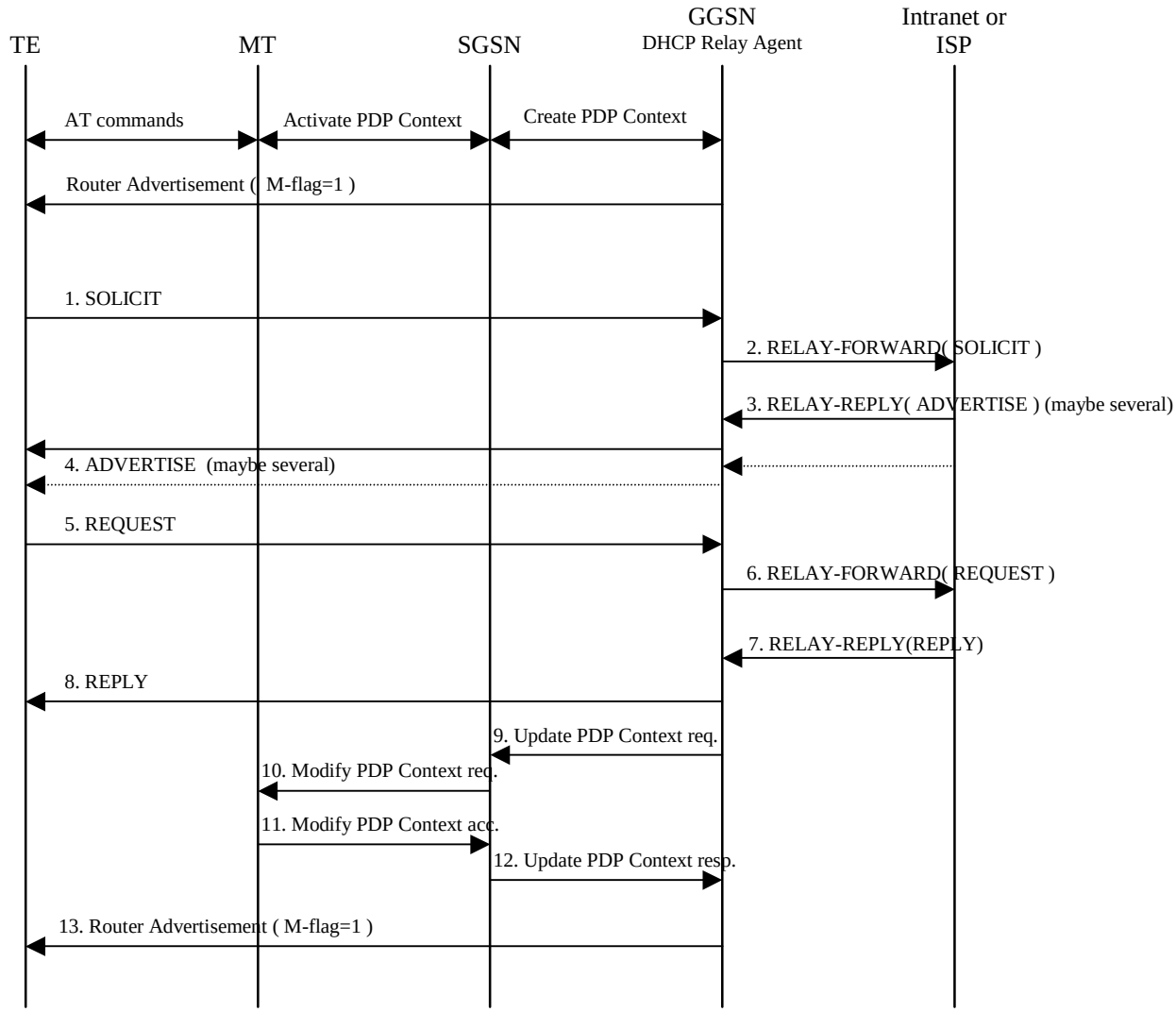


Figure 16e: DHCPv6 signal flow

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 RFC 3315 [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 RFC 3315 [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 "Relay 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.

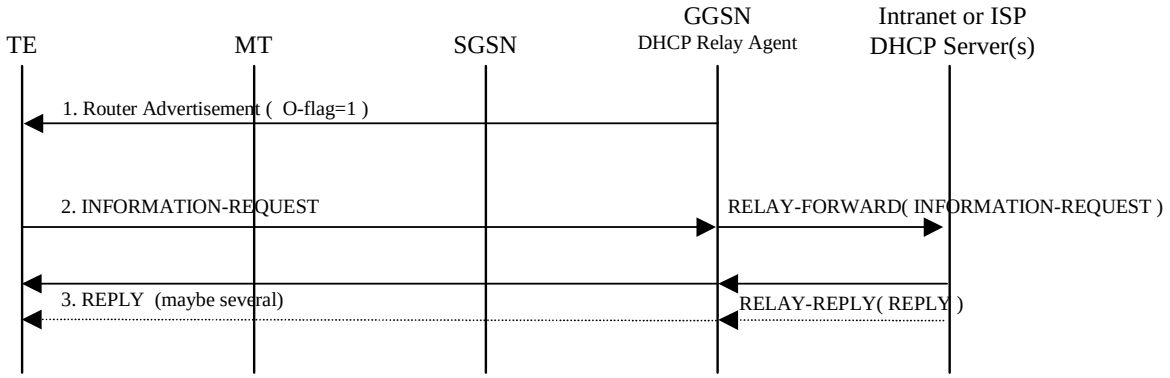


Figure 16f: DHCPv6 Other configuration signal flow

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 or without enhanced QoS); 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 PDF. 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 providing 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.

The GGSN shall have configurable policy rules for controlling PDP contexts used for signalling as specified in section 13a.2.2.2.

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 for Signalling

The following applies for establishing a PDP context for signalling in the GGSN:

I. 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.

II. 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 [47]) by setting the IM CN Subsystem signalling flag in the PCO IE. If dedicated signalling PDP contexts are not supported, GGSN will reset the signalling flag in the response to the MS.

In both cases, I and II, the GGSN may receive the Signalling Indication parameter in the QoS IE. This indicates a request for prioritised handling over the radio interface. The GGSN shall be able to downgrade the QoS (dependent on operator policy) by resetting the Signalling Indication according to the normal procedures for QoS negotiation, see 3GPP TS 23.060 [3].

The operator may provide other properties to dedicated signalling PDP contexts, e.g. special charging. 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/PDF. The interaction between the GGSN and the P-CSCF/PDF, 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. The GGSN shall handle Create PDP Context Requests that include binding information as specified in 3GPP TS 29.207 [53].

The GGSN identifies the PDF to interact with using a PDF identifier. The PDF 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)

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.

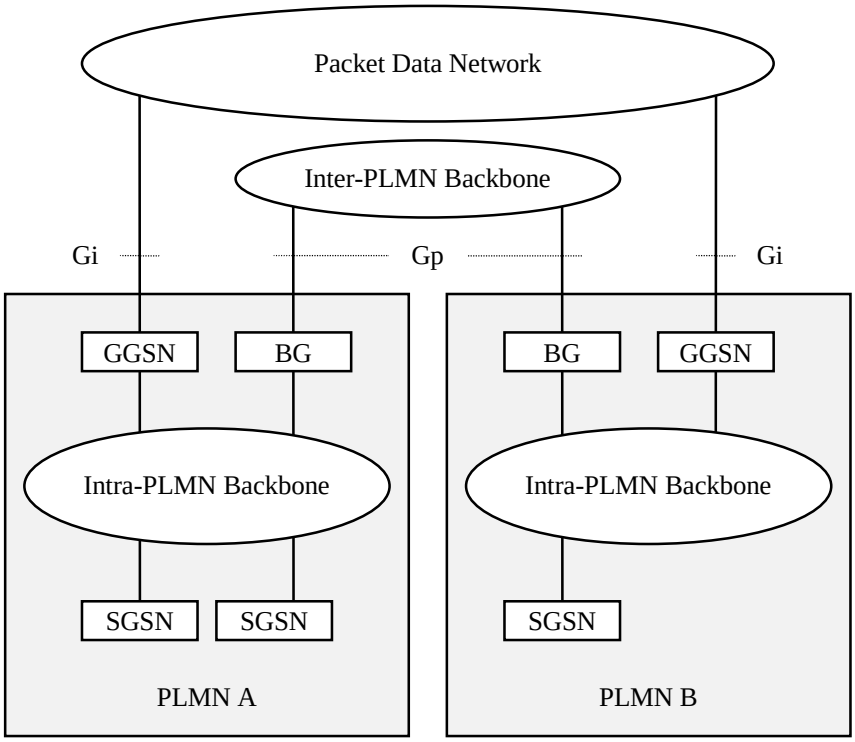


Figure 21: General interworking between Packet Domains to support roaming subscribers.

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) 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.

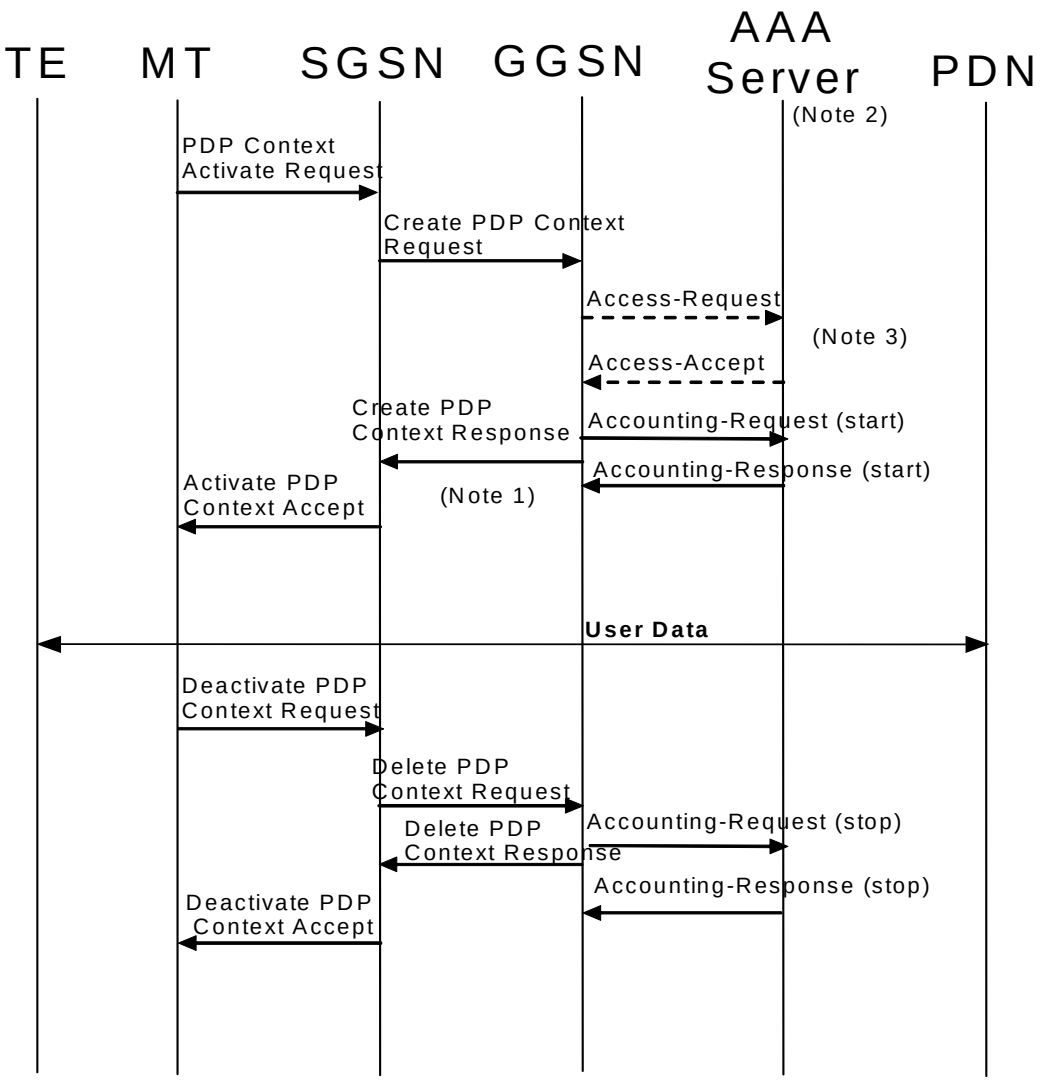
If the AAA server is used for IP address or IPv6 prefix assignment, then, upon reception of a RADIUS Accounting-Request STOP message for all PDP contexts associated to a session defined by APN and IMSI or MSISDN, the AAA server may make the associated IP address or IPv6 prefix available for assignment.

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

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. The session is uniquely identified by the Acct-Session-Id that is composed of the Charging-Id and the GGSN-Address.

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.

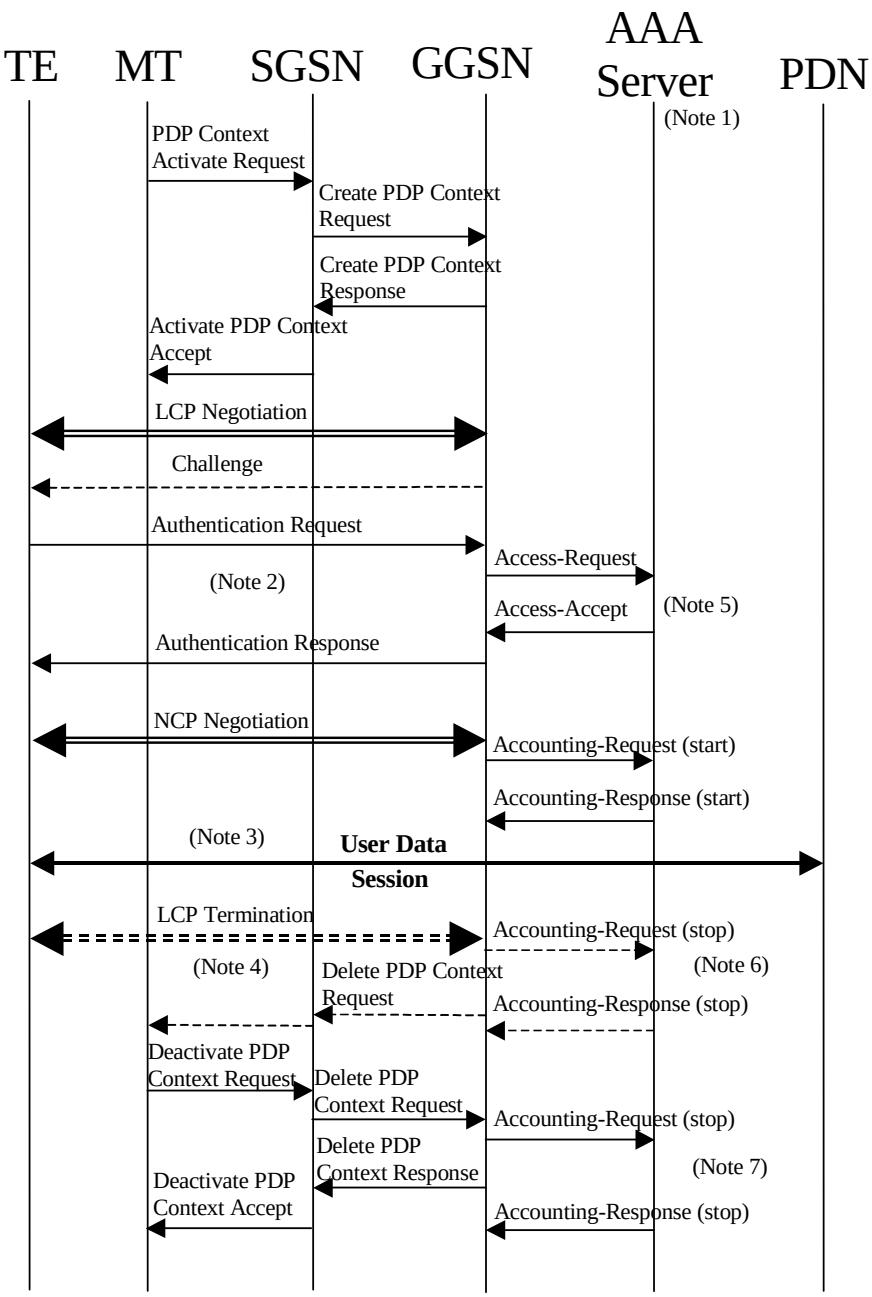
The GGSN may send an Accounting-Request ON message to the AAA server to indicate that a restart has occurred. The AAA server may then release the associated resources.

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

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 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.

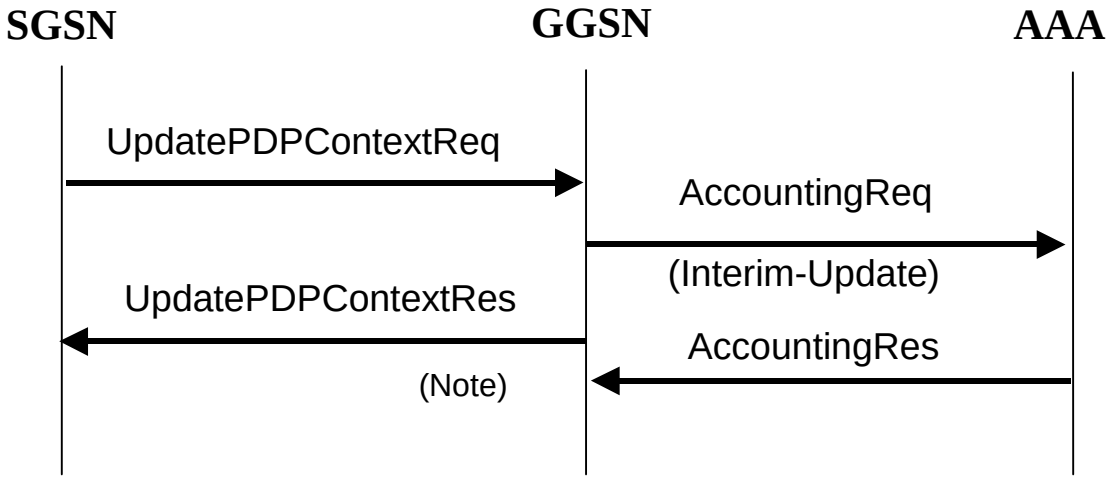
The GGSN may send an Accounting-Request ON message to the AAA server to indicate that a restart has occurred. The AAA server may then release the associated resources.

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: 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.

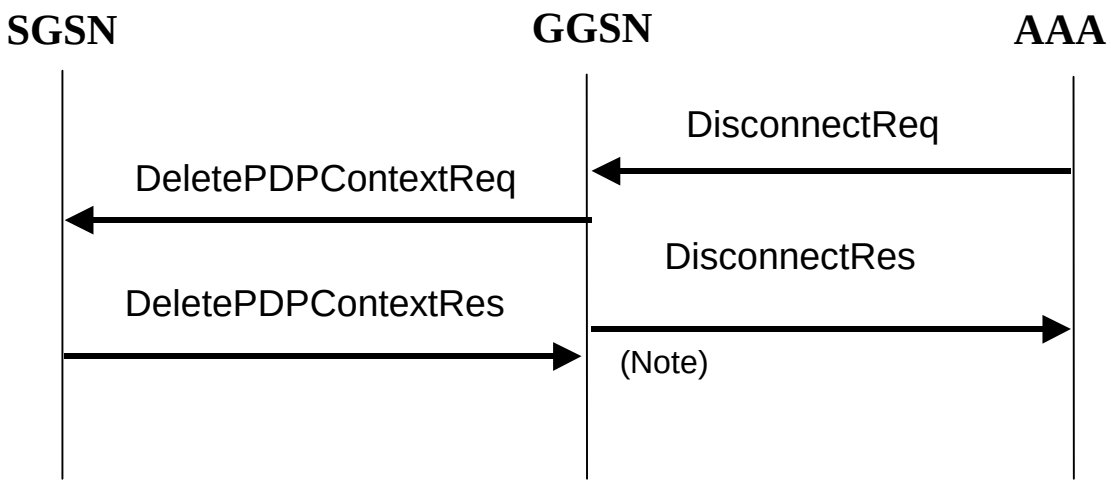
Figure 24: RADIUS for PDP context Update

16.3.4 AAA-Initiated PDP context termination

RADIUS is used as the protocol between the GGSN and an 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 3576 [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.

The Teardown-Indicator in the RADIUS Disconnect Request message indicates to the GGSN that all PDP contexts for this particular user and sharing the same user session shall be deleted. The PDP contexts (primary and secondary) are identified by the Acct-Session-Id. The Charging-Id contained in the Acct-Session-Id can be of any primary or secondary PDP contexts of the user. The GGSN is able to find out all the related PDP contexts sharing the same user session once it has found the exact PDP context from the Acct-Session-Id. If a user has the same user IP address for different sets of PDP contexts towards different networks, only the PDP contexts linked to the one identified by the Acct-Session-Id shall be deleted.

Since the Charging-Id contained in the Acct-Session-Id is already sufficient to uniquely identify PDP context(s) for a user session on a GGSN, it has no impact if the user IP address is not known by the GGSN (e.g. in the case of transparent PPP PDP sessions). In this case the user IP address in the Disconnect message should be set to zero (e.g. 0.0.0.0 for IPv4).



NOTE: 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)

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 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 4
95	NAS-IPv6-Address	IP address of the GGSN for communication with the AAA server.	IPv6	Conditional Note 3 and 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

Attr #	Attribute Name	Description	Content	Presence Requirement
8	Framed-IP-Address	IP address allocated for this user	IPv4	Conditional Note 4
9	Framed-IP-Netmask	Netmask for the user IP address	IPv4	Conditional Note 4
97	Framed-IPv6-Prefix	IPv6 address prefix allocated for this user	IPv6	Conditional Note 4
96	Framed-Interface-Id	User IPv6 Interface Identifier	IPv6	Conditional Notes 4 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 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 subclause 16.4.7	See subclause 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 4: Either IPv4 or IPv6 address/prefix attribute shall be present. The IP protocol version for end-user and network may be different.
NOTE 5: 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)

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 2
9	Framed-IP-Netmask	Netmask for the user IP address, if the AAA server is used to allocate IP netmask.	IPv4	Conditional Note 2
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

Attr #	Attribute Name	Description	Content	Presence Requirement
100	Framed-IPv6-Pool	Name of the prefix pool for the specific APN	IPv6	Optional Note 2
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 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
26/311	MS-Secondary-DNS-Server	Contains the secondary DNS server address for this APN	IPv4	Optional Note 3
26/311	MS-Primary-NBNS-Server	Contains the primary NetBios name server address for this APN	IPv4	Optional Note 3
26/311	MS-Secondary-NBNS-Server	Contains the secondary NetBios server address for this APN	IPv4	Optional Note 3
26/10415/17	3GPP-IPv6-DNS-Servers	List of IPv6 addresses of DNS servers for this APN	IPv6	Optional Note 3
NOTE 1: The presence of this attribute is conditional upon this attribute being received in the Access-Accept message NOTE 2: Either IPv4 or IPv6 address/prefix attribute shall be present. The IP protocol version for end-user and network may be different. NOTE 3: Either IPv4 or IPv6 address attribute shall be present				

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

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 1 and 3
95	NAS-IPv6-Address	GGSN IPv6 address for communication with the AAA server.	IPv6	Conditional Notes 1 and 3
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 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 Note 3
97	Framed-IPv6-Prefix	User IPv6 Prefix	IPv6	Conditional Note 3
96	Framed-Interface-Id	User IPv6 Interface Identifier	IPv6	Conditional Notes 3 and 4
25	Class	Received in the access accept	String	Conditional (Note 2)
30	Called-Station-Id	Identifier for the target network	APN (UTF-8	Mandatory

Attr #	Attribute Name	Description	Content	Presence Requirement
			encoded)	
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)	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 (IPv4 or IPv6) and Charging-ID concatenated in a UTF-8 encoded hexadecimal. (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 subclause 16.4.7.	See subclause 16.4.7	Optional except sub-attribute 3 which is conditional

NOTE 1: Either NAS-IP-Address or NAS-Identifier shall be present.
NOTE 2: The presence of this attribute is conditional upon this attribute being received in the Access-Accept message
NOTE 3: Either IPv4 or IPv6 address/prefix attribute shall be present. The IP protocol version for end-user and network may be different.
NOTE 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.

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

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) 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

Attr #	Attribute Name	Description	Content	Presence Requirement
95	NAS-IPv6-Address	IP address of the GGSN for communication with the AAA server.	IPv6	Conditional Notes 1 and 3
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 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 Note 3
97	Framed-IPv6-Prefix	User IPv6 Prefix	IPv6	Conditional Note 3
96	Framed-Interface-Id	User IPv6 Interface Identifier	IPv6	Conditional Notes 3 and 4
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 23.003 [40], UTF-8 encoded. (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 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 subclause 16.4.7.	See subclause 16.4.7	Optional except sub-attribute 3 which is conditional

Attr #	Attribute Name	Description	Content	Presence Requirement
NOTE 1: Either NAS-IP-Address or NAS-Identifier shall be present. NOTE 2: The presence of this attribute is conditional upon this attribute being received in the Access-Accept message NOTE 3: Either IPv4 or IPv6 address/prefix attribute shall be present. The IP protocol version for end-user and network may be different. NOTE 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)

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 Notes 1 and 2
95	NAS-IPv6-Address	IP address of the GGSN for communication with the AAA server.	IPv6	Conditional Notes 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
NOTE 1: Either NAS-IP-Address or NAS-Identifier shall be present. NOTE 2: Either IPv4 or IPv6 address attribute shall be present.				

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

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 1 and 2
95	NAS-IPv6-Address	IP address of the GGSN for communication with the AAA server.	IPv6	Conditional Notes 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
NOTE 1: Either NAS-IP-Address or NAS-Identifier shall be present. NOTE 2: Either IPv4 or IPv6 address attribute shall be present.				

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

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

Table 7: List of the 3GPP Vendor-Specific sub-attributes

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-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	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

Sub-attr #	Sub-attribute Name	Description	Presence Requirement	Associated attribute (Location of Sub-attr)
19	3GPP-Teardown-Indicator	Indicate to the GGSN that all PDP contexts for this particular user and sharing the same user session need to be deleted.	Optional	Disconnect Request
20	3GPP-IMEISV	International Mobile Equipment Id and its Software Version	Optional	Accounting-Request START, Access-Request
21	3GPP-RAT-Type	Indicate which Radio Access Technology is currently serving the UE	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
22	3GPP-User-Location-Info	Indicate details of where the UE is currently located (e.g. SAI or CGI).	Optional	Accounting-Request START, Access-Request, Accounting-Request STOP, Accounting-Request Interim-Update
23	3GPP-MS-TimeZone	Indicate the offset between universal time and local time in steps of 15 minutes of where the MS currently resides.	Optional	Accounting-Request START, Access-Request, Accounting-Request STOP, Accounting-Request Interim-Update
24	3GPP-CAMEL-Charging-Info	Used to copy any CAMEL Information present in S-CDR(s).	Optional	Accounting-Request START, Access-Request
25	3GPP-Packet-Filter	Packet Filter used for this PDP context	Optional	Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
26	3GPP-Negotiated-DSCP	DSCP used to mark the IP packets of this PDP context on the Gi interface	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]. 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: L ≤ 33 (release 5 or higher) or L ≤ 27 (release 4 or release 99) or L = 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 or release 4

"05"= Release 5 or higher

<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 and release 4 QoS profile data is 11 octets long, which results in a 22 octets UTF-8 encoded string.

The release 5 (and higher) QoS profile data is 14 octets long, which results in a 28 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] 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] 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 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] 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.

19 - 3GPP-***Teardown Indicator***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 19							
2	3GPP Length= 3							
3	spare							TI

3GPP Type: 19

Length: 3

If the value of TI is set to "1", then all PDP contexts that share the same user session with the PDP context identified by the NSAPI included in the Delete PDP Context Request Message shall be torn down. Only the PDP context identified by the NSAPI included in the Delete PDP context Request shall be torn down if the value of TI is "0".

20 -3GGP- ***IMEISV***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP Type = 20							
2	3GPP Length = 18							
3	IMEISV digits 1 - n							

3GPP Type: 20

n = 16 where TAC = 8 digits SNR = 6 digits & SVN = 2 digits

21 - 3GPP-***RAT-Type***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 21							
2	3GPP Length= 3							
3	RAT							

3GPP Type: 21

The 3GPP-RAT-Type attribute indicates which Radio Access Technology is currently serving the UE.

RAT field: Radio Access Technology type values. It shall be coded as specified in TS 29.060 [24]

22 - 3GPP-***User-Location-Info***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 22							
2	3GPP Length= m							
3	Geographic Location Type							
4-m	Geographic Location							

3GPP Type: 22

Length=m, where m depends on the Geographic Location Type

m= 11 in the CGI and SAI types.

Geographic Location Type filed is used to convey what type of location information is present in the 'Geographic Location' field. The geographic loction type values and coding are as defined in TS 29.060 [24].

Geographic Location filed is used to convey the actual geographic information as indicated in the Geographic Location Type. The coding of this field is as specified in TS 29.060 [24]

23 - 3GPP-***MS-TimeZone***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 23							
2	3GPP Length= 4							
3	Time Zone							
4	Daylight Saving Time							

3GPP Type: 23

Length=4

The Time Zone field and the Dyalight Saving Time fields are used to indicate the offset between universal time and local time in steps of 15 minutes of where the MS current resides. Both fields are coded as specified in 3GPP TS 29.060 [24].

24 - 3GPP-***Camel-Charging-Info***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 24							
2	3GPP Length= m							
3-m	CAMEL Charging Information Container							

3GPP Type: 24

Length=m

m depends on the size of the CAMELInformationPDP IE.

The CAMEL Charging Information Container field is used to copy the CAMELInformationPDP IE including Tag and Length from the SGSN's CDR (S-CDR). The coding of this field is as specified in 3GPP TS 29.060 [24]

25 - 3GPP-***Packet-Filter***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 25							
2	3GPP Length= n							
3-z	Packet Filter							

3GPP Type: 25

Length: n

Each 3GPP-Packet-Filter attribute contains only one packet filter. Multiple 3GPP-Packet-Filter attributes can be sent in one RADIUS Accounting Request message.

When the GGSN sends the packet filter information, the RADIUS message shall carry ALL (or none) of the packet filters.

Packet Filter Value:

8	7	6	5	4	3	2	1	
Packet filter identifier								Octet 1
Packet filter evaluation precedence								Octet 2
Length of Packet filter contents								Octet 3
Direction of Packet Filter								Octet 4
Packet filter contents								Octet 5 Octet m

Direction Value:

00000000: Downlink

00000001: Uplink

The packet filter content is defined below:

Type	Value
1: IPv4 address type	Contains the source address if the direction value is set to Downlink, and the destination address if the direction value is set to Uplink. shall be encoded as a sequence of a four octet *IPv4 address* field and a four octet *IPv4 address mask* field. The *IPv4 address* field shall be transmitted first

2: IPv6 address type	Contains the source address if the direction value is set to Downlink, and the destination address if the direction value is set to Uplink. shall be encoded as a sequence of a sixteen octet *IPv6 address* field and a sixteen octet *IPv6 address mask* field. The *IPv6 address* field shall be transmitted first
3: Protocol identifier/Next header type	shall be encoded as one octet which specifies the IPv4 protocol identifier or IPv6 next header
4: Single destination port type	shall be encoded as two octet which specifies a port number
5 : Destination port range type	shall be encoded as a sequence of a two octet *port range low limit* field and a two octet *port range high limit* field. The *port range low limit* field shall be transmitted first
6 : Single source port type	shall be encoded as two octet which specifies a port number
7: Source port range type	shall be encoded as a sequence of a two octet *port range low limit* field and a two octet *port range high limit* field. The *port range low limit* field shall be transmitted first
8: Security parameter index type (IPv6)	shall be encoded as four octet which specifies the IPSec security parameter index
9: Type of service/Traffic class type	shall be encoded as a sequence of a one octet *Type-of-Service/Traffic Class* field and a one octet *Type-of-Service/Traffic Class mask* field. The *Type-of-Service/Traffic Class* field shall be transmitted first
10: Flow label type (IPv6)	shall be encoded as three octets which specify the IPv6 flow label. The bits 8 through 5 of the first octet shall be spare whereas the remaining 20 bits shall contain the IPv6 flow label

Note: The sending of this attribute is not recommended for an inter-operator interface for security reason

26 - 3GPP-***Negotiated-DSCP***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 26							
2	3GPP Length= 3							
3	Negotiated DSCP							

3GPP Type: 26

Length: 3

Negotiated DSCP value: String

The DSCP value is converted into an octet string.

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

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
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
95	NAS-IPv6-Address	IP address of the GGSN for communication with the AAA server.	IPv6	Conditional Notes 1 and 3
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 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 Note 3
97	Framed-IPv6-Prefix	User IPv6 address	IPv6	Conditional Note 3
96	Framed-Interface-Id	User IPv6 Interface Identifier	IPv6	Conditional Notes 3 and 4
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 23.003 [40], UTF-8 encoded. (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 5)	Mandatory
45	Acct-Authentic	Authentication method	RADIUS or	Optional

Attr #	Attribute Name	Description	Content	Presence Requirement
			LOCAL	
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 subclause 16.4.7.	See subclause 16.4.7	Optional except sub-attribute 3 which is conditional
NOTE 1: Either NAS-IP-Address or NAS-Identifier shall be present. NOTE 2: The presence of this attribute is conditional upon this attribute being received in the Access-Accept message NOTE 3: Either IPv4 or IPv6 address/prefix attribute shall be present. The IP protocol version for end-user and network may be different. NOTE 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.				

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

Table 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
97	Framed-IPv6-Prefix	User IPv6 address	IPv6	Conditional Note 2
96	Framed-Interface-Id	User IPv6 Interface Identifier	IPv6	Conditional Notes 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 3)	Mandatory
26/10415	3GPP Vendor-Specific	Sub-attributes according to subclause 16.4.7.	See subclause 16.4.7	Optional
NOTE 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 2: Either IPv4 or IPv6 address/prefix attribute shall be present. See subclause 16.3.4. NOTE 3: The GGSN IP address is the same as that used in the GCDRs.				

17 Usage of Diameter on Gmb interface

Signalling between GGSN and BM-SC is exchanged at Gmb reference point. BM-SC functions for different MBMS bearer services may be provided by different physical network elements. To allow this distribution of BM-SC functions, the Gmb protocol must support the use of proxies to correctly route the different signalling interactions in a manner which is transparent to the GGSN.

The GGSN uses the Gmb interface

- to request authorisation/deactivation of a user for a multicast MBMS service,
- to register/de-register the GGSN for receiving a multicast MBMS service.
- to receive indication of session start and session stop messages, which shall cause the GGSN, SGSN and RAN to set up/tear down the appropriate resources for the service. For further details, see 3GPP TS 23.246 [65].

The support of Gmb within the GGSN is optional, and needed for MBMS.

The Gmb application is defined as an IETF vendor specific Diameter application, where the vendor is 3GPP. The vendor identifier assigned by IANA to 3GPP (http://www.iana.org/assignments/enterprise-numbers) is 10415. The Gmb application identifier value assigned by IANA is 16777223.

Due to the definition of the commands used in Gmb protocol, there is no possibility to skip the Auth-Application-Id AVP and use the Vendor-Specific-Application-Id AVP instead. Therefore the Gmb application identifier value shall be included in the Auth-Application-Id AVP.

The BM-SC and the GGSN shall advertise the support of the Gmb application by including the value of the application identifier in the Auth-Application-Id AVP and the value of the 3GPP (10415) in the Vendor-Id AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands as specified in RFC 3588 [66], i.e. as part of the Vendor-Specific-Application-Id AVP. The Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands are specified in the Diameter Base Protocol.

17.1 MBMS user authorisation

Upon reception of an IGMP (IPv4) or MLD (IPv6) Join message for an IP multicast address allocated to MBMS services, the GGSN shall request authorisation of the user for this multicast MBMS bearer service (identified by the PDP context over which the IGMP join is received).

The GGSN shall support pre-configuration of a BM-SC or Gmb proxy server for authorisation purposes to which the request shall be sent. The GGSN may support a list of pre-configured BM-SC servers based on the MBMS bearer service requested, for authorisation purposes.

Upon receipt of an MBMS UE Context Establishment Request for a user who has not already been authorised for the MBMS bearer service, the GGSN shall request authorisation of the user for this service.

17.2 MBMS service registration / de-registration

The MBMS service registration of the GGSN at the BM-SC shall be performed after authorisation of the first user on a particular GGSN, for a particular multicast MBMS Bearer service. The MBMS service de-registration of the GGSN shall be performed when the last user leaves a particular GGSN, for a particular multicast MBMS bearer service.

The MBMS de-registration procedure shall be initiated by BM-SC when the specific multicast MBMS service is terminated.

The GGSN shall support pre-configuration of a BM-SC or Gmb proxy server for registration/de-registration purposes. The GGSN may support a list of pre-configured BM-SC servers based on the MBMS bearer service requested for bearer registration purposes.

17.3 MBMS session start / stop

The MBMS session start shall be used by the BM-SC to trigger the bearer resource establishment and announce the arrival of data for a MBMS bearer service (along with the attributes of the data to be delivered e.g. QoS or MBMS service area) to every GGSN that will deliver the MBMS bearer service.

The MBMS session stop shall be used by the BM-SC to indicate the end of the data stream for an MBMS bearer service to every GGSN that has been delivering the MBMS bearer service.

17.4 MBMS user deactivation

The MBMS user deactivation is a procedure that removes the MBMS UE context from the GGSN for a particular multicast MBMS bearer service (also called "leaving procedure"). This procedure can be initiated by the GGSN or the BM-SC over the Gmb interface.

When the last user leaves a particular GGSN, for a particular MBMS multicast service, a de-registration process shall be initiated.

17.5 Message flows

17.5.1 Service activation

The multicast MBMS bearer service activation procedure registers the user in the network to enable the reception of data from a specific multicast MBMS bearer service

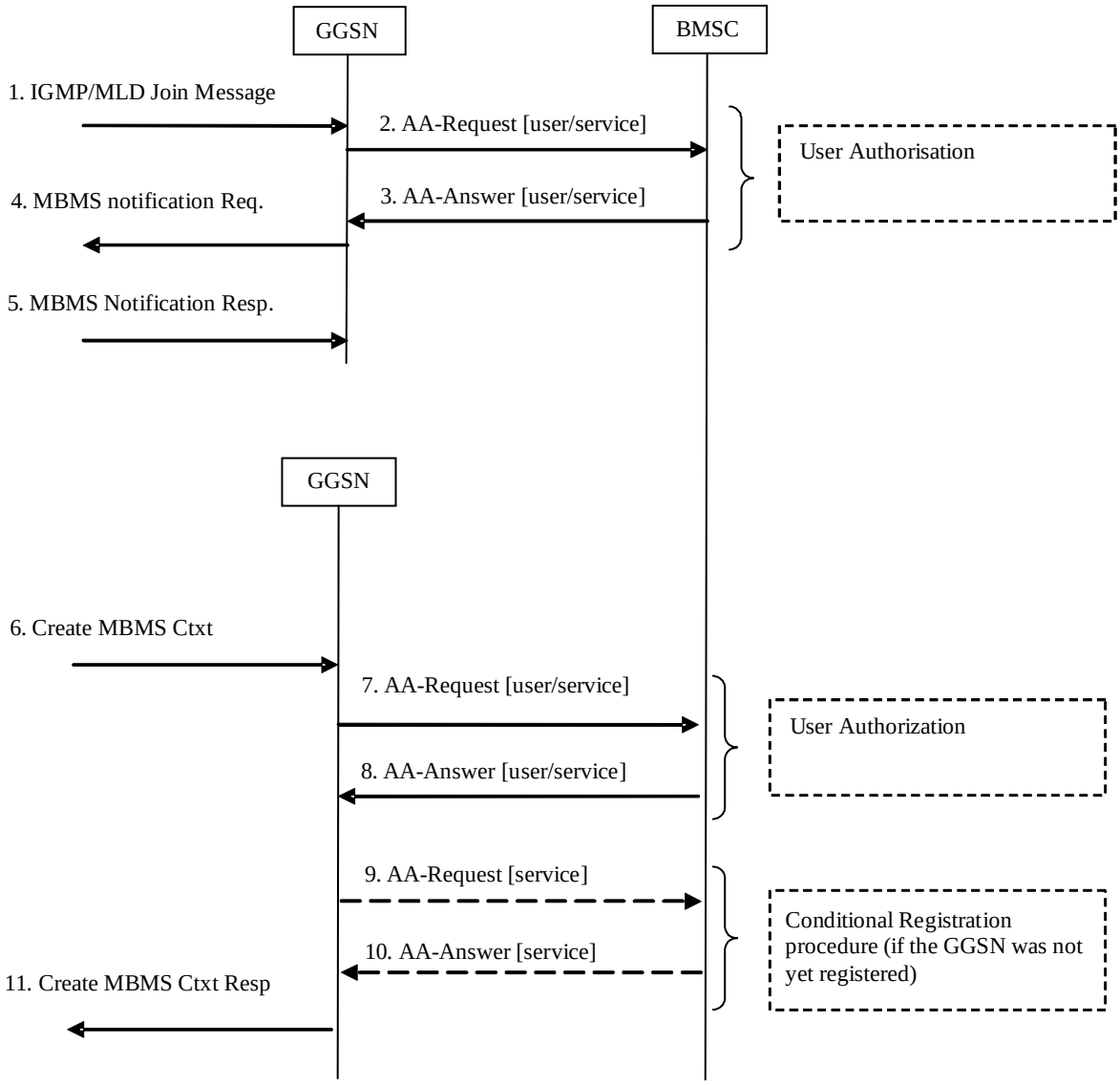


Figure 26; Activation of an MBMS multicast service

1. The GGSN receives an IGMP (IPv4) or MLD (IPv6) Join message from a UE, over the default PDP context to signal its interest in receiving a particular multicast MBMS bearer service identified by an IP multicast address.

2. The GGSN sends an AAR seeking authorization for the activating UE to receive data from a particular service.

3. The authorization decision is provided in the AAA together with the APN to be used for creation of the MBMS UE context. If the AAA indicates that the UE is not authorized to receive the MBMS data the process terminates with no additional message exchange.

4. The GGSN sends an MBMS Notification Request (IP multicast address, APN, Linked NSAPI) to the SGSN. Linked NSAPI is set equal to the NSAPI of the PDP context over which the Join request was received. The IP multicast address is the one requested by the UE in the Join request. The APN may be different from the APN to which the default PDP context has been activated. In any case, the APN may resolve to a GGSN that is different from the GGSN receiving the IGMP/MLD Join request. The GGSN starts a MBMS Activation Timer as GGSN may receive no response, e.g. in case SGSN or UE does not support MBMS.

5. The SGSN sends a MBMS Notification Response (Cause) to the GGSN that sent the MBMS Notification Request, where Cause shall indicate successful or unsuccessful MBMS context activation for the reason of SGSN or UE . Upon reception of the response message with Cause indicating unsuccessful operation or time-out of the MBMS Activation Timer in the GGSN, the GGSN may fallback to IP multicast access as defined in clause 11.7.

6. The SGSN creates an MBMS UE context and sends a Create MBMS Context Requests (IP multicast address, APN, RAI) to the GGSN. That GGSN may be different from the GGSN receiving the IGMP/MLD Join request.

7. The GGSN sends an AAR seeking authorization for the activating UE.

8. The authorization decision is provided in the AAA

9. If the GGSN does not have the MBMS Bearer Context information for this MBMS bearer service, i.e. the GGSN was not yet registered, the GGSN sends a AAR to the BM-SC. See subclause 17.5.4 "Registration Procedure".

   If no TMGI has been allocated for this MBMS bearer service, the BM-SC will allocate a new TMGI. This TMGI will be passed to GGSN via the AAA message.

10. The BM-SC responds with a AAA containing the MBMS Bearer Context information for this MBMS bearer service and adds the identifier of the GGSN to the "list of downstream nodes" parameter in its MBMS Bearer Context. See subclause 17.5.4 "Registration Procedure".

11. The GGSN creates an MBMS UE context and sends a Create MBMS Context Response to the SGSN

17.5.2 Session start procedure

The BM-SC initiates the MBMS session start procedure when it is ready to send data. This informs the GGSN of the imminent start of the transmission and MBMS session attributes are provided to the GGSNs included in the list of downstream nodes in BM-SC. For a multicast MBMS service these are the GGSNs that have previously registered for the corresponding MBMS bearer service. The bearer plane is allocated.

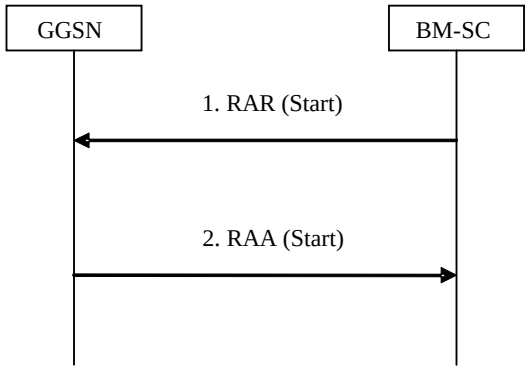


Figure 27: MBMS Session Start procedure

1. The BM-SC sends a RAR message to indicate the impending start of the transmission and to provide the session attributes to the GGSNs listed in the "list of downstream nodes" parameter of the corresponding MBMS Bearer Context. The BM-SC sets the state attribute of its MBMS Bearer Context to "Active".

2. For a broadcast MBMS bearer service the GGSN creates an MBMS Bearer Context. The GGSN stores the session attributes in the MBMS Bearer Context, sets the state attribute of its MBMS Bearer Context to "Active" and sends a RAA message to the BM-SC. An AAR message is not mandated for the Gmb application in response to a RAR- RAA command exchange.

17.5.3 Session stop procedure

The BM-SC initiates the MBMS session stop procedure when it considers the MBMS session terminated. Typically this will happen when there is no more MBMS data expected to be transmitted for a sufficiently long period of time to justify the release of bearer plane resources in the network.

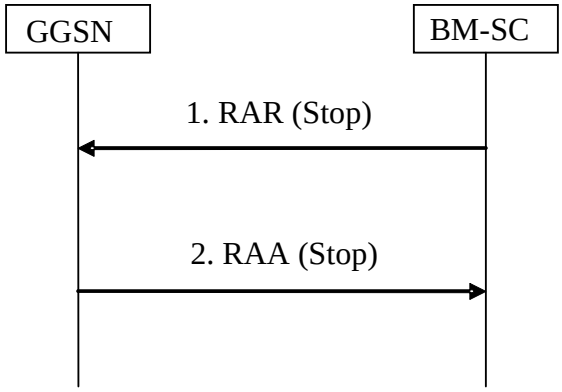


Figure 28: MBMS Session Stop procedure

1. The BM-SC sends a RAR message to all GGSNs listed in the "list of downstream nodes" parameter of the affected MBMS Bearer Context to indicate that the MBMS session is terminated and the bearer plane resources can be released.

2. The GGSN sets the state attribute of its MBMS Bearer Context to "Standby" and sends a RAA message to the BM-SC. An AAR message is not mandated for the Gmb application in response to a RAR- RAA command exchange.

17.5.4 Registration procedure

The registration procedure occurs when the GGSN indicates the BM-SC that it would like to receive session attributes and data for a particular multicast MBMS bearer service, in order to be distributed further downstream. A corresponding MBMS Bearer Context is established as a result between the GGSN and the BM-SC.

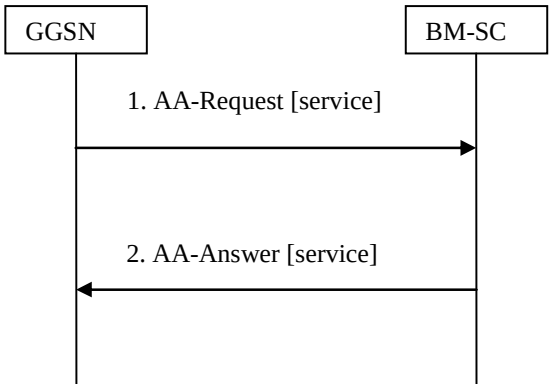


Figure 29: MBMS Registration procedure

1. When the GGSN has no MBMS Bearer Context for an MBMS bearer service and the GGSN receives an MBMS Registration from an SGSN for this MBMS bearer service, or when the first MBMS UE Context is created in the GGSN for an MBMS bearer service for which the GGSN has no MBMS Bearer Context, the GGSN sends a AAR message (containing the IP multicast address and the APN) to the BM-SC.

2. Upon reception of an AAR from a GGSN, the BM-SC adds the identifier of the GGSN to the "list of downstream nodes" parameter in its MBMS Bearer Context and responds with an AAA message (containing TMGI, and Required Bearer Capabilities). If the MBMS Bearer Context is in the 'Active' state, the BM-SC initiates the Session Start procedure with the GGSN, as described in clause 17.5.2 "Session Start Procedure".

17.5.5 De-registration procedure (GGSN initiated)

The MBMS de-registration is the procedure by which the GGSN informs the BM-SC that it does not need to receive signalling, session attributes and data for a particular multicast MBMS bearer service anymore and therefore would like to be removed from the corresponding distribution tree.

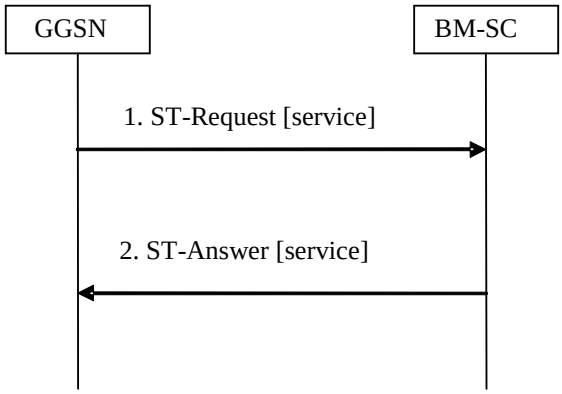


Figure 30: MBMS De-Registration procedure

1. When the "list of downstream nodes" of a particular MBMS Bearer Context in the GGSN becomes empty and the GGSN has no MBMS UE Contexts linked to that MBMS Bearer Context, the GGSN sends a STR message to the BM-SC. If a bearer plane had been established over Gi for this MBMS bearer service, the bearer plane is released.

2. The BM-SC removes the identifier of the GGSN from the "list of downstream nodes" parameter of the affected MBMS Bearer Context and confirms the operation by sending a STA message to the GGSN.

17.5.6 De-registration procedure (BM-SC initiated)

This MBMS de-registration procedure is initiated by BM-SC when the specific multicast MBMS bearer service is terminated. This procedure tears down the distribution tree for the delivery of session attributes and MBMS data. This procedure results in releasing of all MBMS Bearer Contexts.

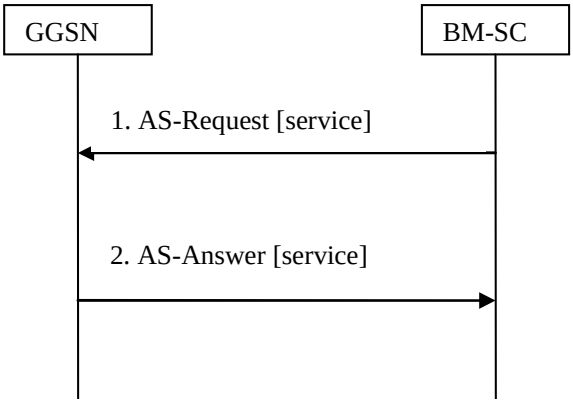


Figure 31: MBMS De-Registration procedure BM-SC initiated

1. The BM-SC sends a ASR message to all GGSNs contained in the "list of downstream nodes" parameter of the corresponding MBMS Bearer Context to indicate that a specific MBMS bearer service is terminated.

2. The GGSN returns a ASA message to the BM-SC. The BM-SC releases all MBMS UE Contexts and removes the identifier of the GGSN from the "list of downstream nodes" parameter of the corresponding MBMS Bearer context.

17.5.7 Service deactivation

The multicast service deactivation is a signalling procedure that will terminate the user registration to a particular MBMS multicast service. The multicast service deactivation can be initiated by the GGSN, when indicated so by the UE, or by the BM-SC, for service specific reasons.

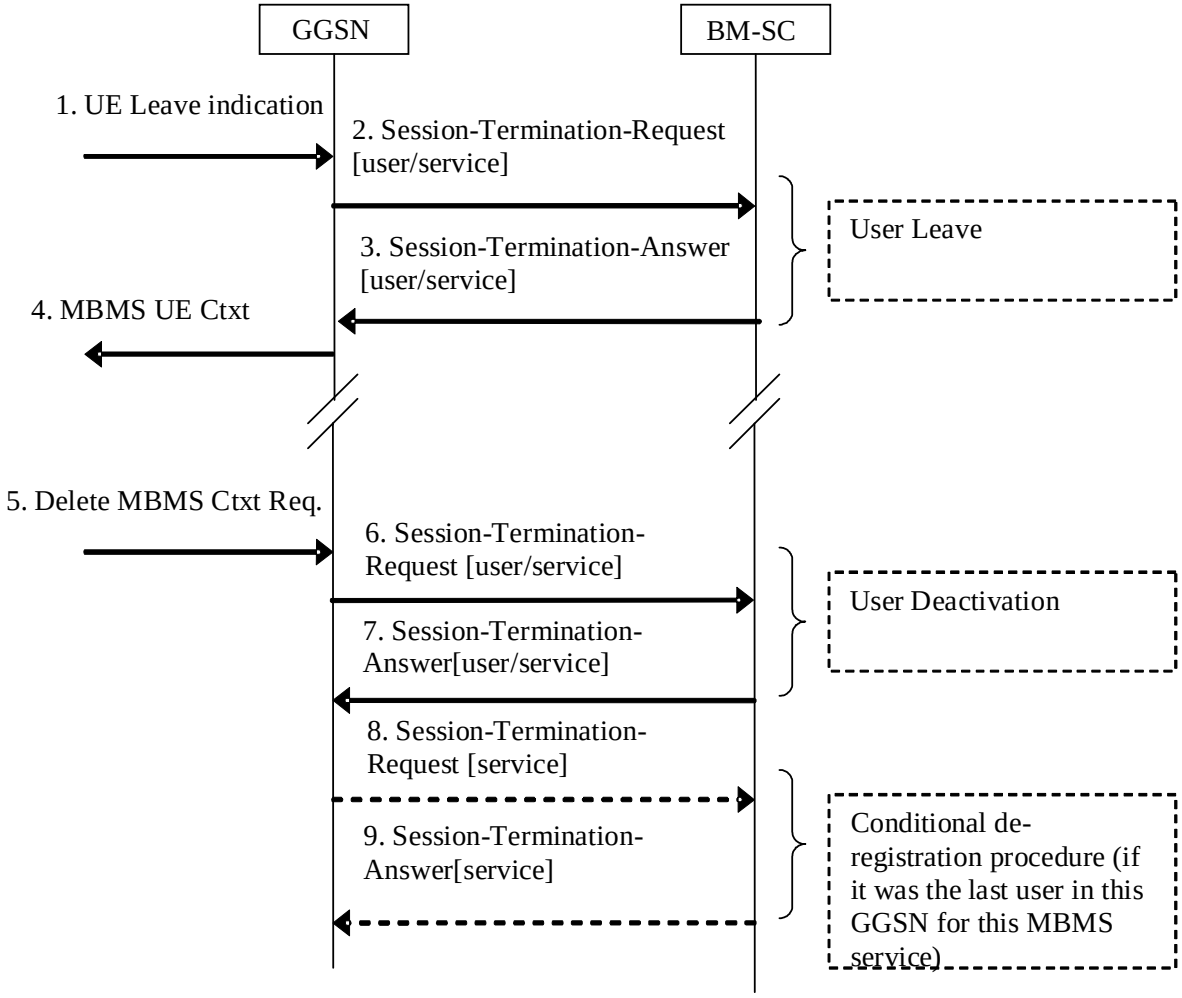


Figure 32: MBMS Service deactivation procedure

1. The UE sends an IGMP (IPv4) or MLD (IPv6) Leave message over the default PDP context to leave a particular multicast service identified by an IP multicast address.

2. The GGSN sends a STR to the BM-SC, indicating that the UE is requesting to leave the multicast service. The session to be terminated is uniquely identified by the Diameter session-id.

3. Upon reception of the STR, the BM-SC verifies that the IP multicast address corresponds to a valid MBMS bearer service and sends a STA to the GGSN that originated the Leave Indication. The APN shall be the same that was provided during service activation (see " Service Activation" procedure).

4. Upon reception of the STA the GGSN sends an MBMS UE Context Deactivation Request to the SGSN. The IP multicast address, APN and IMSI together identify the MBMS UE Context to be deleted by the SGSN. The APN is the one received in step 3.

5. The GGSN receives a Delete MBMS Context Request (NSAPI). This GGSN may be different from the GGSN that receives IGMP Leave request in step 1.

6. The GGSN deletes the MBMS UE Context and sends a STR to the BM-SC to confirm the successful deactivation of the MBMS UE Context.

7. The BM-SC, then, deletes the MBMS UE Context and sends a confirmation to the GGSN in a STA message.

8. If the GGSN does not have any more users interested in this MBMS bearer service and the "list of downstream nodes" in the corresponding MBSM Bearer Context is empty, the GGSN initiates a De-Registration procedure as specified in 17.5.5.

9. The BM-SC confirms the operation by sending a STA message to the GGSN as specified in 17.5.5.

17.5.7.1 BM-SC Initiated Multicast Service Deactivation

This section defines the BM-SC initiated Multicast Service Deactivation procedure.

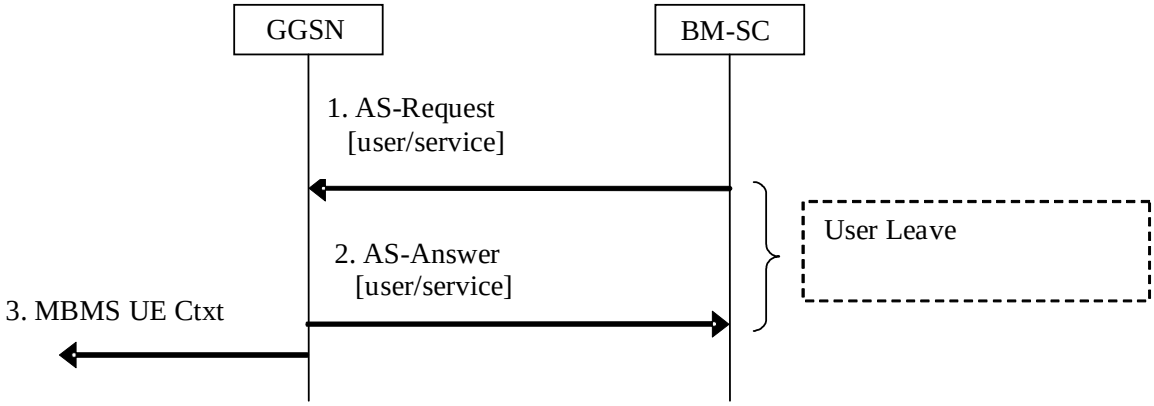


Figure 32a: BM-SC initiated MBMS Service deactivation procedure

1. The BM-SC sends an ASR to the GGSN, indicating that the UE shall be removed from the multicast service. The session to be terminated is uniquely identified by the Diameter session-id.

2. Upon reception of the ASR, the GGSN sends an ASA to the BM-SC

3. Upon reception of the ASR the GGSN sends an MBMS UE Context Deactivation Request to the SGSN. The IP multicast address, APN and IMSI together identify the MBMS UE Context to be deleted by the SGSN.

Steps from 5 to 9 of figure 32 in section 17.5.7 follow.

17.5.8 Trace Session Activation procedure

The Trace Session Activation procedure occurs when the GGSN indicates to the BM-SC that a Trace Session needs to be activated.

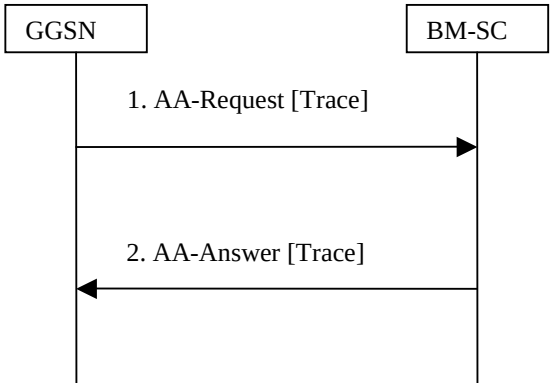


Figure 33: Trace Session Activation procedure

1. When the GGSN has received a Trace Activation message from the SGSN, in a Create MBMS Context Request/Update MBMS Context Request, that requires the activation of a Trace Session in the BM-SC, the GGSN sends an AAR message (containing the IMSI and the Additional MBMS Trace Info AVPs) to activate a trace session in the BM-SC.

2. Upon reception of an AAR from a GGSN to activate a Trace Session, the BM-SC responds with an AAA message.

17.5.9 Trace Session Deactivation procedure

The Trace Session Deactivation procedure occurs when the GGSN indicates to the BM-SC that a Trace Session, previously activated, needs to be deactivated.

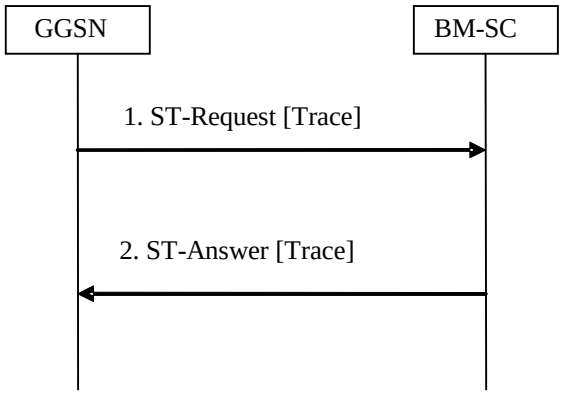


Figure 34: Trace Session Deactivation procedure

1. When the GGSN has received a Trace Deactivation message from the SGSN, in a Create MBMS Context Request/Update MBMS Context Request, that requires the deactivation of a Trace Session in the BM-SC, the GGSN sends a STR message (containing the Additional MBMS Trace Info AVP) to deactivate a trace session in the BM-SC and to tear down the corresponding Diameter Session previously established to activate the Trace Session.

2. Upon reception of an STR from a GGSN to deactivate a Trace Session, the BM-SC responds with an STA message.

17.5.10 MBMS UE Context Modification Procedure

During the multicast MBMS bearer service activation, the MBMS UE Context is stored in the BM-SC. Later, the MBMS UE Context shall be updated when the UE enters a new Routeing Area (RA) served by a new SGSN or the UE is transitioning between UTRAN and A/Gb mode GERAN or vice versa (Inter-system Intra-SGSN change). See 3GPP TS23.246 [65] and 3GPP TS29.060 [24]. GGSN shall pass the relevant data via the Gmb interface to enable the BM-SC to update its MBMS UE context accordingly.

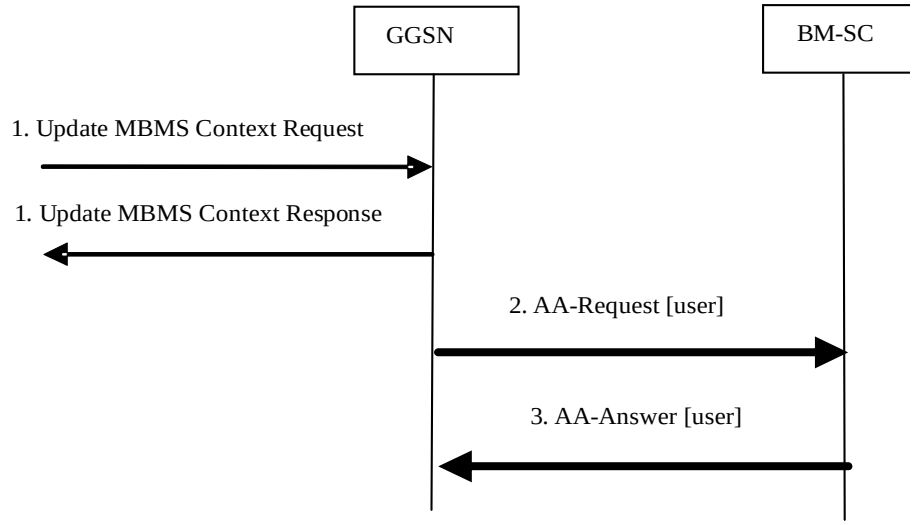


Figure 35; Modification of an MBMS UE Context in BM-SC

1. On request from SGSN, the MBMS UE Context is updated in the GGSN.
2. The GGSN sends updated MBMS UE Context parameters (RAI, and CGI/SAI as specified in clause 17.6.1) to BM-SC in an AAR message.
3. The BM-SC updates its MBMS UE Context fields and responds with an AAA message.

If the GGSN receives new or updated trace information in step 1, then the above procedure may be followed by a Trace Session Activation procedure (see clause 17.5.8) or a Trace Session Deactivation procedure (see clause 17.5.9).

17.6 Gmb Messages

This clause defines the Gmb interface Diameter messages.

The relevant AVPs that are of use for the Gmb interface are detailed in this clause. Other Diameter NASREQ (IETF RFC 4005 [67]) AVPs, even if their AVP flag rules is marked with "M", are not required for being compliant with the current specification.

All Gmb specific AVPs for Gmb are needed to be compliant to the Gmb interface unless otherwise stated.

17.6.1 AAR Command

The AAR command, defined in Diameter NASREQ (IETF RFC 4005 [67]), is indicated by the Command-Code field set to 265 and the "R" bit set in the Command Flags field. It, is sent by the GGSN to the BM-SC to request user authorization (authorize the activating UE to receive Data) , to modify an MBMS UE Context in the BM-SC or to register the GGSN for a particular multicast MBMS bearer service. When used for these purposes, the Additional-MBMS-Trace-Info AVP shall not be included.

When the AAR command is used by the GGSN to modify an MBMS UE context in the BM-SC, it shall include all the parameters that have been changed according to the triggering Update MBMS Context Request, ref. fig. 35. The inclusion of CGI/SAI in the 3GPP-User-Location-Info AVP shall be according to the rules detailed in subclause 15.1.1a in 3GPP TS 23.060[3]). The Called-Station-Id AVP, Calling-Station-Id AVP, Framed-IP-Address AVP, Framed-IPv6-Prefix AVP, Framed-Interface-Id AVP and 3GPP-GPRS-Negotiated-QoS-Profile AVP shall not be included,

The AAR command is also used when the GGSN needs to activate a Trace Session in the BM-SC. In this case the Called-Station-Id AVP, Calling-Station-Id AVP, Framed-IP-Address AVP, Framed-IPv6-Prefix AVP, Framed-Interface-Id AVP, 3GPP-GPRS-Negotiated-QoS-Profile AVP and RAI AVP shall not be included. For more detailed description of Trace Session activation/deactivation procedures see 3GPP TS 32.422 [69].

The relevant AVPs that are of use for the Gmb interface are detailed in the ABNF description below. Other valid AVPs for this command are not used for Gmb purposes and should be ignored by the receiver or processed according to the relevant specifications.

The bold marked AVPs in the message format indicate new optional AVPs for Gmb, or modified existing AVPs.

Message Format:

```
<AA-Request> ::= < Diameter Header: 265, REQ, PXY >
                      < Session-Id >
                      { Auth-Application-Id }
                      { Origin-Host }
                      { Origin-Realm }
                      { Destination-Realm }
                      { Auth-Request-Type }
                      [ Destination-Host ]
                      [ Called-Station-Id ]
                      [ Calling-Station-Id ]
                      [ Framed-IP-Address]
                      [ Framed-IPv6-Prefix ]
                      [ Framed-Interface-Id ]
                    * [ Proxy-Info ]
                    * [ Route-Record ]
                      [ 3GPP-GPRS-Negotiated-QoS-Profile ]
                      [ 3GPP-IMSI]
                      [ RAI ]
                      [ 3GPP-IMEISV ]
                      [ 3GPP-RAT-Type ]
                      [ 3GPP-User-Location-Info ]
                      [ 3GPP-MS-TimeZone ]
                      [ Additional-MBMS-Trace-Info ]
```

The GGSN shall allocate a new Session-Id for each time an AAR command is sent.

A request for user authorisation for an MBMS bearer service is indicated by the presence of the MSISDN within the Calling-Station-Id AVP and the 3GPP-IMSI. Otherwise the request is for the GGSN to be authorised (i.e. registered) to receive the MBMS bearer service.The Framed-IPv6-Prefix AVP contains the IPv6 prefix of the multicast address identifying the MBMS bearer service.

The Framed-Interface-Id AVP contains the IPv6 interface identifier of the multicast address identifying the MBMS bearer service.

The Framed-IP-Address AVP contains the IPv4 multicast address identifying the MBMS bearer service.

The Called-Station-Id AVP contains the Access Point Name (APN) on which the MBMS bearer service authorisation request was received.

17.6.2 AAA Command

The AAA command, defined in Diameter NASREQ (IETF RFC 4005 [67]), is indicated by the Command-Code field set to 265 and the "R" bit cleared in the Command Flags field., It is sent by the BM-SC to the GGSN in response to the AAR command.

When the AAA command is used to acknolewdge an AAR that activated a Trace Session, the only Gmb specific AVP that shall be included is the 3GPP-IMSI AVP.

The relevant AVPs that are of use for the Gmb interface are detailed in the ABNF description below. Other valid AVPs for this command are not used for Gmb purposes and should be ignored by the receiver or processed according to the relevant specifications.

The bold marked AVPs in the message format indicate new optional AVPs for Gmb, or modified existing AVPs.

Message Format:

```
<AA-Answer> ::= < Diameter Header: 265, PXY >
                     < Session-Id >
                     { Auth-Application-Id }
```

```
                    { Origin-Host }
                    { Origin-Realm }
                    [ Result-Code ]
                    [ Experimental-Result ]
                    [ Error-Message ]
                    [ Error-Reporting-Host ]
                  * [ Failed-AVP ]
                  * [ Proxy-Info ]
                    [ Alternative-APN ]
                    [ 3GPP-GPRS-Negotiated-QoS-Profile ]
                    [ 3GPP-IMSI]
                    [ TMGI ]
                    [ Required-MBMS-Bearer-Capabilities ]
```

17.6.3 STR Command

The STR command, defined in IETF RFC3588 (DIAMETER BASE) [66], is indicated by the Command-Code field set to 275 and the "R" bit set in the Command Flags field, It is sent by the GGSN to the BM-SC to terminate a DIAMETER session.

A DIAMETER session for a multicast MBMS service is terminated when the last MBMS UE context for the MBMS bearer service is deleted. This informs the BM-SC that the GGSN would like to be deleted from the distribution tree of a particular MBMS bearer service (De-registration procedure).

A DIAMETER session for an individual UE"s multicast MBMS service authorisation is terminated when the UE has requested to the GGSN to leave the MBMS bearer service.

The STR command is also used to deactivate a Trace Session previously activated in the BM-SC and to terminate the associated Diameter Session initiated by the AAR that activated the Trace session. The Gmb specific AVP Additonal-MBMS-Trace-Info shall be included in the STR command only in the case of a Trace Session deactivation. For more detailed description of Trace Session activation/deactivation procedures see 3GPP TS 32.422 [69].

The relevant AVPs that are of use for the Gmb interface are detailed in the ABNF description below. Other valid AVPs for this command are not used for Gmb purposes and should be ignored by the receiver or processed according to the relevant specifications.

Message Format:

```
<ST-Request> ::= < Diameter Header: 275, REQ, PXY >
                      < Session-Id >
                      { Origin-Host }
                      { Origin-Realm }
                      { Destination-Realm }
                      { Auth-Application-Id }
                      { Termination-Cause }
                      [ Destination-Host ]
                    * [ Class ]
                      [ Origin-State-Id ]
                    * [ Proxy-Info ]
                    * [ Route-Record ]
                      [ Additional-MBMS-Trace-Info ]
```

17.6.4 STA Command

The STA command, defined in IETF RFC3588 (DIAMETER BASE) [66], is indicated by the Command-Code field set to 275 and the "R" bit cleared in the Command Flags field, is sent in response to an STR command (De-registration procedure).

The relevant AVPs that are of use for the Gmb interface are detailed in the ABNF description below. Other valid AVPs for this command are not used for Gmb purposes and should be ignored by the receiver or processed according to the relevant specifications.

Message Format:

```
<ST-Answer>  ::= < Diameter Header: 275, PXY >
                       < Session-Id >
                       { Result-Code }
```

```
                  { Origin-Host }
                  { Origin-Realm }
                * [ Class ]
                  [ Error-Message ]
                  [ Error-Reporting-Host ]
                * [ Failed-AVP ]
                  [ Origin-State-Id ]
                * [ Redirect-Host ]
                  [ Redirect-Host-Usage ]
                  [ Redirect-Max-Cache-Time ]
                * [ Proxy-Info ]
```

17.6.5 Re-Auth-Request Command

The Re-Auth-Request (RAR) command, defined in IETF RFC3588 (DIAMETER BASE) [66], is indicated by the Command-Code set to 258 and the message flags' 'R' bit set.

The relevant AVPs that are of use for the Gmb interface are detailed in the ABNF description below. Other valid AVPs for this command are not used for Gmb purposes and should be ignored by the receiver or processed according to the relevant specifications.

The bold marked AVPs in the message format indicate new optional AVPs for Gmb, or modified existing AVPs.

Message Format:

```
<RAR>  ::= < Diameter Header: 258, REQ, PXY >
           < Session-Id >
           { Origin-Host }
           { Origin-Realm }
           { Destination-Realm }
           { Destination-Host }
           { Auth-Application-Id }
           { Re-Auth-Request-Type }
           [ Called-Station-Id ]
           [ Framed-IP-Address]
           [ Framed-IPv6-Prefix ]
           [ Framed-Interface-Id ]
           [ MBMS-StartStop-Indication ]
          *[ MBMS-Service-Area ]
           [ 3GPP-GPRS-Negotiated-QoS-Profile ]
           [ MBMS-Session-Duration ]
           [ MBMS-Service-Type ]
           [ MBMS-Session-Identity ]
           [ MBMS-Session-Identity-Repetition-number ]
           [ TMGI ]
         * [ 3GPP-SGSN-Address ]            ; broadcast case only
         * [ 3GPP-SGSN-IPv6-Address ]       ; broadcast case only
           [ MBMS-2G-3G-Indicator ]
           [ MBMS-Time-To-Data-Transfer ]
           [ Origin-State-Id ]
         * [ Proxy-Info ]
         * [ Route-Record ]
```

The MBMS-StartStop-Indication AVP will indicate if the command is indicating a MBMS Session Start procedure or a MBMS Session Stop procedure.

For the MBMS Session Start procedure, RAR is sent by the BM-SC to the GGSN(s) that will deliver the MBMS service (e.g. in the multicast case these are the GGSNs that have previously registered for the corresponding multicast MBMS bearer service), when it is ready to send data. This is a request to activate all necessary bearer resources in the network for the transfer of MBMS data and to notify interested UEs of the imminent start of the transmission. For broadcast MBMS bearer services the RAR message contains either an IPv4 address or an IPv6 address for each participating SGSN.

For MBMS Session Stop procedure, RAR is sent by the BM-SC to the GGSN(s) when it considers the MBMS session to be terminated. The session is typically terminated when there is no more MBMS data expected to be transmitted for a sufficiently long period of time to justify a release of bearer plane resources in the network.

The MBMS session to be started/stopped is identified by the TMGI and the MBMS-Session-Identity.

The information of the MBMS-2G-3G-Indicator is passed from BM-SC transparently through GGSN to the SGSN(s) that are relevant for the actual MBMS bearer service.

According to 3GPP TS 23.246 [65], a specific MBMS bearer service is uniquely identified by its IP multicast address and an APN. For the MBMS Session Start procedure for broadcast MBMS bearer services, the following AVPs are included (either IPv4 or IPv6 address) to enable GGSN to relate incoming payload packets to the actual MBMS bearer service and distribute the packets to the downstream SGSNs related to this service:

- The Framed-IPv6-Prefix AVP contains the IPv6 prefix of the multicast address.
- The Framed-Interface-Id AVP contains the IPv6 interface identifier of the multicast address.
- The Framed-IP-Address AVP contains the IPv4 multicast address.
- The Called-Station-Id AVP contains the Access Point Name (APN) for which the MBMS bearer service is defined.

17.6.6 RE-Auth-Answer Command

The Re-Auth-Answer (RAA) command, defined in IETF RFC3588 (DIAMETER BASE) [66], is indicated by the Command-Code set to 258 and the message flags' 'R' bit clear, is sent in response to the RAR.

The relevant AVPs that are of use for the Gmb interface are detailed in the ABNF description below. Other valid AVPs for this command are not used for Gmb purposes and should be ignored by the receiver or processed according to the relevant specifications.

The bold marked AVPs in the message format indicate new optional AVPs for Gmb, or modified existing AVPs.

Message Format:

```
<RAA>  ::= < Diameter Header: 258, PXY >
           < Session-Id >
           { Origin-Host }
           { Origin-Realm }
           [ Result-Code ]
           [ Experimental-Result ]
           [ MBMS-StartStop-Indication ]
           [ Origin-State-Id ]
           [ Error-Message ]
           [ Error-Reporting-Host ]
         * [ Failed-AVP ]
         * [ Redirected-Host ]
           [ Redirected-Host-Usage ]
           [ Redirected-Host-Cache-Time ]
         * [ Proxy-Info ]
```

17.6.7 Abort-Session-Request Command

The Abort-Session-Request (ASR) command, defined in IETF RFC3588 (DIAMETER BASE) [66], is indicated by the Command-Code set to 274 and the message flags' 'R' bit set, is sent by the BM-SC to the GGSN to request that the session identified by the Session-Id be stopped.

The relevant AVPs that are of use for the Gmb interface are detailed in the ABNF description below. Other valid AVPs for this command are not used for Gmb purposes and should be ignored by the receiver or processed according to the relevant specifications.

Message Format

```
<ASR>  ::= < Diameter Header: 274, REQ, PXY >
           < Session-Id >
           { Origin-Host }
           { Origin-Realm }
           { Destination-Realm }
```

```
            { Destination-Host }
            { Auth-Application-Id }
            [ Origin-State-Id ]
          * [ Proxy-Info ]
          * [ Route-Record ]
```

17.6.8 Abort-Session-Answer Command

The Abort-Session-Answer (ASA) command, defined in IETF RFC3588 (DIAMETER BASE) [66], is indicated by the Command-Code set to 274 and the message flags' 'R' bit clear, is sent in response to the ASR.

The relevant AVPs that are of use for the Gmb interface are detailed in the ABNF description below. Other valid AVPs for this command are not used for Gmb purposes and should be ignored by the receiver or processed according to the relevant specifications.

Message Format

```
<ASA>  ::= < Diameter Header: 274, PXY >
           < Session-Id >
           { Result-Code }
           { Origin-Host }
           { Origin-Realm }
           [ Origin-State-Id ]
           [ Error-Message ]
           [ Error-Reporting-Host ]
         * [ Failed-AVP ]
         * [ Redirected-Host ]
           [ Redirected-Host-Usage ]
           [ Redirect-Max-Cache-Time ]
         * [ Proxy-Info ]
```

17.7 Gmb specific AVPs

Table 10 describes the Gmb specific Diameter AVPs. The Vendor-Id header of all Gmb specific AVPs defined in the present specification shall be set to 3GPP (10415).

The Gmb specific AVPs require to be supported to be compliant to the present specification. All AVPs in table 10 are mandatory within Gmb interface unless otherwise stated.

Table 10: Gmb specific AVPs

	AVP Flag rules

Attribute Name	AVP Code	Section defined	Value Type	Must	May	Should not	Must not	May Encr.
TMGI	900	17.7.2	OctectString	M,V	P			Y
Required-MBMS-Bearer-Capabilities	901	17.7.3	UTF8String	M,V	P			Y
MBMS-StartStop-Indication	902	17.7.5	Enumerated	M,V	P			Y
MBMS-Service-Area	903	17.7.6	OctectString	M,V	P			Y
MBMS-Session-Duration	904	17.7.7	Unsigned32	M,V	P			Y
3GPP-GPRS-Negotiated-QoS-Profile	5	16.4.7 (see Note)	UTF8String	M,V	P			Y
3GPP-IMSI	1	16.4.7 (see Note)	UTF8String	M.V	P			Y
Alternative-APN	905	17.7.8	UTF8String	M,V	P			Y
MBMS-Service-Type	906	17.7.9	Enumerated	M,V	P			Y
3GPP-SGSN-Address	6	16.4.7 (see note)	UTF8String	M, V	P			Y
3GPP-SGSN-IPv6-Address	15	16.4.7 (see note)	UTF8String	M, V	P			Y
MBMS-2G-3G-Indicator	907	17.7.10	Enumerated	M, V	P			Y
MBMS-Session-Identity	908	17.7.11	OctetString	M.V	P			Y
RAI	909	17.7.12	UTF8String	M, V	P			Y
3GPP-IMEISV	20	16.4.7 (see Note)	OctetString	M,V	P			Y
3GPP-RAT-Type	21	16.4.7 (see Note)	OctetString	M,V	P			Y
3GPP-User-Location-Info	22	16.4.7 (see Note)	OctetString	M,V	P			Y
3GPP-MS-TimeZone	23	16.4.7 (see Note)	OctetString	M,V	P			Y
Additional-MBMS-Trace-Info	910	17.7.13	OctetString	M,V	P			Y
MBMS-Time-To-Data-Transfer	911	17.7.14	OctetString	M,V	P			Y
MBMS-Session-Identity-Repetition-Number	912	17.7.15	Unsigned32	M.V	P			Y
NOTE: The use of Radius VSA as a Diameter vendor AVP is described in Diameter NASREQ (IETF RFC 4005 [67]) and the P flag may be set.								

Table 11 lists the set of Diameter AVPs that are not Gmb specific, but are reused from other Diameter applications by the Gmb interface. A reference is done to the specifications where the AVPs are specified. This set of AVPs requires to be supported to be compliant to the present specification.

Table 11: Gmb reused AVPs from other Diameter applications.

AVP Name	Reference
Called-Station-Id	NASREQ, IETF RFC 4005 [67]
Calling-Station-Id	NASREQ, IETF RFC 4005 [67]
Framed-Interface-Id	NASREQ, IETF RFC 4005 [67]
Framed-IP-Address	NASREQ, IETF RFC 4005 [67]
Framed-IPv6-Prefix	NASREQ, IETF RFC 4005 [67]

NOTE: Diameter Base AVPs are not listed as support of them is mandated by IETF RFC 3588 [66].

17.7.1 3GPP-Vendor-Specific AVP

Void.

17.7.2 TMGI AVP

The TMGI AVP (AVP code 900) is of type OctectString, and contains the Temporary Mobile Group Identity allocated to a particular MBMS bearer service. TMGI use and structure is specified in 3GPP TS 23.003 [40].

17.7.3 Required-MBMS-Bearer-Capabilities AVP

The Required-MBMS-Bearer-Capabilities AVP (AVP code 901) is of type UTF8String, and contains the minimum bearer capabilities the UE needs to support. The information contained in this AVP is UTF-8 encoded QoS profile as defined in 3GPP TS 24.008 [54].

17.7.4 Void

17.7.5 MBMS-StartStop-Indication AVP

The MBMS-StartStop-Indication AVP (AVP code 902) is of type Enumerated. The following values are supported:

START (0)

The message containing this AVP is indicating a MBMS session start procedure.

STOP (1)

The message containing this AVP is indicating a MBMS session stop procedure.

17.7.6 MBMS-Service-Area AVP

The MBMS-Service-Area AVP (AVP code 903) is of type OctetString, and indicates the area over which the MBMS bearer service has to be distributed.

17.7.7 MBMS-Session-Duration AVP

The MBMS-Session-Duration AVP (AVP code 904) is of type Unsigned32, and indicates the estimated session duration (MBMS Service data transmission). The time is indicated in seconds.

The highest value of this AVP (i.e. all 1"s), is reserved to indicate an indefinite value to denote sessions that are expected to be always-on.

17.7.8 Alternative-APN AVP

The Alternative-APN AVP (AVP code 905) is of type UTF8String, and contains the value of a new APN. This AVP is optional within the Gmb interface. BM-SC only includes it if the UE must use a different APN for the MBMS PDP Context from the one used in the Join message.

17.7.9 MBMS-Service-Type AVP

The MBMS-Service-Type AVP (AVP code 906) is of type Enumerated, and contains explicit information about the type of service that the BM-SC Start Procedure is about to start.

MULTICAST (0)

The Start Procedure signalled by the BM-SC is for a Multicast Service.

BROADCAST (1)

The Start Procedure signalled by the BM-SC is for a Broadcast Service.

17.7.10 MBMS-2G-3G-Indicator AVP

The MBMS-2G-3G-Indicator AVP (AVP code 907) is of type Enumerated. It indicates whether the MBMS bearer service will be delivered in 2G- only, 3G- only of both coverage areas. The following values are supported:

2G (0)

The MBMS bearer service shall only be delivered in 2G only coverage areas.

3G (1)

The MBMS bearer service shall only be delivered in 3G only coverage areas.

2G-AND-3G (2)

The MBMS bearer service shall be delivered both in 2G and 3G coverage areas.

17.7.11 MBMS-Session-Identity AVP

The MBMS-Session-Identity AVP (AVP code 908) is of type OctetString. Its length is one octet. It is allocated by the BM-SC. Together with TMGI it identifies a transmission of a specific MBMS session. The initial transmission and subsequent retransmissions of the MBMS session will use the same values of these parameters. This AVP is optional within the Gmb interface.

17.7.12 RAI AVP

The RAI AVP (AVP Code 909) is of type UTF8String, and contains the Routing Area Identity of the SGSN where the UE is registered. RAI use and structure is specified in 3GPP TS 23.003 [40].

17.7.13 Additional-MBMS-Trace-Info AVP

The Additional-MBMS-Trace-Info AVP (AVP Code 910) is of type OctetString. This AVP contains Trace Reference2, Trace Recording Session Reference, Triggering Events in BM-SC, Trace Depth for BM-SC, List of interfaces in BM-SC, Trace Activity Control For BM-SC which are all part of the Additional MBMS Trace Info IE as specified in TS 29.060 [24].

17.7.14 MBMS-Time-To-Data-Transfer AVP

The MBMS-Time-To-Data-Transfer AVP (AVP code 911) is of type OctetString. Its length is one octet. It indicates the expected time between reception of the MBMS Session Start (RAR(Start) command) and the commencement of the MBMS Data flow. The coding is specified as per the Time to MBMS Data Transfer Value Part Coding of the Time to MBMS Data Transfer IE in 3GPP TS 48.018 [70].

17.7.15 MBMS-Session-Identity-Repetition-Number AVP

The MBMS-Session-Identity-Repetition-Number AVP (AVP code 912) is of type Unsigned32. It contains the session identity repetition number of the MBMS transmission session on the Gmb interface. When the optional MBMS-Session-Identity AVP is included in the MBMS Session Start RAR (Start) command by the BM-SC, the BM-SC shall also provide the corresponding MBMS-Session-Identity-Repetition-Number AVP.

17.8 Gmb specific Experimental-Result-Code AVP values

There are two different types of errors in Diameter; protocol and application errors. A protocol error is one that occurs at the base protocol level, those are covered in the Diameter Base RFC 3588 [66] specific procedures. Application errors, on the other hand, generally occur due to a problem with a function specified in a Diameter application.

Diameter Base RFC 3588 [66] defines a number of Result-Code AVP values that are used to report protocol errors and how those are used. Those procedures and values apply for the present specification.

Due to the Gmb specific AVPs, new applications errors can occur. The Gmb specific errors are described by the Experimental-Result-Code AVP in this clause, below. Note that according to RFC 3588 [66], the Diameter node reports only the first error encountered and only one Result-Code AVP or one Experimental-Result AVP is included in the Diameter answer.

17.8.1 Success

Resulting codes that fall within the Success category are used to inform a peer that a request has been successfully completed.

The Result-Code AVP values defined in Diameter Base RFC 3588 [66] are applicable.

17.8.2 Permanent Failures

Errors that fall within the Permanent Failures category are used to inform the peer that the request failed, and should not be attempted again.

The Result-Code AVP values defined in Diameter Base RFC 3588 [66] are applicable. Also the following specific Gmb Experimental-Result-Code values are defined:

DIAMETER_ERROR_START_INDICATION (5120)

> This error covers the case when a MBMS Session Start procedure could not be performed due to some of the required session attributes that are necessary to activate the bearer resources are missing (QoS, MBMS Service Area…). The Failed-AVP AVP must contain the missing AVP.

DIAMETER_ERROR_STOP_INDICATION (5121)

> An indication of session stop has been received with no session start procedure running.

DIAMETER_ERROR_UNKNOWN_MBMS_BEARER_SERVICE (5122)

The requested MBMS service is unknown at the BM-SC.

DIAMETER_ERROR_SERVICE_AREA (5123)

The MBMS service area indicated for a specific MBMS Bearer Service is unknown or not available.

18 Usage of RADIUS at the Pk Reference Point

18.1 General

The Pk Reference Point is defined in 3GPP TS 23.141 [68] and allows the GGSN to report presence relevant events to the Presence Network Agent (such as PDP context activation/de-activation). This reference point is implemented using the mechanisms for Accounting of the RADIUS interface on the Gi reference point as defined in Clause 16.

18.2 Radius Profile for Pk Reference Point

The RADIUS interface on Gi reference point as defined in Clause 16 is used for the Pk Reference Point as clarified in the Profile in this Clause.

Only the following messages are required for the Radius Profile for the Pk reference Point:

- Accounting-Request START
- Accounting-Response START
- Accounting-Request STOP
- Accounting-Response STOP

For the Radius Profile for the Pk Reference Point, only the mandatory Parameters within the Accounting-Request START and Accounting-Request STOP messages according to Clauses 16.4.3 and 16.4.4, respectively, and the Parameter "Calling-Station-Id" need to be supported. The usage of other parameters is optional. They may be ignored by the Presence Network Agent.

18.3 Interconnecting the Presence Network Agent and the GGSN

The Presence Network Agent may be directly attached to the GGSN or via a Radius Proxy.

If the GGSN needs to connect both to an AAA server and a Presence Network Agent for the same APN, but supports only a single RADIUS interface, the GGSN can be directly attached to the AAA server. The Presence Network Agent can in turn be attached to the AAA server, which acts as a RADIUS proxy. If the AAA server is configured as a RADIUS Proxy between the Presence Network Agent and the GGSN, the Radius Profile for the Pk Reference Point shall be applicable on the interface between the Presence Network Agent and the AAA server.

Annex A (informative): Interworking PCS1900 with PSDNs

Void.

Annex B (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
03-2004	TSG#23	NP-040148	103	2	IMEISV Passed on the Gi Interface	5.8.0	6.0.0
06-2004	TSG#24	NP-040244	111	2	Gmb Commands and AVPs (II)	6.0.0	6.1.0
06-2004	TSG#24	NP-040244	112	2	Gmb Message Flows	6.0.0	6.1.0
06-2004	TSG#24	NP-040244	113	1	Command to indicate Session Start/Stop	6.0.0	6.1.0
06-2004	TSG#24	NP-040244	114	1	Gmb introduction	6.0.0	6.1.0
06-2004	TSG#24	NP-040238	118		Length of QoS profile	6.0.0	6.1.0
09-2004	TSG#25	NP-040337	119	2	Scope update to include Gmb	6.1.0	6.2.0
09-2004	TSG#25	NP-040337	120	2	Gmb. General corrections	6.1.0	6.2.0
09-2004	TSG#25	NP-040337	121	2	New Gmb specific AVPs, and new specific result-codes values.	6.1.0	6.2.0
09-2004	TSG#25	NP-040335	122		New sub-attributes 3GPP VSA passed on the Gi interface for charging purposes	6.1.0	6.2.0
12-2004	TSG#26	NP-040591	137	3	Prevention of IP spoofing	6.2.0	6.3.0
12-2004	TSG#26	NP-040615	138	1	RADIUS Enhancements on the Gi interface to enable QoS correlation (Packet Filters)	6.2.0	6.3.0
12-2004	TSG#26	NP-040615	139	1	RADIUS Enhancements on the Gi interface for QoS information (Negotiated DSCP)	6.2.0	6.3.0
12-2004	TSG#26	NP-040616	140		Gmb interface. Corrections, addition of missing AVPs and code values assignation	6.2.0	6.3.0
12-2004	TSG#26				Editorial correction of the figures in clause 17 as MS word picture object into the document	6.3.0	6.3.1
03-2005	TSG#27	NP-050102	155	1	Update of IETF related references	6.3.1	6.4.0
03-2005	TSG#27	NP-050107	157	1	Pk Interface	6.3.1	6.4.0
03-2005	TSG#27	NP-050108	141		Adding the TMGI to the Gmb Session Start message	6.3.1	6.4.0
03-2005	TSG#27	NP-050108	142	1	Adding list of downsteam nodes in the Session Start message	6.3.1	6.4.0
03-2005	TSG#27	NP-050108	143	1	Various corrections of Gmb	6.3.1	6.4.0
03-2005	TSG#27	NP-050108	144		Adding in the 2G/3G indicator to the Gmb Session Start message	6.3.1	6.4.0
03-2005	TSG#27	NP-050108	145	2	Adding the MBMS session identity to the Gmb Session Start message	6.3.1	6.4.0
03-2005	TSG#27	NP-050108	146	1	Adding the multicast address and the APN to the Gmb Session Start message	6.3.1	6.4.0
03-2005	TSG#27	NP-050108	147		Text corection and multiple MBMS-Service-Area	6.3.1	6.4.0
03-2005	TSG#27	NP-050108	148	1	Providing the BM-SC with approximate UE location information at MBMS context activation	6.3.1	6.4.0
03-2005	TSG#27	NP-050108	158	1	Indefinite MBMS session duration	6.3.1	6.4.0
06-2005	TSG#28	CP-050222	159	1	Correction to MBMS-2G-3G-Indicator AVP	6.4.0	6.5.0
06-2005	TSG#28	CP-050222	160		Unnecessary IMSI information	6.4.0	6.5.0
06-2005	TSG#28	CP-050222	161		MBMS-Session-Identity is optional	6.4.0	6.5.0
06-2005	TSG#28	CP-050223	162	2	Correction to charging information for MBMS	6.4.0	6.5.0
06-2005	TSG#28	CP-050044	163	4	Tracing information for MBMS	6.4.0	6.5.0
06-2005	TSG#28	CP-050224	165	1	Correction to MBMS-Session-Identity	6.4.0	6.5.0
06-2005	TSG#28	CP-050043	166	1	Correction to the use of Auth-Application-Id in Gmb	6.4.0	6.5.0
06-2005	TSG#28	CP-050222	167		MBMS-Session-Duration is mandatory	6.4.0	6.5.0
09-2005	TSG#29	CP-050376	169	2	Application-id for Gmb application	6.5.0	6.6.0
09-2005	TSG#29	CP-050376	170	2	Time to Data transfer	6.5.0	6.6.0
09-2005	TSG#29	CP-050376	171	1	MBMS Session Identity Repetition number	6.5.0	6.6.0
09-2005	TSG#29	CP-050376	172		Modification of MBMS UE Context in the BM-SC	6.5.0	6.6.0
09-2005	TSG#29	CP-050376	173		Correction of MBMS service activation	6.5.0	6.6.0
09-2005	TSG#29	CP-050376	174	4	BM-SC initiated MBMS Multicast Service Deactivation procedure	6.5.0	6.6.0
09-2005	TSG#29				Editorial correction to the title of clause 17.7.4	6.5.0	6.6.0
12-2005	TSG#30	CP-050509	178		Correction of the Time to Data transfer	6.6.0	6.7.0
12-2005	TSG#30	CP-050509	179		Inter-system Intra-SGSN change	6.6.0	6.7.0
06-2006	TSG#32	CP-060219	180		NASREQ reference update	6.7.0	6.8.0

History

Document history		
V6.3.1	January 2005	Publication
V6.4.0	March 2005	Publication
V6.5.0	June 2005	Publication
V6.6.0	September 2005	Publication
V6.7.0	December 2005	Publication
V6.8.0	June 2006	Publication