ETSI TS 129 061 V14.4.0 (2018-01)

**Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
LTE;
Interworking between the Public Land Mobile Network (PLMN)
supporting packet based services and
Packet Data Networks (PDN)
(3GPP TS 29.061 version 14.4.0 Release 14)**

Reference
RTS/TSGC-0329061ve40

Keywords
GSM,LTE,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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Intellectual Property Rights

Essential patents

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 (https://ipr.etsi.org/).

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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

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.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

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.

For inter-working between EPC PLMN and external networks, the present document is valid for both 3GPP accesses and non-3GPP accesses.

The present document also defines, in clause 17, the protocol for the Gmb interface, in clause 20, the protocol for the SGmb interface, and in clause 19, the protocol for the Mz 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.

The term "Packet Domain" includes both EPC based and non-EPC based Packet Domains.

The present document also defines the specific requirements for rate control related to CIoT optimisations.

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] Void

[29] Void.

[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] Void.

[33] Void.

[34] Void.

[35] Void.

[36] Void.

[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] Void.

[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] Void

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

[55] Void.

[56] Void

[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] Void.

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

[66] Void.

[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)".

[71] 3GPP TS 23.107: "Quality of Service (QoS) Concept and Architecture".

[72] 3GPP TS 25.346: "Introduction of the Multimedia Broadcast Multicast Service (MBMS) in the Radio Access Network (RAN)".

[73] IETF RFC 4604 (2006): "Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast".

[74] IETF RFC 4607 (2006): "Source-Specific Multicast for IP".

[75] 3GPP TS 29.212: "Policy and Charging Control (PCC); Reference points".

[76] 3GPP TS 29.213: "Policy and charging control signalling flows and Quality of Service (QoS) parameter mapping".

[77] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[78] 3GPP TS 23.402: "Architecture enhancements for non-3GPP accesses".

[79] IETF RFC 4039 (2005): "Rapid Commit Option for the Dynamic Host Configuration Protocol version 4 (DHCPv4)".

[80] IETF RFC 3736 (2004): "Stateless Dynamic Host Configuration Protocol (DHCP) Service for Ipv6".

[81] 3GPP TS 29.274: "Evolved GPRS Tunnelling Protocol for EPS (GTPv2)".

[82] IETF RFC 4291 (2006): "IP Version 6 Addressing Architecture".

[83] IETF RFC 4862 (2007): "Ipv6 Stateless Address Autoconfiguration".

[84] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS)".

[85] IETF RFC 2132 (1997): "DHCP Options and BOOTP Vendor Extensions".

[86] IETF RFC 3361 (2002): "Dynamic Host Configuration Protocol (DHCP-for-Ipv4) Option for Session Initiation Protocol (SIP) Servers".

[87] IETF RFC 3646 (2003): "DNS Configuration options for Dynamic Host Configuration Protocol for Ipv6 (DHCPv6)".

[88] IETF RFC 3319 (2003): "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers".

[89] IETF RFC 4861 (2007): "Neighbor Discovery for IP Version 6 (Ipv6)".

[90] 3GPP TS 23.203: "Policy and charging control architecture".

[91] IETF RFC 4739 (2006): "Multiple Authentication Exchanges in the Internet Key Exchange (IKEv2) Protocol".

[92] 3GPP TS 25.413: "UTRAN Iu Interface RANAP Signalling".

[93] IETF RFC 5176 (2008): "Dynamic Authorization Extentions to Remote Authentication Dial In User Service (RADIUS)".

[94] 3GPP TS 36.331: "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification".

[95] 3GPP TS 23.380: "IMS Restoration Procedures".

[96] 3GPP TS 29.303: "Domain Name System Procedures; Stage 3".

[97] IETF RFC 4818 (2007): "RADIUS Delegated-Ipv6-Prefix Attribute".

[98] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description"

[99] 3GPP TS 23.221: "Architectural requirements".

[100] 3GPP TS 23.682: "Architecture Enhancements to facilitate communications with Packet Data Networks and Applications".

[101] 3GPP TS 29.336: "Home Subscriber Server (HSS) Diameter interfaces for interworking with packet data networks and applications".

[102] IETF RFC 4282 (2005): "The Network Access Identifier".

[103] 3GPP TS 29.275: "Proxy Mobile Ipv6 (PMIPv6) based Mobility and Tunnelling protocols; Stage 3".

[104] 3GPP TS 23.007: "Restoration procedures".

[105] 3GPP TS 29.229: "Cx and Dx interfaces based on Diameter protocol; Protocol details".

[106] 3GPP TS 25.446: "MBMS synchronisation protocol (SYNC)".

[107] 3GPP TS 25.323: "Packet Data Convergence Protocol (PDCP) specification".

[108] Void.

[109] IETF RFC 4960 (2007): "Stream Control Transmission Protocol".

[110] 3GPP TS 29.128: "Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) interfaces for interworking with packet data networks and applications ".

[111] IETF RFC 6733: "Diameter Base Protocol".

[112] 3GPP TS 23.285: "Architecture Enhancements for V2X services".

[113] 3GPP TS 29.468: "Group Communication System Enablers for LTE (GCSE_LTE); MB2 Reference point; Stage 3".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TS 22.060 [2], 3GPP TS 23.060 [3], 3GPP TS 23.401 [77], 3GPP TS 23.402 [78] 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.

IP-CAN session: association between a UE and an IP network
The association is identified by a UE represented by an Ipv4 address and/or an Ipv6 prefix together with a UE identity information, if available, and a PDN identity (e.g. APN). An IP-CAN session incorporates one or more IP-CAN bearers. Support for multiple IP-CAN bearers per IP-CAN session is IP-CAN specific. An IP-CAN session exists as long as the related UE Ipv4 address and/or Ipv6 prefix are established and announced to the IP network.

EPC based Packet Domain: Packet domain which makes use of EPC nodes (e.g. P-GW, S-GW, etc.).

Packet Domain Bearer: A transmission path between a UE and a GGSN/P-GW, terminating at the User Plane protocol stack under the IP layers.

3.2 Abbreviations

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

AMBR	Aggregate Maximum Bit Rate
APN	Access Point Name
ARP	Allocation and Retention Priority
ATM	Asynchronous Transfer Mode
APCO	Additional Protocol Configuration Options
BG	Border Gateway
BM-SC	Broadcast/Multicast Service Centre
CHAP	Challenge Handshake Authentication Protocol
CIoT	Cellular Internet of Things
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol version 6
DNS	Domain Name System
DSMIPv6	Dual-Stack MIPv6
DVMRP	Distance Vector Multicast Routing Protocol
EPC	Evolved Packet Core
ePDG	Evolved Packet Data Gateway
EPS	Evolved Packet System
FQDN	Fully Qualified Domain Name
GBR	Guaranteed Bit Rate
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 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
MBR	Maximum Bit Rate
MIP	Mobile IP
MLD	Multicast Listener Discovery
MME	Mobility Management Entity
MOSPF	Multicast Open Shortest Path First
MS	Mobile Station
MT	Mobile Terminal
MTC	Machine Type Communication
MTU	Maximum Transfer Unit
NAI	Network Access Identifier
PAP	Password Authentication Protocol
PCC	Policy and Charging Control
PCO	Protocol Configuration Options
PCRF	Policy and Charging Rules Function
P-CSCF	Proxy Call Session Control Function
PDCP	Packet Data Convergence Protocol
PDN	Packet Data Network
PDU	Protocol Data Unit
P-GW	PDN Gateway
PIM-SM	Protocol Independent Multicast – Sparse Mode
PPP	Point-to-Point Protocol

PS	Packet Switched
QCI	QoS Class Identifier
RADIUS	Remote Authentication Dial In User Service
SCEF	Service Capability Exposure Function
SGSN	Serving GPRS Support Node
S-GW	Serving Gateway
SMDS	Switched Multimegabit Data Service
TCP	Transmission Control Protocol
TE	Terminal Equipment
TEID	Tunnel End-point Identifier
TMGI	Temporary Mobile Group Identity
TWAN	Trusted WLAN Access Network
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.
S2a	It provides the user plane with related control and mobility support between trusted non-3GPP IP access and P-GW.
S2b	It provides the user plane with related control and mobility support between ePDG and P-GW.
S2c	It provides the user plane with related control and mobility support between UE and P-GW. This reference point is implemented over trusted and/or untrusted non-3GPP Access and/or 3GPP access.
S5	Interface between a S-GW and a P-GW within the same PLMN.
S8	Interface between a S-GW and a P-GW in different PLMNs.
Sgi	The reference point between the EPC based PLMN and the packet data network.
Sgi-mb	The reference point between BM-SC and MBMS GW for MBMS data delivery.
SGmb	The reference point for the control plane between BM-SC and MBMS GW.
T6a	Reference point used between SCEF and serving MME.
T6b	Reference point used between SCEF and serving SGSN.
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 23.060 [3] , 3GPP TS 23.401 [77] and 3GPP TS 23.402 [78].

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. 16orrecti), 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/Sgi 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

6.1 General

The figures depicted in subclauses 6.2 and 6.3 below are the logical representation of the EPC and the non-EPC based Packet Domains. Physically, an operator's PLMN may consist of both EPC and non-EPC nodes. In other words, for example, an operator's PLMN may have both GGSNs and P-GWs; and a Rel-8 SGSN may initiate PDP context activation procedure via both Gn/Gp and S4/S5/S8 reference points.

6.2 Access Interfaces and Reference Points for non-EPC based Packet Domain

Figure 1a shows the relationship between the MS, its terminal equipment and the PLMN network in the non-EPC based overall Packet Domain environment.

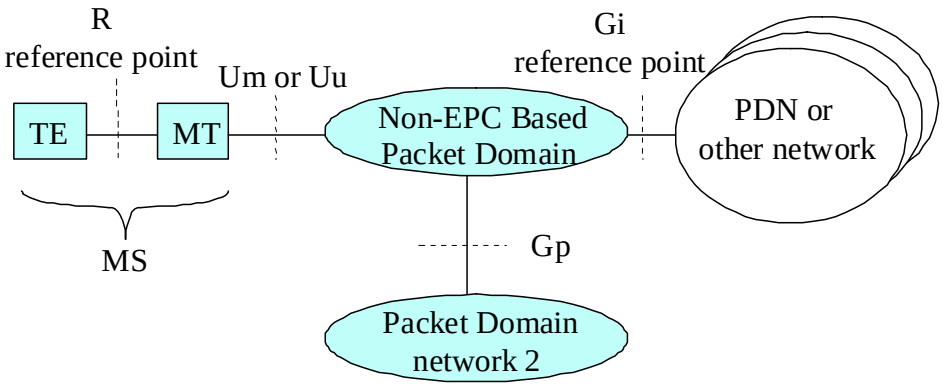


Figure 1a: Non-EPC based Packet Domain Access Interfaces and Reference Points

6.3 Access Interfaces and Reference Points for EPC based Packet Domain

Figure 1b shows the relationship between the UE and the EPS network for both the 3GPP access and the non-3GPP access in the EPC based Packet Domain environment. The S8/S2a/S2b interface includes GTP-based and PMIP-based.

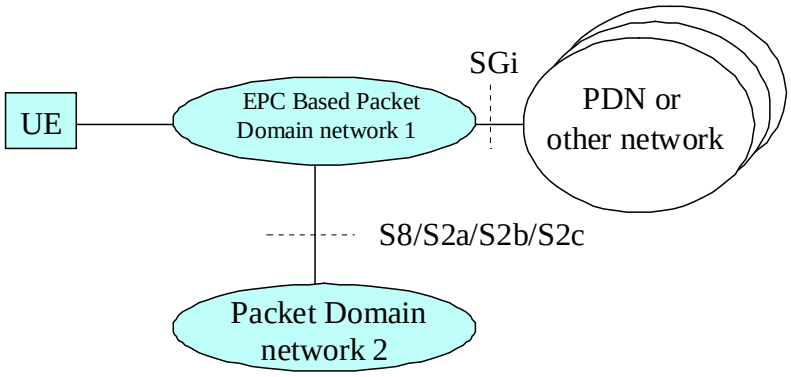


Figure 1b: EPC based Packet Domain Access Interfaces and Reference Points

7 Interface to Packet Domain Bearer Services

7.1 A/Gb mode

Figure 2a shows the relationship of the non-EPC based 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].

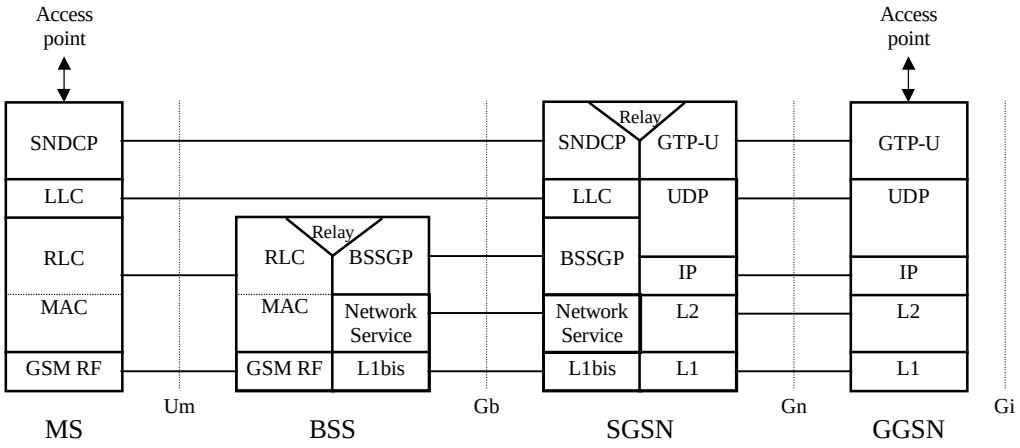


Figure 2a: User Plane for Packet Domain services in A/Gb mode

7.2 Iu mode

Figure 2b shows the relationship of the non-EPC based 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].

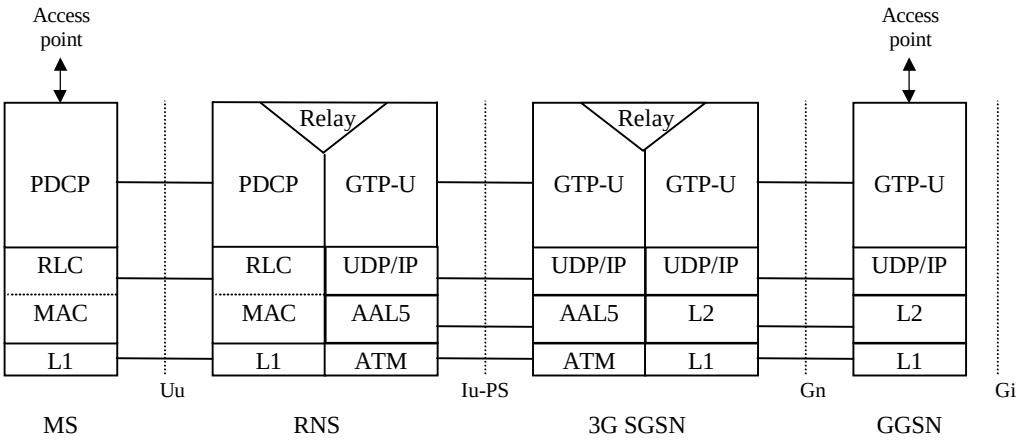


Figure 2b: User Plane for Packet Domain services in Iu mode

7.3 Interface to EPC-based Packet Domain Bearer Services

The user plane for EPC based packet domain services can be found in 3GPP TS 23.401 [77] , 3GPP TS 23.402 [78] and 3GPP TS 23.060 [3].

8 Subscription checking

The subscription of an MS/UE is checked by the PLMN during IP-CAN session establishment procedure as described in 3GPP TS 23.060 [3], 3GPP TS 23.401 [77] and 3GPP TS 23.402 [78]. The GGSN/P-GW implicitly checks its internal context related to the destination address for each mobile terminated packet. For PDN types other than Non-IP, if there is a context IP-CAN session associated with the IP address the packet shall be forwarded towards the MS/UE; otherwise the packet shall be discarded or rejected depending on the implemented protocol. For PDN type "Non-IP", the packet shall be forwarded towards the MS/UE, discarded or rejected depending on the implemented protocol.

8A Prevention of IP spoofing

For PDN types other than "Non-IP", if IP spoofing has to be prevented, the GGSN/P-GW shall verify the source IP address of the IP packets issued by the UE and compare it against the address, IPv4 or IPv6, assigned for the IP-CAN session. If the verification fails for a packet,the GGSN/P-GW 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], 3GPP TS 23.060 [3], 3GPP TS 23.401 [77] and 3GPP TS 23.402 [78]. 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. Packet Domain may also support interworking with networks handling Non-IP data services.

11.2 PDN Interworking Model

The Packet Domain can interwork with IP networks and networks handling Non-IP data services. When interworking with the IP networks, the Packet Domain can operate IPv4 and/or IPv6. The interworking point with the IP networks or networks handling Non-IP data services is at the Gi and Sgi reference point. Additionally, the interworking point with network handling Non-IP data services may also be the T6a (T6) reference point for Control Plane CIoT EPS Optimizations (see 3GPP TS 29.128 [110]) . These interworking points are shown in figure 7.

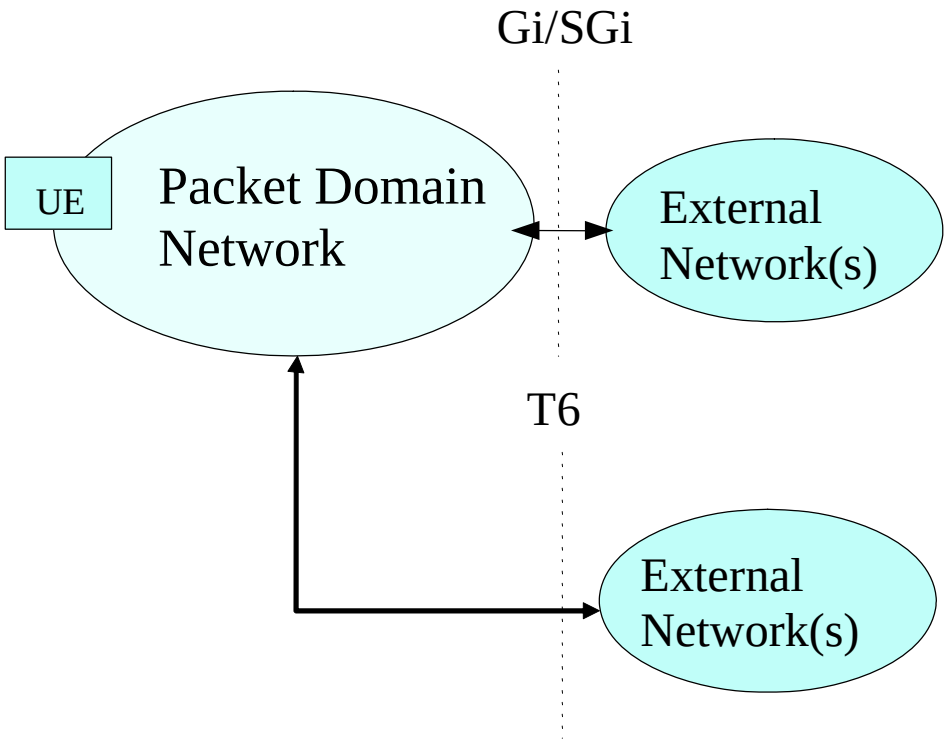


Figure 7: IP network interworking

The GGSN/P-GW 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.

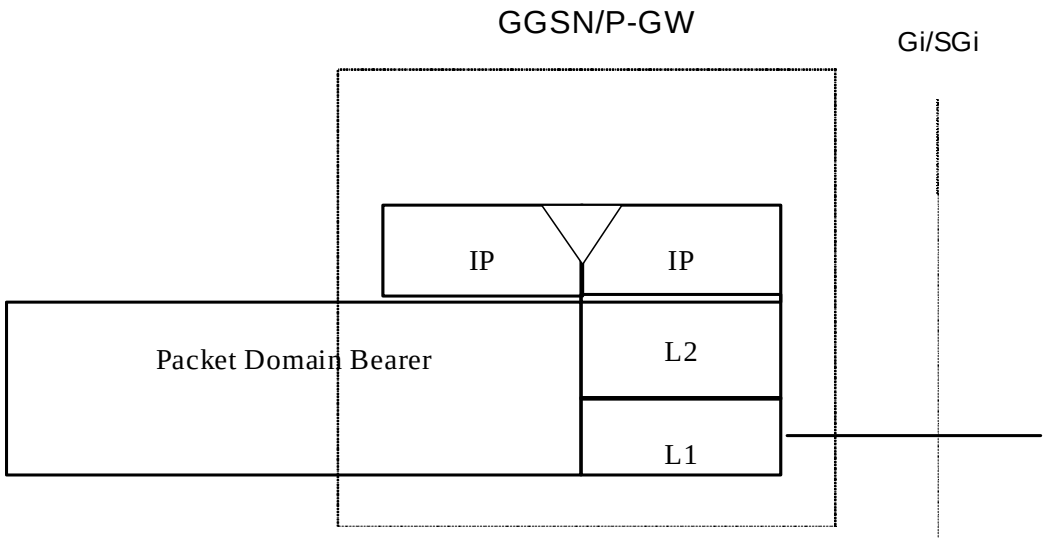


Figure 8: The protocol stacks of GGSN and P-GW for the IP network interworking

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; and the Sgi reference point is between the P-GW and the external IP network. From the external IP network's point of view, the GGSN/P-GW 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/Sgi 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/P-GW.

Both the GGSN/P-GW (for both Control Plane and User Plane CIoT EPS Optimizations) and the SCEF (for Control Plane CIoT EPS Optimization) for interworking with the network handling Non-IP data services are the access points of the Packet Domain. See 3GPP TS 23.401 [77] and 3GPP TS 23.060 [3] for further details.

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/P-GW, takes part in the functions listed above.

The mechanisms for host configuration and user authentication described in this subclause and its subclauses are applicable for the initial IP-CAN session establishment to allocate IP addresses (Ipv4 and/or Ipv6) to the MS. For GTP based access, the activation of any subsequent IP-CAN bearers for that IP-CAN session, (i.e.secondary PDP context activation Procedure', dedicated bearer activation), as well as the use of TFTs, is described in 3GPP TS 23.060 [3], 3GPP TS 23.401 [77].

11.2.1.1 Transparent access to the Internet

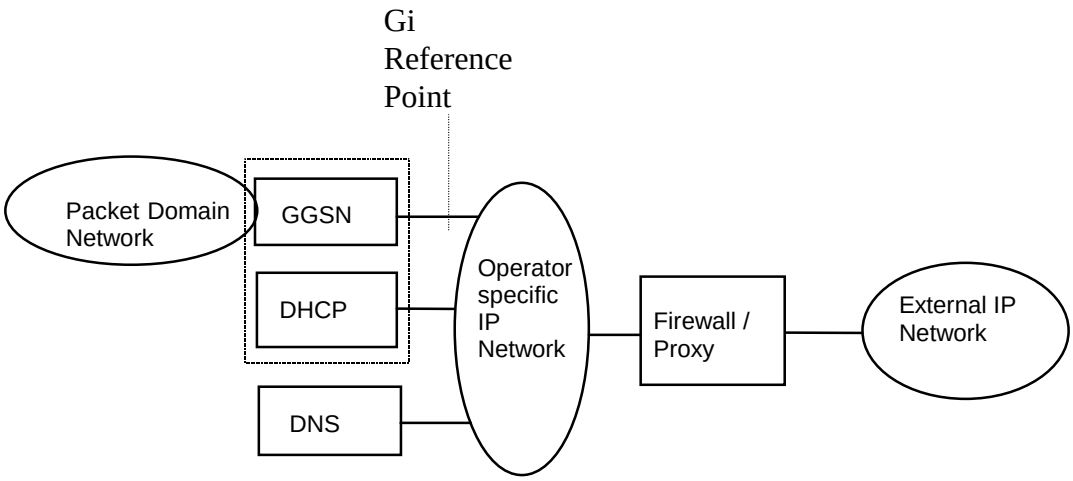


Figure 9: Example of the PDN Interworking Model, transparent case

In figure 9, an example PDN interworking model for transparent access to the Internet is provided for a GGSN and its Gi reference point.

In transparent access to the Internet case:

- the MS is given an Ipv4 address and/or an Ipv6 prefix belonging to the operator addressing space. The Ipv4 address and/or Ipv6 prefix is assigned either at subscription in which case it is a static address or at IP-CAN session establishment in which case it is a dynamic address. This Ipv4 address and/or Ipv6 prefix if applicable is used for packet forwarding between the Internet and the GGSN/P-GW and within the packet domain. With Ipv6, Stateless 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 MS need not send any authentication request at IP-CAN session establishment procedure and the GGSN/P-GW 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.

Note that the remainder of this subclause deals with this specific use-case as depicted in figure 10.

- 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.

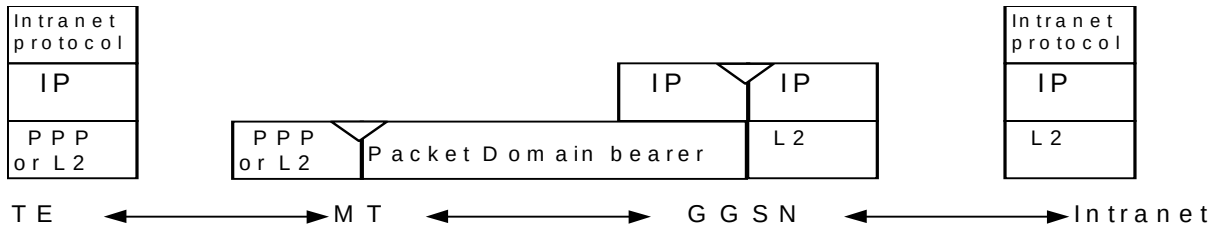


Figure 10: Transparent access to an Intranet

In figure 10, an example for transparent access to an Intranet is provided for a GGSN and its Gi reference point, but the same principle is applicable to EPC.

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 the GGSN and the Intranet because security is ensured on an end to end basis between the 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

11.2.1.2.1 non-EPC based Ipv4 Non Transparent access

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.

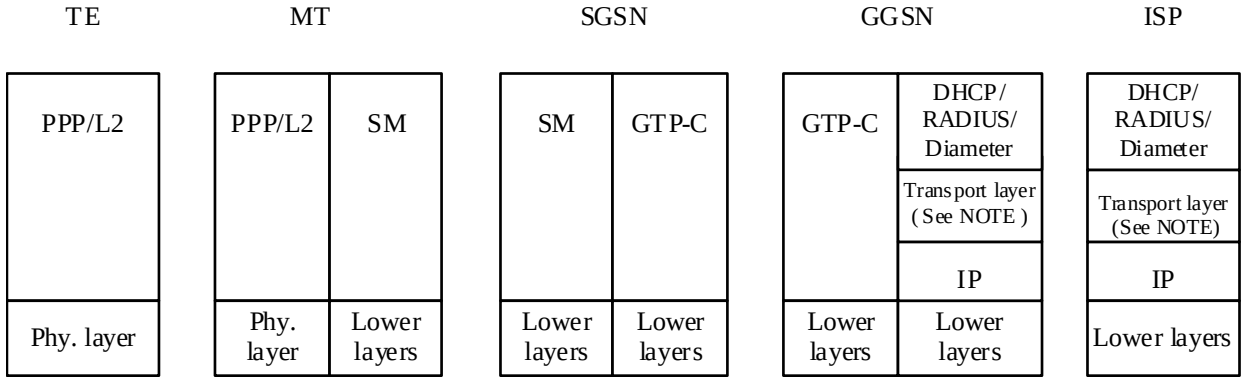


Figure 11a: Signalling plane of non transparent case

NOTE: The transport protocol UDP is used for DHCP and RADIUS, and TCP or SCTP are used for Diameter.

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.

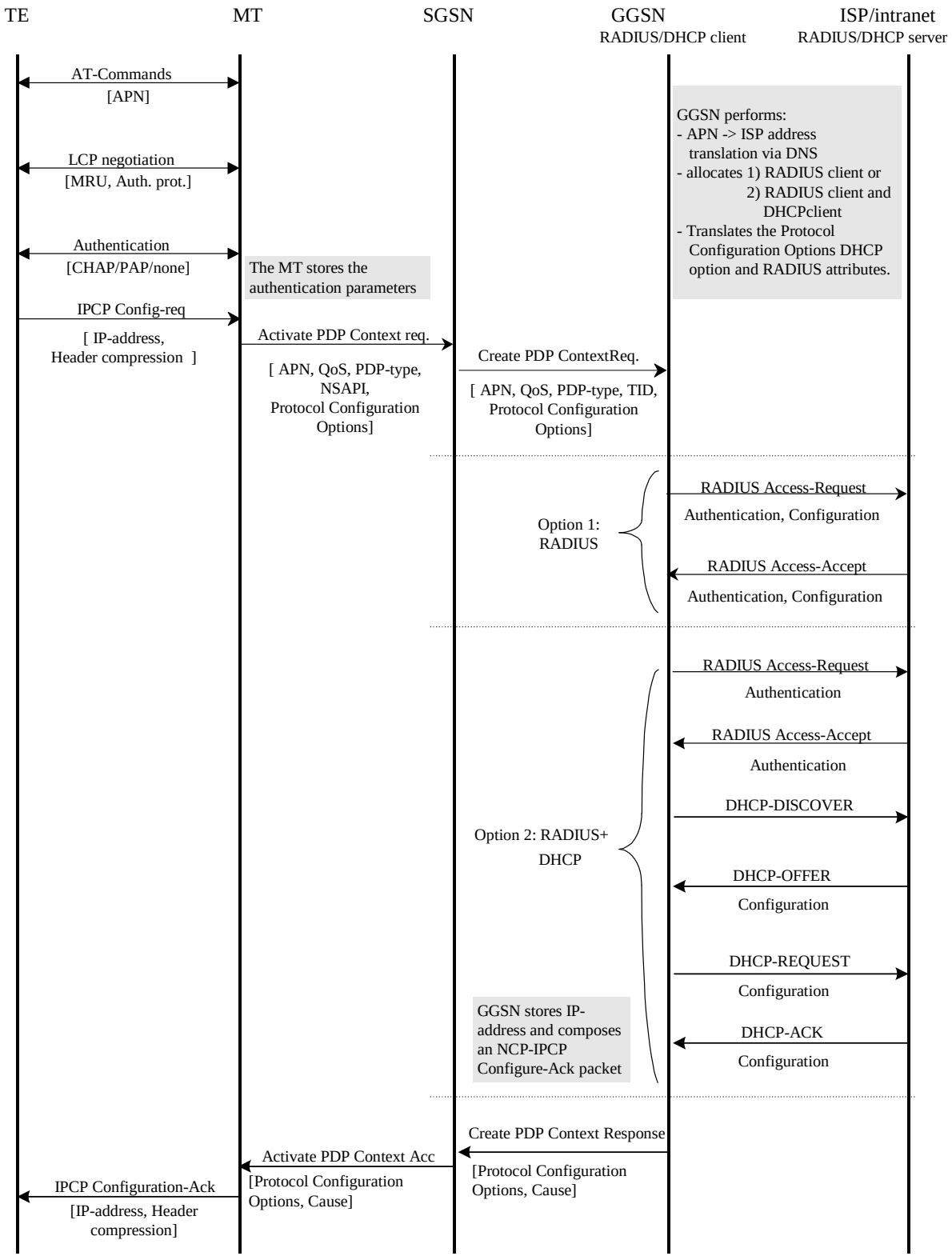


Figure 11b: PDP Context Activation for the Ipv4 Non-transparent case

11.2.1.2.2 EPC based Ipv4 Non Transparent access

In this case:

- a static or a dynamic Ipv4 address belonging to the Intranet/ISP addressing space is allocated to a UE at IP-CAN session establishment. The methods of allocating IP address to the UE are specified in 3GPP TS 23.060 [3],

3GPP TS 23.401 [77] and 3GPP TS 23.402 [78]. The allocated Ipv4 address is used for packet forwarding within the P-GW and for packet forwarding on the Intranet/ISP;

- as a part of the IP-CAN session establishment, the P-GW may request user authentication from an external AAA server (i.e. RADIUS, Diameter) belonging to the Intranet/ISP;

- the Ipv4 address allocation to the UE may be performed based on the subscription or a local address pool, which belongs to the Intranet/ISP addressing space, provisioned in the P-GW. The Ipv4 address allocation to the UE may also be done via the address allocation servers (i.e. DHCPv4, RADIUS AAA, Diameter AAA) belonging to the Intranet/ISP;

- if requested by the UE at IP-CAN session establishment, the P-GW may retrieve the Protocol Configuration Options or Ipv4 configuration parameters from a locally provisioned database in P-GW and/or from some external server (i.e. DHCPv4, RADIUS AAA, Diameter AAA) belonging to the Intranet/ISP;

- the communication between the Packet Domain and the Intranet/ISP may be performed over any network, even an insecure network ,e.g. the Internet. In case of an insecure connection between the P-GW 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.

Table 0 summarizes the Ipv4 address allocation and parameter configuration use cases between the UE and the P-GW that may lead the P-GW to interwork with the external DHCPv4, RADIUS AAA and Diameter AAA servers over Sgi reference point. For detailed description of the signalling flows between the UE and the P-GW, see the references in the table. The detailed description of the signalling use cases that may be triggered between the P-GW and the external servers are specified in this document, as referenced in the table.

Table 0 : Ipv4 address allocation and parameter configuration use cases

Signalling use cases between UE and P-GW	**Signalling use cases between P-GW and external servers**		
	Authentication via RADIUS or Diameter server (Clauses 16 or 16a) (NOTE 1,2,5)	Ipv4 Address allocation via DHCPv4 or RADIUS or Diameter server (Clauses 13.3, 16 or 16a) (NOTE 1 and 2)	Ipv4 parameter configuration via DHCPv4 or RADIUS or Diameter server (Clauses 13.3, 16 or 16a) (NOTE 1 and 2)
(1) Ipv4 address allocation and parameter configuration via default bearer activation (2) Ipv4 address allocation and parameter configuration via DHCPv4 signalling from UE towards P-GW (NOTE 3 and 4) deployment options applicable to both use cases (1) and (2): - GTP-based S5/S8 (Subclauses 5.3.1, 5.3.2, 5.10.2 in TS 23.401 [77]) - PMIP-based S5/S8 (Subclauses 4.7.1, 5.2, 5.6 in TS 23.402 [78])	X	X	X
(3) Ipv4 adress allocation and parameter configuration during primary PDP context activation using S4-based SGSN (4) Ipv4 address allocation and parameter configuration using DHCPv4 signalling from UE towards P-GW (NOTE 3 and 4) and using - GTP-based S5/S8 (Subclauses 9.2, 9.2.2.1A in TS 23.060 [3]) - PMIP-based S5/S8 (Subclauses 4.7.1, 5.2, 5.6, 5.10 in TS 23.402 [78])	X	X	X
(5) Ipv4 address allocation in trusted non-3GPP IP access using on S2a (NOTE 4) - PMIPv6 (Subclauses 4.7.2, 6.2.1, and 6.2.4 in TS 23.402 [78])	X	X	X

Signalling use cases between UE and P-GW	Signalling use cases between P-GW and external servers		
	Authentication via RADIUS or Diameter server (Clauses 16 or 16a) (NOTE 1,2,5)	Ipv4 Address allocation via DHCPv4 or RADIUS or Diameter server (Clauses 13.3, 16 or 16a) (NOTE 1 and 2)	Ipv4 parameter configuration via DHCPv4 or RADIUS or Diameter server (Clauses 13.3, 16 or 16a) (NOTE 1 and 2)
- GTPv2 (Subclauses 16.1.5, and 16.2 in TS 23.402 [78]) and using - achoring in P-GW - chained S2a and PMIP-based S8 (6) Ipv4 address allocation in trusted non-3GPP IP access using MIPv4 FACoA on S2a and anchoring in P-GW (NOTE 4) (Subclause 6.2.3 of TS 23.402 [78]) (7) Ipv4 address allocation and parameter configuration via DHCPv4 signalling in non-3GPP IP access on S2a (NOTE 3 and 4) (Subclauses 4.7.2 in TS 23.402 [78])			
(8) Ipv4 address allocation and parameter configuration in untrusted non-3GPP IP access using on S2b (NOTE 4) - PMIPv6 (Subclauses 4.7.3, 7.2.1, and 7.2.3 in TS 23.402 [78]) - GTPv2 (Subclauses 7.2.4 in TS 23.402 [78]) and using - anchoring in P-GW - chained S2b and PMIP-based S8	X	X	X
(9) Ipv4 parameter configuration via DHCPv4 with DSMIPv6 on S2c (Subclauses 4.7.4 in TS 23.402 [78]) (10) Ipv4 address allocation with DSMIPv6 on S2c - in trusted non-3GPP IP access - in untrusted non-3GPP IP access (Subclauses 4.7.4, 6.3 and 7.3 of TS 23.402 [78])	X	X	X
NOTE 1: When the P-GW interworks with AAA servers, the APN may be configured to interwork with either Diameter AAA or RADIUS AAA server. NOTE 2: If RADIUS AAA or Diameter AAA server is used, the authentication, Ipv4 address allocation and parameter configuration signalling may be combined. Similarly, if DHCPv4 server is used for Ipv4 address allocation and parameter configuration, the signalling towards the DHCPv4 server may be combined. NOTE 3: If the 27orrection27ion procedure towards RADIUS AAA or Diameter AAA is required, it is performed by the PGW before the DHCPv4 signalling when it receives the initial access request (e.g. Create Session Request, or Proxy Binding Update). NOTE 4: For PMIP-based S5/S8, S2a and S2b, the P-GW shall obtain the Ipv4 address from the external server after receiving Proxy Binding Update and before sending the Proxy Binding Ack. See 3GPP TS 23.402 [78] for details. NOTE 5: The UEs may provide PAP/CHAP user credentials in the PCO IE when accessing to EPS on 3GPP and non-3GPP IP accesses. If such information is provided to the P-GW, the P-GW may perform user authentication based on these credentials. For S2c, the P-GW may receive such credentials from the UE based on IETF RFC 4739 [91] during the establishment of security association signalling via IKEv2. For S2b, the UEs may provide such credentials in the IKEv2 protocol as specified in IETF RFC 4739 [91], and if the ePDG supports multiple authentications, it shall include such credentials in the APCO IE (see 3GPP TS 29.275 [103] subclause 12.1.1.19) on the S2b interface.			

11.2.1.3 Ipv6 Non Transparent access to an Intranet or ISP

When using Ipv6 Address Autoconfiguration, 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 or

initial attach (e.g. create default bearer) for EPC based access, followed by a second signalling phase done in the user plane.

The user plane signalling phase shall be stateless. The stateless procedure, which involves only the MS/UE and the GGSN/P-GW, is described in subclause "Ipv6 Stateless Address Autoconfiguration".

For APNs that are configured for Ipv6 address allocation, the GGSN/P-GW 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 4291 [82].

The GGSN/P-GW indicates to the MS/UE that Stateless Autoconfiguration shall be performed by sending Router Advertisements as described in the corresponding subclause below and according to the principles defined in RFC 4861 [89] and RFC 4862 [83].

For MS/UE having Ipv6, Ipv6 Stateless Address Autoconfiguration is mandatory.

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 stateless 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.

- 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 or Ipv4v6. 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:

   - the source of Ipv6 Prefixes (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.

   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.

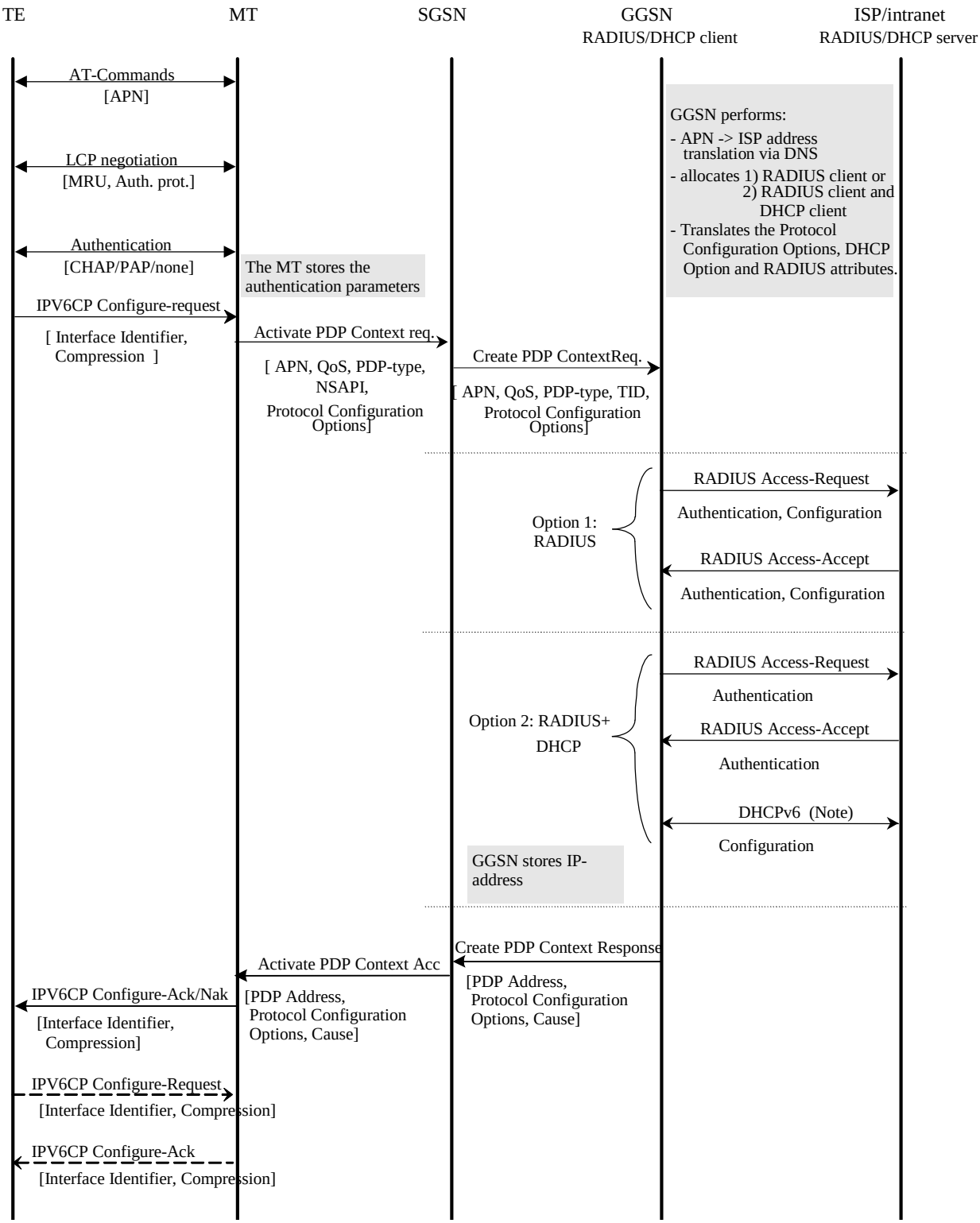
   If the Interface-Identifier extracted from the address contained in the PDP Address IE is not identical to the tentative Interface-Identifier indicated in the IPV6CP Configure-Request message sent from the TE, the MT sends an IPV6CP Configure-Nak packet, indicating the Interface-Identifier extracted 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

11.2.1.3.1a Ipv6 EPC based Bearer Activation

In this case, the P-GW provides the UE with an Ipv6 Prefix belonging to the Intranet/ISP addressing space. A dynamic Ipv6 address is given using stateless address autoconfiguration. This Ipv6 address is used for packet forwarding within the packet domain and for packet forwarding on the Intranet/ISP.

When a P-GW receives an initial access request (e.g. Create Session Request or Proxy Binding Update) message, the P-GW deduces from local configuration data associated with the APN:

- The source of Ipv6 Prefixes (P-GW 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, i.e. RADIUS, Diameter or DHCPv6, to be used with the server(s);
- The communication and security feature needed to communicate with the server(s);

As an example the P-GW may use one of the following options:

- P-GW internal Prefix pool for Ipv6 prefixes allocation and no authentication;
- P-GW internal Prefix pool for Ipv6 prefixes allocation and RADIUS for authentication. The AAA server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the P-GW;
- 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 P-GW;

The P-GW includes the PDP Address IE in the the initial access response (e.g. Create Session Response or Proxy Binding Acknowledgement) and 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 that the P-GW has selected for its own side of the UE-P-GW link. The Prefix assigned by the P-GW or the external AAA server shall be globally or site-local unique (see the Note in subclause 11.3 of this document regarding the usage of site-local addresses).

Table 0.a summarizes the Ipv6 prefix allocation and parameter configuration use cases between the UE and the P-GW that may lead the P-GW to interwork with the external RADIUS AAA, Diameter AAA and DHCPv6 servers over Sgi reference point. For detailed description of the signalling flows between the UE and the P-GW, see the references in the table. The detailed description of the signalling use cases that may be triggered between the P-GW and the external servers are specified in this document, as referenced in the table.

Table 0.a : Ipv6 prefix allocation and parameter configuration use cases

Signalling use cases between UE and P-GW	**Signalling use cases between P-GW and external servers**		
	Authentication via RADIUS or Diameter server (Clauses 16 or 16a) (NOTE 1, and 2, 3)	Ipv6 prefix allocation via DHCPv6 or RADIUS or Diameter server (Clauses 13.3, 16 or 16a) (NOTE 1 and 2)	Ipv6 parameter configuration via DHCPv6 or RADIUS or Diameter server (Clauses 13.3, 16 or 16a) (NOTE 1 and 2)
(1) Ipv6 address allocation and parameter configuration (2) Ipv6 parameter configuration via stateless DHCPv6 deployment options applicable to both use cases (1) and (2): - GTP-based S5/S8 (Subclauses 5.3.1, 5.3.2, 5.10.2 in TS 23.401 [77]) - PMIP-based S5/S8 (Subclauses 4.7.1, 5.2, 5.6 in TS 23.402 [78])	X	X	X
(3) Ipv6 address allocation and parameter configuration via S4-based SGSN (4) Ipv6 parameter configuration via stateless DHCPv6 and using - GTP-based S5/S8 (Subclauses 9.2, 9.2.2.1A in TS 23.060 [3]) - PMIP-based S5/S8 (Subclauses 4.7.1, 5.2, 5.6, 5.10 in TS 23.402 [78])	X	X	X

Signalling use cases between UE and P-GW	Signalling use cases between P-GW and external servers		
	Authentication via RADIUS or Diameter server (Clauses 16 or 16a) (NOTE 1, and 2, 3)	Ipv6 prefix allocation via DHCPv6 or RADIUS or Diameter server (Clauses 13.3, 16 or 16a) (NOTE 1 and 2)	Ipv6 parameter configuration via DHCPv6 or RADIUS or Diameter server (Clauses 13.3, 16 or 16a) (NOTE 1 and 2)
(5) Ipv6 address allocation and parameter configuration in trusted non-3GPP IP access using on S2a - PMIPv6 (Subclauses 4.7.2, 6.2.1, and 6.2.4 in TS 23.402 [78]) - GTPv2 (Subclauses 16.1.5, and 16.2 in TS 23.402 [78]) (6) Ipv6 parameter configuration via stateless DHCPv6 and using - achoring in P-GW - chained S2a and PMIP-based S8	X	X	X
(7) Ipv6 address allocation and parameter configuration in untrusted non-3GPP IP access using on S2b - PMIPv6 (Subclauses 4.7.3, 7.2.1, and 7.2.3 in TS 23.402 [78]) - GTPv2 (Subclauses 7.2.4 in TS 23.402 [78]) and using - anchoring in P-GW - chained S2b and PMIP-based S8	X	X	X
(8) Ipv6 address allocation and parameter configuration on S2c - in trusted non-3GPP IP access - in untrusted non-3GPP IP access (Subclauses 4.7.4, 6.3 and 7.3 of TS 23.402 [78]) (9) Ipv6 parameter configuration via stateless DHCPv6 on S2c (Subclauses 4.7.4 in TS 23.402 [78])	X	X	X
NOTE 1: When the P-GW interworks with AAA servers, the APN may be configured to interwork with either Diameter AAA or RADIUS AAA server. NOTE 2: If RADIUS AAA or Diameter AAA server is used, the authentication, Ipv6 prefix allocation and parameter configuration signalling may be combined. Similarly, if DHCPv6 server is used for Ipv6 prefix allocation and parameter configuration, the signalling towards the DHCPv6 server may be combined. NOTE 3: The UEs may provide PAP/CHAP user credentials in the PCO IE when accessing to EPS on 3GPP and non-3GPP IP accesses. If such information is provided to the P-GW, the P-GW may perform user authentication based on these credentials. For S2c, the P-GW may receive such credentials from the UE based on IETF RFC 4739 [91] during the establishment of security association signalling via IKEv2. For S2b, the UEs may provide such credentials in the IKEv2 protocol as specified in IETF RFC 4739 [91], and if the ePDG supports multiple authentications, it shall include such credentials in the APCO IE (see 3GPP TS 29.275 [103] subclause 12.1.1.19) on the S2b interface.			

11.2.1.3.2 Ipv6 Stateless Address Autoconfiguration

As described in 3GPP TS 23.060 [3], the Ipv6 prefix of a PDP Context of PDP type Ipv6 or Ipv4v6 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 4291 [82]). 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 4291 [82].

   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 4862 [83].

   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. The GGSN may set the O-flag if there are additional configuration parameters that need to be fetched by the MS (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 4861 [89]. 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 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.

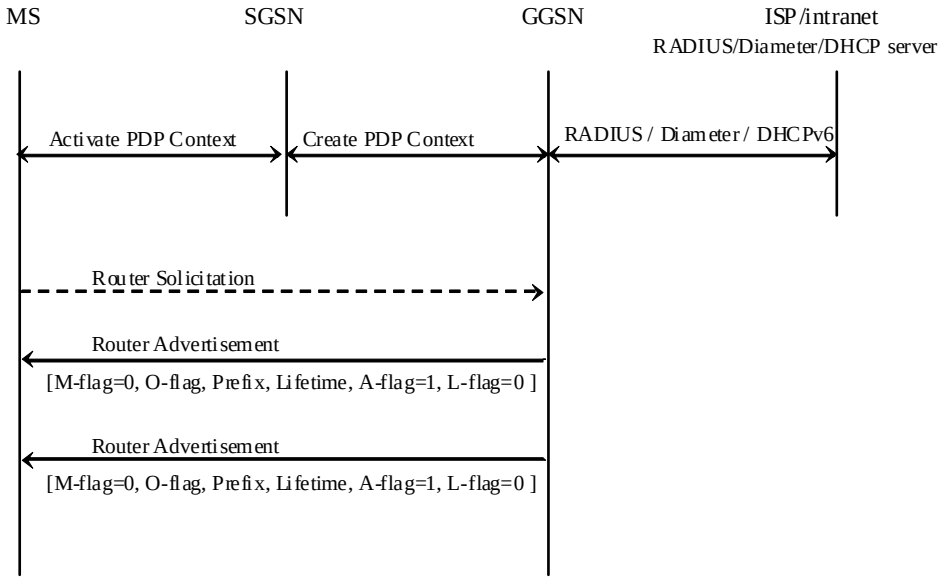


Figure 11bb: Ipv6 Stateless Address Autoconfiguration

11.2.1.3.2a Ipv6 Stateless Address Autoconfiguration for EPC

This subclause describes the signalling flows for the Ipv6 Stateless Address Autoconfiguration procedures for EPC, in the case of using GTP-based S5/S8/S2a, and PMIP-based S5/S8/S2a. The procedures are based on the descriptions in TS 23.401 [77] and TS 23.402 [78]. Subclause 11.2.3.1a lists the use cases between the UE to the P-GW that may trigger the P-GW to interwork with the external PDNs for Ipv6 Prefix allocation.

Ipv6 prefix is delivered to UE in Router Advertisement message from the access router, in the process of Ipv6 Stateless Address Autoconfiguration.

In the procedure in the cases of using GTP-based S5/S8, P-GW acts as an access router, and allocates to a UE a globally unique /64 Ipv6 prefix if the PLMN allocates the prefix, or P-GW retrieves Ipv6 prefix from an external PDN if one is allocated by the external PDN and advertises it to the UE. In the latter procedure, P-GW uses RADIUS, Diameter or DHCPv6 protocol for the retrieval of an Ipv6 prefix.

Following is the flow for Ipv6 Stateless Address Autoconfiguration for EPC using GTP-based S5/S8.

1. UE initiates the Attach procedure, indicating ‘Ipv6’ or ‘Ipv4v6’ for PDN type in PDP type information element.

2. MME requests for Default Bearer creation by sending Create Session Request to the S-GW.

2x. The S-GW sends Create Session Request to the P-GW.

3. P-GW retrieves Ipv6 prefix using RADIUS, Diameter, or DHCPv6 mechanism. This procedure is performed when an external PDN allocates an Ipv6 prefix.

4. The P-GW sends Create Session Response. It includes the Ipv6 interface identifier I Ipv6 prefix.

5. S-GW sends Create Session Response message to the MME. It includes the Ipv6 interface identifier I Ipv6 prefix.

5x. The MME sends Attach Accept message to the UE without the Ipv6 prefix. The UE shall ignore the Ipv6 prefix if it receives one in the message.

6. After receiving the Attach Accept message, the UE may send a Router Solicitation to the P-GW to solicit a Router Advertisement message.

7. The P-GW sends a Router Advertisement message to the UE, solicited or unsolicited. It shall include an Ipv6 prefix in Prefix Information option field of the message. The prefix is the same as the one in the Attach Accept message, if it is provided during the default bearer establishment. For the handling of M, O, L and A flags, and the lifetime of the prefix in the Router Advertisement message, follow the description in subclause 11.2.1.3.2.

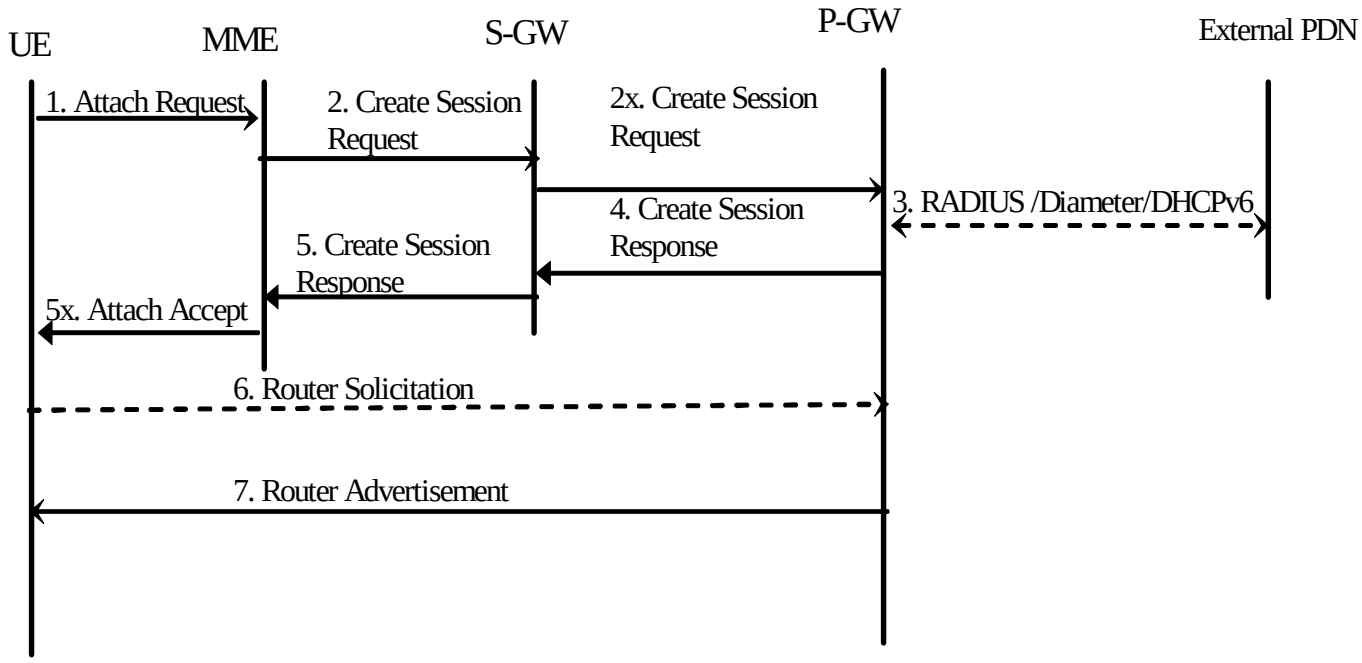


Figure 11bc: Ipv6 Stateless Address Autoconfiguration for GTP-based S5/S8

If PMIP-based S5/S8 is used, S-GW acts as an access router. Therefore, it is responsible for receiving Router Solicitation from and sending Router Advertisement message to the UE. Other than this, procedure is the same as the case of using GTP-based S5/S8; P-GW allocates, or retrieves an Ipv6 prefix from the external PDN. The prefix is delivered from the P-GW to the S-GW in the Ipv6 Home Network Prefix Option IE of a Proxy Binding Ackowledgement message.

In addition, the S-GW shall initiate sending the Ipv6 Router Advertisement message (either solicited or unsolicited) to the UE once the PDN connection with PDN type Ipv4v6 or Ipv6 is setup after the procedure of E-UTRAN initial Attach, UE requested PDN connectivity, intra-3GPP access handover with Serving GW relocation, or handover from non-3GPP IP Access with S2a/S2b to 3GPP Access.

Following diagram shows the case where PMIP-based S5/S8 is used.

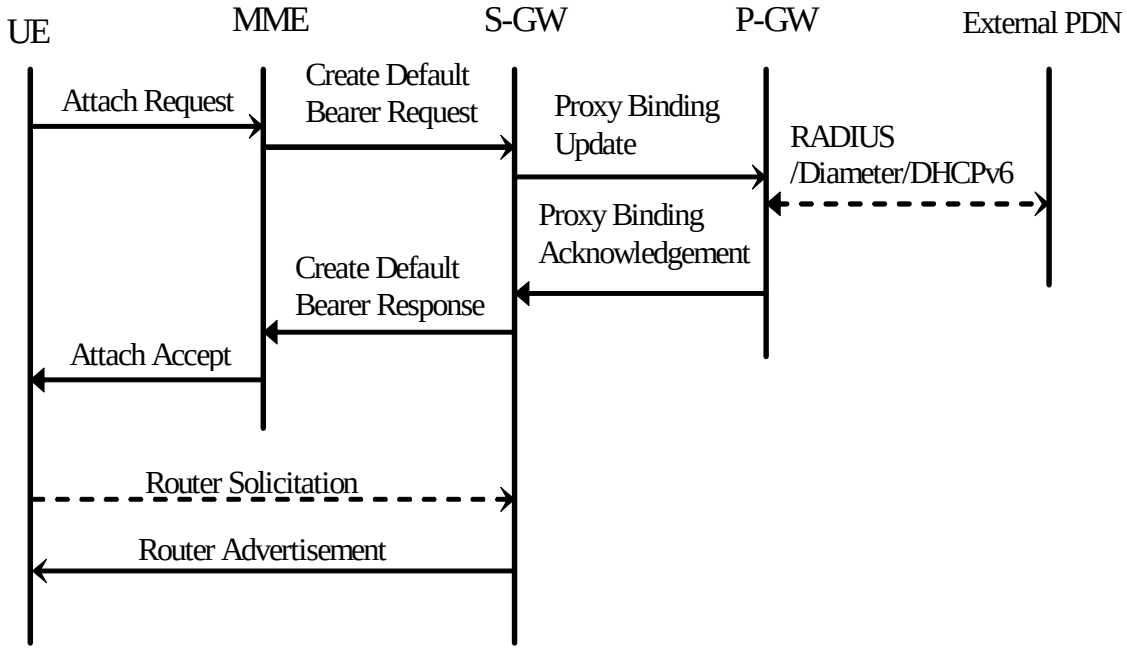


Figure 11bd: Ipv6 Stateless Address Autoconfiguration for PMIP-based S5/S8

For trusted non-3GPP accesses, the non-3GPP network supports prefix advertisement for Ipv6 prefix received from the P-GW in PMIPv6 Proxy Binding Acknowledgement. If the trusted non-3GPP access network is a WLAN network, for GTP/PMIP –based S2a, TWAN acts as an access router. Therefore, TWAN is responsible for receiving Router Solicitation from and sending Router Advertisement message to the UE. Other than this, procedure is the same as the case of using GTP/PMIP-based S5/S8; P-GW allocates, or retrieves an Ipv6 prefix from the external PDN. The prefix is delivered from the P-GW to the TWAN in the Ipv6 Home Network Prefix Option IE of a Proxy Binding Ackowledgement message or in the PDN Address Allocation IE of Create Session Response message.

Following diagram shows the case for trusted non-3GPP access network for WLAN access where GTP/PMIP-based S2a is used.

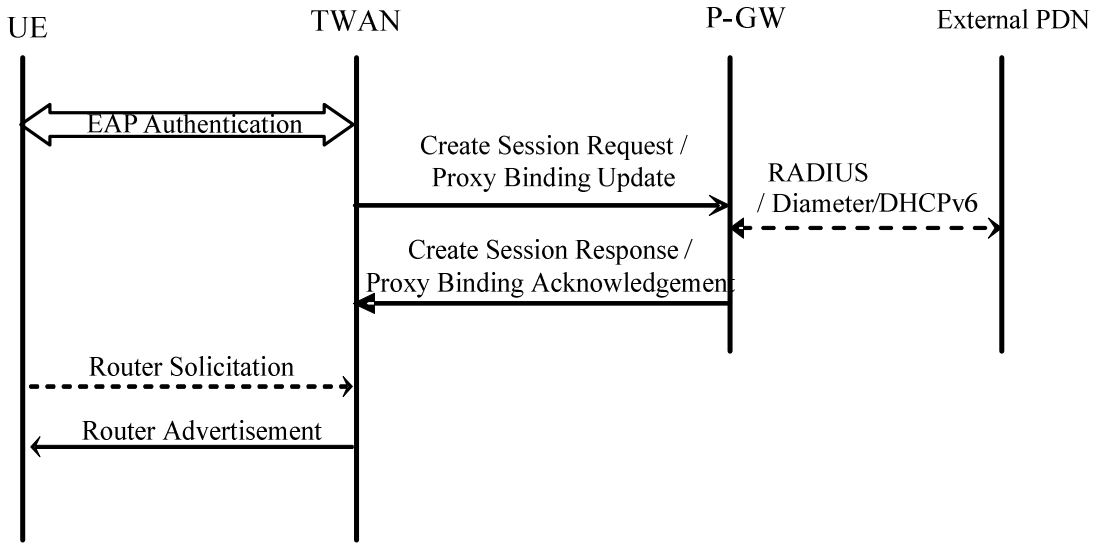


Figure 11be: Ipv6 Stateless Address Autoconfiguration for trusted WLAN access for GTP/PMIP-based S2a

The P-GW ensures that the advertised Ipv6 prefix is globally unique. Regarding the handling of Duplicate Address Detection, follow subclause 11.2.1.3.2.

The UE constructs its full Ipv6 address in accordance with RFC 4862[83]. For the handling of Ipv6 interface identifier, refer to subclause 11.2.1.3.2.

If the P-GW, S-GW and TWAN receive Neighbor Solicitation message from the UE, it shall answer with Neighbor Advertisement message.

To renew the allocated Ipv6 prefix, the P-GW (GTP based S5/S8), S-GW (PMIPv6 based S5/S8) or TWAN (GTP/PMIP based S2a) shall send an Ipv6 Router Advertisement (solicited or unsolicited) to the UE with the same assigned Ipv6 prefix and and new non-zero values in preferred and valid lifetime fields for the PDN connection (PDN type Ipv4v6 or Ipv6), before the Router Advertisement lifetime and prefix lifetime expiry, as specified in IETF RFC 4861 [89]. When sending the Ipv6 Router Advertisement message, the S-GW may trigger the paging (e.g. by sending a Downlink Data Notification message to the MME) if the UE is in idle state. In order to reduce paging an idle UE to deliver RA, the Router Advertisement lifetime and Ipv6 prefix lifetime shall be configured accordingly.

If a UE supports multiple PDN connections functionality, it can connect to multiple P-GWs simultaneously, or it can access multiple PDNs through a single P-GW. In the former case, the Ipv6 prefix allocated for its default bearer is used for the UE's dedicated bearers toward the same PDN. In the latter case, Ipv6 Stateless Address Autoconfiguration procedure is applied for each PDN connection.

11.2.1.3.3 Ipv6 Stateful Address Autoconfiguration

Void.

Figure 11bc : Void

11.2.1.3.4 Ipv6 Router Configuration Variables

For Ipv6 Address Autoconfiguration to work properly , network entities which act as an access router towards the MS/UE, i.e. PDN GW, Serving GW, ePDG and TWAN, shall be consistent with the RFCs specifying this process (for example RFC 4862 [83] and RFC 4861 [89]), unless stated otherwise in this or other 3GPP specifications.

RFC 4861 [89] specifies a set of conceptual router configuration variables. Some of these variables require particular attention in GPRS and EPC in order to preserve radio resources and MS/UE 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 and EPC. 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 EPC, and supersede those specified in RFC 4861 [89].

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/Bearer Deactivation.

AdvPreferredLifetime

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

RFC 4861 [89] also specifies a number of protocol constants. The following shall have specific values for GPRS and EPC:

MAX_INITIAL_RTR_ADVERT_INTERVAL

This constant may be a variable within GPRS and EPC. 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 or MS/UE-PDN GW/Serving GW/ePDG/TWAN links in most cases, while still allowing the MS/UE 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 or MS/UE-PDN GW/Serving GW/ePDG/TWAN links have 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/UE 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.

11.2.1.3.5 Ipv6 Prefix Delegation via DHCPv6

Optionally, a single network prefix shorter than the default /64 prefix may be assigned to a PDN connection. In this case, the /64 default prefix used for Ipv6 stateless autoconfiguration will be allocated from this network prefix; the remaining address space from the network prefix can be delegated to the PDN connection using prefix delegation after the PDP context activation/default bearer establishment and Ipv6 prefix allocation via Ipv6 stateless address autoconfiguration as defined in clause 11.2.1.3.2/11.2.1.3.2a. When PLMN based parameter configuration is used, the GGSN / PDN GW provides the requested Ipv6 prefix from a locally provisioned pool. When external PDN based Ipv6 prefix allocation is used, the GGSN / PDN GW may obtain the prefix from the external PDN as per subclauses 16.4 and 16a.4.

For the detailed description of the UE uses DHCPv6 to request additional Ipv6 prefixes refer to 3GPP TS 23.060 [3] and 3GPP TS 23.401 [77].

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 39orrectio 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.

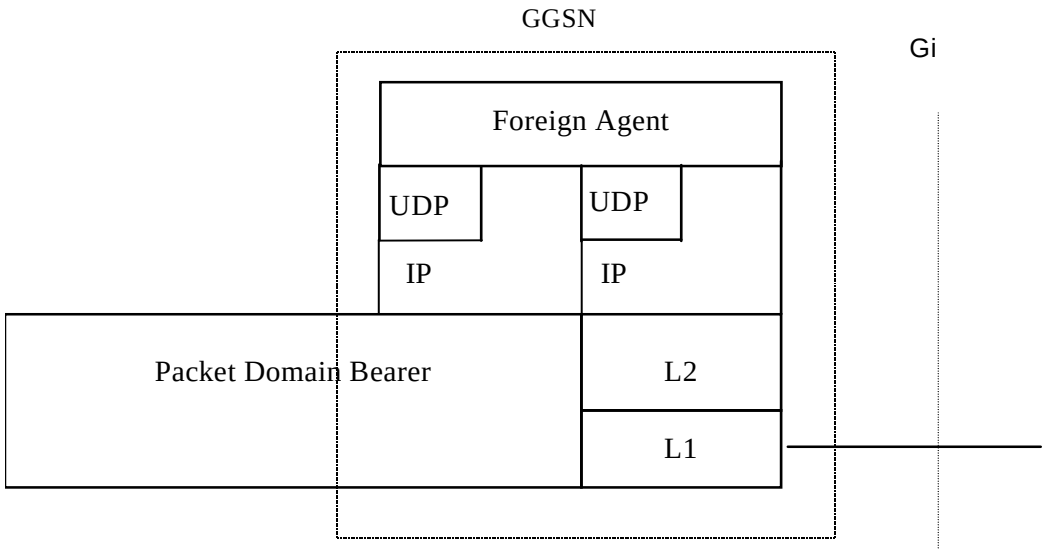


Figure 11c: The protocol stacks for the Gi IP reference point in the MIP signalling plane

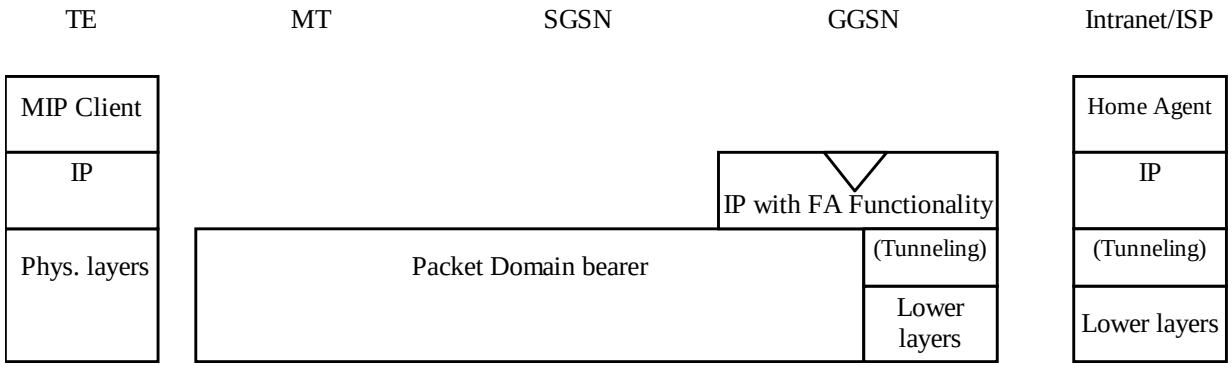


Figure 11d: Protocol stacks for user access with MIP

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

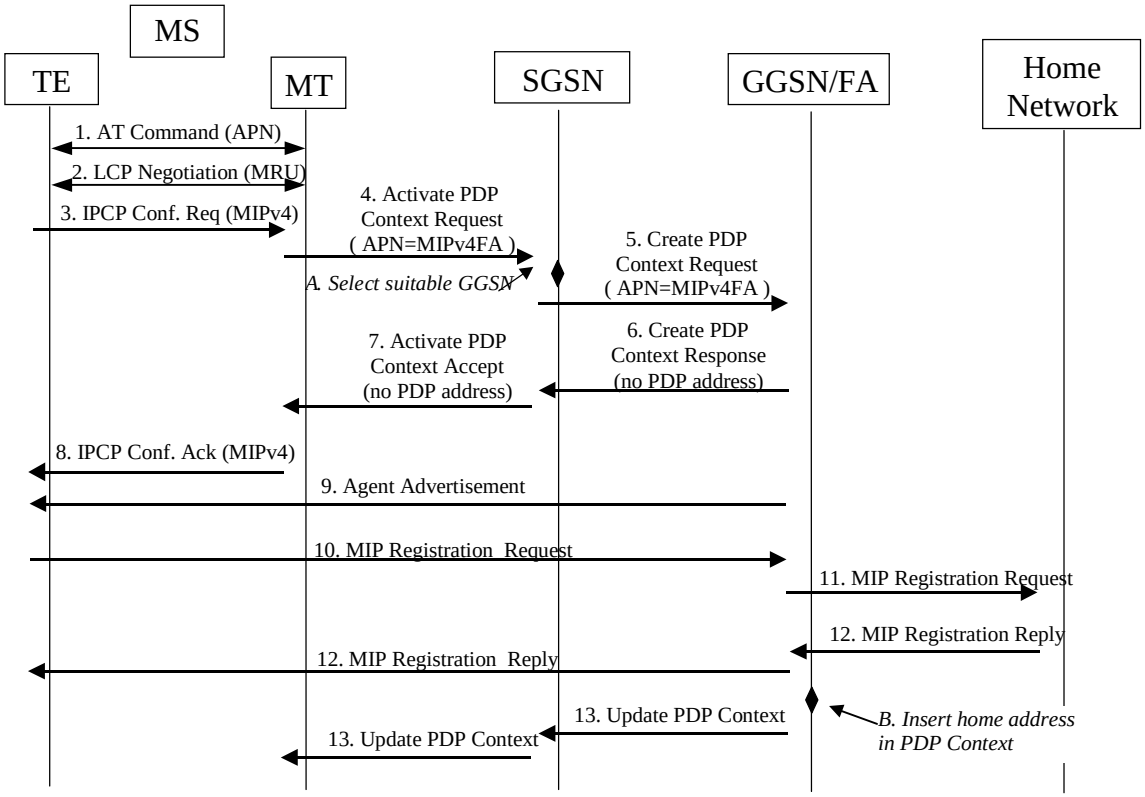


Figure 11e: Example of PDP Context activation with Mobile IP registration (the PS attach procedure not included)

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.

11.2.1.5 IP Fragmentation Across Gi/Sgi

3GPP and non-3GPP accesses provide IP services for a MS/UE. The GGSN/P-GW endpoint is a GTPv1-U tunnel (controlled by GTP Gn/Gp or S5/S8/S2a/S2b) or IP tunnel (controlled by S5/S8/S2a/S2b PMIPv6 or employed by a UE with MIPv4 or DSMIPv6).

The MTU of the IP tunnel on the MS/UE side of the IP link may be different than the MTU of the IP link connecting the GGSN/P-GW to the PDN. As a result IP packets crossing the Gi/Sgi interface may need to be fragmented. Unnecessary fragmentation should be avoided when possible due to the following;

- Fragmentation is bandwidth inefficient, since the complete IP header is duplicated in each fragment.

- Fragmentation is CPU intensive since more fragments require more processing at IP endpoints and IP routers. It also requires additional memory at the receiver.

- If one fragment is lost, the complete IP packet has to be discarded. The reason is there is no selective retransmission of IP fragments provided in Ipv4 or Ipv6.

To avoid unnecessary fragmenting of IP packets the MS/UE, or a server in an external IP network, may find out the end-to-end MTU by path MTU discovery and hence fragment correctly at the source. IP Fragmentation on Gi/Sgi shall be handled according to IETF RFC 791 [16] and IETF RFC 2460 [49]. The GGSN/P-GW shall enforce the MTU of IP packets to/from the MS/UE based on IETF RFC 791 [16] and IETF RFC 2460 [49].

11.2.2 Access to networks handling Non-IP data services through Packet Domain

The support of Non-IP data is part of the CIoT EPS optimisations (see 3GPP TS 23.401 [77]) and 3GPP TS 23.060 [3]). A PDN/PDP Type "Non-IP" is used for Non-IP data. The Non-IP data delivery to the network handling Non-IP data services is accomplished by one of two mechanisms:

- Delivery using SCEF
- Delivery using a Point-to-Point (PtP) SGi tunnel

Data delivery using SCEF is further described in 3GPP TS 29.128 [110].

In order to allow Non-IP delivery data using SGi PtP tunnelling based on UDP/IP (see subclause 11.8), the Packet Domain may offer direct transparent access to the Non-IP Packet Data Network with the following characteristics:

- The IPv4 address and/or IPv6 prefix is assigned as part of the PDN connection establishment and identifies the PDN connection of the UE within the PLMN domain.
- IP address allocation procedures for the UE (i.e. PDN connection) are performed by the GGSN/P-GW based on APN configuration. Only a single IP address is used (i.e. either IPv4 or IPv6 prefix+Interface Identifier is allocated/assigned). In case of IPv6 the GGSN/P-GW assigns an Interface Identifier for the PDN connection. The IP address or IP prefix is not provided to the UE (i.e. SLAAC / Router Advertisements are not performed. DHCP or DHCPv6 are not used).
- The assigned IPv4 address or IPv6 prefix is used for UDP/IP encapsulation for PtP tunneling between the Non-IP network and the GGSN/P-GW (see subclause 11.8).
- Stateless Address Autoconfiguration does not apply for IPv6. Both IPv4 and IPv6 addresses belong to the operator addressing space.

User authentication and encryption of user data when accessing networks handling Non-IP data services is outside 3GPP specification.

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 PLMN operator manages internally the subnetwork IPv4 addresses and/ or IPv6 prefixes as applicable. Each private network is assigned a unique subnetwork IPv4 addresses and/ 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/P-GW and each private network. In this case the IP address alone is not necessarily unique. The pair of values, Access Point Name (APN) and IPv4 address and/or IPv6 prefixes, is unique.

NOTE 1: In IPv6, "site-local addresses"were originally designed to be used for addressing inside of a site that is similar to the usage of "private addresses" in IPv4. The usage of "site-local-addresses" is deprecated as specified in RFC 4291 [82]. Existing implementations and deployments may continue using site-local addresses. However, in new implementations the prefix that was allocated for "site local addresses" shall be treated as for "global unicast addresses", see RFC 4291 [82].

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

- The PLMN operator allocates a static IPv4 address and/or a static IPv6 prefix when the subscription record is built. The IPv4 address and/or IPv6 prefix are respectively reserved from a pool of free IPv4 addresses and/or IPv6 prefixes. Each external network has its own pool of IPv4 addresses and/or IPv6 prefixes.
- The PLMN operator allocates (either on its own or in conjunction with the external network) a dynamic IPv4 address and/or a dynamic IPv6 prefix as described in 3GPP TS 23.060 [3], 3GPP TS 23.401 [77] and 3GPP TS 23.402 [78].

For UEs used for Machine-Type Communications (MTC) as described in 3GPP TS 23.401 [77] and 3GPP TS 23.060 [3] and Cellular Internet of Things (CIoT) as described in 3GPP TS 23.401 [77] and 3GPP TS 23.060 [3], IPv6 address allocation should be the primary mechanism for IP address allocation. IPv4 based address allocation is considered a transition solution and is deprecated for MTC used over 3GPP accesses.

NOTE 2: For implementation guidelines related to transition and other aspects of IPv4 address usage see 3GPP TS 23.221 [99] Annex B.

In case of transferring Non-IP data over SGi PtP tunnelling based on UDP/IP (see subclause 11.8) the PLMN operator uses private network addresses for the establishment of the tunnel.

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. For non-EPS networks see 3GPP TS 23.060 [3] (DNS documentation is provided in RFC 1034 [19] and RFC 1035 [58]) and for EPS networks see 3GPP TS 29.303 [96].

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

NOTE: This section is applicable only to GERAN and UTRAN.

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/UE to subscribe to multicast groups from outside the PLMN, the GGSN/P-GW 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/P-GW 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/P-GW 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/P-GW 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/UE has attached to the Packet Domain, and a bearer (e.g. Activated PDP context(s)) (including possibly authentication) pointing to the preferred ISP/external network for this purpose. 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) for the non-EPC based domain case. 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. If the protocol configuration for handling Multicast traffic (control plane) is applied for Sgi (i.e EPC based packet domain), the P-GW has the functionality of GGSN and Sgi corresponds to the Gi in Figure 12.

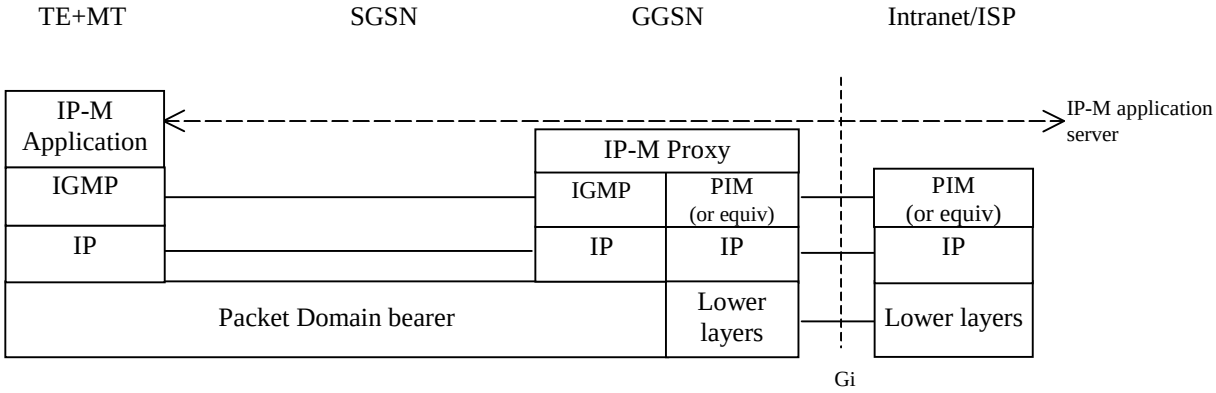


Figure 12: Protocol configuration for IP-Multicast handling (control plane)

11.8 Non-IP data transfering over SGi

11.8.1 General

When support of Non-IP data is provided at the Gi/SGi interface, different Point-to-Point (PtP) tunneling techniques may be used. When using PtP tunneling by UDP/IP encapsulation subclause 11.8.2 below shall be followed. Other techniques as described in clause 11.8.3 below may be used.

The Gi/SGi based Non-IP data delivery is applicable to the User Plane CIoT EPS Optimization and the Control Plane CIoT EPS Optimization (see 3GPP TS 23.401 [77] and 3GPP TS 23.060 [3]).

11.8.2 Gi/SGi PtP tunnelling based on UDP/IP

Gi/SGi PtP tunnelling based on UDP/IP may be used to deliver Non-IP data to an AS via Gi/SGi.

The PtP tunnel is set up by configuration of tunnel parameters in both end of the tunnel.
The following parameters are pre-configured in the GGSN/P-GW per APN;

- the UDP destination port number to use when sending Non-IP data;
- the UDP port number it wants to receive Non-IP data;
- the destination IP address to be used for sending Non-IP data.

NOTE 1: Many APNs can resolve to the same P-GW, but each APN can be unique to a particular AS.

The following is pre-configured in the AS;

- the UDP destination port number to use when sending Non-IP data;
- the UDP port number it wants to receive Non-IP data.

NOTE 2: The GGSN/P-GW as well as the AS can use any UDP port numbers not assigned by IANA. The port numbers used need to be aligned between peers.

IP address allocation procedures for the UE (i.e. PDN connection) are performed by the GGSN/P-GW as described in subclause 11.2.2.
The UE IP address for the PDN connection or IPv6 prefix allocated for the PDN connection+suffix assigned for the PtP tunnel end point in the GGSN/P-GW is used as source address in the GGSN/P-GW and as destination address in the AS for the PtP tunnel.

During the PDP context/PDN connection establishment, the GGSN/P-GW associates the GTP-U tunnel for the PDP context/PDN connection with the Gi/SGi PtP tunnel. The GTP-U tunnel with PDP/PDN type “Non-IP” is used.

The GGSN/P-GW acts as a transparent forwarding node between the UE used for CIoT and the AS.

NOTE 3: The UE can include application level identity to AS, what kind of identity is out of scope of this specification.

For uplink delivery, if the uplink data is received from the GTP-U tunnel the GGSN/P-GW shall forward the received data to the AS over the Gi/SGi PtP tunnel associated with the GTP-U tunnel using UDP/IP encapsulation with the destination address of the AS and the configured UDP destination port number for “Non-IP” data as described above.

For downlink delivery, the AS shall send the data using UDP/IP encapsulation with the IP address or IPv6 prefix+suffix of the UE as destination address and the configured UDP destination port number for “Non-IP” data as described above.

NOTE 3: The UDP source port number to use for both uplink and downlink Non-IP data transfer can be a pre-configured or a locally allocated port number in the GGSN/P-GW and AS respectively.

NOTE 4: For downlink delivery, the GGSN/P-GW decapsulates the received data (i.e. removes the UDP/IP headers) and forwards the data to SGSN/S-GW on the GTP-U tunnel identified by the IP address or the IPv6 prefix of the UE (i.e. PDN connection) for delivery to the UE.

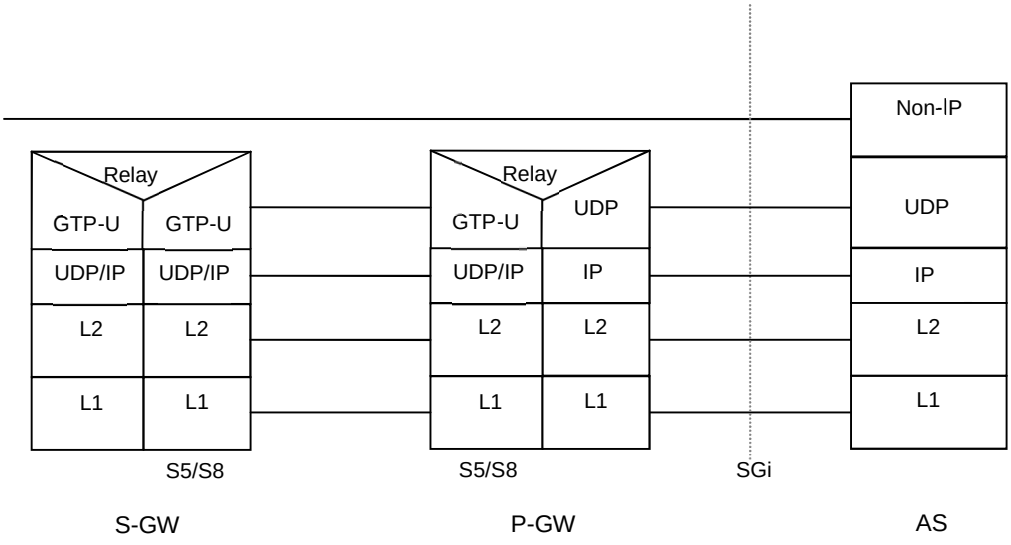


Figure 11.8: Protocol configuration for Non-IP data (user plane) using SGiPtP tunneling

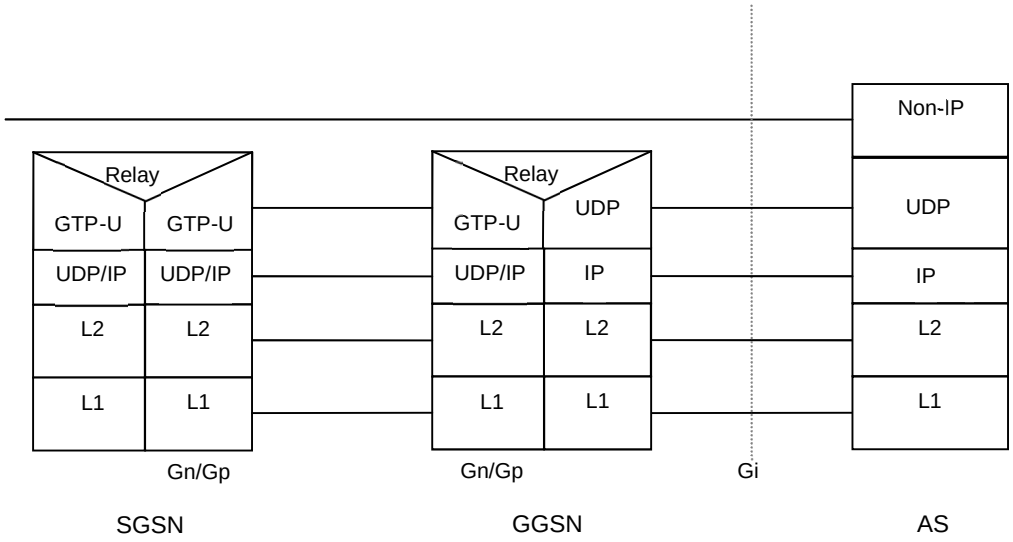


Figure 11.9: Protocol configuration for Non-IP data (user plane) using Gi PtP tunneling.

11.8.3 Other SGi PtP tunnelling mechanisms

SGi PtP tunnelling mechanisms such as PMIPv6/GRE, L2TP, GTP-C/U, etc, may be used to deliver Non-IP data to AS via SGi.

The PtP tunnel is established towards the AS by the P-GW. Depending on the type of protocol employed on the SGi PtP tunnel, the SGi PtP tunnel setup may be done at the time of attach or at the time of first MO datagram being sent by the CIoT UE.

The P-GW selects the AS based on the P-GW configuration (eg. per APN, or per PtP tunnel type etc).

NOTE: IP address allocation procedures for the UE are not performed by the P-GW.

For uplink Non-IP data, the P-GW forwards the received data to the AS over the established SGi PtP tunnel.

For downlink Non-IP data, the AS locates the right SGi PtP tunnel for the UE (using information such as UE identifiers in the Non-IP protocol itself, etc) to forward the data. The AS sends the data to P-GW over the established SGi PtP tunnel. The P-GW inturn sends the data to S-GW on the GTP-U tunnel identified by the associated SGi PtP tunnel for delivery to the UE.

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.

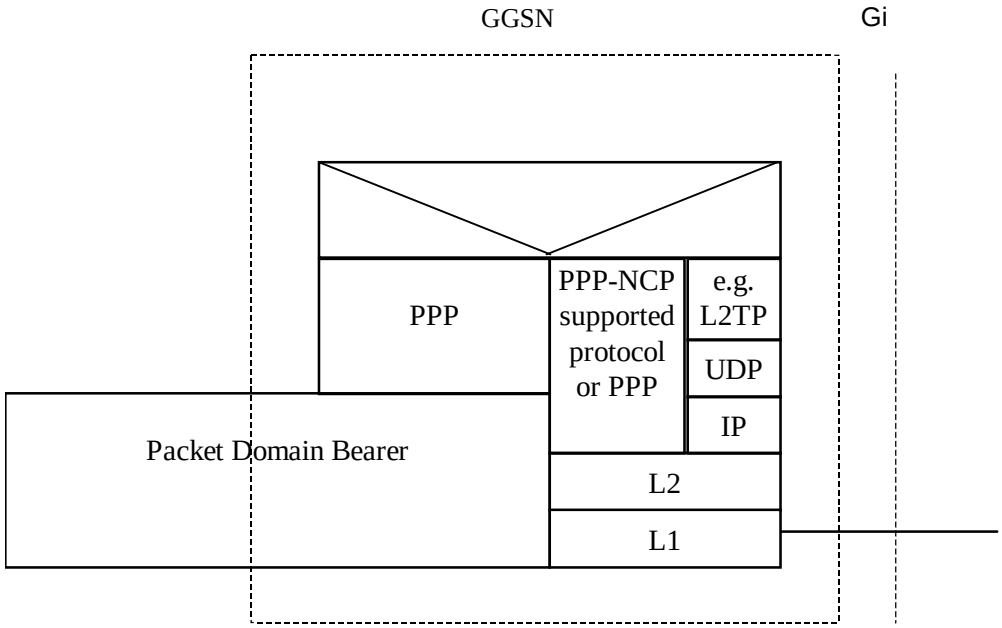


Figure 13: The protocol stacks for the Gi PPP reference point

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);

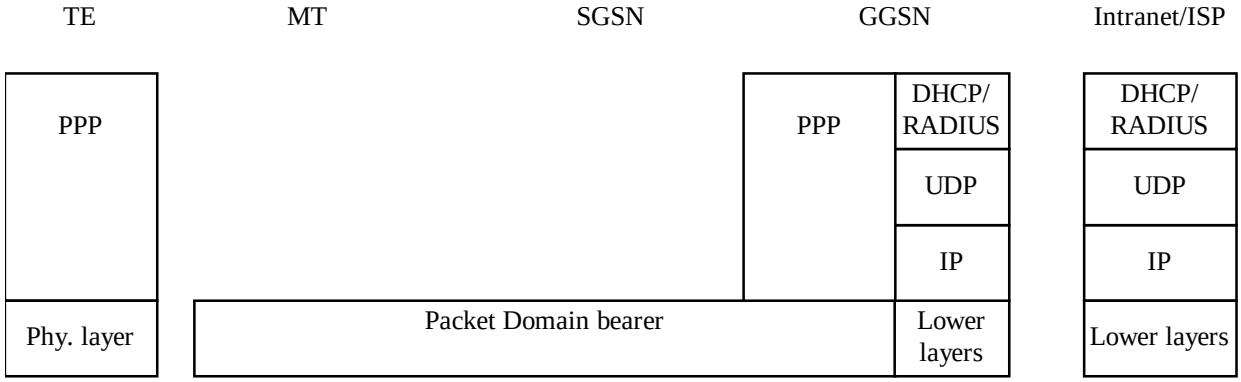


Figure 14: Protocol stack for direct access to IP-based Intranets/ISPs

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

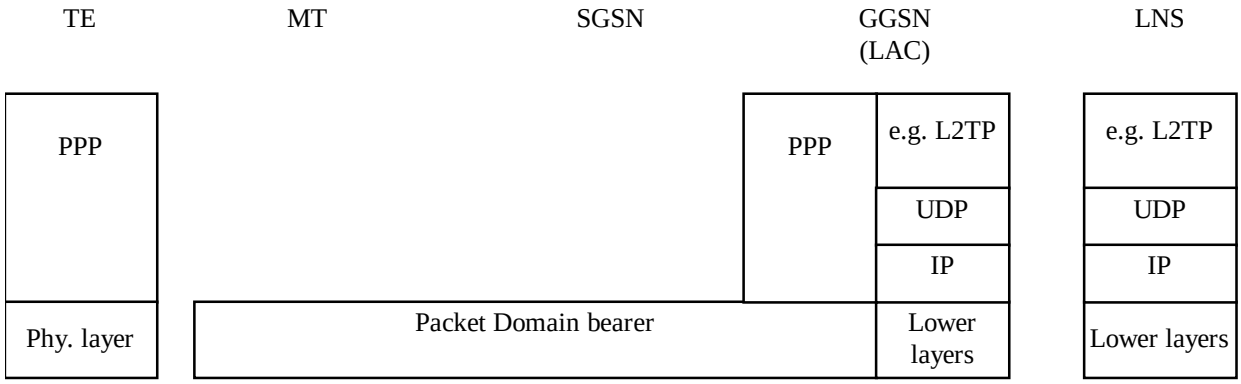


Figure 15: Protocol stack for virtual dial-up access with PPP frame tunnelling

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.

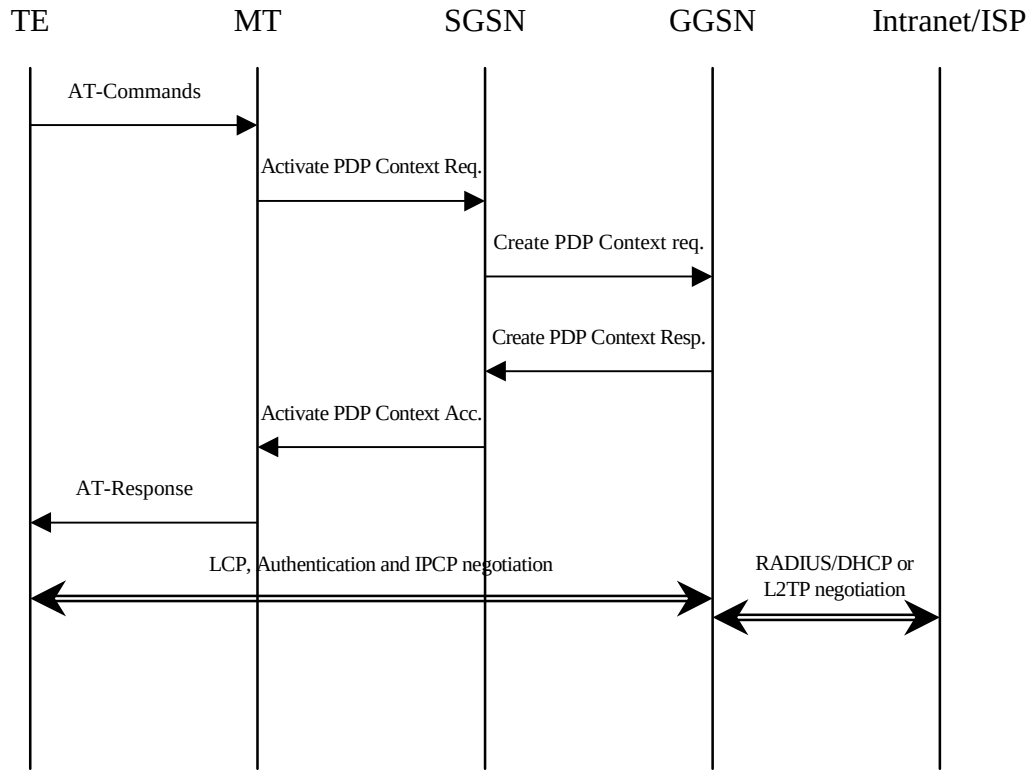


Figure 16a

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 may obtain IP address via external DHCP server during the packet bearer establishment procedures (e.g. PDP Context activation, default bearer establishment). The GGSN/P-GW acts as a DHCP client towards the external DHCP server.

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 in non-EPC based Packet Domain, a DHCP relay agent function is needed in the GGSN so as to allow correct routing of DHCP requests and replies between the TE and the DHCP servers. In EPC based Packet Domain for 3GPP access networks, the P-GW acts a DHCP server towards the UE and it acts as a DHCP client towards the external DHCP server. For trusted non-3GPP access networks, the non-3GPP access network may act as a DHCP relay or DHCP server. In the trusted WLAN access network, the TWAN acts a DHCP server towards the UE and PGW acts as a DHCP client towards the external DHCP server for the GTP/PMIP-based S2a.

In non-EPC based Packet Domain,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 bearer associated with the allocated IP address (i.e. Ipv4 address or Ipv6 prefix) shall be released:

- 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 associated bearer shall be released.

13.2 PDN Interworking Model of GGSN 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.

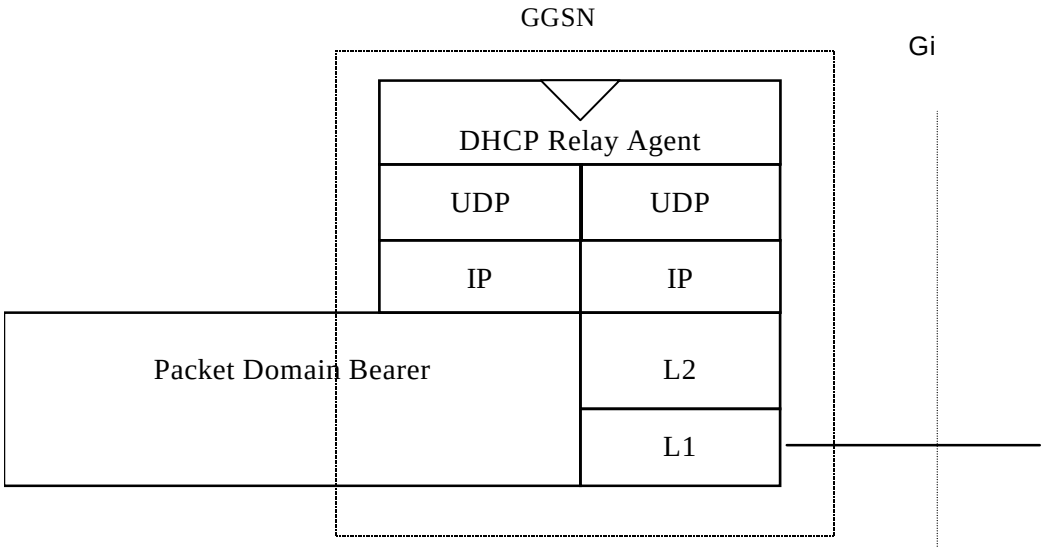


Figure 16b: The protocol stacks for the Gi IP reference point for DHCP

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.

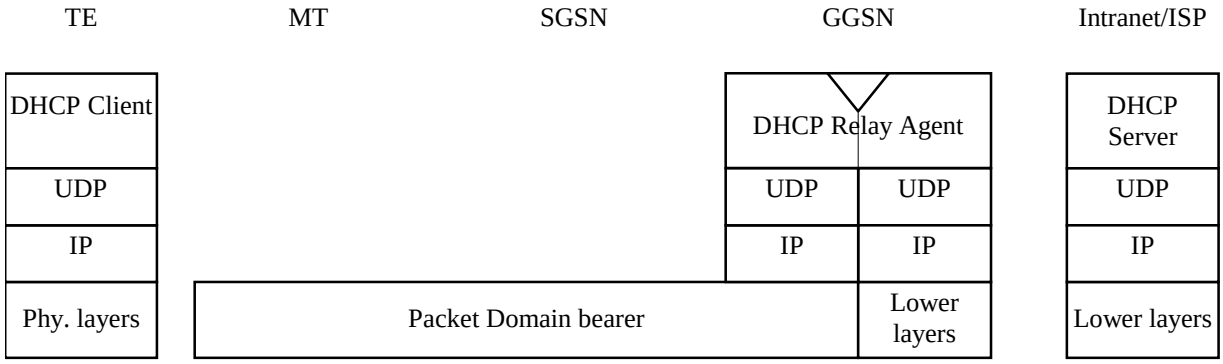


Figure 16c: Protocol stack for access with DHCP end-to-end

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.

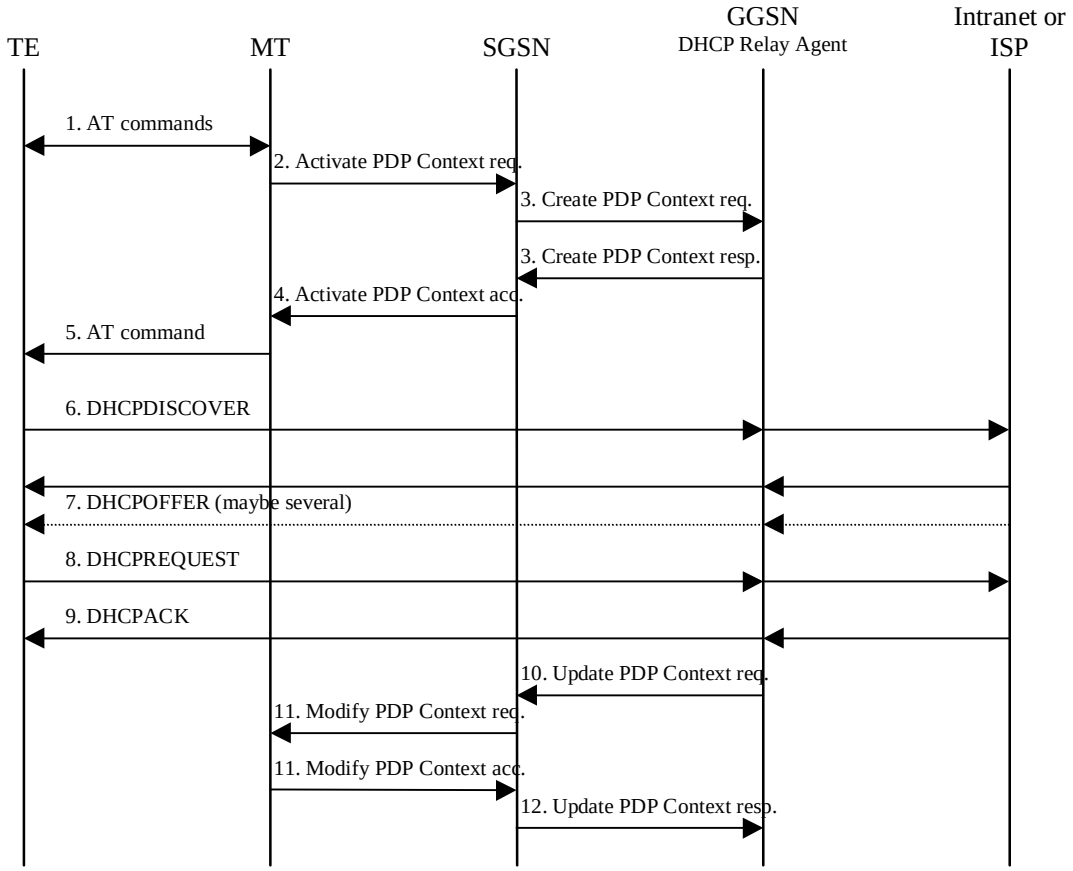


Figure16d: DHCPv4 signal flow

13.2.1.2 Void.

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.

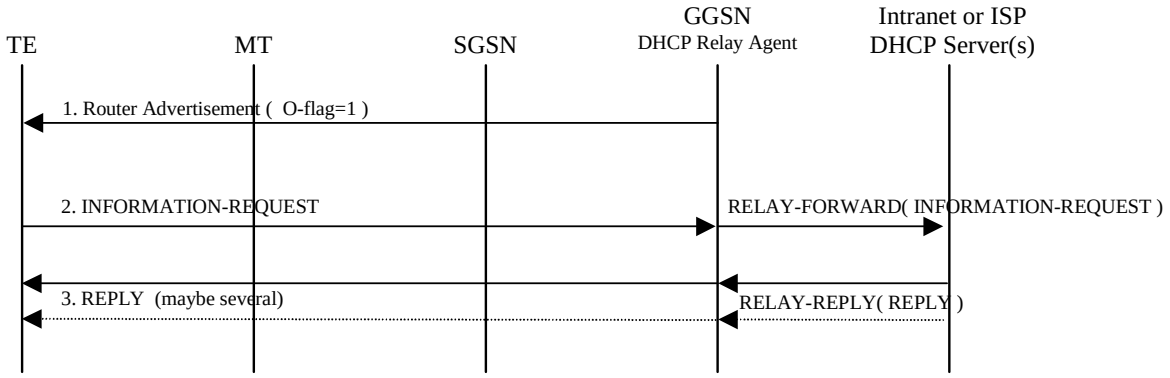


Figure 16f: DHCPv6 Other configuration signal flow

13.3 PDN Interworking Model of P-GW for DHCP

A DHCP Client shall be located in the P-GW used for interworking with the IP network as illustrated in Figure 16g.

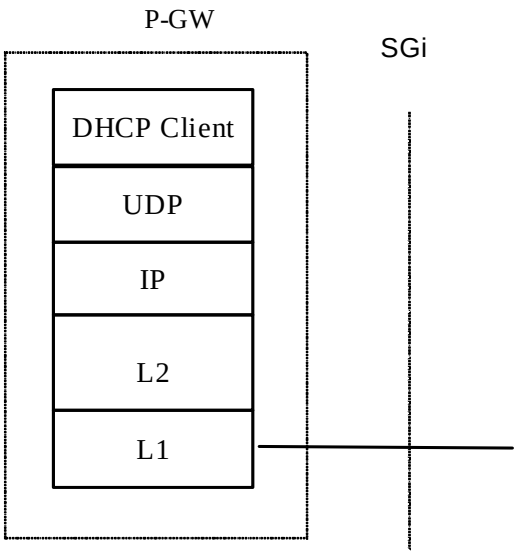


Figure 16g: The protocol stacks for the Sgi IP reference point for DHCP

The DHCP client function in P-GW shall be used to allocate IP address(es) to the UE and/or to configure associated parameters via external DHCP servers in PDN(s). As both Ipv4 and Ipv6 address allocation are supported in EPS, the P-GW shall have both DHCPv4 and DHCPv6 client functions.

The procedures where the DHCP client function in the P-GW is used are further described in TS 23.060 [3], TS 23.401 [77] and TS 23.402 [78]. The procedures are Ipv4 address allocation and Ipv4 parameter configuration via an external DHCPv4 server in a PDN; Ipv6 Prefix allocation via stateless address autoconfiguration; and Ipv6 parameter configuration via stateless DHCPv6. These procedures are detailed in the subclauses below.

13.3.1 Address allocation by the Intranet or ISP

The subclauses below provide the signalling flows when the IP address allocation and/or the IP parameter configuration to a UE is performed via an external DHCP server in the PDN.

13.3.1.1 Ipv4 Address allocation and Ipv4 parameter configuration via DHCPv4

The UE may obtain the Ipv4 address and/or its configuration parameters at or after the initial access signalling (e.g. default bearer establishment) to the packet domain. The request for Ipv4 address and/or configuration parameters from the UE may trigger the P-GW acting as DHCPv4 client to request the Ipv4 address and/or configuration parameters from an external DHCPv4 server and deliver them to the UE. See subclause 11.2.1.2.2 for details. The DHCPv4 functions in the P-GW, the UE and the external DHCPv4 server shall be compliant to RFC 2131 [26], RFC 1542 [27] and RFC 4039 [79].

The following bullet items describe the successful Ipv4 address allocation and parameter configuration signalling flow between the P-GW and the external DHCPv4 server as depicted Figure 16h. For a detailed description of the DHCPv4 messages, refer to RFC 2131 [26], RFC 1542 [27] and RFC 4039 [79].

Figure 16h is an example signalling flow for Ipv4 address allocation and parameter configuration at the default bearer setup using DHCPv4 as specified in RFC 2131 [26]. If the optimized signalling (Rapid Commit Option) is used as per RFC 4039 [79], the messages 2-3 can be eliminated.

1) The DHCPv4 client function in the P-GW sends a DHCPDISCOVER as an IP limited broadcast message, i.e. the destination address 255.255.255.255, towards the external PDN. If the P-GW has the DHCPv4 server IP addresses configured for the APN, the DHCPDISCOVER shall be send as unicast (or even multicast) to the external DHCPv4 servers.

2) Upon receiving the DHCPDISCOVER request message, the external DHCPv4 servers reply by sending a DHCPOFFER message including an offered IP address. Several DHCPOFFER messages may be received by the P-GW if multiple DHCPv4 servers respond to the DHCPDISCOVER.

3) The DHCPv4 client function in the P-GW processes the messages and sends a DHCPREQUEST towards the selected external DHCPv4 server.

4) Upon receiving the DHCPREQUEST message, the selected external DHCPv4 server acknowledges the address allocation by sending a DHCPACK containing the lease period (T1), the time-out time (T2) and the configuration information requested in DHCPREQUEST. The P-GW stores the allocated Ipv4 address, the lease timers and the configuration parameters. The Ipv4 address and the configuration parameters shall be delivered to the UE through P-GW to UE messages.

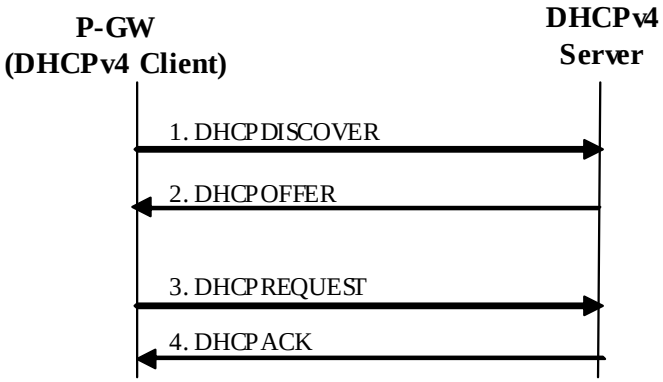


Figure 16h: The signalling flow for Ipv4 address allocation and parameter configuration using DHCPv4

Figure 16i is an example signalling flow for Ipv4 address lease renew by using DHCPv4 protocol as specified in RFC 2131 [26].

1) The DHCPv4 client function in the P-GW sends a unicast DHCPREQUEST towards the external DHCPv4 server to extend the lease period of the allocated Ipv4 address.

2) The external DHCPv4 server replies with a DHCPACK message confirming the renewed lease and the T1 and T2 timers are restarted.

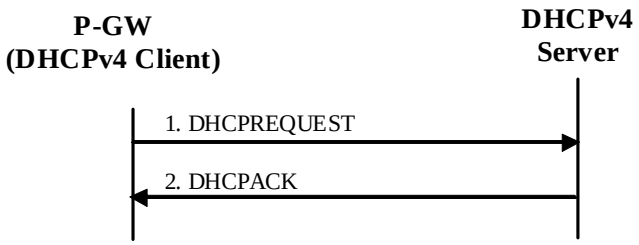


Figure 16i: The signalling flow for Ipv4 address lease renew using DHCPv4

13.3.1.2 Ipv6 Prefix allocation via Ipv6 stateless address autoconfiguration via DHCPv6

When the Ipv6 prefix is allocated from the external PDN, it is the P-GW's responsibility to obtain the Ipv6 prefix for external PDN, allocate and release the Ipv6 prefix. The P-GW may use DHCPv6 to obtain the Ipv6 prefix from the external PDN. In this context, the P-GW shall act as a DHCP client as per IETF RFC 3315 [46] towards the external DHCPv6 server. The use cases between the UE and the P-GW that may lead the P-GW to interwork with the external DHCPv6 servers are described in subclause 11.2.1.3.1a.

13.3.1.3 Ipv6 parameter configuration via stateless DHCPv6

A UE that has obtained an Ipv6 address can use stateless DHCP to request other configuration information such as a list of DNS recursive name servers or SIP servers.

For 3GPP networks if such Ipv6 configuration parameters are locally provisioned in the P-GW, the P-GW returns the requested parameters to the UE via its DHCPv6 server function. For trusted non-3gpp access networks, if such Ipv6

configuration parameters are locally provisioned in the P-GW, the P-GW may return the requested parameters to the UE via its DHCPv6 server function or the P-GW may return the Ipv6 configuration parameters to the non-3gpp access network and then the non-3GPP access network may send the parameters to the UE via its DHCPv6 server function. When the non-3GPP access network is a trusted WLAN network, the PGW always returns the Ipv6 configuration parameters to the TWAN via GTP/PMIP message, and then the TWAN sends the parameters to the UE via its DHCPv6 server function. When an external DHCP6 server in a PDN is used to obtain the requested parameters, which is the use case covered in this subclause, the P-GW acts as a DHCPv6 client towards the external DHCPv6 server while acting a DHCPv6 server towards the UE.

The Ipv6 parameter configuration via stateles DHCPv6 function in the UE, the P-GW and the external DHCPv6 Server shall be compliant to RFC 3736 [80]. An example signalling flow for the GGSN is described in Subclause 13.2.2. For the P-GW, the signalling flow is same with the following modifications:

- For 3GPP access networks, the P-GW sends Router Advertisement for GTP-based S5/S8. In the case of PMIP-based S5/S8, the S-GW sends the Router Advertisement. For trusted non-3GPP access networks, the trusted non-3GPP access network sends the Router Advertisement for PMIP S2a.When the non-3GPP access network is a trusted WLAN network, the TWAN sends the Router Advertisement

As stated above, the P-GW acts as a DHCPv6 server towards the UE, while acting as a DHCPv6 client towards the external DHCPv6 server.

13a Interworking with IMS

13a.1 General

Interworking with the IP Multimedia Core Network Subsystem (IMS) puts additional requirements on the GGSN/P-GW. When the MS/UE 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, P-CSCF restoration support, returned P-CSCF address(es) and flow identifier(s).

For interworking with the IMS, the Gx interface (see 3GPP TS 29.212 [75]) is used to correlate the session (SIP/SDP) and the bearer (PDP Contexts).

The mechanisms in GGSN/P-GW to support IMS shall be:

- P-CSCF discovery.
- Dedicated signalling bearer (e.g. PDP contexts) (with or without enhanced QoS) for IMS signalling; with associated packet filters to permit signalling to/from designated servers.
- Gx interface for policy and charging control of bearer (e.g. PDP contexts) for IMS media flows.
- P-CSCF restoration.

These mechanisms are however not restricted to the IMS and could be used for other services that could benefit from these mechanisms.

The P-GW shall not modify the fields Type of Service (IPv4) and Traffic Class (IPv6).

NOTE: The P-CSCF can support paging policy differentiation for different traffic or service types over LTE by marking the fields Type of Service (IPv4) and Traffic Class (IPv6) (see clause L.3.2.4 of 3GPP TS 24.229 [47]).

13a.2 IMS Interworking Model

The signalling interface between MS/UE and P-CSCF is a logical interface, i.e. it is using GPRS or EPC as a bearer. The Gx interface is used for network communication between the GGSN/P-GW and the PCRF. For a description of the IMS architecture, refer to 3GPP TS 23.228 [52]. For a more detailed view of GGSN/P-GW IMS interworking, see 3GPP TS 29.213 [76].

13a.2.1 IMS Specific Configuration in the GGSN/P-GW

The GGSN/P-GW shall have a list of preconfigured addresses of signalling servers (P-CSCF servers). This list shall be provided to MSs/UEs on request. The list shall be possible to preconfigure per APN.

The GGSN/P-GW shall have locally preconfigured packet filters, and/or applicable PCC rules, as specified in 3GPP TS 29.212 [75] to be applied on the dedicated signalling bearer (e.g. PDP context). The packet filters shall filter up-link and down-link packets and only allow traffic to/from the signalling servers and to DNS and DHCP servers. The locally preconfigured packet filters shall be possible to pre-configure per APN.

It shall be possible to enable/disable the use of the Gx interface per APN. When Gx is enabled the GGSN/P-GW shall handle IP-CAN Bearer Establishment (e.g. Create PDP Context Requests) as specified in 3GPP TS 29.212 [75].

The GGSN/P-GW shall support Ipv4 and/or Ipv6 addresses and protocol for IMS signalling and IMS bearers.

The methods for an MS/UE to discover P-CSCF address(es) may vary depending on the access technology that the MS/UE is on. The details of the P-CSCF discovery mechanisms for various accesses are specified in 3GPP TS 23.228 [52] and 3GPP TS 24.229 [47]. For example, for an MS/UE accesing to IMS via GPRS in GERAN and UTRAN, the GGSN shall provide support for P-CSCF discovery in three different ways (see 3GPP TS 23.228 [52] and 3GPP TS 24.229 [47]):

- 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 DHCP servers i.e. the GGSN shall provide the functionality of a DHCP relay agent
- If the MS/UE has a P-CSCF FQDN locally configured and request the DNS IP address(es) from the GGSN (via PCO or DHCP procedures), the GGSN shall be able to provide DNS IP address(es) to the MS/UE.

Similarly, the PGW shall have similar functional support depending on the P-CSCF discovery methods supported by the UE on the access technology. For example, for a UE in 3GPP access network (i.e. GERAN, UTRAN, EUTRAN), the P-GW shall support same functions as the GGSN that are specified above except that the P-GW does not act as a DHCP relay agent between the MS/UE and the external DHCP server. In other words, as specified in clause 13 of this document, the P-GW shall have DHCP server function towards the MS/UE while acting as a DHCP client towards external DHCP server, if the P-GW is configured to request DNS and/or P-CSCF IP addresses from external DHCP servers.

The GGSN/P-GW shall be able to deliver DNS and/or P-CSCF addresses to the MS/UE if requested by the MS/UE via PCO (see 3GPP TS 24.008 [54] and 3GPP TS 24.301 [84]) or via DHCP procedures using the relevant DHCP options for Ipv4/Ipv6 DNS and SIP servers (see RFC 2132 [85], RFC 3361 [86], RFC 3646 [87] and RFC 3319 [88]).

On APNs providing IMS services, the information advertised in Router Advertisements from GGSN/P-GW to MSs/UEs 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.

NOTE: The "O- flag" shall be set in Ipv6 Router Advertisement messages sent by the GGSN/P-GW for APNs used for IMS services. This will trigger a DHCP capable MS/UE to start a DHCPv6 session to retrieve server addresses and other configuration parameters. An MS/UE which doesn't support DHCP will simply ignore the "O-flag". An MS/UE, which doesn't support DHCP, shall request IMS specific configuration (e.g. P-CSCF address) via the other discovery methods supported in the MS/UE (i.e. via locally configured P-CSCF address/FQDN in the MS/UE or via PCO procedure, if applicable).

The GGSN/P-GW shall have configurable policy rules for controlling bearers (e.g. PDP contexts) used for signalling as specified in section 13a.2.2.2.

13a.2.2 IMS Specific Procedures in the GGSN/P-GW

13a.2.2.1 Request for Signalling Server Address

When an MS/UE indicates a request for a P-CSCF address in the PCO IE in a Create PDP Context Request message on GERAN/UTRAN or for E-UTRAN in initial access request (e.g. Attach Request, PDN Connectivity Request), the GGSN/P-GW shall respond with one or more P-CSCF server addresses if preconfigured for this APN. If the GGSN/P-GW has no P-CSCF address available, the GGSN/P-GW shall ignore the request. If the GGSN/P-GW provides more

than one P-CSCF Ipv4/Ipv6 address in the response, the GGSN/P-GW shall sort the addresses with the highest priority P-CSCF server first in the PCO IE. The GGSN/P-GW may use different prioritisations for different Mses/UEs, e.g. for load sharing between the P-CSCF servers.

The GGSN/P-GW may use a keep alive mechanism and/or other type based on local policy (e.g. statistical monitoring) to be able to detect a failure of P-CSCF address(es) preconfigured in the APN. The keep alive mechanism should make use of STUN or CRLF as specified for the UE in 3GPP TS 24.229 [47], clause K.2.1.5. As an alternative, ICMP echo request/response may be used. The GGSN/P-GW shall then provide only those P-CSCF address(es) that are available in a Create PDP Context Response/Create Bearer Response.

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/UE uses a dedicated PDP context/EPS bearer for IMS signalling, and irrespective of the Gx status for the APN.

13a.2.2.1a Failure of Signalling Server Address

If the GGSN/P-GW detects a failure:

- in P-CSCF address(es) being used by the MS/UEs, if received via Gx (as specified in 3GPP TS 23.380 [95], clause 5); or

- upon receiving a P-CSCF restoration indication from the MME/SGSN or the PCRF,

then the GGSN/P-GW shall act as specified in 3GPP TS 23.380 [95], clause 5.

13a.2.2.2 Establishment of a PDP Context/EPS Bearer for Signalling

The following applies for establishing a PDP context/EPS bearer for IMS signalling in the GGSN/P-GW as per 3GPP TS 23.228 [52]:

I. The GGSN/P-GW shall allow IMS signalling on a "general-purpose PDP context"/default EPS bearer, in which case the IMS signalling shall be provided like any other transparent services provided by the packet domain.

II. The GGSN/P-GW may (dependent on operator policy) also support PDP Contexts/EPS Bearers dedicated for IMS services. If the the bearer establishment selected for the APN is controlled by the MS/UE, the MS/UE may request a dedicated PDP context/EPS Bearer for IMS signalling (see 3GPP TS 24.229 [47]) by setting the IM CN Subsystem signalling flag in the PCO IE. Specifically, the GGSN/P-GW may receive the IM CN Subsystem signalling flag in the PCO IE in the PDP context activation or Secondary PDP context activation for GERAN and UTRAN 59orrecti; in the Attach, UE-requested PDN connectivity request or UE-requested bearer resource modification procedures for E-UTRAN access. If the bearer establishment selected for the APN is controlled by the network, depending on the operator policy, the GGSN or P-GW may also activate a PDP context or dedicated EPS bearer for IMS signalling via network-initiated Secondary PDP context activation or network-initiated Dedicated Bearer activation procedures, respectively. If dedicated PDP contexts/EPS Bearers for IMS signalling are not supported, the GGSN/P-GW will reset the signalling flag in the response to the MS/UE. For P-GW, if the APN offers non-IMS services, the default bearer shall not be allowed to be set up as a dedicated IM CN signalling bearer. If the PDP context/EPS bearer can be established as a dedicated bearer for IMS signalling, the GGSN/P-GW can provide a set of UL filters for the PDP context/EPS bearer used for IMS. The UL filters provide the MS/UE with the rules and restrictions applied by the GGSN/P-GW for the dedicated PDP context/EPS bearer for IMS signalling. The GGSN/P-GW can in addition provide the IMS signalling flag to explicitly indicate to the MS/UE the intention of using the PDP context/EPS bearer for IMS related signalling.

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].

- During the (default or dedicated) EPS bearer activation procedure, the P-GW may receive the request for appropriate QCI for IMS signalling traffic as specified in 3GPP TS 23.203 [90] in EPS bearer QoS IE that indicates the prioritised handling of the EPS bearer over the radio interface. The P-GW may either accept or reject the request based on the operator policy configured at the P-GW.

IM CN subsystem signalling flag and Signalling Indication or appropriate QCI for IMS signalling in the QoS IE may be used independently of each other. However, based on the operator policy, the network may honor the Signalling Indication or appropriate QCI for IMS signalling if the IM CN Subsystem signalling flag is present in PCO IE.

The operator may provide other properties to the PDP contexts/EPS bearers dedicated for IMS signalling, e.g. special charging. It is out of the current scope of this TS to further specify these properties.

For a PDP Context/EPS bearer marked as a dedicated for IMS signalling, the GGSN/P-GW shall apply the applicable PCC rules, as specified in 3GPP TS 29.212 [75], and/or locally preconfigured packet filters, which shall only allow packets to be sent to and from a set of signalling servers, such as P-CSCF(s), DHCP server(s) and DNS server(s). The TFT filters on the dedicated signalling bearer shall have a precedence value so that they precede any other TFT filters. This will secure the use of the correct PDP context/EPS bearer for the signalling traffic, and that only authorized traffic uses the signalling PDP context. The locally preconfigured packet filters shall be defined in the GGSN/P-GW by the operator.

13a.2.2.3 Creation of a PDP Context/EPS Bearer for IMS Media Flows

For PDP Contexts/EPS bearers 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/EPS bearers, see 3GPP TS 29.212 [75].

The creation of a PDP Context/EPS bearer to be used to carry media flows involves interaction between the MS/UE and the GGSN/P-GW and between the GGSN/P-GW and the PCRF. The interaction between the GGSN/P-GW and the PCRF, i.e. the Gx interface, is described in detail in 3GPP TS 29.212 [75]. The interaction between the MS/UE and GGSN/P-GW is described in 3GPP TS 29.213 [76].

If Gx is enabled for the APN, the GGSN/P-GW contacts the PCRF selected during the establishment of the APN.

13b Interworking with BM-SC in EPS

13b.1 General

MBMS GW is used for interworking with the BM-SC in EPS. One or more MBMS GWs may be used in a PLMN. The specific message, i.e. session start/session update/session stop, and specific parameters, e.g. TMGI, MBMS service area, list of MBMS control plane nodes, are handled.

MBMS GW provides the Sgi-mb (user plane) reference point and the SGmb (control plane) reference point for interworking with the BM-SC.

13b.2 BM-SC interworking model of MBMS GW

The control plane and user plane protocol stacks of the MBMS GW for interworking with BM-SC are illustrated in Figure 16j , Figure 16k and Figure 16l. The figures include the following protocols:

- The "Diameter" SGmb application, as specified in clause 20.
- The Control part of the Evolved GPRS Tunnelling Protocol for EPS, GTPv2-C, as specified in 3GPP TS 29.274 [81].
- The User Datagram Protocol,UDP, as specified in IETF RFC 768 [15].
- The Transmission Control Protocol, TCP, as specified in IETF RFC 793 [18]
- The Stream Control Transmission Protocol, SCTP, as specified in IETF RFC 4960 [109].
- The Packet Data Convergence Protocol, PDCP, as specified in 3GPP TS 25.323 [107].
- The MBMS synchronisation protocol, SYNC, as specified in 3GPP TS 25.446 [106].
- The Internet Protocol, IP.

- L1 and L2 transport protocols for IP (various options exist).

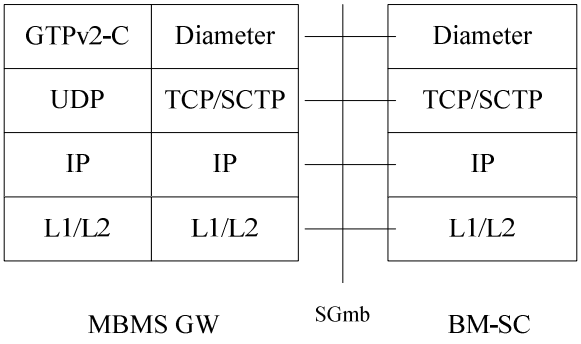


Figure 16j: The control plane protocol stacks of MBMS GW for interworking with BM-SC

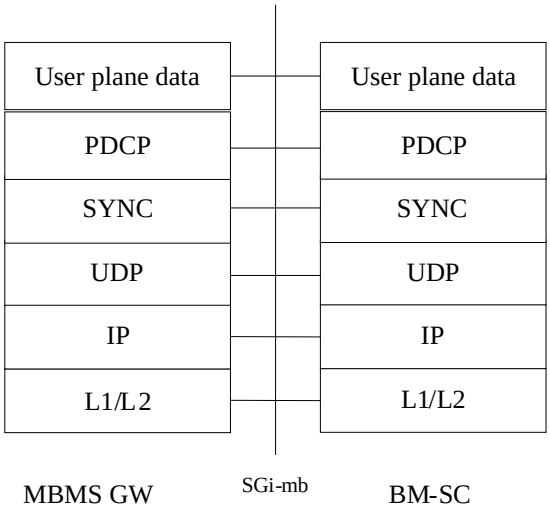


Figure 16k: The user plane protocol stacks of MBMS GW for interworking with BM-SC for multicast

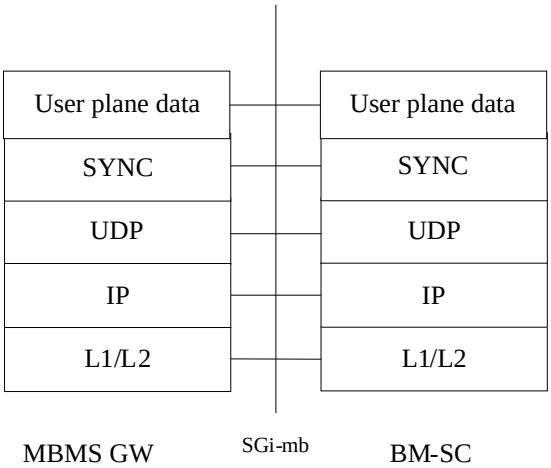


Figure 16l: The user plane protocol stacks of MBMS GW for interworking with BM-SC for broadcast

A BM-SC sends user plane data to an MBMS GW either by IP unicast (default), or by IP multicasting. Through the control plane communication a BM-SC provides an MBMS GW with necessary data, so that MBMS GW could forward the user plane data downlink either by multicast (default) or by unicast.

PDCP is not used when the MBMS service is broadcasted in the E-UTRAN, refer to 3GPP TS 36.331 [94].

13b.3 Forwarding of user plane packets at the MBMS GW

If user plane data are to be sent to the MBMS Gateway using IP unicast, the MBMS Gateway allocates an IP transport address and a separate UDP port for each MBMS bearer (i.e the service uniquely identified by its TMGI and Flow ID and provided by the EPS to deliver the same IP datagrams to multiple receivers in a designated location). The MBMS Gateway uses that destination unicast IP address and destination UDP port of user plane packets received over the SGi-mb interface to determine on which MBMS bearer to forward the received user plane packet.

If user plane data are to be sent to the MBMS Gateway using IP multicast encapsulation, the MBMS Gateway uses, the SGi-mb (transport) plane destination multicast address used and the SGi-mb (transport) plane source UDP port number provided by the BM-SC of user plane packets received over the SGi-mb interface to determine on which MBMS bearer to forward the received user plane packet.

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 both GPRS and EPS Packet Domain interworking is shown in figure 21.

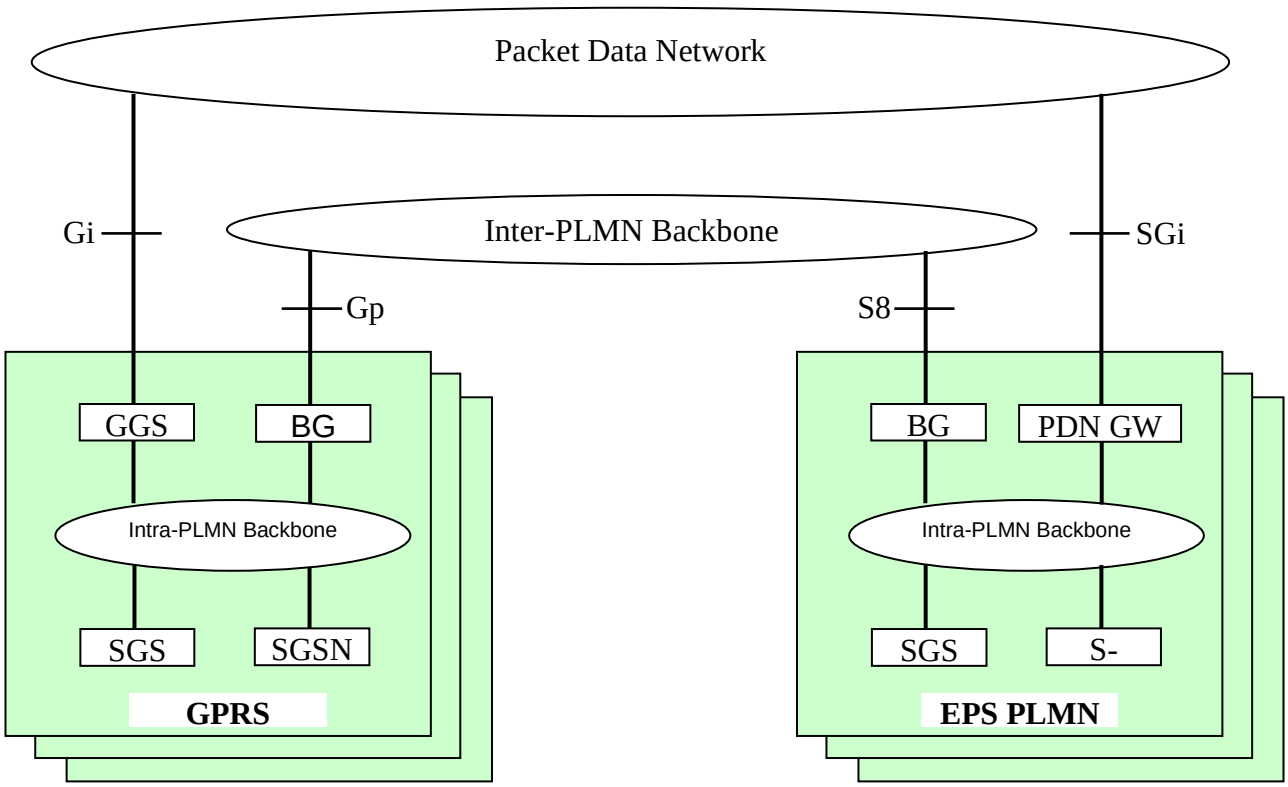


Figure 21: General interworking model for GPRS Packet Domains and EPS Packet Domains to support roaming subscribers.

NOTE: There may be multiple Packet Domains of the same type which interwork each other, such as the case of interwork between two GPRS Packet Domains.

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.

In the case of interworking between EPS Packet Domains, S8 reference point is the inter-PLMN interface, linking PDN GW of HPLMN and Serving GW of VPLMN. The procedure for setting the link is described in 3GPP TS 23.401 [77] and TS 23.402 [78].

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/Sgi 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 and Authorization

RADIUS Authentication and Authorization shall be used according to RFC 2865 [38], RFC 3162 [50] and RFC 4818 [97].

The RADIUS client function may reside in a GGSN/P-GW. When the GGSN receives a Create PDP Context request message or the P-GW receives an initial access request (e.g. Create Session Request) 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 Ipv4 address and/or Ipv6 prefix for the user when the GGSN or P-GW is interworking with the AAA server.

The information delivered during the RADIUS authentication can be used to automatically correlate the users identity (the MSISDN or IMSI) to the Ipv4 address and/or Ipv6 prefix, if applicable, assigned/confirmed by the GGSN/P-GW 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. The GGSN may also use the RADIUS re-authorization procedure for the purpose of Ipv4 address allocation to the MS for PDP type of Ipv4v6 after establishment of a PDN connection.

For EPS, RADIUS Authentication is applicable to the initial access request. When the P-GW receives an Access-Accept message from the authentication server it shall complete the initial access procedure. If Access-Reject or no response is received, the P-GW shall reject the initial access procedure with a suitable cause code. The P-GW may also use the RADIUS re-authorization procedure for the purpose of Ipv4 address allocation to the UE for PDN type of Ipv4v6 after establishment of a PDN connection. The use cases that may lead this procedure are:

- Deferred Ipv4 address allocation via DHCPv4 procedure after successful attach on 3GPP accesses.
- Deferred Ipv4 address allocation after successful attach in trusted non-3GPP IP access on S2a.
- Deferred Ipv4 home address allocation via DSMIPv6 Re-Registration procedure via S2c.

16.2 RADIUS Accounting

RADIUS Accounting shall be used according to RFC 2866 [39] , RFC 3162 [50] and RFC 4818 [97].

The RADIUS accounting client function may reside in a GGSN/P-GW. 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 Packet Domain network has authenticated the subscriber (i.e. SIM card and possibly other authentication methods).

The GGSN/P-GW may use the RADIUS Accounting-Request Start and Stop messages during IP-CAN bearer (e.g. primary and secondary PDP context, default and dedicated bearer) activations and deactivations procedures, respectively. For EPC based Packet domain, if the P-GW is not aware of the IP-CAN bearers, e.g. in case of PMIP-based S5/S8, the P-GW may use the RADIUS Accounting-Request Start and Stop messages per IP-CAN session as it would be one IP-CAN bearer.

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/P-GW information.

If the AAA server is used for Ipv4 address and/or Ipv6 prefix assignment, then, upon reception of a RADIUS Accounting-Request STOP message for all IP-CAN bearers associated to an IP-CAN session defined by APN and IMSI or MSISDN, the AAA server may make the associated Ipv4 address and/or Ipv6 prefix available for assignment.

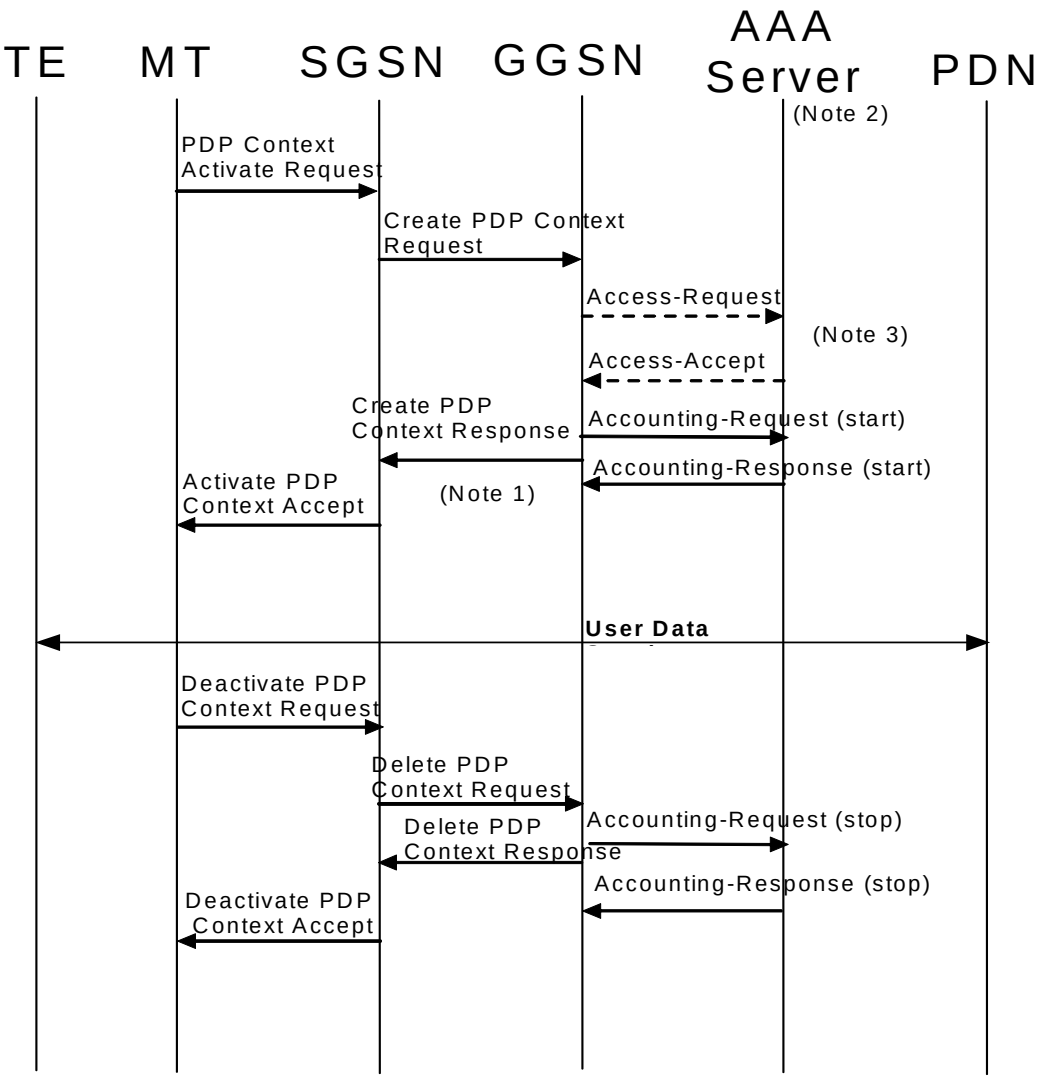
For PDN/PDP type Ipv4v6 and deferred Ipv4 address allocation, when the Ipv4 address is allocated or re-allocated, the accounting session that was established for the Ipv6 prefix allocation shall be used to inform the accounting server about the allocated Ipv4 address by sending RADIUS Accounting-Request Interim-Update with Framed-IP-Address attribute and its value field containing the allocated Ipv4 address. Similarly, the release of Ipv4 address shall be indicated to the accounting server by sending RADIUS Accounting-Request Interim-Update without the Framed-IP-Address attribute.

In order to avoid race conditions, the GGSN/P-GW shall include a 3GPP Vendor-Specific sub-attribute "Session Stop indicator" when it sends the Accounting-Request STOP for the last IP-CAN bearer of an IP-CAN session and the IP-CAN session is terminated (i.e. the Ipv4 address and/or Ipv6 prefix and any associated GTP tunnels or PMIP tunnel can be released). The AAA server shall not assume the IP-CAN session terminated until an Accounting-Request STOP with the Session Stop indicator is received.

16.3 Authentication and accounting message flows on Gi interface

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 IP address allocation via DHCPv4 after successful PDP context activation signalling.

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 Ipv4 address and/or Ipv6 prefix allocation the AAA server shall return the allocated Ipv4 address and/or Ipv6 prefix in the Access-Accept message.

When PDP type is Ipv4v6 and deferred Ipv4 addressing via Ipv4 address pool in the AAA server is used, the GGSN may intiate RADIUS re-authorization procedures after successful initial attach for the purpose of Ipv4 address allocation or to renew the lease for a previously allocated Ipv4 address. In this case, the GGSN shall set the Service-Type attribute to "Authorize Only" and the 3GPP-Allocate-IP-Type subattribute to the type of IP address to be allocated in the Access-Request message sent to the AAA server. See subclause 16.4.7.2 for the conditions to use 3GPP-Allocate-IP-Type sub-attribute in Access-Request messages. If the GGSN is using DHCPv4 signalling towards the MS and the RADIUS server includes the Session-Timeout attribute in the Access-Accept, the GGSN may use the Session-Timeout value as the DHCPv4 lease time. The GGSN shall not set the DHCPv4 lease time value higher than the Session-Timeout value. The GGSN may renew the DHCP lease to the MS without re-authorization towards the AAA server providing that the new lease expiry is no later than the Session-Timeout timer expiry. If the GGSN wishes to extend the lease time beyond the current Session-Timeout expiry, it shall initiate a new AAA re-authorization.

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 Ipv4 address and/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.

For PDP type Ipv4, at Ipv4 address allocation via DHCP4 signalling between the TE and the PDN, no Ipv4 address 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 Ipv4 address in a DHCPACK.

For PDP type Ipv4v6 and deferred Ipv4 addressing, when the Ipv4 address is allocated or re-allocated, the accounting session that was established for the Ipv6 prefix allocation shall be used to inform the accounting server about the allocated Ipv4 address by sending RADIUS Accounting-Request Interim-Update with the Framed-IP-Address attribute and its value field containing the allocated Ipv4 address.

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 Ipv4 address and/or Ipv6 prefix (if any) initially allocated to the subscriber, if there is no session for the subscriber.

For PDP type Ipv4v6 and deferred Ipv4 addressing, when the GGSN receives a message from the MS or the network indicating the release of the Ipv4 address (e.g. receiving DHCPRELEASE) or decides to release the Ipv4 address on its own (e.g. due to DHCP lease timer expiry or GGSN assigned Ipv4 address), the GGSN shall inform the accounting server about the deallocation of the Ipv4 address by sending RADIUS Accounting-Request Interim-Update without the Framed-IP-Address attribute.

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.

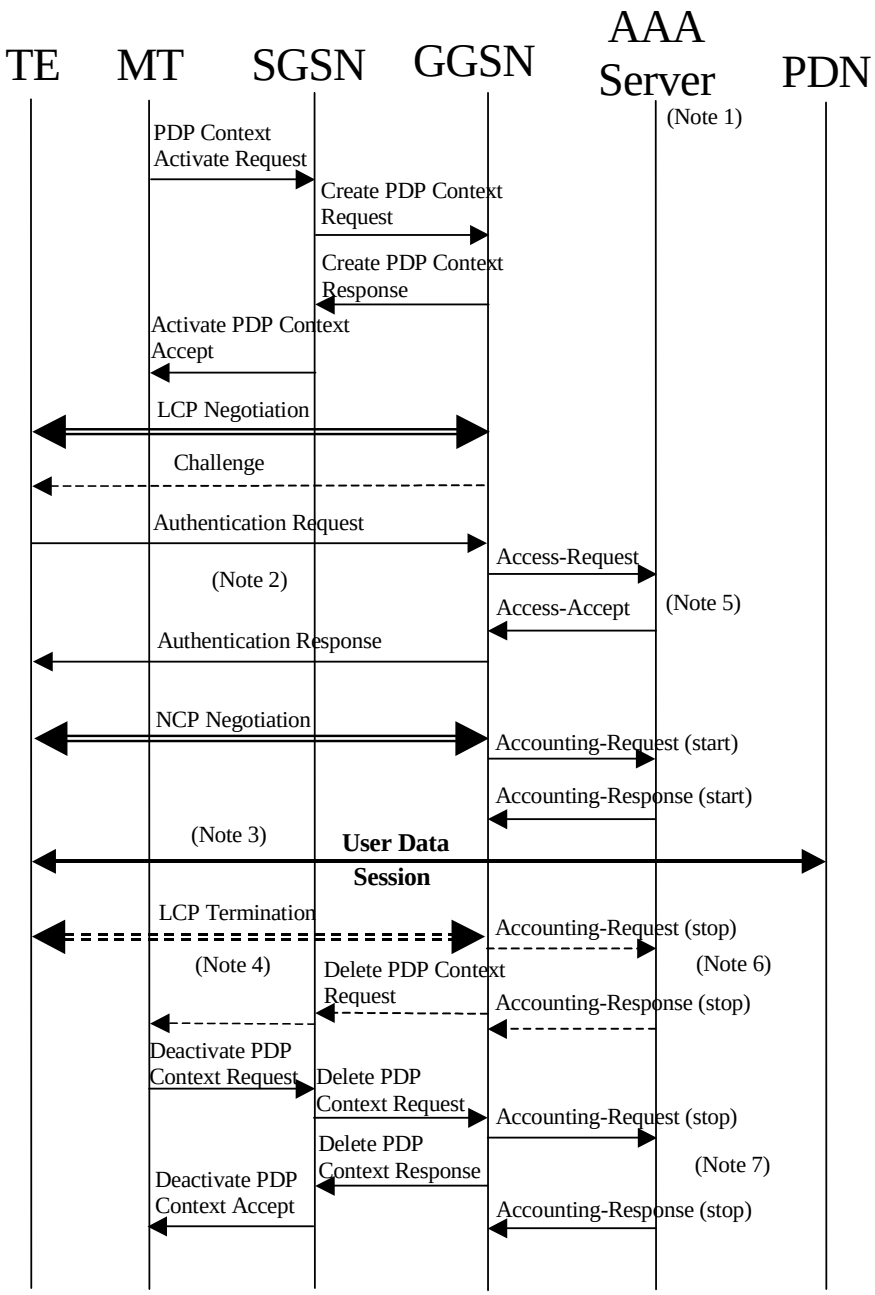
The GGSN may send an Accounting-Request ON message to the AAA server to indicate that a restart has occurred. The AAA server may then release the associated resources.

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.

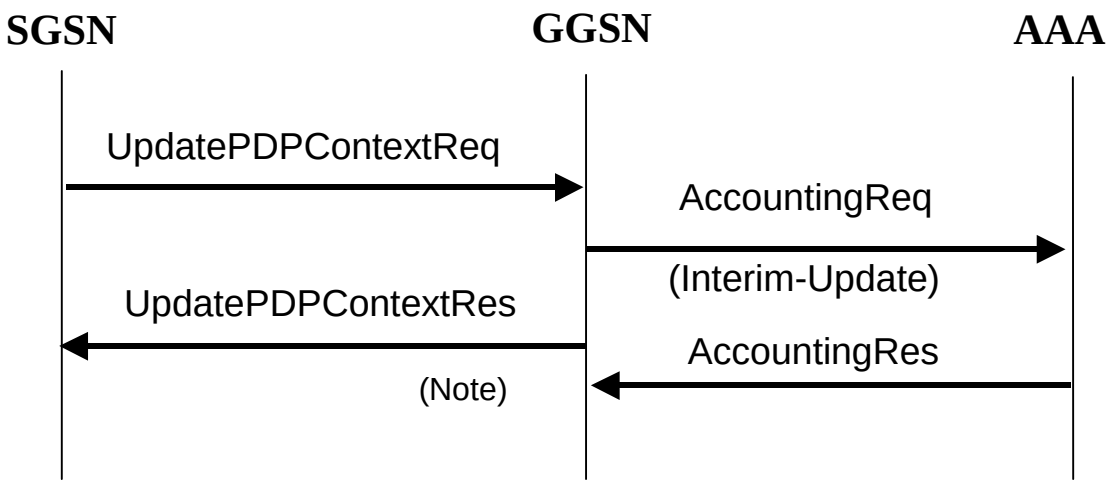
The GGSN may send an Accounting-Request ON message to the AAA server to indicate that a restart has occurred. The AAA server may then release the associated resources.

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). Interim updates are also used when the Ipv4 address is allocated/released/re-allocated for deferred Ipv4 addressing for the PDP type Ipv4v6. If the GGSN receives an UpdatePDPContextRequest from the SGSN that specifically indicates a direct tunnel establishment or a direct tunnel teardown (switching the user plane tunnel end back to the SGSN), and only the GTP user plane address and/or the GTP-U TEID have changed, then the GGSN should not send the Accounting Request Interim-Update to the AAA server. In such cases, 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.

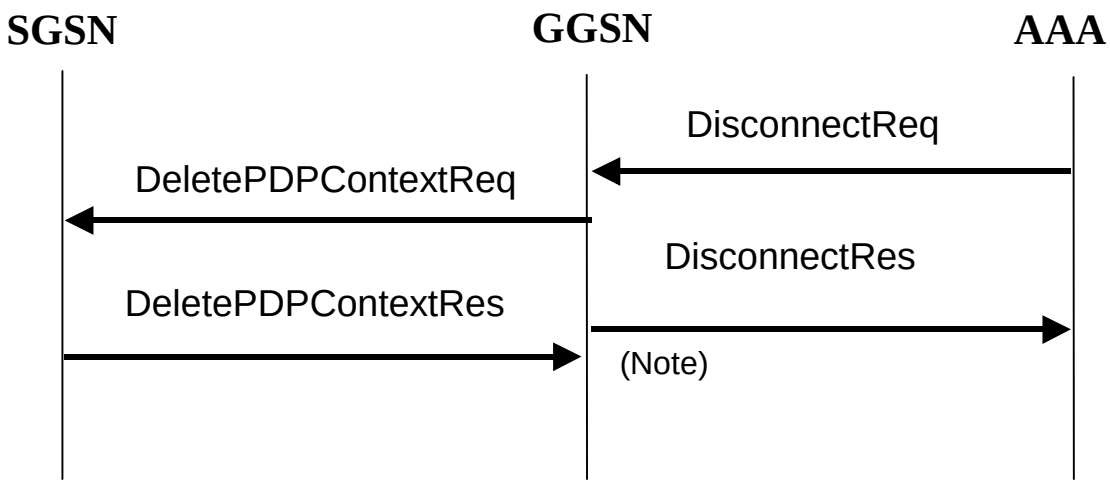
Figure 24: RADIUS for PDP context Update

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 belong to the same IP-CAN session are identified by the Acct-Session-Id. The Charging-Id contained in the Acct-Session-Id can be of any PDP context 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 IP-CAN 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

16.3a Authentication and accounting message flows on Sgi interface

16.3a.1 Authentication, Authorization and Accounting procedures

When a P-GW receives an initial access request (e.g. Create Session Request or Proxy Binding Update) message for a given APN, the P-GW 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 the RADIUS server is also responsible for Ipv4 address and/or Ipv6 prefix allocation, the AAA server shall return the allocated Ipv4 address and/or Ipv6 prefix in the Access-Accept message.

When PDN type is Ipv4v6 and deferred Ipv4 addressing via Ipv4 address pool in the AAA server is used, the P-GW may intiate RADIUS re-authorization procedures after successful initial attach for the purpose of Ipv4 address allocation or to renew the lease for a previously allocated Ipv4 address. In this case, the P-GW shall set the Service-Type attribute to "Authorize Only" and the 3GPP-Allocate-IP-Type subattribute to the type of IP address to be allocated in the Access-Request message sent to the AAA server. See subclause 16.4.7.2 for the conditions to use 3GPP-Allocate-IP-Type sub-attribute in Access-Request messages. If the P-GW is using DHCPv4 signalling towards the UE and the RADIUS server includes the Session-Timeout attribute in the Access-Accept, the P-GW may use the Session-Timeout value as the DHCPv4 lease time. The P-GW shall not set the DHCPv4 lease time value higher than the Session-Timeout value. The P-GW may renew the DHCP lease to the UE without re-authorization towards the AAA server providing that the new lease expiry is no later than the Session-Timeout timer expiry. If the P-GW wishes to extend the lease time beyond the current Session-Timeout expiry, it shall initiate a new AAA re-authorization.

Even if the P-GW was not involved in user authentication, it may send a RADIUS Accounting-Request (START) message to an AAA server. This message may contain parameters, e.g. the tuple which includes the user-id and Ipv4 address and/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 PGW-Address.

If some external applications require RADIUS Accounting-Request (START) information before they can process user packets, then the selected APN (P-GW) may be configured in such a way that the P-GW drops user data until the Accounting-Response (START) is received from the AAA server. The P-GW may wait for the Accounting-Response (START) before sending the initial access response (e.g. Create Session Response or Proxy Binding Acknowledgement). The P-GW may reject the initial access request if the Accounting-Response (START) is not received. The authentication and accounting servers may be separately configured for each APN.

For PDN type Ipv4, at Ipv4 address allocation via DHCPv4 signalling between the UE and the PDN, no Ipv4 address is available at initial access. In that case the P-GW may wait to send the Accounting-Request (START) message until the UE receives its Ipv4 address in a DHCPACK.

For PDN type Ipv4v6 and deferred Ipv4 addressing, when the Ipv4 address is allocated or re-allocated, the accounting session that was established for the Ipv6 prefix allocation shall be used to inform the accounting server about the allocated Ipv4 address by sending RADIUS Accounting-Request Interim-Update with the Framed-IP-Address attribute and its value field containing the allocated Ipv4 address.

When the P-GW receives a message indicating a bearer deactivation request or PDN disconnection request or detach request (e.g. Delete Bearer Command or Proxy Binding Update with lifetime equal 0) and providing a RADIUS Accounting-Request (START) message was sent previously, the P-GW shall send a RADIUS Accounting-Request (STOP) message to the AAA server, which indicates the termination of this particular bearer or user session. The P-GW shall immediately send the corresponding response (e.g. Delete Bearer Request or Proxy Binding Ack with lifetime equal 0) to the peer node (e.g. S-GW) in the Packet Domain, without waiting for an Accounting-Response (STOP) message from the AAA server.

The AAA server shall deallocate the Ipv4 address and/or Ipv6 prefix initially allocated to the subscriber, if there is no session for the subscriber.

For PDN type Ipv4v6 and deferred Ipv4 addressing, when the P-GW receives a message from the UE or the network indicating the release of the Ipv4 address (e.g. receiving DHCPRELEASE) or decides to release the Ipv4 address on its own (e.g. due to DHCP lease timer expiry or P-GW assigned Ipv4 address), the P-GW shall inform the accounting server about the deallocation of the Ipv4 address by sending RADIUS Accounting-Request Interim-Update without the Framed-IP-Address attribute.

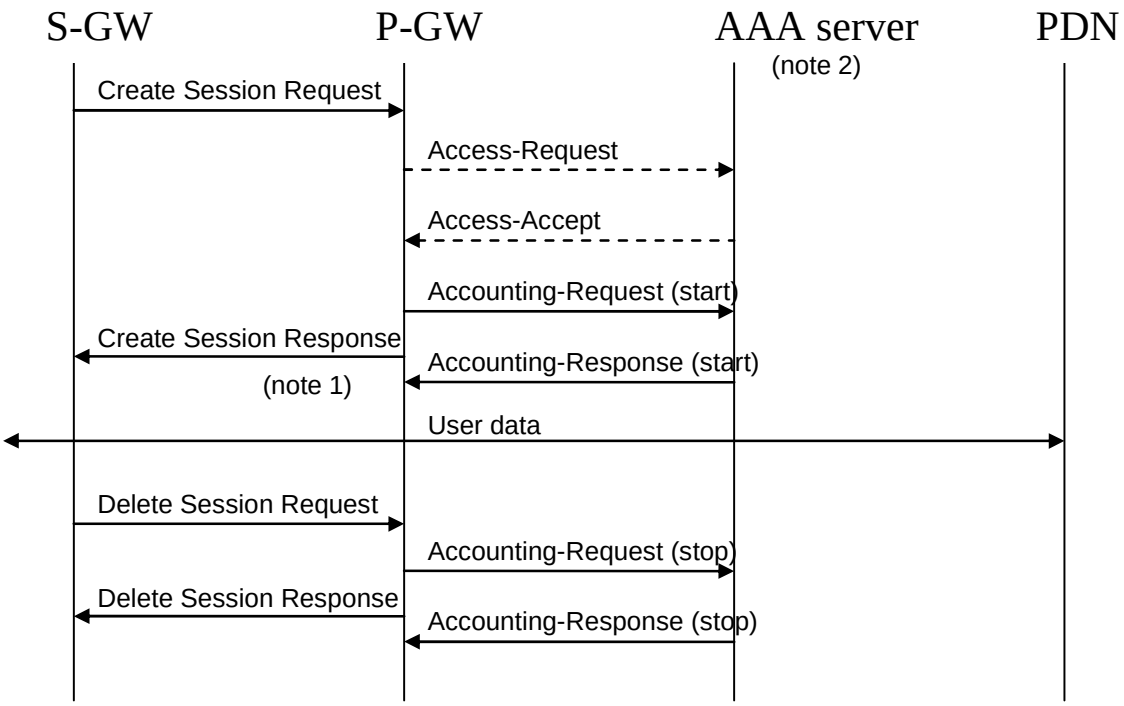
Accounting-Request (ON) and Accounting-Request (OFF) messages may be sent from the P-GW to the AAA server to ensure the correct synchronization of the session information in the P-GW and the AAA server.

The P-GW 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 P-GW 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 P-GW when an Access-Request message is pending, the P-GW 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].

For example, figure 25a.1 represents the RADIUS message flows between a P-GW and an Authentication, Authorization and Accounting (AAA) server, which is applicable for GTP based S5/S8:



NOTE 1: If some external applications require RADIUS Accounting request (Start) information before they can process user packets, then the selected APN (P-GW) may be configured in such a way that the P-GW drops user data until the Accounting Response (START) is received from the AAA server. The P-GW may wait for the Accounting Response (START) before sending the Create Session Response. The P-GW may reject the bearer if the Accounting Response (START) is not received.

NOTE 2: Separate accounting and authentication servers may be used.

Figure 25a.1: An example of RADIUS message flow on Sgi interface for GTP-based S5/S8 (successful user authentication case)

16.3a.2 Accounting Update

During the life of an IP-CAN bearer some information related to this bearer may change. Upon occurrence of the following events, the P-GW may send RADIUS Accounting Request Interim-Update to the AAA server: RAT change, S-GW address change and QoS change. Interim updates are also used when the Ipv4 address is allocated/released/re-allocated for deferred Ipv4 addressing for the PDN type Ipv4v6.

When the P-GW receives a signalling request (e.g. Modify Bearer Request in case of GTP-based S5/S8) that indicates the occurrence of one of these chargeable events, the P-GW may send an Accounting Request Interim-Update to the AAA server to update the necessary information related to this bearer. The P-GW need not wait for the RADIUS AccountingResponse message from the AAA server before sending the response for the triggering signalling message (e.g. Modify Bearer Response). The P-GW may delete the bearer if the AccountingResponse is not received from the AAA.

The P-GW may also send interim updates at the expiry of an operator configured time limit.

The following Figure 25a.2 is an example message flow to show the procedure of RADIUS accounting update, which applicable for GTP based S5/S8:

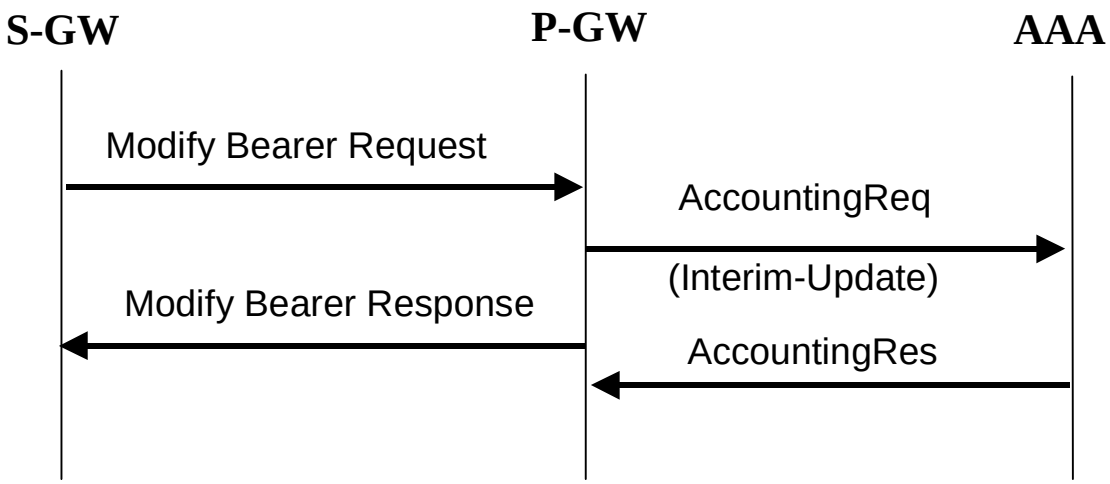


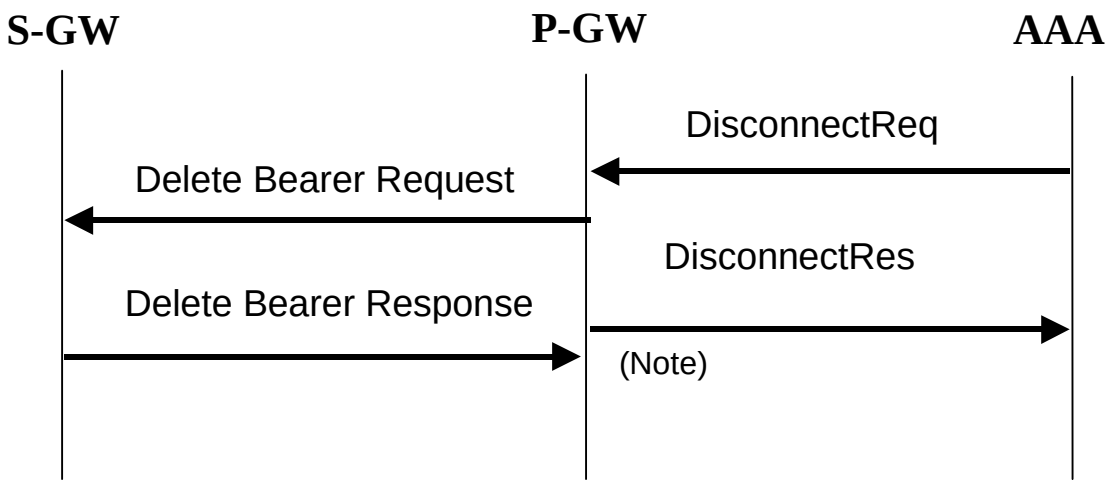
Figure 25a.2: RADIUS accounting update for Modify Bearer Request

16.3a.3 AAA-Initiated Bearer termination

RADIUS is used as the protocol between the P-GW and the AAA server or proxy for applications (e.g. MMS) to deliver information related to EPS user session. However some IP applications could need to interwork with the P-GW to release the corresponding resource (e.g. terminate a particular bearer or Resource Allocation Deactivation procedures as defined in TS 23.402 [78]). For this purpose, the AAA server or proxy may send a RADIUS Disconnect Request to the P-GW. On receipt of the Disconnect-Request from the AAA server, the P-GW shall release the corresponding resources and reply with a Disconnect-ACK. If the P-GW is unable to release the corresponding resources, it shall reply to the AAA server with a Disconnect-NAK. For more information on RADIUS Disconnect, see IETF RFC 3576 [41]. If the P-GW deletes the corresponding bearer, it need not wait for the response from the S-GW or non-3GPP IP access or ePDG before sending the RADIUS DisconnectResponse to the AAA server.

The Teardown-Indicator in the RADIUS Disconnect Request message indicates to the P-GW that all IP-CAN bearers for this particular user and sharing the same user session shall be deleted. The IP-CAN bearers that belong to the same IP-CAN session are identified by the Acct-Session-Id. The Charging-Id contained in the Acct-Session-Id can be of any IP-CAN bearer of the user. The P-GW is able to find out all the related IP-CAN bearers sharing the same user session once it has found the exact IP-CAN bearer from the Acct-Session-Id. If a user has the same user IP address for different sets of IP-CAN bearers towards different networks, only the IP-CAN bearers linked to the one identified by the Acct-Session-Id shall be deleted. If the value of Teardown-Indicator is set to "0" or if TI is missing, and if the Acct-Session-Id identifies the default bearer, the P-GW shall tear-down all the IP-CAN bearers that share the same user session identified by the Acct-Session-Id.

The following Figure 25a.3 is an example message flow to show the procedure of RADIUS AAA-Initiated Bearer termination, which applicable for GTP based S5/S8:



NOTE: As shown on figure 25a.3, the P-GW need not wait for the Delete Bearer Response from the S-GW to send the RADIUS DisconnectResponse to the AAA server.

Figure 25a.3: AAA-initiated bearer termination with RADIUS

16.4 List of RADIUS attributes

The following tables describe the actual content of the RADIUS messages exchanged between the GGSN/P-GW 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.

NOTE: Any digit is converted into UTF-8 character. For example, digit 5 is converted to UTF-8 character '5', which in hexadecimal representation has a value 0x35. Similarly, a hexadecimal digit F is converted to either UTF-8 character 'F', which in hexadecimal representation has a value 0x46, or to UTF-8 character 'f', which in hexadecimal representation has a value 0x66.

16.4.1 Access-Request message (sent from GGSN/P-GW 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 to the GGSN/P-GW by the user in Protocol Configuration Options (PCO) or for the case of the P-GW when multiple authentications are supported in the Additional Protocol Configuration Options (APCO) received during IP-CAN session establishment procedure. If PPP PDP type is used, it is provided to the GGSN by the user during PPP authentication phase. If no username is available, a generic username, configurable on a per APN basis, shall be present.	String	Mandatory
2	User-Password	User password is provided to the GGSN/P-GW by the user in the PCO or for the case of the P-GW when multiple authentications are supported in the APCO received during IP-CAN session establishment procedure if PAP is used, If PPP PDP type is used, it is provided to the GGSN by the user during PPP authentication phase. If no password is available a generic password, configurable on a per APN basis, shall be present.	String	Conditional Note 1

Attr #	Attribute Name	Description	Content	Presence Requirement
3	CHAP-Password	CHAP password is provided to the GGSN/P-GW by the user in the PCO or for the case of the P-GW when multiple authentications are supported in the APCO received during IP-CAN session establishment procedure, If PPP PDP type is used, it is provided to the GGSN by the user during PPP authentication phase.	String	Conditional Note 2
4	NAS-IP-Address	Ipv4 address of the GGSN/P-GW for communication with the AAA server.	Ipv4	Conditional Note 3 and 7
95	NAS-Ipv6-Address	Ipv6 address of the GGSN/P-GW for communication with the AAA server.	Ipv6	Conditional Note 3 and 7
32	NAS-Identifier	Hostname of the GGSN/P-GW for communication with the AAA server.	String	Conditional Note 3
6	Service-Type	Indicates the type of service for this user	2 (Framed) or 17 (Authorize Only) Note 9	Optional
7	Framed-Protocol	Indicates the type of protocol for this user	7 (GPRS PDP Context)	Optional Note 8
8	Framed-IP-Address	Ipv4 address allocated for this user	Ipv4	Conditional Note 4
9	Framed-IP-Netmask	Netmask for the user Ipv4 address	Ipv4	Conditional Note 4
97	Framed-Ipv6-Prefix	Ipv6 prefix allocated for this user	Ipv6	Conditional Note 4
123	Delegated-Ipv6-Prefix	Ipv6 prefix delegated to the user.	Ipv6	Conditional Note 10
96	Framed-Interface-Id	Ipv6 Interface Identifier provided by the GGSN/P-GW to the UE at Initial Attach.	64 bits as per IETF RFC 3162 [50]	Optional Note 5
30	Called-Station-Id	Identifier for the target network	APN (UTF-8 encoded characters)	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 character. (Note 6)	Optional
60	CHAP-Challenge	CHAP Challenge is provided to the GGSN/P-GW by the user in the PCO or for the case of the P-GW when multiple authentications are supported in the APCO received during the IP-CAN session establishment procedure. If PPP PDP type is used, it is provided to the GGSN by the user durng PPP authentication phase.	String	Conditional Note 2
61	NAS-Port-Type	Port type for the GGSN/P-GW	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 and 27 which are conditional

Attr #	Attribute Name	Description	Content	Presence Requirement
NOTE 1: Shall be present if PAP is used. NOTE 2: Shall be present if CHAP is used. NOTE 3: Either NAS-IP-Address or NAS-Identifier shall be present. NOTE 4: Ipv4 address and/or Ipv6 prefix attributes shall be present. The IP protocol version for end-user and network may be different. NOTE 5: As per subclause 9.2.1.1 of 3GPP TS 23.060 [3] and subclause 5.3.1.2.2 of 3GPP TS 23.401 [77] the UE shall use this interface identifier to configure its link-local address, however the UE can choose any interface identifier to generate its Ipv6 address(es) other than link-local without involving the network . NOTE 6: There are no leading characters in front of the country code. NOTE 7: Either Ipv4 or Ipv6 address attribute shall be present. NOTE 8: Framed-Protocol value of 7 is used by both GGSN and P-GW when interworking with RADIUS AAA servers. When used for P-GW, it represents the IP-CAN bearer. NOTE 9: Service-Type attribute value of "Authorize Only" (RFC 5176 [93]) is only applicable for P-GW/GGSN when deferred Ipv4 addressing for a UE needs to be performed for PDN/PDP type Ipv4v6. In this use case, the Access Request at UE's initial access shall have Service-Type value "Framed", but the subsequent Access Request shall have Service-Type value of "Authorize Only". In both Access-Request messages, the 3GPP-Allocate-IP-Type sub-attribute shall be present. See subclause 16.4.7.2 for the typical uses cases how 3GPP-Allocate-IP-Type subattribute is utilised in Access-Request messages. NOTE 10: Delegated Ipv6 prefix shall be present if the user was delegated an Ipv6 prefix from a local pool.				

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

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 Note 4
8	Framed-IP-Address	Ipv4 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 Ipv4 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 Ipv6 address prefixes.	Ipv6	Conditional Note 2
123	Delegated-Ipv6-Prefix	Ipv6 prefix delegated to the user.	Ipv6	Conditional Note 6
96	Framed-Interface-Id	Ipv6 Interface Identifier provided by the GGSN/P-GW to the UE at Initial Attach.	64 bits as per IETF RFC 3162 [50]	Optional Note 7
100	Framed-Ipv6-Pool	Name of the Ipv6 prefix pool for the specific APN	String	Optional Note 2
12	Framed-MTU	Maximum Transmission Unit of the PDP PDUs, between the MS and GGSN/P-GWs (Note 5)	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

Attr #	Attribute Name	Description	Content	Presence Requirement
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: Ipv4 address and/or Ipv6 prefix attributes shall be present.The IP protocol version for end-user and network may be different.
NOTE 3: Depending on IP address(es) allocated to the user, either or both Ipv4 and Ipv6 address attributes shall be present.
NOTE 4: Framed-Protocol value of 7 is used by both GGSN and P-GW when interworking with RADIUS AAA servers. When used for P-GW, it represents the IP-CAN bearer.
NOTE 5: In network deployments that have MTU size of 1500 octets in the transport network, providing a link MTU value of 1358 octets to the MS as part of the IP configuration information from the network will prevent the IP layer fragmentation within the transport network between the MS and the GGSN/P-GW. Link MTU considerations are discussed further in Annex C of 3GPP TS 23.060 [3].
NOTE 6: Delegated Ipv6 prefix shall be present if the user was delegated an Ipv6 prefix.
NOTE 7: As per subclause 9.2.1.1 of 3GPP TS 23.060 [3] and subclause 5.3.1.2.2 of3GPP TS 23.401 [77] the UE shall use this interface identifier to configure its link-local address, however the UE can choose any interface identifier to generate its Ipv6 address(es) other than link-local without involving the network.

16.4.3 Accounting-Request START (sent from GGSN/P-GW 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 is provided to the GGSN/P-GW by the user in received during IP-CAN session establishment procedure. If PPP PDP type is used, it is provided to the GGSN by the user during PPP authentication phase. 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/P-GW Ipv4 address for communication with the AAA server.	Ipv4	Conditional Notes 1 and 7
95	NAS-Ipv6-Address	GGSN/P-GW Ipv6 address for communication with the AAA server.	Ipv6	Conditional Notes 1 and 7
32	NAS-Identifier	Hostname of the GGSN/P-GW 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 Note 8
8	Framed-IP-Address	User Ipv4 address	Ipv4	Conditional Note 3

Attr #	Attribute Name	Description	Content	Presence Requirement
97	Framed-Ipv6-Prefix	User Ipv6 Prefix	Ipv6	Conditional Note 3
123	Delegated-Ipv6-Prefix	Delegates Ipv6 Prefix to the user	Ipv6	Conditional Note 9
96	Framed-Interface-Id	Ipv6 Interface Identifier provided by the GGSN/P-GW to the UE at Initial Attach.	64 bits as per IETF RFC 3162 [50]	Optional Note 4
25	Class	Received in the Access-Accept	String	Conditional (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 decimal character. (Note 6)	Optional
40	Acct-Status-Type	Type of accounting message	START	Mandatory
41	Acct-Delay-Time	Indicates how many seconds the GGSN/P-GW 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/P-GW IP address (Ipv4 or Ipv6) and Charging-ID concatenated in a UTF-8 encoded hexadecimal character. (Note 5)	Mandatory
45	Acct-Authentic	Authentication method	RADIUS or LOCAL	Optional
61	NAS-Port-Type	Port type for the GGSN/P-GW	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: Ipv4 address and/or Ipv6 prefix attributes shall be present.The IP protocol version for end-user and network may be different.
NOTE 4: As per subclause 9.2.1.1 of 3GPP TS 23.060 [3] and subclause 5.3.1.2.2 of 3GPP TS 23.401 [77] the UE shall use this interface identifier to configure its link-local address, however the UE can choose any interface identifier to generate its Ipv6 address(es) other than link-local without involving the network .
NOTE 5: The GGSN/P-GW IP address is the same one that is used in the CDRs generated by the GGSN/P-GW.
NOTE 6: There are no leading characters in front of the country code.
NOTE 7: Either Ipv4 or Ipv6 address attribute shall be present.
NOTE 8: Framed-Protocol value of 7 is used by both GGSN and P-GW when interworking with RADIUS AAA servers. When used for P-GW, it represents the IP-CAN bearer.
NOTE 9: Delegated Ipv6 prefix shall be present if the user was delegated an Ipv6 prefix from a local pool.

16.4.4 Accounting Request STOP (sent from GGSN/P-GW 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 is provided to the GGSN/P-GW by the user in the PCO or for the case of the P-GW when multiple authentications are supported in the APCO received during IP-CAN session establishment procedure. If PPP PDP type is used, it is provided to the GGSN by the user during PPP authentication phase. 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 username shall be used in preference to the above.	String	Optional
4	NAS-IP-Address	Ipv4 address of the GGSN/P-GW for communication with the AAA server.	Ipv4	Conditional Notes 1 and 7
95	NAS-Ipv6-Address	Ipv6 address of the GGSN/P-GW for communication with the AAA server.	Ipv6	Conditional Notes 1 and 7
32	NAS-Identifier	Hostname of the GGSN/P-GW 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 Note 8
8	Framed-IP-Address	User Ipv4 address	Ipv4	Conditional Note 3
97	Framed-Ipv6-Prefix	User Ipv6 Prefix	Ipv6	Conditional Note 3
123	Delegated-Ipv6-Prefix	Delegated Ipv6 Prefix to the user	Ipv6	Conditional Note 9
96	Framed-Interface-Id	Ipv6 Interface Identifier provided by the GGSN/P-GW to the UE at Initial Attach	64 bits as per IETF RFC 3162 [50]	Optional Note 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 characters)	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 characters. (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/P-GW 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/P-GW counted number of octets sent by the user for the IP-CAN bearer	32 bit unsigned integer	Optional
43	Acct-Output-Octets	GGSN/P-GW counted number of octets received by the user for the IP-CAN bearer	32 bit unsigned integer	Optional
44	Acct-Session-Id	User session identifier.	GGSN/P-GW IP address (Ipv4 or Ipv6) and Charging-ID concatenated in a UTF-8 encoded hexadecimal character.	Mandatory

Attr #	Attribute Name	Description	Content	Presence Requirement
			(Note 5)	
45	Acct-Authentic	Authentication method	RADIUS or LOCAL	Optional
46	Acct-Session-Time	Duration of the session	Second	Optional
47	Acct-Input-Packets	GGSN/P-GW counted number of packets sent by the user	Packet	Optional
48	Acct-Output-Packets	GGSN/P-GW 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/P-GW	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: Ipv4 address and/or Ipv6 prefix attributes shall be present. The IP protocol version for end-user and network may be different.
NOTE 4: As per subclause 9.2.1.1 of 3GPP TS 23.060 [3] and subclause 5.3.1.2.2 of 3GPP TS 23.401 [77] the UE shall use this interface identifier to configure its link-local address, however the UE can choose any interface identifier to generate its Ipv6 address(es) other than link-local without involving the network .
NOTE 5: The GGSN/P-GW IP address is the same one that is used in the CDRs generated by the GGSN/P-GW.
NOTE 6: There are no leading characters in front of the country code.
NOTE 7: Either Ipv4 or Ipv6 address attribute shall be present.
NOTE 8: Framed-Protocol value of 7 is used by both GGSN and P-GW when interworking with RADIUS AAA servers. When used for P-GW, it represents the IP-CAN bearer.
NOTE 9: Delegated Ipv6 prefix shall be present if the user was delegated an Ipv6 prefix from a local pool.

16.4.5 Accounting Request ON (optionally sent from GGSN/P-GW 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	Ipv4 address of the GGSN/P-GW for communication with the AAA server.	Ipv4	Conditional Notes 1 and 2
95	NAS-Ipv6-Address	Ipv6 address of the GGSN/P-GW 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 characters)	Optional
32	NAS-Identifier	Hostname of the GGSN/P-GW for communication with the AAA server.	String	Conditional Note 1
40	Acct-Status-Type	Type of accounting message	Accounting-On	Mandatory

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/P-GW 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/P-GW for communication with the AAA server.	Ipv4	Conditional Notes 1 and 2
95	NAS-Ipv6-Address	IP address of the GGSN/P-GW 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 characters)	Optional
32	NAS-Identifier	Hostname of the GGSN/P-GW for communication with the AAA server.	String	Conditional Note 1
40	Acct-Status-Type	Type of accounting message	Accounting-Off	Mandatory
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. The applicability of each sub-attribute to Gi and Sgi reference points is also indicated in Table 7.

16.4.7.1 Presence of the 3GPP Vendor-Specific attribute in RADIUS 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)	Applicable Reference Points
1	3GPP-IMSI	IMSI for this user	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update	Gi, Sgi
2	3GPP-Charging-Id	For GGSN, Charging ID for this PDP Context (this together with the GGSN IP Address constitutes a unique identifier for the PDP context). For P-GW, Charging ID for this IP-CAN bearer (this together with the P-GW IP address constitutes a unique identifier for the IP-CAN bearer).	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update	Gi, Sgi
3	3GPP-PDP-Type	For GGSN, it indicates the type of PDP context, e.g. IP or PPP. For P-GW, it indicates the PDN Type, i.e. Ipv4, Ipv6, Ipv4v6.	Conditional (mandatory if attribute 7 is present)	Access-Request Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update	Gi Sgi
4	3GPP-CG-Address	Charging Gateway IP address	Optional	Access-Request, Accounting-Request START, Accounting-	Gi, Sgi

Sub-attr #	Sub-attribute Name	Description	Presence Requirement	Associated attribute (Location of Sub-attr)	Applicable Reference Points
				Request STOP, Accounting-Request Interim-Update	
5	3GPP-GPRS-Negotiated-QoS-Profile	For GGSN, it represents the QoS profile for the PDP context. For P-GW, it represents the QoS profile for the EPS bearer and the authorized APN-AMBR.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update	Gi Sgi
6	3GPP-SGSN-Address	For GGSN, it represents the SGSN Ipv4 address that is used by the GTP control plane for the handling of control messages. For P-GW, it represents the Ipv4 address of the S-GW, trusted non-3GPP IP access or ePDG that is used on S5/S8, S2a or S2b, or the SGSN Ipv4 address for GnGp SGSN accesses to the PGW for the handling of control messages. The address 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	Gi, Sgi
7	3GPP-GGSN-Address	For GGSN, it represents the GGSN Ipv4 address that is used by the GTP control plane for the context establishment. For P-GW, it representsthe P-GW Ipv4 address that is used on S5/S8, S2a, S2b or S2c control plane for the IP-CAN session establishment. The address is the same as the GGSN/P-GW Ipv4 address used in the CDRs generated by the GGSN/P-GW.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update	Gi, Sgi
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	Gi, Sgi
9	3GPP-GGSN- MCC-MNC	MCC-MNC of the network the GGSN or the P-GW belongs to.	Optional	Access-Request, Accounting-Request START,	Gi, Sgi

Sub-attr #	Sub-attribute Name	Description	Presence Requirement	Associated attribute (Location of Sub-attr)	Applicable Reference Points
				Accounting-Request STOP, Accounting-Request Interim-Update	
10	3GPP-NSAPI	For GGSN, it identifies a particular PDP context for the associated PDN and MSISDN/IMSI from creation to deletion. For P-GW, it identifies the EPS Bearer ID if it is known to the P-GW (i.e. GTP-based S5/S8 is in use).	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP Accounting-Request Interim-Update	Gi, Sgi
11	3GPP-Session-Stop-Indicator	Indicates to the AAA server that the last PDP context or EPS Bearer of a session is released and that the IP-CAN session has been terminated.	Optional	Accounting Request STOP	Gi, Sgi
12	3GPP-Selection-Mode	For GGSN it contains the Selection mode for this PDP Context received in the Create PDP Context Request message For P-GW it contains the Selection mode for this EPS Bearer received in the Create Session Request message.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update	Gi, Sgi
13	3GPP-Charging-Characteristics	For GGSN, it contains the charging characteristics for this PDP Context received in the Create PDP Context Request Message (only available in R99 and later releases). For P-GW, it contains the charging characteristics for the IP-CAN bearer.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update	Gi, Sgi
14	3GPP-CG-Ipv6-Address	Charging Gateway Ipv6 address	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update	Gi, Sgi
15	3GPP-SGSN-Ipv6-Address	For GGSN, it represents the SGSN Ipv6 address that is used by the GTP control plane for the handling of control messages.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update	Gi, Sgi

Sub-attr #	Sub-attribute Name	Description	Presence Requirement	Associated attribute (Location of Sub-attr)	Applicable Reference Points
		For P-GW, it represents the Ipv6 address of the S-GW, trusted non-3GPP IP access or ePDG that is used on S5/S8, S2a or S2b, or the SGSN Ipv6 address for GnGp SGSN accesses to the PGW for the handling of control messages. The address may be used to identify the PLMN to which the user is attached.			
16	3GPP-GGSN-Ipv6-Address	For GGSN, it represents the GGSN Ipv6 address that is used by the GTP control plane for the context establishment. For P-GW, it represents the P-GW Ipv6 address that is used on S5/S8, S2a, S2b or S2c control plane for the IP-CAN session establishment.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update	Gi, Sgi
17	3GPP-Ipv6-DNS-Servers	List of Ipv6 addresses of DNS servers for an APN	Optional	Access-Accept	Gi, Sgi
18	3GPP-SGSN-MCC-MNC	For GGSN and PGW connected to a Gn/Gp SGSN, it represents the MCC and MNC extracted from the RAI within the Create PDP Context Request or Update PDP Context Request message. For P-GW in GTP/PMIP S5/S8 it represents the MCC and MNC extracted from the Serving Network. For PGW connected to S2a, it represents the MCC and MNC extracted from the Serving Network. For PGW connected to S2b, it represents the MCC and MNC extracted from the Serving Network.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update	Gi, Sgi

Sub-attr #	Sub-attribute Name	Description	Presence Requirement	Associated attribute (Location of Sub-attr)	Applicable Reference Points
19	3GPP-Teardown-Indicator	Indicate to the GGSN/P-GW that all IP-CAN bearers for this particular user and sharing the same user session need to be deleted.	Optional	Disconnect Request	Gi Sgi
20	3GPP-IMEISV	International Mobile Equipment Id and its Software Version	Optional	Accounting-Request START, Accounting-Request STOP, Access-Request	Gi, Sgi
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	Gi, Sgi
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	Gi, Sgi
23	3GPP-MS-TimeZone	Indicate the offset between universal time and local time in steps of 15 minutes of where the MS/UE currently resides.	Optional	Accounting-Request START, Access-Request, Accounting-Request STOP, Accounting-Request Interim-Update	Gi, Sgi
24	3GPP-CAMEL-Charging-Info	Used to copy any CAMEL Information present in S-CDR(s).	Optional	Accounting-Request START, Access-Request	Gi
25	3GPP-Packet-Filter	Packet Filter used for this PDP context or EPS bearer.	Optional	Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update	Gi, Sgi
26	3GPP-Negotiated-DSCP	DSCP used to mark the IP packets of this PDP context on the Gi interface or EPS Bearer context on the Sgi interface	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update	Gi, Sgi
27	3GPP-Allocate-IP-Type	Indicates whether the Access-Request is sent for user authentication only and/or for allocation of an Ipv4	Conditional (see subclause 16.4.7.2 for conditions)	Access-Request	Gi, Sgi

Sub-attr #	Sub-attribute Name	Description	Presence Requirement	Associated attribute (Location of Sub-attr)	Applicable Reference Points
		address and/or of an Ipv6 prefix			
28	External-Identifier	A globally unique identifier of a UE used towards external servers instead of IMSI and MSISDN, refer to 3GPP TS 23.682 [100] and 3GPP TS 23.003 [40].	Optional	Access-Request, Access-Accept, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update	Gi, Sgi
29	TWAN-Identifier	Indicates the UE location in a Trusted WLAN Access Network.	Optional	Accounting-Request START, Access-Request, Accounting-Request STOP, Accounting-Request Interim-Update	Sgi
30	3GPP-User-Location-Info-Time	Indicate the time at which the UE was last known to be in the location which is reported during bearer deactivation or PDN disconnection procedure.	Optional	Accounting-Request STOP	Gi, Sgi

The information represented by some of the Sgi sub-attributes may not be available to the P-GW depending on the UE's radio access and the S5/S8 protocol type (GTP or PMIP). For example, the P-GW will be aware of the User Location Info (e.g. TAI) if the user is in LTE access and GTP based S5/S8 is used. However, such information is not passed to the P-GW when PMIP based S5/S8 is utilised. In such scenarios, if a sub-attribute is configured in the P-GW to be transferred to the RADIUS AAA server, but the information in the P-GW is not up to date or not available; the P-GW shall not send the corresponding sub-attribute, unless otherwise stated in the following subclause where the encoding of each sub-attribute is specified.

16.4.7.2 Coding 3GPP Vendor-Specific RADIUS attributes

In this subclause the provisions of IETF RFC 2865 [38] apply, which in particular specify the following:

- the Length field of an attribute is one octet, and it indicates the length of this Attribute including the Type, Length and Value fields.
- type String may be 1-253 octets long and it contains binary data (values 0 through 255 decimal, inclusive). Strings of length zero (0) shall not be sent, but the entire attribute shall be omitted. A NULL terminating character shall not be appended to an attribute of type String.
- type Text may be 1-253 octets long and it contains UTF-8 encoded characters. Text of length zero (0) shall not be sent, but the entire attribute shall be omitted. A NULL terminating character shall not be appended to an attribute of type Text.
- type Address is 32 bit value and most significant octet is the first one.
- type Integer is 32 bit unsigned value and most significant octet is the first one.

The RADIUS vendor Attribute is encoded as follows (as per IETF 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							

$n \geq 7$

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							

$m \geq 2$ and $m \leq 248$

The 3GPP specific attributes encoding is clarified below.

NOTE: Unless otherwise stated, the encoding of the value field of a 3GPP vendor-specific attribute is identical for Gi and Sgi.

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 characters)							

3GPP Type: 1

$n \leq 15$

Length: $m \leq 17$

IMSI value: Text type:

A GGSN (or a P-GW) receives IMSI that is encoded according to 3GPP TS 29.060 [24] (or 3GPP TS 29.274 [81]) and converts IMSI into the UTF-8 characters, which are encoded as defined in 3GPP TS 23.003 [40]. 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 (or the P-GW) 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 type

PDP type may have the following values:

0 = Ipv4

1 = PPP

2 = Ipv6

3 = Ipv4v6

4 = Non-IP

For P-GW, this sub-attribute represents PDN Type and therefore only the values "0", "2", "3" and "4" are applicable.

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 type.

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: For GGSN, L ≤ 37 (release 7 or higher) or L ≤ 33 (release 6 or release 5) or L ≤ 27 (release 4 or release 99) or L = 11 (release 98). For P-GW, the length varies depending on the value of QCI. See below for details.

QoS profile value: Text type

UTF-8 encoded QoS profile syntax:

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

<Release indicator> = UTF-8 encoded number (two characters) :

For GGSN:

"98" = Release 98

"99"= Release 99 or release 4

"05"= Release 5 or release 6

"07"= Release 7 or higher

For P-GW:

"08"= Release 8 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 characters, defining its hexadecimal representation.

For GGSN:

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 release 6 QoS profile data is 14 octets long, which results in a 28 octets UTF-8 encoded string.

The release 7 (and higher) QoS profile data is 16 octets long, which results in a 32 octets UTF-8 encoded string.

For P-GW:

It contains the following QoS parameters associated with the EPS bearer:

- QCI
- ARP

- GBR QoS information (UL/DL MBR, UL/DL GBR) or UL/DL APN-AMBR. In other words if the value of QCI indicates a GBR bearer, the GBR QoS information shall be present. If the value of QCI indicates a non-GBR bearer, the APN-AMBR information shall be present.

  The encoding of the EPS bearer QoS profile parameters is specified in 3GPP TS 29.274 [81]: ARP is specified in Bearer QoS IE; QCI, UL MBR, DL MBR, UL MBR and DL MBR are specified in Flow QoS IE; UL APN-AMBR and DL APN-AMBR are specified in AMBR IE.

  For GBR QCIs, the encoding of UTF-8 encoded QoS Profile field shall be as follows:

1-3	<Release indicator> -“ = “08-“ (UTF-8 encoded)
4-5	ARP (UTF-8 encoded)
6-7	QCI (UTF-8 encoded)
8-m	UL MBR (UTF-8 encoded)
(m+1)-n	DL MBR (UTF-8 encoded)
(n+1)-o	UL GBR (UTF-8 encoded)
(o+1)-p	DL GBR (UTF-8 encoded)

  For non-GBR QCIs, the UL/DL MBR and UL/DL GBR fields shall not be present; UL APN-AMBR and DL APN-AMBR fields shall be encoded (in UTF-8 encoded format) respectively after the QCI field.

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 type.

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 type.

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 character)							
4	MCC digit2 (UTF-8 encoded character)							
5	MCC digit3 (UTF-8 encoded character)							
6	MNC digit1 (UTF-8 encoded character)							
7	MNC digit2 (UTF-8 encoded character)							
8	MNC digit3 if present (UTF-8 encoded character)							

3GPP Type: 8

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

IMSI MCC-MNC address value: Text type.

This is the UTF-8 encoded characters representing the IMSI MCC-MNC numerical values. In accordance with 3GPP TS 29.060 [24] (for GGSN), 3GPP TS 29.274 [81] (for P-GW) and 3GPP TS 23.003 [40], 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 character)							
4	MCC digit2 (UTF-8 encoded character)							
5	MCC digit3 (UTF-8 encoded character)							
6	MNC digit1 (UTF-8 encoded character)							
7	MNC digit2 (UTF-8 encoded character)							
8	MNC digit3 if present (UTF-8 encoded character)							

3GPP Type: 9

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

GGSN address value: Text type.

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 (UTF-8 encoded character)							

3GPP Type: 10

Length: 3

NSAPI value: Text Type.

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 one UTF-8 encoded character. The GGSN should receive NSAPI values in the following hexadecimal range 05 – 0F. The GGSN shall discard digit 0 and convert the remaining digit into one UTF-8 coded character.

For P-GW, the value of this sub-attribute represents the EPS Bearer ID as specified in 3GPP TS 29.274 [81].

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 (bit string)							

3GPP Type: 11

Length: 3

Value is set to all 1.

3GPP-Session Stop Indicator value: Bit String type.

12 – 3GPP-*Selection-Mode*

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

3GPP Type: 12

Length: 3

Selection mode value: Text type.

The format of this sub-attribute shall be a character that represents a single digit, mapping from the binary value of the selection mode in the Create PDP Context message (3GPP TS 29.060 [24]) for the GGSN, and the Create Session Request message (3GPP TS 29.274 [81]) for the P-GW. 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 type.

The charging characteristics is value of the 2 octets. The value field is taken from the GTP IE described in 3GPP TS 29.060 [24], subclause 7.7.23 for the GGSN and 3GPP TS 29.274 [81] for the P-GW.

Each octet of this IE field value is represented via 2 UTF-8 encoded character, 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.

Charging GW Ipv6 address is Octet String type.

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.

SGSN Ipv6 address is Octet String type.

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.

SGSN Ipv6 address is Octet String type.

17 – 3GPP-*Ipv6-DNS-Servers*

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 17							
2	3GPP Length= m							
3-18	(1st) DNS Ipv6 addr Octet 1-16							
19-34	(2nd) DNS Ipv6 addr Octet 1-16							
k-m	(n-th) DNS Ipv6 addr Octet 1-16							

3GPP Type: 17

Length: m = n × 16 + 2; n ≥ 1 and n ≤ 15; k = m-15

Ipv6 DNS Server value: Ipv6 Address.

Ipv6 DNS Server address is Octet String type.

The 3GPP- Ipv6-DNS-Servers sub-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 sub-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 character)							
4	MCC digit2 (UTF-8 encoded character)							
5	MCC digit3 (UTF-8 encoded character)							
6	MNC digit1 (UTF-8 encoded character)							
7	MNC digit2 (UTF-8 encoded character)							
8	MNC digit3 if present (UTF-8 encoded character)							

3GPP Type: 18

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

SGSN MCC-MNC address value: Text type.

This is the UTF-8 encoding of the MCC-MNC values extracted from the RAI or from the Serving Network. In accordance with 3GPP TS 23.003 [40] and 3GPP TS 29.060 [24] (for the GGSN and P-GW connected to a Gn/Gp SGSN) and 3GPP TS 29.274 [81] (for the P-GW in GTP/PMIP S5/S8, S2a, S2b), 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

Octet 3 is Octet String type.

For GGSN, 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 Acct-Session-Id shall be torn down. Only the PDP context identified by the Acct-Session-Id shall be torn down if the value of TI is "0" (see subclause 16.3.4 "AAA-Initiated PDP context termination"), or if TI is missing.

For P-GW, the usage of Teardown-Indicator is as follows (see subclause 16.3a.3 for more deails):

- if the value of TI is set to "1", then all IP-CAN bearers that share the same user session with the IP-CAN bearer identified by the Acct-Session-Id shall be torn down.
- if the value of TI is "0", or if TI is missing, only the IP-CAN bearer identified by the Acct-Session-Id shall be torn down. If the Acct-Sesssion-Id identifies the default bearer, the P-GW shall tear down all the IP-CAN bearers that share the same user session identified by the Acct-Session-Id.

20 -3GGP- *IMEISV*

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP Type = 20							
2	3GPP Length = 2+n							
3 – (2+n)	IMEI(SV) digits 1 – n (UTF-8 encoded characters)							

3GPP Type: 20

IMEISV value: Text type.

A GGSN receives IMEI(SV) that is encoded according to 3GPP TS 29.060 [24]. A P-GW receives IMEI(SV) that is encoded in *ME Identity* IE specified in 3GPP TS 29.274 [81]. The GGSN or the P-GW converts IMEI(SV) into a sequence of UTF-8 characters.IMEI(SV) shall be encoded as defined in 3GPP TS 23.003 [40].

$14 \leq n \leq 16$

n = 16 for IMEISV, where TAC = 8 digits SNR = 6 digits & SVN = 2 digits;

n = 15 for IMEI, where TAC = 8 digits SNR = 6 digits & Spare = 1 digit;

n = 14 for IMEI, where TAC = 8 digits SNR = 6 digits (Spare digit is not sent)

21 – 3GPP-*RAT-Type*

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 21							
2	3GPP Length= 3							
3	RAT (octet string)							

3GPP Type: 21

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

RAT field: Radio Access Technology type values. RAT field is Octet String type. For GGSN, it shall be coded as specified in 3GPP TS 29.060 [24]. For P-GW, it shall be coded as follows:

0-8 As specified in 3GPP TS 29.274 [81]
9-100 Spare for future use
101 IEEE 802.16e
102 3GPP2 eHRPD
103 3GPP2 HRPD

104 3GPP2 1xRTT
105 3GPP2 UMB
106-255 Spare for future use

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 (octet string)							

3GPP Type: 22

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

For example, m= 10 in the CGI and SAI types.

Geographic Location Type field is used to convey what type of location information is present in the 'Geographic Location' field. For GGSN, the Geographic Location Type values and coding are as defined in 3GPP TS 29.060 [24]. For P-GW, the Geographic Location Type values and coding are defined as follows:

0 CGI
1 SAI
2 RAI
3-127 Spare for future use
128 TAI
129 ECGI
130 TAI and ECGI
131 eNodeB ID
132 TAI and eNodeB ID
133 extended eNodeB ID
134 TAI and extended eNodeB ID
135-255 Spare for future use

Geographic Location field is used to convey the actual geographic information as indicated in the Geographic Location Type. For GGSN, the coding of this field is as specified in 3GPP TS 29.060 [24]. For P-GW, the coding of this field shall be as follows:

- If the Geographic Location Type has a value indicating CGI, SAI, RAI, TAI or ECGI (i.e. the value field is equal to 0, 1, 2, 128, or 129), the coding of the Geographic Location field shall be as per clauses 8.21.1 to 8.21.5, respectively, in 3GPP TS 29.274 [81],

- If the Geographic Location Type has a value indicating TAI and ECGI (i.e. the value field is equal to 130), in Geographic Location field both TAI and ECGI shall be encoded one after another as per clauses 8.21.4 and 8.21.5 in 3GPP TS 29.274 [81]. TAI information shall be encoded first starting with Octet 4 of 3GPP-User-Location-Info.

- If the Geographic Location Type has a value indicating eNodeB ID (i.e. the value field is equal to 131), the coding of the Geographic Location field shall be as defined in subclause 8.21.7 in 3GPP TS 29.274 [81].

- If the Geographic Location Type has a value indicating TAI and eNodeB ID (i.e. the value field is equal to 132), in Geographic Location field both TAI and eNodeB ID shall be encoded one after another as per subclauses 8.21.4 and 8.21.7 in 3GPP TS 29.274 [81].

- If the Geographic Location Type has a value indicating extended eNodeB ID (i.e. the value field is equal to 133), the coding of the Geographic Location field shall be as defined in subclause 8.21.8 in 3GPP TS 29.274 [81].

- If the Geographic Location Type has a value indicating TAI and extended eNodeB ID (i.e. the value field is equal to 134), in Geographic Location field both TAI and extended eNodeB ID shall be encoded one after another as per subclauses 8.21.4 and 8.21.8 in 3GPP TS 29.274 [81].

Geographic Location Type and Geographic Location fields are Octet String type.

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 (octet string)							

3GPP Type: 23

Length=4

The Time Zone field and the Daylight Saving Time fields are used to indicate the offset between universal time and local time in steps of 15 minutes of where the MS/UE currently resides.

For GGSN, both fields are coded as specified in 3GPP TS 29.060 [24] and represented as Octet String type. For, P-GW, both fields are coded as specified in 3GPP TS 29.274 [81] in UE-Time Zone IE and represented as Octet String type.

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 (octet string)							

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] and represented as Octet String type.

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							

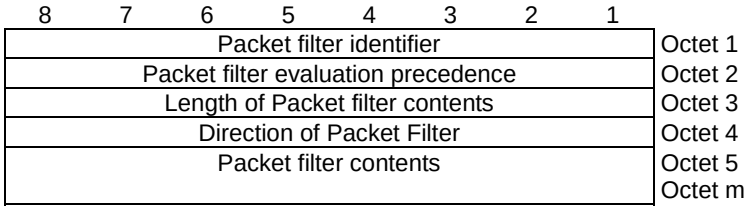
3GPP Type: 25

Length: n

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

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

Packet Filter Value:



Direction Value:

00000000: Downlink

00000001: Uplink

The packet filter content is represented as Octet String type. 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 sub-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 (octet string)							

3GPP Type: 26

Length: 3

Negotiated DSCP value: Octet String

DSCP value: Octet String type.

27 – 3GPP-*Allocate-IP-Type*

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 27							
2	3GPP Length= 3							
3	IP Type (octet string)							

3GPP Type: 27

If multiple Access-Request signalling towards a AAA server is needed during the lifetime of a PDN connection (e.g. for PDN/PDP type Ipv4v6 and deferred Ipv4 addressing), this sub-attribute shall be included in the Access-Request message to indicate how the AAA server needs to treat the request. The P-GW/GGSN may also use this sub-attribute if the AAA server is configured to allocate both Ipv4 address and Ipv6 prefix but the P-GW/GGSN requires assignment of only one IP type or both IP types (e.g. because the UE supports single IP stack and it has requested PDN/PDP type of Ipv4 or Ipv6).

If this sub-attribute does not exist in Access-Request from P-GW/GGSN to the AAA server, the IP address allocation shall be based on the IP address allocation policy configured in the the AAA server.

IP Type field: It is encoded in Octet String type and the following decimal equivalent values apply:

0 Do not allocate Ipv4 address or Ipv6 prefix.
The typical use case is for PDN/PDP type Ipv4v6 and deferred Ipv4 addressing and only Ipv4 address is allocated by the AAA 99orrec but Ipv6 prefix is allocated by some other means, e.g. local pool in the P-GW/GGSN. The Access-Request from the P-GW/GGSN to the AAA server during the UE's initial access to the network shall set the value of this sub-attribute to 0.

1 Allocate Ipv4 address
The typical use case is for PDN/PDP type Ipv4v6 and deferred Ipv4 addressing and the Ipv4 address (and/or Ipv6 prefix) is allocated by the AAA server. The Access-Request from the P-GW/GGSN to the AAA server when the P-GW/GGSN receives UE-initiated Ipv4 address allocation signalling (e.g. DHCPv4) after UE's successful initial access to the PDN shall set the value of this attribute to 1. In this case, if the AAA server had allocated an Ipv6 prefix earlier during UE's initial access to the network, same Ipv6 prefix shall be kept allocated.

2 Allocate Ipv6 prefix
The typical use case is for PDN/PDP type Ipv4v6 and deferred Ipv4 addressing and both Ipv4 address and Ipv6 prefix are allocated by the AAA server. The Access-Request from the P-GW/GGSN to the AAA server during the UE's initial access to the network shall set the value of this sub-attribute to 2.

3 Allocate Ipv4 address and Ipv6 prefix
Currently there is no use case identified to use this specific value for PDN/PDP tpe Ipv4v6 and deferred Ipv4 addressing. One potential use case is for PDN/PDP type Ipv4v6 and non-deferred Ipv4 addressing and both Ipv4 address and Ipv6 prefix are allocated by the AAA server. The Accesss-Request from the P-GW/GGSN to the AAA server may use this value to have both Ipv4 address and Ipv6 prefix assigned to the UE.

4-255 Reserved for future use

28 – External-Identifier

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 28							
2	3GPP Length= m							
3-m	Identifier characters 1-n (UTF-8 encoded characters)							

3GPP Type: 28

n ≤ 72 / 253 (n ≤ 72 octets shall be supported, n ≤ 253 octets recommended, refer to 3GPP TS 29.336 [101] and IETF RFC 4282 [102])

Length: m ≤ 74 / 255 (m ≤ 74 octets shall be supported, m ≤ 255 octets recommended, refer to 3GPP TS 29.336 [101] and IETF RFC 4282 [102])

External-Identifier value: Text type.

A globally unique identifier of a UE used towards external server instead of IMSI and MSISDN, refer to 3GPP TS 23.682 [100] and 3GPP TS 23.003 [40].

29 – TWAN-Identifier

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 29							
2	3GPP Length= m							
3-m	TWAN Identifier (octet string)							

3GPP Type: 29

Length=m, where m depends on the type of location that is present as described in 3GPP TS 29.274 [81].

TWAN Identifier field is used to convey the location information in a Trusted WLAN Access Network (TWAN). The coding of this field shall be the same as for the GTP TWAN Identifier starting with Octet 5, as per clause 8.100 in 3GPP TS 29.274 [81].

TWAN Identifier field is Octet String type.

30 – 3GPP-User-Location-Info-Time

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 30							
2	3GPP Length= 6							
3-6	User Location Info time							

3GPP Type: 30

Length=6

User Location Info time field is Unsigned32 type, it indicates the NTP time at which the UE was last known to be in the location which is reported during bearer deactivation or UE detach procedure.

16.4.8 Accounting Request Interim-Update (sent from GGSN/P-GW 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 is provided to the GGSN/P-GW by the user in the PCO or for the case of the P-GW when multiple authentications are supported in the APCO received during IP-CAN session establishment procedure. If PPP PDN type is used, it is provided to the GGSN by the user during PPP authentication phase. 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 username shall be used in preference to the above.	String	Optional
4	NAS-IP-Address	Ipv4 address of the GGSN/P-GW for communication with the AAA server.	Ipv4	Conditional Notes 1 and 7
95	NAS-Ipv6-Address	Ipv6 address of the GGSN/P-GW for communication with the AAA server.	Ipv6	Conditional Notes 1 and 7
32	NAS-Identifier	Hostname of the GGSN/P-GW 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 Note 8
8	Framed-IP-Address	User Ipv4 address	Ipv4	Conditional Note 3
97	Framed-Ipv6-Prefix	User Ipv6 prefix	Ipv6	Conditional Note 3
123	Delegated-Ipv6-Prefix	Delegated Ipv6 prefix to the user	Ipv6	Conditional Note 9
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 characters. (Note 6)	Optional
40	Acct-Status-Type	Indicates the type of accounting request	Interim-Update	Mandatory

Attr #	Attribute Name	Description	Content	Presence Requirement
41	Acct-Delay-Time	Indicates how many seconds the GGSN/P-GW 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/P-GW counted number of octets sent by the user for the IP-CAN bearer	32 bit unsigned integer	Optional
43	Acct-Output-Octets	GGSN/P-GW counted number of octets received by the user for the IP-CAN bearer	32 bit unsigned integer	Optional
44	Acct-Session-Id	User session identifier.	GGSN/P-GW IP address (Ipv4 or Ipv6) and Charging-ID concatenated in a UTF-8 encoded hexadecimal characters. (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/P-GW counted number of packets sent by the user	Packet	Optional
48	Acct-Output-Packets	GGSN/P-GW counted number of packets received by the user	Packet	Optional
61	NAS-Port-Type	Port type for the GGSN/P-GW	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: Ipv4 and/or Ipv6 address/prefix attributes 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 a static Ipv6 address is assigned.
NOTE 5: The GGSN/P-GW IP address is the same one that is used in the CDRs generated by the GGSN/P-GW.
NOTE 6: There are no leading characters in front of the country code.
NOTE 7: Either Ipv4 or Ipv6 address attribute shall be present.
NOTE 8: Framed-Protocol value of 7 is used by both GGSN and P-GW when interworking with RADIUS AAA servers. When used for P-GW, it represents the IP-CAN bearer.
NOTE 9: Delegated Ipv6 prefix shall be present if the user was delegated an Ipv6 prefix from a local pool.

16.4.9 Disconnect Request (optionally sent from AAA server to GGSN/P-GW)

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/APCO field received during PDN connection establishment) 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	String	Optional

		user-name shall be used in preference to the above		
8	Framed-IP-Address	User Ipv4 address	Ipv4	Conditional Note 2
97	Framed-Ipv6-Prefix	User Ipv6 prefix	Ipv6	Conditional Note 2
123	Delegated-Ipv6-Prefix	Delegated Ipv6 prefix to the user.	Ipv6	Conditional Note 4
96	Framed-Interface-Id	User Ipv6 Interface Identifier	Ipv6	Conditional Notes 1and 2
44	Acct-Session-Id	User session identifier.	GGSN/P-GW IP address (Ipv4 or Ipv6) and Charging-ID concatenated in a UTF-8 encoded hexadecimal characters. (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 a static Ipv6 address is assigned. NOTE 2: Either Ipv4 or Ipv6 address/prefix attribute shall be present. See subclause 16.3.4. NOTE 3: The GGSN/P-GW IP address is the same one that is used in the CDRs created by the GGSN/P-GW. NOTE 4: Delegated Ipv6 prefix shall be present if the user was delegated an Ipv6 prefix from a local pool.				

16a Usage of Diameter on Gi/Sgi interface

As an operator option, it is also possible to use the Diameter protocol in order to provide Authentication, Authorization and Accounting services.

A GGSN/P-GW may, on a per APN basis, use Diameter authentication to authenticate a user and Diameter accounting to provide information to a Diameter server.

16a.1 Diameter Authentication and Authorization

Diameter Authentication and Authorization shall be used according to RFC 4005 [67].

The GGSN/P-GW and the Diameter server shall advertise the support of the Diameter NASREQ Application by including the value of the appropriate application identifier in the Capability-Exchange-Request and Capability-Exchange-Answer commands as specified in IETF RFC 6733 [111].

The Diameter client function may reside in a GGSN/P-GW. When the GGSN/P-GW receives an initial attach (e.g. Create PDP Context) request message the Diameter 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 Ipv4 address and/or Ipv6 prefix for the user when the GGSN/P-GW is interworking with the AAA server.

The information delivered during the Diameter authentication can be used to automatically correlate the users identity (the MSISDN or IMSI) to the Ipv4 address and/or Ipv6 prefix, if applicable, assigned/confirmed by the GGSN/P-GW or the authentication server respectively. The same procedure applies, in case of sending the authentication to a 'proxy' authentication server.

Diameter Authentication is applicable to the initial access (e.g. primary PDP context or the default bearer). When the GGSN/P-GW receives a positive response from the authentication server it shall complete the initial access (e.g. PDP

context activation) procedure. If a failure or no response is received, the GGSN/P-GW shall reject the initial access (e.g. PDP Context Activation) attempt with a suitable cause code, e.g. User Authentication failed.

The GGSN may also use the Diameter re-authorization procedure for the purpose of Ipv4 address allocation to the UE for PDP type of Ipv4v6 after establishment of a PDN connection.

For EPS, the P-GW may also use the Diameter re-authorization procedure for the purpose of Ipv4 address allocation to the UE for PDN type of Ipv4v6 after establishment of a PDN connection. The use cases that may lead this procedure are:

- Deferred Ipv4 address allocation via DHCPv4 procedure after successful attach on 3GPP accesses.
- Deferred Ipv4 address allocation after successful attach in trusted non-3GPP IP access on S2a.
- Deferred Ipv4 home address allocation via DSMIPv6 Re-Registration procedure via S2c.

16a.2 Diameter Accounting

Diameter Accounting shall be used according to RFC 4005 [67].

The Diameter accounting client function may reside in a GGSN/P-GW. The Diameter 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 PS access network has authenticated the subscriber (i.e. SIM card and possibly other authentication methods).

Diameter Accounting messages may be used during both primary and secondary PDP context activation for non-EPC based packet domain (both the default bearer and dedicated bearer for the EPC based packet domain) and deactivation procedures respectively.

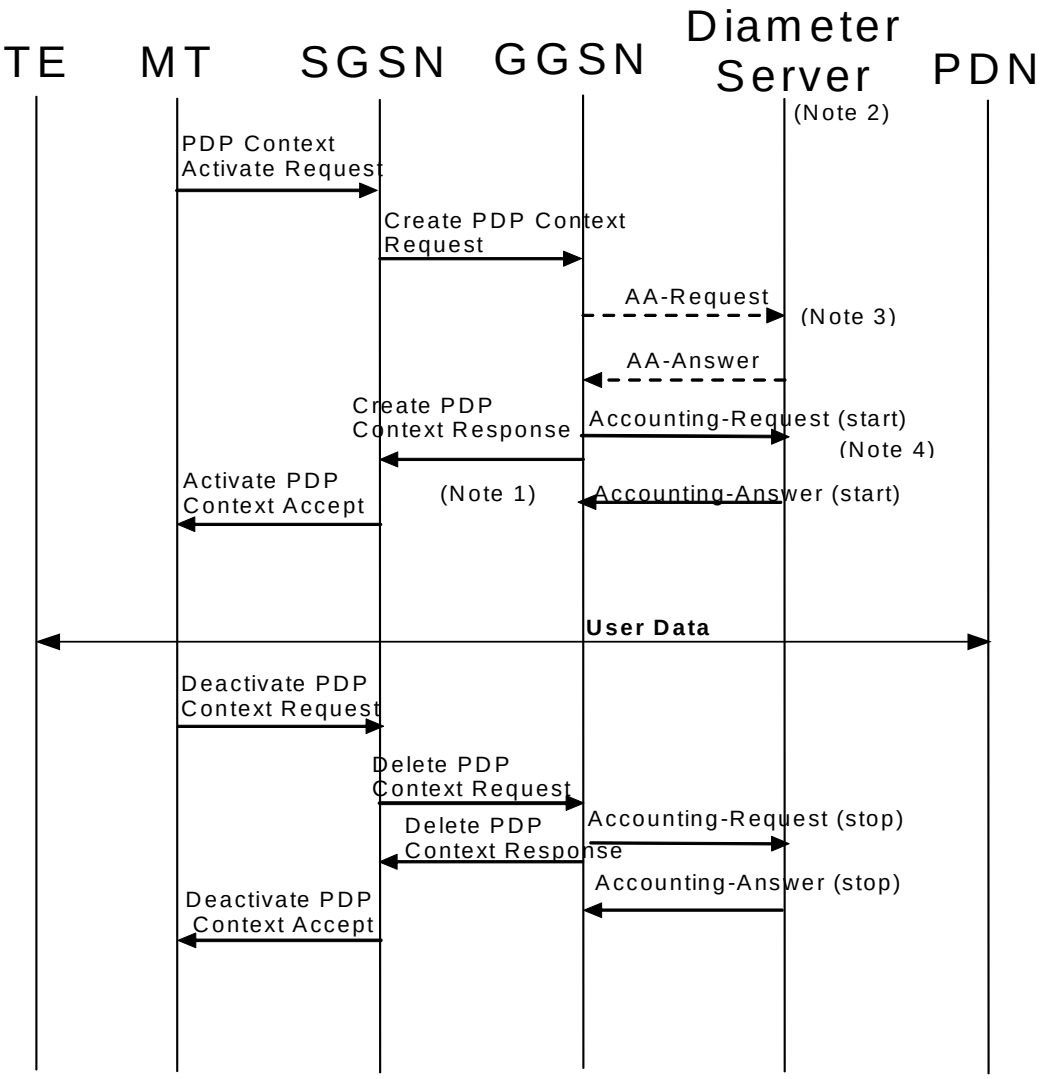
If the AAA server is used for Ipv4 address and/or Ipv6 prefix assignment, then, upon reception of a Diameter Accounting-Request STOP message for all IP-CAN bearers associated to an IP-CAN session defined by APN and IMSI or MSISDN, the AAA server may make the associated Ipv4 address and/or Ipv6 prefix available for assignment.

For PDN/PDP type Ipv4v6 and deferred Ipv4 address allocation, when the Ipv4 address is allocated or re-allocated, the accounting session that was established for the Ipv6 prefix allocation shall be used to inform the accounting server about the allocated Ipv4 address by sending Diameter Accounting-Request Interim-Update with Framed-IP-Address AVP and its value field containing the allocated Ipv4 address. Similarly, the release of Ipv4 address shall be indicated to the accounting server by sending Diameter Accounting-Request Interim-Update without the Framed-IP-Address AVP.

16a.3 Authentication and accounting message flows on Gi interface

16a.3.1 IP PDP type

Figure 25a represents the Diameter message flows between a GGSN and a Diameter server.



NOTE 1: If some external applications require Diameter 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 Answer (START) is received from the Diameter server. The GGSN may wait for the Accounting Answer (START) before sending the CreatePDPContextResponse. The GGSN may reject the PDP context if the Accounting Answer (START) is not received.
NOTE 2: Separate accounting and authentication servers may be used.
NOTE 3: The AA-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 Ipv4 address has been assigned and PDP Context updated, in case of IP address allocation via DHCPv4 after successful PDP context activation signalling.

Figure 25a: Diameter 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 Diameter AA-Request to a Diameter server. The Diameter server authenticates and authorizes the user. If Diameter is also responsible for Ipv4 address and/or Ipv6 prefix allocation the Diameter server

shall return the allocated Ipv4 address and/or Ipv6 prefix in the AA-Answer message. The AA-Request and AA-Answer messages are only used for the primary PDP context.

When PDP type is Ipv4v6 and deferred Ipv4 addressing via Ipv4 address pool in the AAA server is used, the GGSN may intiate Diameter re-authorization procedures after successful initial attach for the purpose of Ipv4 address allocation or to renew the lease for a previously allocated Ipv4 address. In this case, the GGSN shall set the Session-Id to the value used in the initial access request, the Auth-Request-Type AVP to "AUTHORIZE_ONLY" and the 3GPP-Allocate-IP-Type AVP to the type of IP address to be allocated in the AA-Request message sent to the AAA server. See subclause 16.4.7.2 for the conditions to use 3GPP-Allocate-IP-Type AVP in AA-Request messages. If the GGSN is using DHCPv4 signalling towards the MS and the Diameter server includes the Session-Timeout attribute in the Access-Accept, the GGSN may use the Session-Timeout value as the DHCP lease time. The GGSN shall not set the DHCPv4 lease time value higher than the Session-Timeout value. The GGSN may renew the DHCP lease to the MS without re-authorization towards the AAA server providing that the new lease expiry is no later than the Session-Timeout timer expiry. If the GGSN wishes to extend the lease time beyond the current Session-Timeout expiry, it shall initiate a new AAA re-authorization.

Even if the GGSN was not involved in user authentication (e.g. transparent network access mode), it may send a Diameter Accounting-Request (START) message to a Diameter server. If no Diameter session is already open for the user a Diameter session needs to be activated, otherwise the existing Diameter session is used to send the Accounting-Request (START). The NSAPI will identify the particular PDP context this accounting refers to. The Accounting-Request message also indicates to the Diameter server that the user session has started. This message contains parameters, e.g. the tuple which includes the user-id, Ipv4 address and/or Ipv6 prefix, and the MSISDN to be used by application servers (e.g. WAP gateway) in order to identify the user.

If some external applications require Diameter 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 Answer (START) is received from the Diameter server. The GGSN may wait for the Accounting Answer (START) before sending the CreatePDPContextResponse. The GGSN may reject the PDP context if the Accounting Answer (START) is not received. The authentication and accounting servers may be separately configured for each APN.

For PDP type Ipv4, at Ipv4 address allocation via DHCP4 signalling between the TE and the PDN, no Ipv4 address 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 DHCPACK.

For PDP type Ipv4v6 and deferred Ipv4 addressing, when the Ipv4 address is allocated or re-allocated, the accounting session that was established for the Ipv6 prefix allocation shall be used to inform the accounting server about the allocated Ipv4 address by sending Diameter Accounting-Request Interim-Update with the Framed-IP-Address AVP and its value field containing the allocated Ipv4 address.

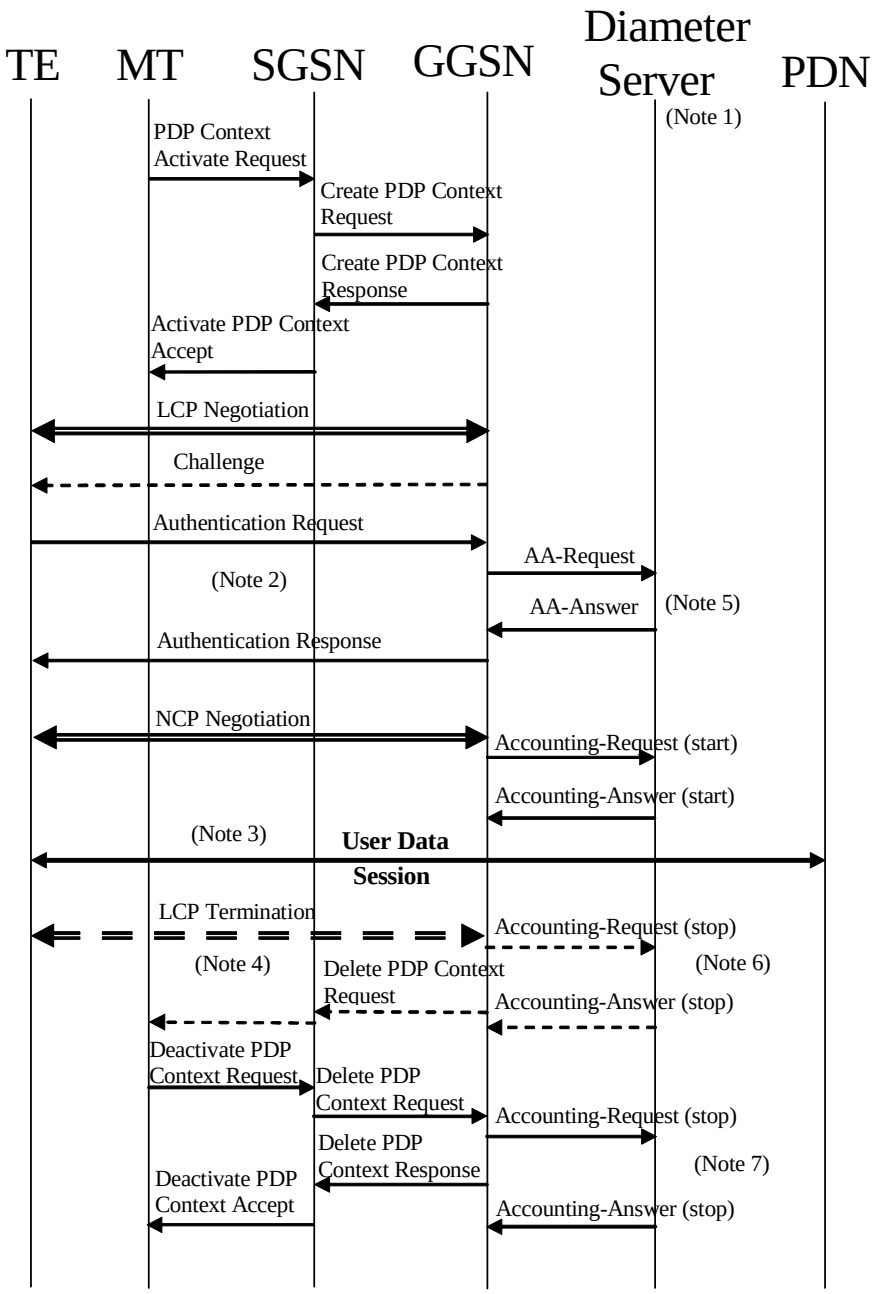
When the GGSN receives a Delete PDP Context Request message and providing a Diameter Accounting-Request (START) message was sent previously, the GGSN shall send a Diameter Accounting-Request (STOP) message to the Diameter server, which indicates the termination of this particular user accounting session. The NSAPI will identify the particular PDP context this accounting refers to. The GGSN shall immediately send a Delete PDP context response, without waiting for an Accounting-Answer (STOP) message from the Diameter server.

If this was the last PDP context for that PDP address, the GGSN shall additionally send an STR message to the Diameter server. The Diameter server shall reply with an STA and shall deallocate the IP address or Ipv6 prefix (if any) initially allocated to the subscriber.

For PDP type Ipv4v6 and deferred Ipv4 addressing, when the GGSN receives a message from the MS or the network indicating the release of the Ipv4 address (e.g. receiving DHCPRELEASE) or decides to release the Ipv4 address on its own (e.g. due to DHCP lease timer expiry for GGSN assigned Ipv4 address), the GGSN shall inform the accounting server about the deallocation of the Ipv4 address by sending Diameter Accounting-Request Interim-Update without the Framed-IP-Address AVP.

16a.3.2 PPP PDP type

Figure 25b describes the Diameter message flows between a GGSN and a Diameter 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 Diameter 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 Answer (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 AA-Request message shall be used for primary PDP context only.
NOTE 6: Network Initiated deactivation.
NOTE 7: User Initiated deactivation.

Figure 25b: Diameter 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 Diameter AA-Request to a Diameter server. The Diameter server authenticates and authorizes the user. If Diameter is also responsible for IP address allocation the Diameter server shall return the allocated IP address or Ipv6 prefix in the AA-answer message (if the user was authenticated).

If the user is not authenticated, the GGSN shall send a Delete PDP context request to the SGSN. The AA-Request and AA-Answer messages are only used for the primary PDP context.

Even if the GGSN was not involved in user authentication (e.g. for PPP no authentication may be selected), it may send a Diameter Accounting-Request (START) message to a Diameter server. If no Diameter session is already open for the user a Diameter session needs to be activated, otherwise the existing Diameter session is used to send the Accounting-Request (START). The NSAPI will identify the particular PDP context this accounting refers to. The Accounting-Request message also indicates to the Diameter server that the user session has started, and the QoS parameters associated to the session. This message contains parameters, e.g. a tuple which includes the user-id, IP address or Ipv6 prefix, and the MSISDN to be used by application servers (e.g. WAP gateway) in order to identify the user.

If some external applications require Diameter 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 Answer (START) is received from the Diameter server. The GGSN may delete the PDP context if the Accounting Answer (START) is not received. The Authentication and Accounting servers may be separately configured for each APN.

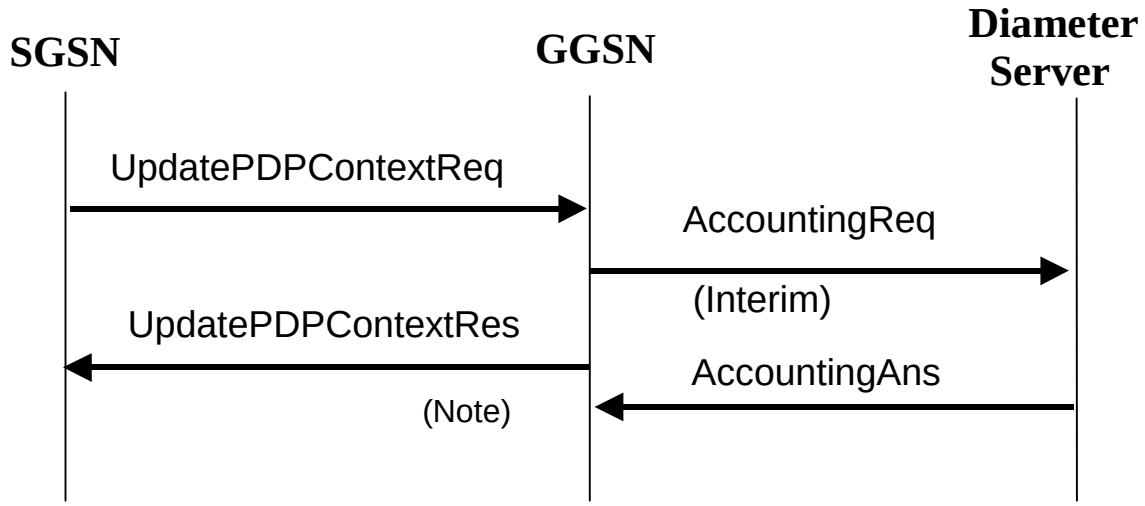
When the GGSN receives a Delete PDP Context Request message and providing a Diameter Accounting-Request (START) message was sent previously, the GGSN shall send a Diameter Accounting-Request (STOP) message to the Diameter server, which indicates the termination of this particular user session. The NSAPI will identify the particular PDP context this accounting refers to. The GGSN shall immediately send a Delete PDP context response, without waiting for an Accounting-Answer (STOP) message from the Diameter server.

If this was the last PDP context for that PDP address, the GGSN shall additionally send an STR message to the Diameter server. The Diameter server shall reply with an STA and shall deallocate the IP address or Ipv6 prefix (if any) initially allocated to the subscriber.

16a.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 an Inter-SGSN RA update occurs). Upon reception of an UpdatePDPContextRequest from the SGSN, the GGSN may send an Accounting Request (Interim) to the Diameter server to update the necessary information related to this PDP context (see figure 25c). Interim updates are also used when the Ipv4 address is allocated/released/re-allocated for deferred Ipv4 addressing for the PDP type Ipv4v6.

If the GGSN receives an UpdatePDPContextRequest from the SGSN that specifically indicates a direct tunnel establishment or a direct tunnel teardown (switching the user plane tunnel end back to the SGSN), and only the GTP user plane address or the GTP-U TEID have changed, then the GGSN should not send the Accounting Request (Interim) message to the Diameter server. In such cases, the GGSN need not wait for the Diameter Accounting Answer from the Diameter server message before sending the UpdatePDPContextResponse to the SGSN. The GGSN may delete the PDP context if the Accounting Answer is not received from the Diameter server.



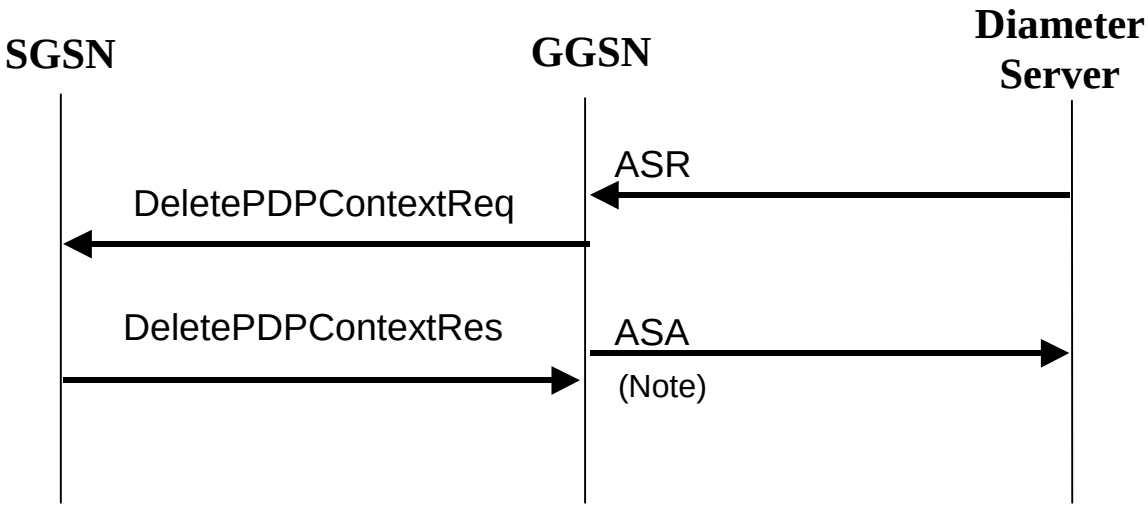
NOTE: As shown the GGSN need not wait for the Diameter Accounting Answer message from the Diameter server to send the UpdatePDPContextResponse to the SGSN. The GGSN may delete the PDP context if the Accounting Answer is not received from the Diameter server.

Figure 25c: Diameter for PDP context Update

16a.3.4 Server-Initiated PDP context termination

Diameter is used as the protocol between the GGSN and a Diameter 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 Diameter server or proxy may send a Diameter ASR to the GGSN along with the NSAPI necessary to identify the particular PDP context to be terminated. As depicted in figure 25d, the GGSN should react by deleting the corresponding PDP context. If the GGSN deletes the corresponding PDP context, it need not wait for the DeletePDPContextResponse from the SGSN before sending the ASA to the server.

The absence of the NSAPI in the Diameter ASR 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 belonging to the same IP-CAN session are identified by the Diameter 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 Diameter Session-Id shall be deleted.



NOTE: As showed on figure 25d, the GGSN need not wait for the DeletePDPContextResponse from the SGSN to send the ASA to the Diameter server.

Figure 25d: PDP Context deletion with Diameter

16a.3a Authentication and accounting message flows on Sgi interface

16a.3a.1 Authentication, Authorization and Accounting procedures

When a P-GW receives an initial access request (e.g.Create Session Request or Proxy Binding Update) message for a given APN, the P-GW may (depending on the configuration for this APN) send a Diameter AA-Request to a Diameter server. The Diameter server authenticates and authorizes the user. If the Diameter server is also responsible for Ipv4 address and/or Ipv6 prefix allocation the Diameter server shall return the allocated Ipv4 address and/or Ipv6 prefix in the AA-Answer message.

When PDN type is Ipv4v6 and deferred Ipv4 addressing via Ipv4 address pool in the AAA server is used, the P-GW may intiate Diameter re-authorization procedures after successful initial attach for the purpose of Ipv4 address allocation or to renew the lease for a previously allocated Ipv4 address. In this case, the P-GW shall set the Session-Id to the value used in the initial access request, the Auth-Request-Type AVP to "AUTHORIZE_ONLY" and the 3GPP-Allocate-IP-Type AVP to the type of IP address to be allocated in the AA-Request message sent to the AAA server. See subclause 16.4.7.2 for the conditions to use 3GPP-Allocate-IP-Type AVP in AA-Request messages. If the P-GW is using DHCPv4 signalling towards the UE and the Diameter server includes the Session-Timeout attribute in the Access-Accept, the P-GW may use the Session-Timeout value as the DHCP lease time. The P-GW shall not set the DHCPv4 lease time value higher than the Session-Timeout value. The P-GW may renew the DHCP lease to the UE without re-authorization towards the AAA server providing that the new lease expiry is no later than the Session-Timeout timer expiry. If the P-GW wishes to extend the lease time beyond the current Session-Timeout expiry, it shall initiate a new AAA re-authorization.

Even if the P-GW was not involved in user authentication, it may send a Diameter Accounting-Request (START) message to a Diameter server. If no Diameter session is already open for the same PDN connection a Diameter session needs to be activated, otherwise the existing Diameter session is used to send the Accounting-Request (START). For GTP-based S5/S8/S2a/S2b, if accounting is used per IP-CAN bearer, the EPS bearer ID will identify the particular bearer this accounting message refers to. The Accounting-Request message also indicates to the Diameter server that the user session has started.This message contains parameters, e.g. the tuple which includes the user-id and Ipv4 address and/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 Diameter server that the user session has started.

If some external applications require Diameter Accounting Request (START) information before they can process user packets, then the selected APN (P-GW) may be configured in such a way that the P-GW drops user data until an Accounting-Answer (START) indicating success is received from the Diameter server. The P-GW may wait for the Accounting-Answer (START) before sending the initial access response (e.g. Create Session Response or Proxy

Binding Acknowledgement). The P-GW may reject the initial access request if the Accounting-Answer (START) is not received. The authentication and accounting servers may be separately configured for each APN.

For PDN type Ipv4, at Ipv4 address allocation via DHCPv4 signalling between the UE and the PDN, no Ipv4 address is available at initial access. In that case the P-GW may wait to send the Accounting-Request START message until the UE receives its Ipv4 address in a DHCPACK.

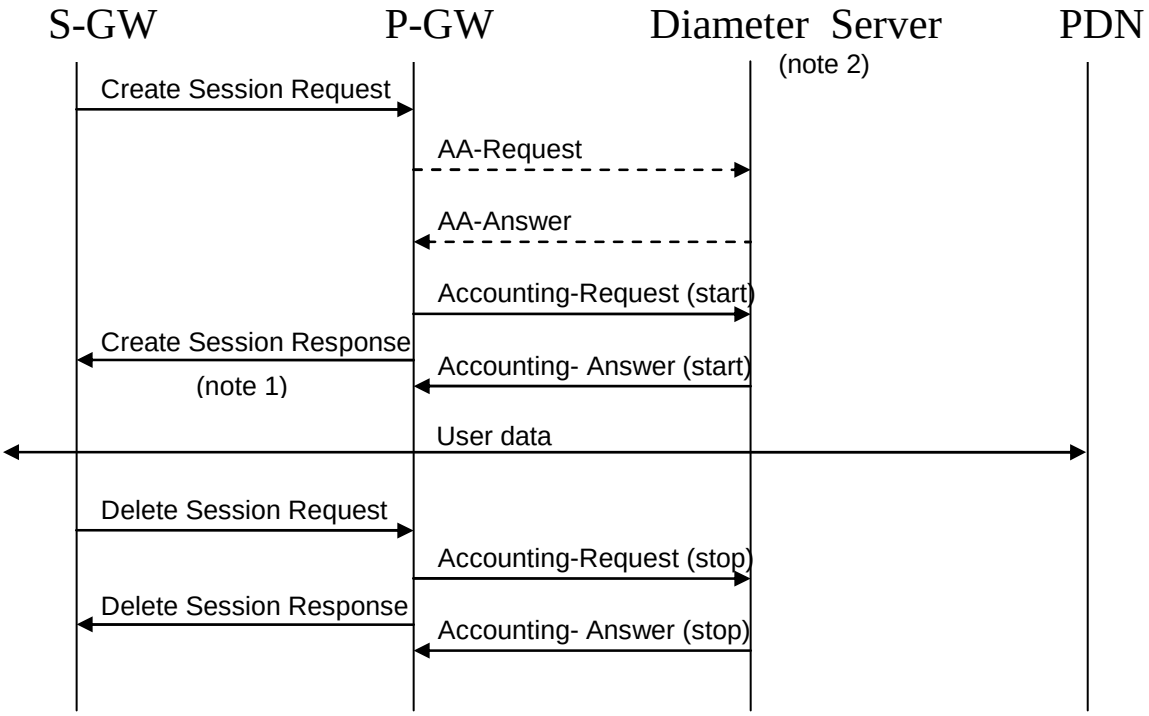
For PDN type Ipv4v6 and deferred Ipv4 addressing, when the Ipv4 address is allocated or re-allocated, the accounting session that was established for the Ipv6 prefix allocation shall be used to inform the accounting server about the allocated Ipv4 address by sending Diameter Accounting-Request Interim-Update with the Framed-IP-Address AVP and its value field containing the allocated Ipv4 address.

When the P-GW receives a message indicating a bearer deactivation request or PDN disconnection request or detach request (e.g. Delete Bearer Command or Proxy Binding Update with lifetime equal 0) and providing a Diameter Accounting-Request START message was sent previously, the P-GW shall send a Diameter Accounting-Request (STOP) message to the Diameter server, which indicates the termination of this particular bearer or user session. The P-GW shall immediately send the corresponding response (e.g. Delete Bearer Request or Proxy Binding Ack with lifetime equal 0) to the peer node (e.g. S-GW) in the Packet Domain, without waiting for an Accounting-Answer (STOP) message from the Diameter server.

If the last bearer of an IP-CAN session is deactivated, the P-GW shall additionally send an STR message to the Diameter server. The Diameter server shall reply with an STA and shall deallocate the Ipv4 address and/or Ipv6 prefix (if any) initially allocated to the subscriber.

For PDN type Ipv4v6 and deferred Ipv4 addressing, when the P-GW receives a message from the UE or the network indicating the release of the Ipv4 address (e.g. receiving DHCPRELEASE) or decides to release the Ipv4 address on its own (e.g. due to DHCP lease timer expiry for P-GW assigned Ipv4 address), the P-GW shall inform the accounting server about the deallocation of the Ipv4 address by sending Diameter Accounting-Request Interim-Update without the Framed-IP-Address AVP.

The following Figure 25d.1 is an example message flow to show the procedure of Diameter Authentication and Accounting, which is applicable for GTP based S5/S8:



NOTE 1: If some external applications require Diameter Accounting request (Start) information before they can process user packets, then the selected APN (P-GW) may be configured in such a way that the P-GW drops user data until the Accounting Answer (START) is received from the Diameter server. The P-GW may wait for the Accounting Answer (START) before sending the Create Session Response. The P-GW may reject the bearer if the Accounting Answer (START) is not received.

NOTE 2: Separate accounting and authentication servers may be used.

Figure 25d.1: An example of Diameter Authentication and Accounting on Sgi for GTP-based S5/S8

16a.3a.2 Accounting Update

During the life of a bearer some information related to this bearer may change. Upon occurrence of the following events the P-GW may send an Accounting Request (Interim) to the Diameter server: RAT change, S-GW address change and QoS change. Interim updates are also used when the Ipv4 address is allocated/released/re-allocated for deferred Ipv4 addressing for the PDN type Ipv4v6.

When the P-GW receives a signalling request (e.g. Modify Bearer Request in case of GTP-based S5/S8) that indicates the occurrence of one of these chargeable events, the P-GW may send an Accounting Request (Interim) to the Diameter server to update the necessary information related to this bearer. The P-GW need not wait for the Diameter Accounting Answer message from the Diameter server before sending the response for the triggering signalling message (e.g. Modify Bearer Response). The P-GW may delete the bearer if the Accounting Answer is not received from the Diameter server.

The P-GW may also send interim updates at the expiry of an operator configured time limit.

The message flow in figure 25d.2 provides an example for Diameter Accounting Update procedure on Sgi interface, which is applicable for GTP based S5/S8:

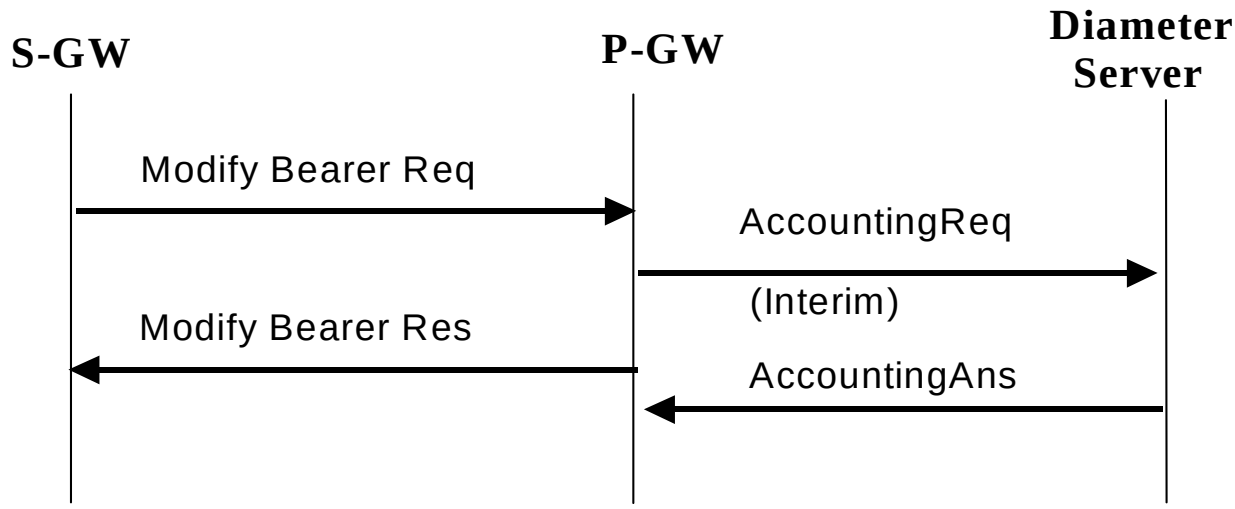


Figure 25d.2: Diameter accounting update for bearer modification

16a.3a.3 Server-Initiated Bearer termination

Diameter is used as the protocol between the P-GW and a Diameter server or proxy for applications (e.g. MMS) to deliver information related to the user session. However some IP applications could need to interwork with the P-GW to release the corresponding resource (e.g. terminate a particular bearer or Resource Allocation Deactivation procedures as defined in TS 23.402 [78]). For this purpose, the Diameter server or proxy may send a Diameter ASR along with the EPS bearer ID, if available, to identify the particular bearer to be terminated to the P-GW. The P-GW should react by deleting the corresponding bearer. If the P-GW deletes the corresponding bearer, it need not wait for the response from the S-GW or trusted non-3GPP IP access or ePDG before sending the ASA to the server.

The absence of the EPS bearer ID in the Diameter ASR message indicates to the P-GW that all bearers/resources for this particular user and sharing the same user session shall be deleted. The bearer(s)/resources belonging to the same IP-CAN session are identified by the Diameter Session-Id. If a user has the same user IP address(es) for different sets of bearers towards different networks, only the bearers linked to the one identified by the Diameter Session-Id shall be deleted.

The message flow in figure 25d.3 provides an example for Server-initiated Bearer Termination procedure on Sgi interface, which is applicable for GTP based S5/S8:

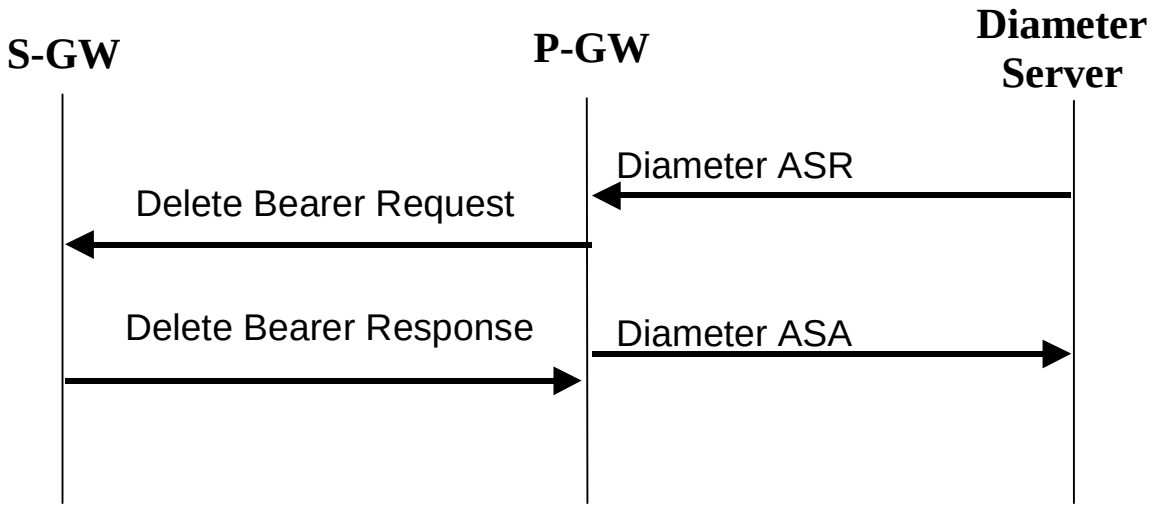


Figure 25d.3: Server-initiated Bearer Termination with Diameter

16a.4 Gi/Sgi Diameter messages

This clause describes the Gi and the Sgi interface Diameter messages.

The relevant AVPs that are of use for the Gi/Sgi 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.

16a.4.1 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 may be sent by the GGSN to a Diameter server, during Primary PDP Context activation only, in order to request user authentication and authorization. In the case of P-GW, the AAR may be sent upon reception of an initial access request (e.g. Create Session Request or Proxy Binding Update) message for a given APN to request user authentication and authorization.

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

The bold marked AVPs in the message format indicate optional AVPs for Gi/Sgi, or modified existing AVPs. For Sgi, some of the optional 3GPP vendor-specific AVPs listed in the message format below are not applicable. See table 9a in subclause 16a.5 to see the list of vendor-specific AVPs that are applicable to the GGSN and the P-GW.

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 ]
                        [ NAS-Port ]
                        [ NAS-Port-Id ]
                        [ NAS-Port-Type ]
                        [ Origin-State-Id ]
                        [ Port-Limit ]
                        [ User-Name ]
                        [ User-Password ]
                        [ Service-Type ]
                        [ Authorization-Lifetime ]
                        [ Auth-Grace-Period ]
                        [ Auth-Session-State ]
                        [ Callback-Number ]
                        [ Called-Station-Id ]
                        [ Calling-Station-Id ]
                        [ Originating-Line-Info ]
                        [ Connect-Info ]
                        [ CHAP-Auth ]
                        [ CHAP-Challenge ]
                      * [ Framed-Compression ]
                        [ Framed-Interface-Id ]
                        [ Framed-IP-Address ]
                      * [ Framed-Ipv6-Prefix ]
                      * [ Delegated-Ipv6-Prefix ]
                        [ Framed-IP-Netmask ]
                        [ Framed-MTU ]
                        [ Framed-Protocol ]
                      * [ Login-IP-Host ]
                      * [ Login-Ipv6-Host ]
                        [ Login-LAT-Group ]
                        [ Login-LAT-Node ]
                        [ Login-LAT-Port ]
                        [ Login-LAT-Service ]
                      * [ Tunneling ]
                      * [ Proxy-Info ]
                      * [ Route-Record ]
                        [ 3GPP-IMSI]
                        [ External-Identifier]
                        [ 3GPP-Charging-ID ]
```

```
                        [ 3GPP-PDP-Type ]
                        [ 3GPP-CG-Address ]
                        [ 3GPP-GPRS-Negotiated-QoS-Profile ]
                        [ 3GPP-SGSN-Address ]
                        [ 3GPP-GGSN-Address ]
                        [ 3GPP-IMSI-MCC-MNC ]
                        [ 3GPP-GGSN-MCC-MNC ]
                        [ 3GPP-NSAPI ]
                        [ 3GPP-Selection-Mode ]
                        [ 3GPP-Charging-Characteristics ]
                        [ 3GPP-CG-Ipv6-Address ]
                        [ 3GPP-SGSN-Ipv6-Address ]
                        [ 3GPP-GGSN-Ipv6-Address ]
                        [ 3GPP-SGSN-MCC-MNC ]
                        [ 3GPP-User-Location-Info ]
                        [ 3GPP-RAT-Type ]
                        [ 3GPP-CAMEL-Charging-Info ]
                        [ 3GPP-Negotiated-DSCP ]
                        [ 3GPP-Allocate-IP-Type ]
                        [ TWAN-Identifier ]
                      * [ AVP ]
```

16a.4.2 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 Diameter server to the GGSN/P-GW in response to the AAR command.

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

The bold marked AVPs in the message format indicate optional AVPs for Gi/Sgi, or modified existing AVPs.

Message Format:

```
<AA-Answer> ::= < Diameter Header: 265, PXY >
                        < Session-Id >
                        { Auth-Application-Id }
                        { Auth-Request-Type }
                        { Result-Code }
                        { Origin-Host }
                        { Origin-Realm }
                        [ User-Name ]
                        [ Service-Type ]
                      * [ Class ]
                        [ Acct-Interim-Interval ]
                        [ Error-Message ]
                        [ Error-Reporting-Host ]
                        [ Failed-AVP ]
                        [ Idle-Timeout ]
                        [ Authorization-Lifetime ]
                        [ Auth-Grace-Period ]
                        [ Auth-Session-State ]
                        [ Re-Auth-Request-Type ]
                        [ Multi-Round-Time-Out ]
                        [ Session-Timeout ]
                      * [ Reply-Message ]
                        [ Origin-State-Id ]
                      * [ Filter-Id ]
                        [ Port-Limit ]
                        [ Prompt ]
                        [ Callback-Id ]
                        [ Callback-Number ]
                      * [ Framed-Compression ]
                        [ Framed-Interface-Id ]
                        [ Framed-IP-Address ]
                      * [ Framed-Ipv6-Prefix ]
                        [ Framed-Ipv6-Pool ]
                      * [ Framed-Ipv6-Route ]
                      * [ Delegated-Ipv6-Prefix ]
                        [ Framed-IP-Netmask ]
                      * [ Framed-Route ]
                        [ Framed-Pool ]
                        [ Framed-IPX-Network ]
                        [ Framed-MTU ]
```

```
                        [ Framed-Protocol ]
                        [ Framed-Routing ]
                      * [ Login-IP-Host ]
                      * [ Login-Ipv6-Host ]
                        [ Login-LAT-Group ]
                        [ Login-LAT-Node ]
                        [ Login-LAT-Port ]
                        [ Login-LAT-Service ]
                        [ Login-Service ]
                        [ Login-TCP-Port ]
                      * [ NAS-Filter-Rule ]
                      * [ QoS-Filter-Rule ]
                      * [ Tunneling ]
                      * [ Redirect-Host ]
                        [ Redirect-Host-Usage ]
                        [ Redirect-Max-Cache-Time ]
                      * [ Proxy-Info ]
                        [ 3GPP-Ipv6-DNS-Servers ]
                      * [ External-Identifier]
                      * [ AVP ]
```

16a.4.3 ACR Command

The ACR command, defined in IETF RFC 6733 (Diameter Base) [111], is indicated by the Command-Code field set to 271 and the 'R' bit set in the Command Flags field. It is sent by the GGSN/P-GW to the Diameter server to report accounting information for a certain IP-CAN bearer (e.g. PDP context) or an IP-CAN session of a certain user.

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

The bold marked AVPs in the message format indicate optional AVPs for Gi/Sgi, or modified existing AVPs. For Sgi, some of the optional 3GPP vendor-specific AVPs listed in the message format below are not applicable. See table 9a in subclause 16a.5 to see the ones that are applicable.

Message Format:

```
<AC-Request> ::= < Diameter Header: 271, REQ, PXY >
                        < Session-Id >
                        { Origin-Host }
                        { Origin-Realm }
                        { Destination-Realm }
                        { Accounting-Record-Type }
                        { Accounting-Record-Number }
                        [ Acct-Application-Id ]
                        [ User-Name ]
                        [ Origin-State-Id ]
                        [ Destination-Host ]
                        [ Event-Timestamp ]
                        [ Acct-Delay-Time ]
                        [ NAS-Identifier ]
                        [ NAS-IP-Address ]
                        [ NAS-Ipv6-Address ]
                        [ NAS-Port ]
                        [ NAS-Port-Id ]
                        [ NAS-Port-Type ]
                      * [ Class ]
                        [ Service-Type ]
                        [ Accounting-Input-Octets ]
                        [ Accounting-Input-Packets ]
                        [ Accounting-Output-Octets ]
                        [ Accounting-Output-Packets ]
                        [ Acct-Authentic ]
                        [ Accounting-Auth-Method ]
                        [ Acct-Session-Time ]
                        [ Acct-Tunnel-Connection ]
                        [ Acct-Tunnel-Packets-Lost ]
                        [ Callback-Id ]
                        [ Callback-Number ]
                        [ Called-Station-Id ]
                        [ Calling-Station-Id ]
                      * [ Connection-Info ]
                        [ Originating-Line-Info ]
                        [ Authorization-Lifetime ]
                        [ Session-Timeout ]
```

```
                    [ Idle-Timeout ]
                    [ Port-Limit ]
                    [ Accounting-Realtime-Required ]
                    [ Acct-Interim-Interval ]
                  * [ Filter-Id ]
                  * [ NAS-Filter-Rule ]
                  * [ Qos-Filter-Rule ]
                    [ Framed-Compression ]
                    [ Framed-Interface-Id ]
                    [ Framed-IP-Address ]
                    [ Framed-IP-Netmask ]
                  * [ Framed-Ipv6-Prefix ]
                    [ Framed-Ipv6-Pool ]
                  * [ Framed-Ipv6-Route ]
                  * [ Delegated-Ipv6-Prefix ]
                    [ Framed-IPX-Network ]
                    [ Framed-MTU ]
                    [ Framed-Pool ]
                    [ Framed-Protocol ]
                  * [ Framed-Route ]
                    [ Framed-Routing ]
                  * [ Login-IP-Host ]
                  * [ Login-Ipv6-Host ]
                    [ Login-LAT-Group ]
                    [ Login-LAT-Node ]
                    [ Login-LAT-Port ]
                    [ Login-LAT-Service ]
                    [ Login-Service ]
                    [ Login-TCP-Port ]
                  * [ Tunneling ]
                  * [ Proxy-Info ]
                  * [ Route-Record ]
                    [ 3GPP-IMSI]
                    [ External-Identifier]
                    [ 3GPP-Charging-ID ]
                    [ 3GPP-PDP-Type ]
                    [ 3GPP-CG-Address ]
                    [ 3GPP-GPRS-Negotiated-QoS-Profile ]
                    [ 3GPP-SGSN-Address ]
                    [ 3GPP-GGSN-Address ]
                    [ 3GPP-IMSI-MCC-MNC ]
                    [ 3GPP-GGSN-MCC-MNC ]
                    [ 3GPP-NSAPI ]
                    [ 3GPP-Selection-Mode ]
                    [ 3GPP-Charging-Characteristics ]
                    [ 3GPP-CG-Ipv6-Address ]
                    [ 3GPP-SGSN-Ipv6-Address ]
                    [ 3GPP-GGSN-Ipv6-Address ]
                    [ 3GPP-SGSN-MCC-MNC ]
                    [ 3GPP-IMEISV ]
                    [ 3GPP-RAT-Type ]
                    [ 3GPP-User-Location-Info ]
                    [ 3GPP-MS-Time-Zone ]
                    [ 3GPP-CAMEL-Charging-Info ]
                    [ 3GPP-Packet-Filter ]
                    [ 3GPP-Negotiated-DSCP ]
                    [ TWAN-Identifier ]
                    [ 3GPP-User-Location-Info-Time ]
                  * [ AVP ]
```

16a.4.4 ACA Command

The ACA command, defined in Diameter Base (IETF RFC 6733 [111]), is indicated by the Command-Code field set to 271 and the 'R' bit cleared in the Command Flags field., It is sent by the Diameter server to the GGSN/P-GW in response to the ACR command.

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

Message Format:

```
<AC-Answer> ::= < Diameter Header: 271, PXY >
                       < Session-Id >
                       { Result-Code }
                       { Origin-Host }
```

```
                        { Origin-Realm }
                        { Accounting-Record-Type }
                        { Accounting-Record-Number }
                        [ Acct-Application-Id ]
                        [ User-Name ]
                        [ Event-Timestamp ]
                        [ Error-Message ]
                        [ Error-Reporting-Host ]
                        [ Failed-AVP ]
                        [ Origin-State-Id ]
                        [ NAS-Identifier ]
                        [ NAS-IP-Address ]
                        [ NAS-Ipv6-Address ]
                        [ NAS-Port ]
                        [ NAS-Port-Id ]
                        [ NAS-Port-Type ]
                        [ Service-Type ]
                        [ Accounting-Realtime-Required ]
                        [ Acct-Interim-Interval ]
                      * [ Class ]
                      * [ Proxy-Info ]
                      * [ Route-Record ]
                      * [ AVP ]
```

16a.4.5 STR Command

The STR command, defined in IETF RFC 6733 (Diameter Base) [111], 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/P-GW to the Diameter server to terminate a DIAMETER session corresponding to an IP-CAN session of a certain user.

The relevant AVPs that are of use for the Gi/Sgi interface are detailed in the ABNF description below. Other valid AVPs for this command are not used for Gi/Sgi 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 }
                        [ User-Name ]
                        [ Destination-Host ]
                      * [ Class ]
                        [ Origin-State-Id ]
                      * [ Proxy-Info ]
                      * [ Route-Record ]
                      * [ AVP ]
```

16a.4.6 STA Command

The STA command, defined in IETF RFC 6733 (Diameter Base) [111], is indicated by the Command-Code field set to 275 and the 'R' bit cleared in the Command Flags field. It is sent by the Diameter server to the GGSN/P-GW in response to an STR command.

The relevant AVPs that are of use for the Gi/Sgi interface are detailed in the ABNF description below. Other valid AVPs for this command are not used for Gi/Sgi 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 }
                        [ User-Name ]
                      * [ Class ]
                        [ Error-Message ]
                        [ Error-Reporting-Host ]
                        [ Failed-AVP ]
                        [ Origin-State-Id ]
```

```
                    * [ Redirect-Host ]
                      [ Redirect-Host-Usage ]
                      [ Redirect-Max-Cache-Time ]
                    * [ Proxy-Info ]
                    * [ AVP ]
```

16a.4.7 ASR Command

The Abort-Session-Request (ASR) command, defined in IETF RFC 6733 (Diameter Base) [111], is indicated by the Command-Code set to 274 and the message flags' 'R' bit set, is sent by the Diameter server to the GGSN to request that the PDP Context identified by the 3GPP-NSAPI AVP is to be terminated. The absence of the 3GPP-NSAPI AVP will indicate to the GGSN that all the PDP contexts for this particular user and sharing the same user session need to be deleted. Similarly, for P-GW, the ASR command is sent by the Diamater server to the P-GW to request that the EPS bearer identified by the 3GPP-NSAPI AVP is to be terminated. In the absence of the 3GPP-NSAPI AVP or if the value of 3GPP-NSAPI AVP points to the default EPS bearer, the P-GW shall terminate the IP-CAN session associated with the same user session.

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

The bold marked AVPs in the message format indicate optional AVPs for Gi/Sgi, or modified existing AVPs.

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 ]
                     [ 3GPP-NSAPI ]
                  *  [ Route-Record ]
                  *  [ AVP ]
```

16a.4.8 ASA Command

The Abort-Session-Answer (ASA) command, defined in IETF RFC 6733 (Diameter Base) [111], 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 Gi/Sgi interface are detailed in the ABNF description below. Other valid AVPs for this command are not used for Gi/Sgi purposes and should be ignored by the receiver or processed according to the relevant specifications.

The bold marked AVPs in the message format indicate optional AVPs for Gi/Sgi or modified existing AVPs.

Message Format:

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

The Experimental-Result AVP contains an Experimental-Result-Code AVP and will signal to the Diameter server that the IP-CAN bearer (e.g. PDP context) has been succesfully terminated as requested. See subclause 16a.6 for the description of the Experimental-Result-Code AVP.

16a.5 Gi/Sgi specific AVPs

The following table lists the Gi/Sgi specific Diameter AVPs. The Vendor-Id header of all Gi/Sgi specific AVPs defined in the present specification shall be set to 3GPP (10415).

Table 9a: Gi/Sgi specific AVPs

				AVP Flag rules					
Attribute Name	**AVP Code**	**Section defined**	**Value Type**	**Must**	**May**	**Should not**	**Must not**	**May Encr.**	**Applicable Reference Points**
3GPP-IMSI	1	16.4.7 (see Note)	UTF8String	V	P		M	Y	Gi, Sgi
3GPP-Charging-Id	2	16.4.7 (see Note)	OctetString	V	P		M	Y	Gi, Sgi
3GPP-PDP-Type	3	16.4.7 (see Note)	Enumerated	V	P		M	Y	Gi, Sgi
3GPP-CG-Address	4	16.4.7 (see Note)	OctetString	V	P		M	Y	Gi, Sgi
3GPP-GPRS-Negotiated-QoS-Profile	5	16.4.7 (see Note)	UTF8String	V	P		M	Y	Gi, Sgi
3GPP-SGSN-Address	6	16.4.7 (see note)	OctetString	V	P		M	Y	Gi, Sgi
3GPP-GGSN-Address	7	16.4.7 (see note)	OctetString	V	P		M	Y	Gi, Sgi
3GPP-IMSI-MCC-MNC	8	16.4.7 (see note)	UTF8String	V	P		M	Y	Gi, Sgi
3GPP-GGSN-MCC-MNC	9	16.4.7 (see note)	UTF8String	V	P		M	Y	Gi, Sgi
3GPP-NSAPI	10	16.4.7 (see note)	OctetString	V	P		M	Y	Gi, Sgi
3GPP-Selection-Mode	12	16.4.7 (see note)	UTF8String	V	P		M	Y	Gi, Sgi
3GPP-Charging-Characteristics	13	16.4.7 (see note)	UTF8String	V	P		M	Y	Gi, Sgi
3GPP-CG-Ipv6-Address	14	16.4.7 (see note)	OctetString	V	P		M	Y	Gi, Sgi
3GPP-SGSN-Ipv6-Address	15	16.4.7 (see note)	OctetString	V	P		M	Y	Gi, Sgi
3GPP-GGSN-Ipv6-Address	16	16.4.7 (see note)	OctetString	V	P		M	Y	Gi, Sgi
3GPP-Ipv6-DNS-Servers	17	16.4.7 (see note)	OctetString	V	P		M	Y	Gi, Sgi
3GPP-SGSN-MCC-MNC	18	16.4.7 (see note)	UTF8String	V	P		M	Y	Gi, Sgi
3GPP-IMEISV	20	16.4.7 (see Note)	OctetString	V	P		M	Y	Gi, Sgi
3GPP-RAT-Type	21	16.4.7 (see Note)	OctetString	V	P		M	Y	Gi, Sgi
3GPP-User-Location-Info	22	16.4.7 (see Note)	OctetString	V	P		M	Y	Gi, Sgi
3GPP-MS-TimeZone	23	16.4.7 (see Note)	OctetString	V	P		M	Y	Gi, Sgi
3GPP-CAMEL-Charging-Info	24	16.4.7 (see Note)	OctetString	V	P		M	Y	Gi
3GPP-Packet-Filter	25	16.4.7 (see Note)	OctetString	V	P		M	Y	Gi, Sgi
3GPP-Negotiated-DSCP	26	16.4.7 (see Note)	OctetString	V	P		M	Y	Gi, Sgi
3GPP-Allocate-IP-Type	27	16.4.7 (see Note)	OctetString	V	P		M	Y	Gi, Sgi
TWAN-Identifier	29	16.4.7 (see Note)	OctetString	V	P		M	Y	Sgi
3GPP-User-Location-Info-Time	30	16.4.7 (see Note)	OctetString	V	P		M	Y	Gi, Sgi
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.									

The information represented by some of the Sgi AVPs may not be available to the P-GW depending on the UE's radio access and the S5/S8 protocol type (GTP or PMIP). For example, the P-GW will be aware of the User Location Info (e.g. TAI) if the user is in LTE access and GTP based S5/S8 is used. However, such information is not passed to the P-GW when PMIP based S5/S8 is utilised. In such scenarios, if an Sgi specific AVP is configured in the P-GW to be transferred to the Diameter AAA server, but the information in the P-GW is not up to date or not available; the P-GW shall not send the corresponding AVP, unless otherwise stated in the AVP definitions in subclause 16.4.7.2.

16a.6 Gi/Sgi specific Experimental-Result-Code AVP

Diameter Base IETF RFC 6733 [111] 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 Gi/Sgi specific AVPs, new application results can occur and the Experimental-Result AVP is used to transfer the 3GPP-specific result codes. The Experimental-Result AVP is a grouped AVP containing the Vendor-Id AVP set to the value of 3GPP's vendor identifier (10415) and an Experimental-Result-Code AVP.

The following Gi/Sgi specific Experimental-Result-Code value is defined:

DIAMETER_PDP_CONTEXT_DELETION_INDICATION (2021)

For GGSN this is an indication to the server that the requested PDP Context or IP-CAN session has been deleted.

For P-GW this is an indication to the server that the requested bearer or IP-CAN session has been deleted.

16a.7 Gi/Sgi re-used AVPs

Table 9b lists the Diameter AVPs re-used by the Gi/Sgi reference point from existing Diameter Applications, reference to the respective specifications and a short description of the usage within the Gi/Sgi reference point.

Table 9b: Gi/Sgi re-used Diameter AVPs

Attribute Name	Reference	Description
External-Identifier	3GPP TS 29.336 [101]	A globally unique identifier of a UE used towards external servers instead of IMSI and MSISDN, refer to 3GPP TS 23.682 [100] and 3GPP TS 23.003 [40].

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, session update 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].
- to receive indication if IP multicast distribution to UTRAN should be used for the MBMS user plane data.

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.

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 IETF RFC 6733 [111], 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 / update/ 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 start shall also be used by the BM-SC to indicate to GGSN if IP multicast mechanism should be used for user plane data distribution to UTRAN.

The MBMS session update shall be used by the BM-SC to trigger the update of MBMS session attributes in the affected GGSNs.

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

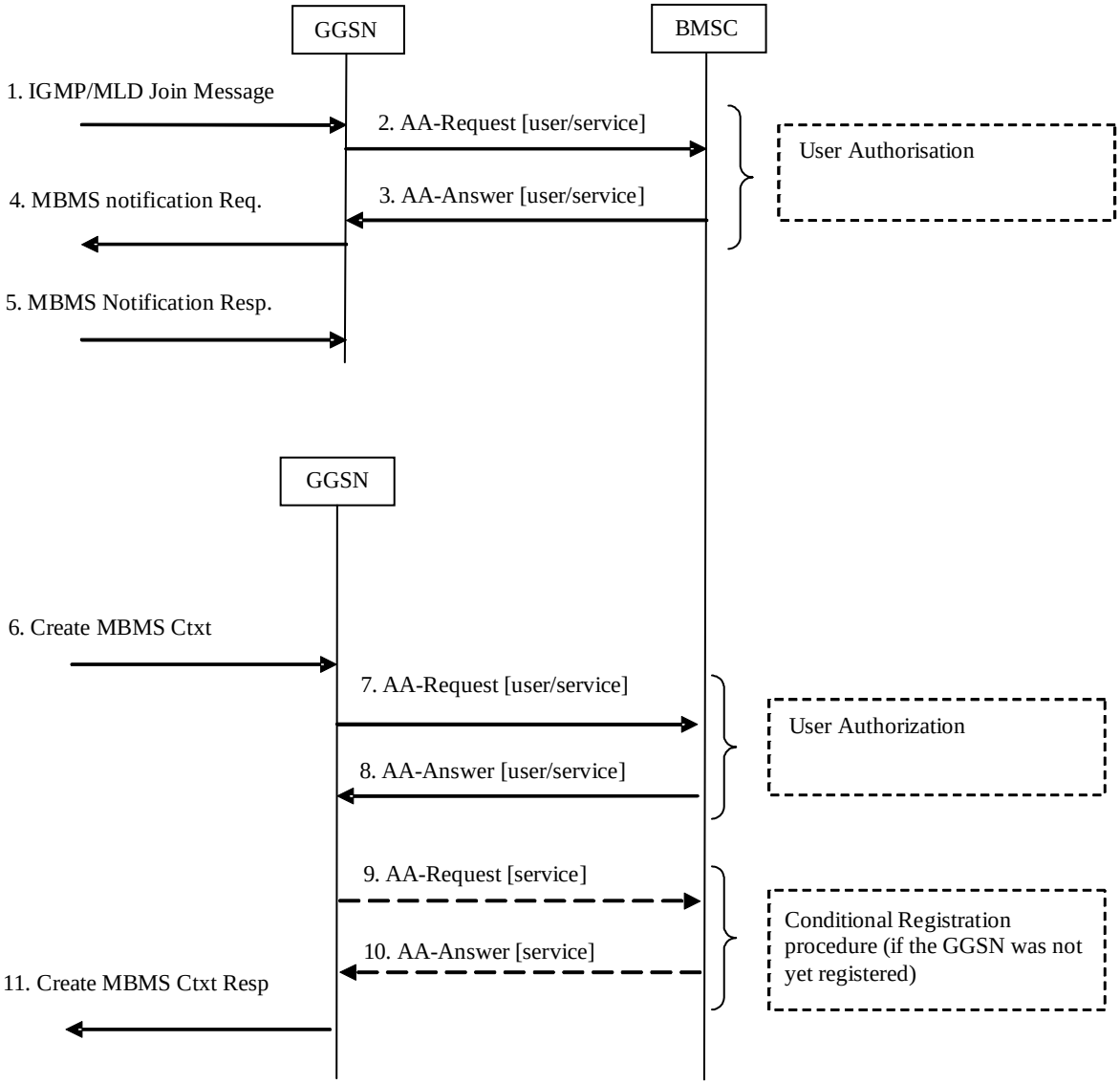


Figure 26; Activation of an MBMS multicast service

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.

BM-SC and GGSN shall at least support IP unicast encapsulation of IP multicast datagrams, which shall be default mode of sending user plane data. BM-SC may support sending user plane IP multicast datagrams to GGSN, and GGSN also may support this mode of operation.

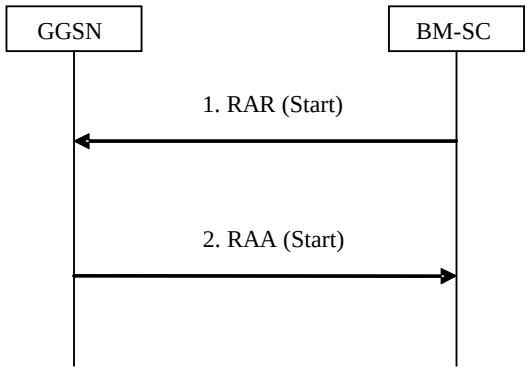


Figure 27: MBMS Session Start procedure

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. BM-SC may indicate to GGSN that BM-SC supports sending the user plane IP multicast data without IP unicast encapsulation. In such case BM-SC shall send multicast source address as specified by IETF RFC 4604 [73] and IETF RFC 4607 [74]. The BM-SC sets the state attribute of its MBMS Bearer Context to ‘Active’. By sending "CN IP Multicast Distribution" parameter to GGSN, the BM-SC indicates if IP multicast mechanism should be used for user plane data distribution to UTRAN. "MBMS HC Indicator" parameter, if present, indicates that a header compression is used for MBMS user plane data.

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. In case GGSN receives BM-SC multicast source address, which indicates BM-SC support for both modes of sending user plane data, GGSN decides in which mode GGSN shall receive the user plane data. In case GGSN decides to receive unicast encapsulated data, then GGSN shall send own IP address and UDP port for the encapsulating unicast IP and UDP layer of the user plane to BM-SC. In case GGSN decides to receive IP multicast packets, then GGSN shall join the multicast group as specified by IETF RFC 4604 [73] and IETF RFC 4607 [74], and indicate to BM-SC about the decision.

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.

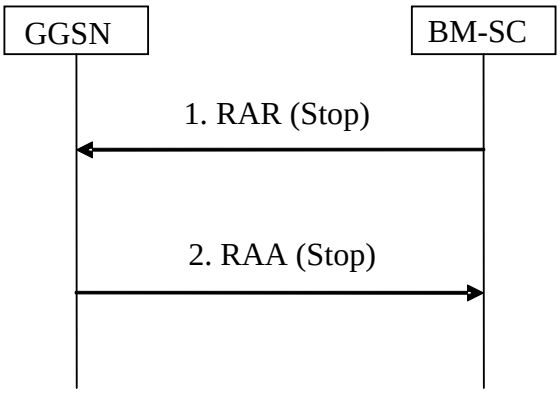


Figure 28: MBMS Session Stop procedure

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.

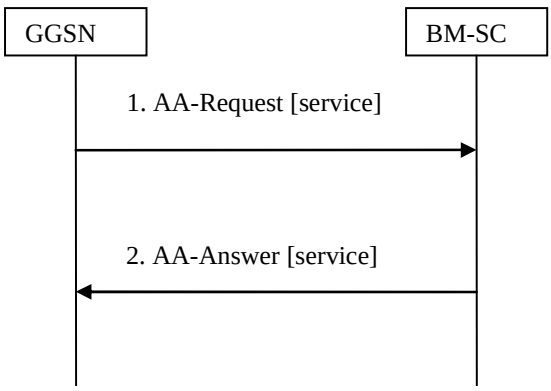


Figure 29: MBMS Registration procedure

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.

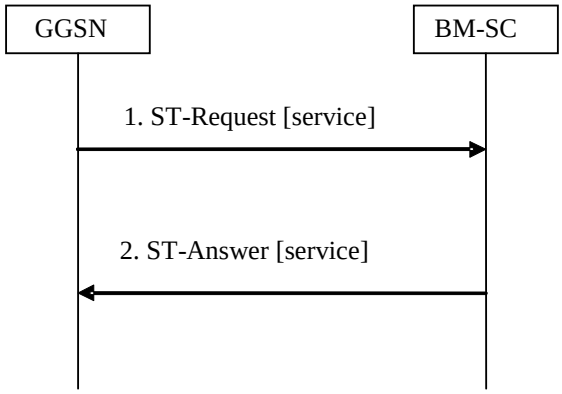


Figure 30: MBMS De-Registration procedure

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.

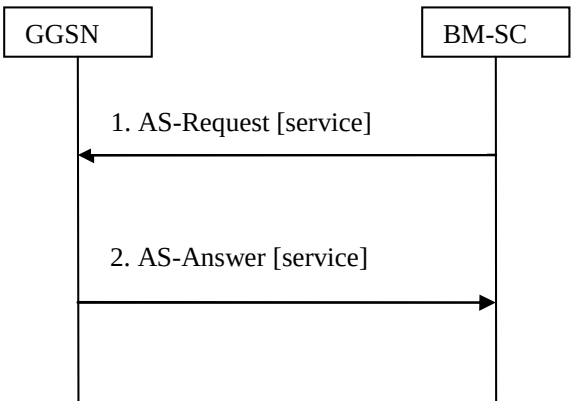


Figure 31: MBMS De-Registration procedure BM-SC initiated

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.

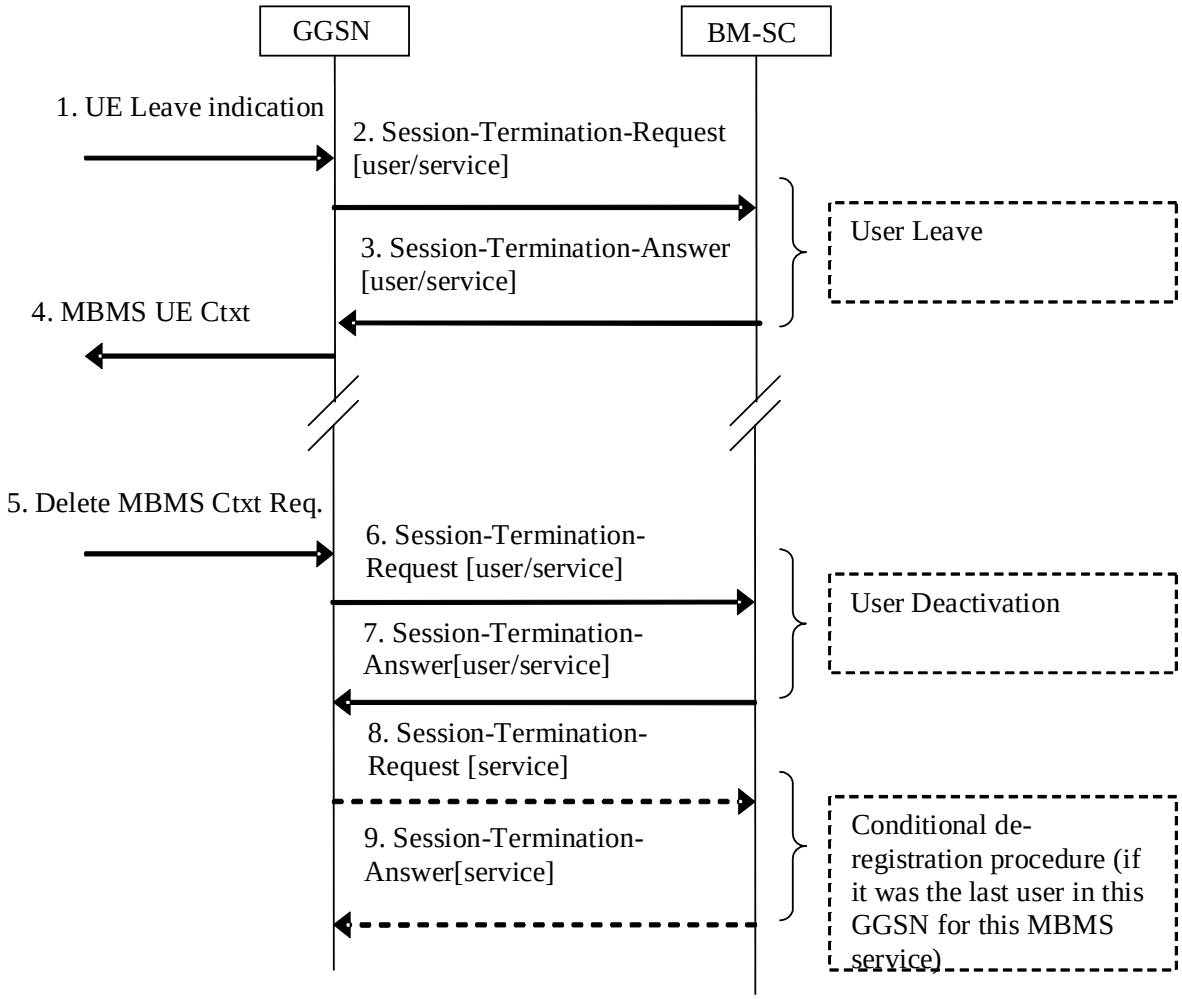


Figure 32: MBMS Service deactivation procedure

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.

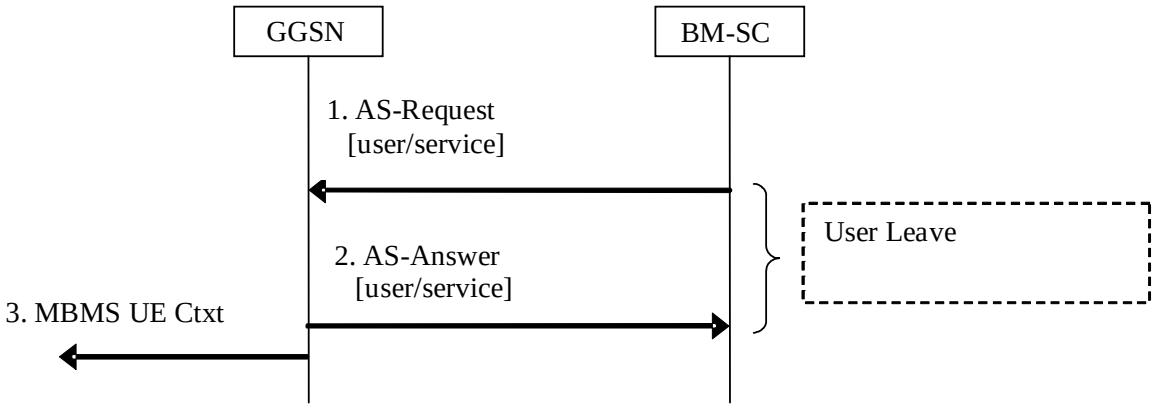


Figure 32a: BM-SC initiated MBMS Service deactivation procedure

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.

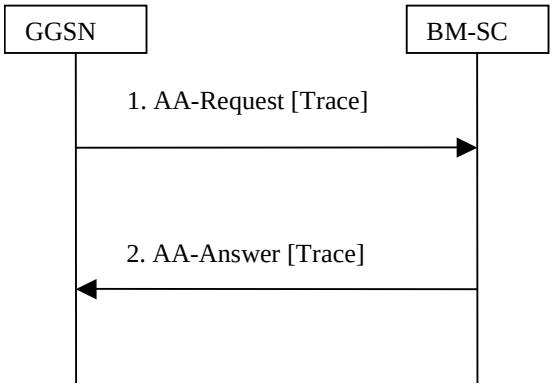


Figure 33: Trace Session Activation procedure

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.

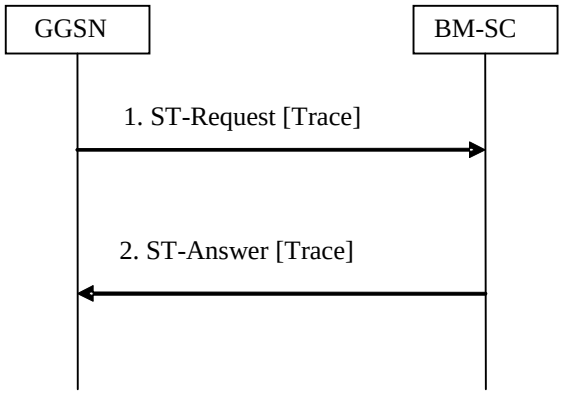


Figure 34: Trace Session Deactivation procedure

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 TS 23.246 [65] and 3GPP TS 29.060 [24]. GGSN shall pass the relevant data via the Gmb interface to enable the BM-SC to update its MBMS UE context accordingly.

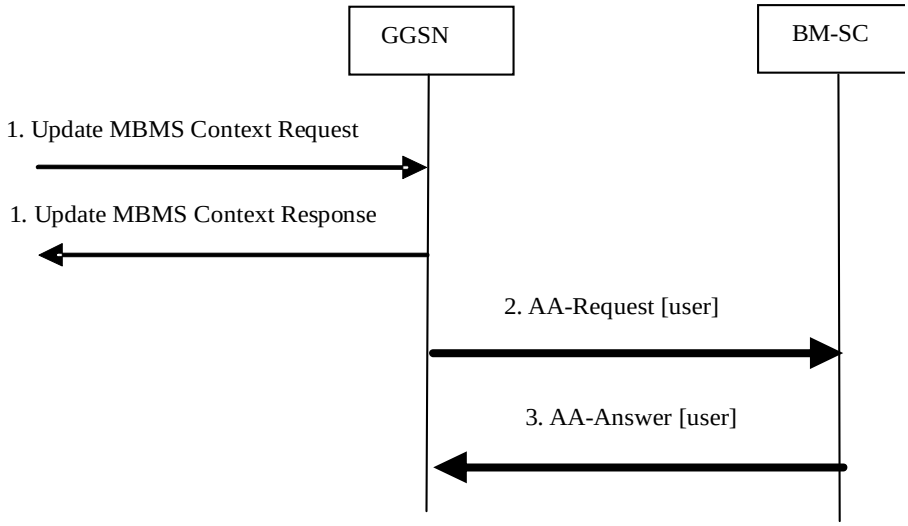


Figure 35; Modification of an MBMS UE Context in BM-SC

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).

17.5.11 Session Update Procedure

The BM-SC initiates the MBMS session update procedure when the service area for an ongoing MBMS session shall be modified. This procedure is defined only for MBMS broadcast services. The MBMS session update procedure is initiated towards one or more of the GGSNs in the list of downstream nodes in the BM-SC, according to the changes in the service area.

NOTE: In addition, when the MBMS Service Area for an ongoing broadcast session is changed in the BM-SC, then GGSN(s) may be added to, or removed from, the list of downstream nodes in the BM-SC. The BM-SC will initiate MBMS session start procedures or MBMS session stop procedures towards these GGSNs accordingly.

The attributes that can be modified by the session update procedure are the MBMS Service Area, and the list of downstream nodes for GGSN.

When a session update message is received , GGSN will update its MBMS Bearer Context accordingly and inform its downstream SGSNs of the changed MBMS service area. If a list of downstream SGSNs is included in the session update message, GGSN shall initiate a session start procedure towards the new downstream SGSNs, and a session stop procedure towards the SGSNs that have been removed from the list.

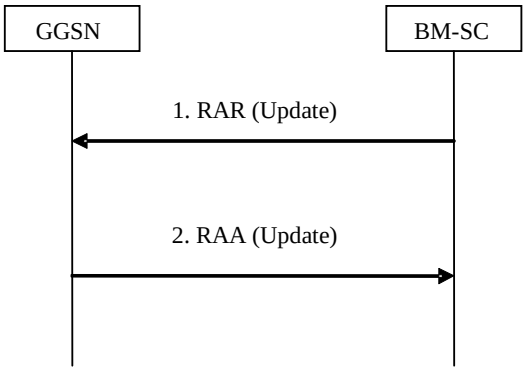


Figure 27: MBMS Session Update procedure

1. The BM-SC sends a RAR message to the GGSNs that need to update its session attributes.
2. GGSN stores the updated session attributes in the MBMS Bearer Context, initiates session start, session stop or session update procedures towards the SGSNs in its list of downstream nodes and sends an RAA message to the BM-SC. An AAR message is not mandated for the Gmb application in response to a RAR-RAA command exchange.

17.5.12 MBMS broadcast session termination (GGSN initiated)

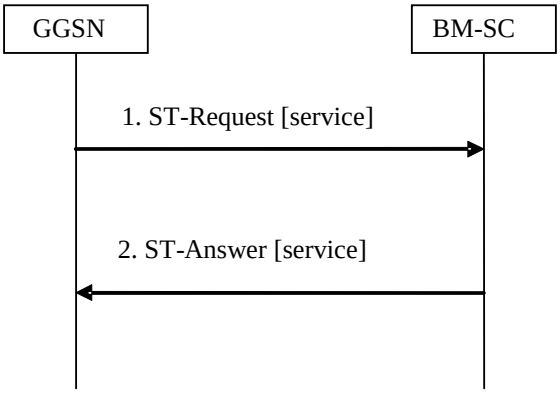


Figure 36: Broadcast session termination

1. In exceptional cases (e.g. resource pre-emption or timeout of the MBMS session), the GGSN may send an STR command to the BM-SC to initiate the termination of the Diameter session related to a broadcast MBMS bearer service. 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 Diameter session and confirms the operation by sending an STA message to the GGSN.

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 and Framed-Interface-Id 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, 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-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 each time an AAR command is sent, except for the case when the AAR is sent to modify an existing MBMS UE Context in the BM-SC.

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 acknowledge 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-IMSI]
                        [ TMGI ]
                        [ Required-MBMS-Bearer-Capabilities ]
```

17.6.3 STR Command

The STR command, defined in IETF RFC 6733 (DIAMETER BASE) [111], 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.

A DIAMETER session for a broadcast MBMS service may be terminated by the GGSN in exceptional cases.

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 RFC 6733 (DIAMETER BASE) [111], 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 (e.g. 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 RFC 6733 (DIAMETER BASE) [111], 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 ]
                    [ MBMS-Required-QoS ]
                    [ MBMS-Session-Duration ]
                    [ MBMS-Service-Type ]
                    [ MBMS-Counting-Information ]
                    [ MBMS-Session-Identity ]
                    [ MBMS-Session-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 ]
                    [ MBMS-User-Data-Mode-Indication ]
                    [ MBMS-BMSC-SSM-IP-Address ]
                    [ MBMS-BMSC-SSM-Ipv6-Address ]
                    [ MBMS-Flow-Identifier ]
                    [ CN-IP-Multicast-Distribution ]
                    [ MBMS-HC-Indicator ]
```

```
   [ Origin-State-Id ]
*  [ Proxy-Info ]
*  [ Route-Record ]
```

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

The Diameter Session-Id is used in subsequent procedures to identify the corresponding MBMS session.

In the multicast case, the BM-SC shall use the Diameter Session-Id that was received during the GGSN Registration procedure. In the broadcast case, the BM-SC shall allocate a Diameter Session-Id for the first RAR message that is used for the first MBMS Session Start procedure of the MBMS bearer service. Then this Diameter Session-Id will be used for the subsequent MBMS sessions of the same MBMS bearer service. The BM-SC will create a new Diameter Session-Id for a subsequent Session Start procedure if, in exceptional cases, the Diameter session for the MBMS bearer service has been deleted.

BM-SC shall not initiate a new Session Start procedure for a certain MBMS bearer service until the previous MBMS session for that service has been stopped.

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 the MBMS Session Update procedure, RAR is sent by the BM-SC in order for the GGSN(s) to update their session attributes. The updated MBMS-Service-Area AVP shall be included. The MBMS-StartStop-Indication AVP with the value UPDATE shall be included. The MBMS-Time-To-Data-Transfer with the value set to 0 shall be included. The MBMS-Session-Duration AVP shall be included to indicate the duration of the remaining part of the MBMS session. The 3GPP-SGSN-Address AVP and the 3GPP-SGSN-Ipv6-Address AVP shall be included if the related lists of downstream nodes in the GGSN(s) have changed. The other bold marked AVPs shall be included as given by the previous, corresponding MBMS Session Start procedure.

For the 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.

For the MBMS Session Start procedure, the MBMS-Required-QoS indicates the QoS that is required for the MBMS bearer service for the actual MBMS session. The information of the MBMS-2G-3G-Indicator, the MBMS-Service-Area and the MBMS-Counting-Information 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.

According to 3GPP TS 23.246 [65], the MBMS-Flow-Identifier is optional, used only for broadcast services with location dependent content. For such services, several sessions with the same TMGI, but different MBMS-Flow-Identifiers, may be going on in parallel. However, at any specific location only one version of the content may be available at any point in time. Hence, the MBMS-Service-Areas of the related MBMS bearer contexts shall not overlap.

17.6.6 RE-Auth-Answer Command

The Re-Auth-Answer (RAA) command, defined in IETF RFC 6733 (DIAMETER BASE) [111], 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 ]
             [ MBMS-GGSN-Address ]            ; for unicast encapsulated user data
             [ MBMS-GGSN-Ipv6-Address ]       ; for unicast encapsulated user data
             [ MBMS-GW-UDP-Port]              ; for unicast encapsulated user data
             [ MBMS-User-Data-Mode-Indication ]
             [ Origin-State-Id ]
             [ Error-Message ]
             [ Error-Reporting-Host ]
             [ Failed-AVP ]
           *  [ Redirected-Host ]
             [ Redirected-Host-Usage ]
             [ Redirected-Host-Cache-Time ]
           *  [ Proxy-Info ]
```

If multicast user plane data are to be sent to the GGSN using IP unicast, the GGSN shall allocate an IP transport address and a separate UDP port for each MBMS bearer (i.e the service uniquely identified by its TMGI and Flow ID and provided by the GPRS to deliver the same IP datagrams to multiple receivers in a designated location). The GGSN shall then use the destination unicast IP address and destination UDP port of user plane packets received over the Gi interface to determine on which MBMS bearer to forward the received user plane packet.

17.6.7 Abort-Session-Request Command

The Abort-Session-Request (ASR) command, defined in IETF RFC 6733 (DIAMETER BASE) [111], 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 RFC 6733 (DIAMETER BASE) [111], 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

17.7.0 General

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	OctetString	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	OctetString	M,V	P			Y
MBMS-Session-Duration	904	17.7.7	OctetString	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)	OctetString	M, V	P			Y
3GPP-SGSN-Ipv6-Address	15	16.4.7 (see note)	OctetString	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-Repetition-Number	912	17.7.15	OctetString	M.V	P			Y
MBMS-Required-QoS	913	17.7.16	UTF8String	M.V	P			Y
MBMS-Counting-Information	914	17.7.17	Enumerated	M.V	P			Y
MBMS-User-Data-Mode-Indication	915	17.7.18	Enumerated	M.V	P			Y
MBMS-GGSN-Address	916	17.7.19	OctetString	M.V	P			Y
MBMS-GGSN-Ipv6-Address	917	17.7.20	OctetString	M.V	P			Y
MBMS-BMSC-SSM-IP-Address	918	17.7.21	OctetString	M.V	P			Y
MBMS-BMSC-SSM-Ipv6-Address	919	17.7.22	OctetString	M.V	P			Y
MBMS-Flow-Identifier	920	17.7.23	OctetString	M,V	P			Y
CN-IP-Multicast-Distribution	921	17.7.24	Enumerated	M,V	P			Y
MBMS-HC-Indicator	922	17.7.25	Enumerated	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 6733 [111].

17.7.1 3GPP-Vendor-Specific AVP

Void.

17.7.2 TMGI AVP

The TMGI AVP (AVP code 900) is of type OctetString, and contains the Temporary Mobile Group Identity allocated to a particular MBMS bearer service. It is allocated by the BM-SC. The encoding of TMGI is specified in 3GPP TS 24.008 [54]. When allocating the TMGI, BM-SC shall always include the MCC and MNC in the TMGI.

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 MBMS bearer capabilities 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 an MBMS session start procedure.

STOP (1)

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

UPDATE (2)

The message containing this AVP is indicating an MBMS session update procedure.

HEARTBEAT (3)

The message containing this AVP is indicating an MBMS heartbeat 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. The AVP consists of the following parts:

Octet	
1	Number N of MBMS service area codes coded as: 1 binary value is '00000000' 256 binary value is '11111111'
2-(2N+1)	A consecutive list of N MBMS service area codes

The MBMS service area code represents the coding for the MBMS Service Area Identity.

The MBMS Service Area Identity and its semantics are defined in subclause 15.3 of 3GPP TS 23.003 [40].

The length of an MBMS service area code is 2 octets.

Each MBMS service area code shall only be present once in the list.

17.7.7 MBMS-Session-Duration AVP

The MBMS-Session-Duration AVP (AVP code 904) is of type OctetString with a length of three octets and indicates the estimated session duration (MBMS Service data transmission). Bit 8 of octet 1 to bit 8 of octet 3 (17 bits) express seconds, for which the maximum allowed value is 86400 seconds. Bits 7 to 1 of octet 3 (7 bits) express days, for which the maximum allowed value is 18 days. The coding is as follows (the 's' bits represent the seconds, the 'd' bits represent the days):

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1	s	s	s	s	s	s	s	s
2	s	s	s	s	s	s	s	s
3	s	d	d	d	d	d	d	d

For the whole session duration the seconds and days are added together and the maximum session duration is 19 days.

The lowest value of this AVP (i.e. all 0'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].

Its value shall be encoded as a UTF-8 string on either 11 (if the MNC contains two digits) or 12 (if the MNC contains three digits) octets as follows:

- The MCC shall be encoded first using three UTF-8 characters on three octets, each character representing a decimal digit starting with the first MCC digit.
- Then, the MNC shall be encoded as either two or three UTF-8 characters on two or three octets, each character representing a decimal digit starting with the first MNC digit.
- The Location Area Code (LAC) is encoded next using four UTF-8 characters on four octets, each character representing a hexadecimal digit of the LAC which is two binary octets long.
- The Routing Area Code (RAC) is encoded last using two UTF-8 characters on two octets, each character representing a hexadecimal digit of the RAC which is one binary octet long.

NOTE: As an example, a RAI with the following information: MCC=123, MNC=45, LAC=41655(0xA2C1) and RAC=10(0x0A) is encoded within the RAI AVP as a UTF-8 string of "12345A2C10A".

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-Repetition-Number AVP

The MBMS-Session-Repetition-Number AVP (AVP code 912) is of type OctetString with a length of one octet. It contains the session identity repetition number of the MBMS transmission session on the Gmb interface. The value 0 indicates the first transmission of a session. The values 1 to 255 represents the retransmission sequence number of a session. 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-Repetition-Number AVP, and vice versa.

17.7.16 MBMS-Required-QoS AVP

The MBMS-Required-QoS AVP (AVP code 913) is the quality of service required for the MBMS bearer service. It is specified as UTF8String with the following encoding:

Octet	
1	Allocation/Retention Priority as specified in 3GPP TS 23.107 [71]. This octet encodes each priority level defined in 3GPP TS 23.107 [71] as the binary value of the priority level. It specifies the relative importance of the actual MBMS bearer service compared to other MBMS and non-MBMS bearer services for allocation and retention of the MBMS bearer service.
2-N	QoS Profile as specified by the Quality-of-Service information element, from octet 3 onwards, in 3GPP TS 24.008 [54].

17.7.17 MBMS-Counting-Information AVP

The MBMS-Counting-Information AVP (AVP code 914) is of type Enumerated, and contains explicit information about whether the MBMS Counting procedures are applicable for the MBMS Service that is about to start. See 3GPP TS 25.346 [72].

This AVP is only valid for UTRAN access type.

The following values are supported:

COUNTING-NOT-APPLICABLE (0)

The MBMS Session Start Procedure signalled by the BM-SC is for a MBMS Service where MBMS Counting procedures are not applicable.

COUNTING-APPLICABLE (1)

The MBMS Session Start Procedure signalled by the BM-SC is for a MBMS Service where MBMS Counting procedures are applicable.

17.7.18 MBMS-User-Data-Mode-Indication AVP

The MBMS-User-Data-Mode-Indication AVP (AVP code 915) is of type Enumerated. The meaning of the message containing this AVP depends on the sending entity. The absence of this AVP indicates unicast mode of operation.

The following values are supported:

Unicast (0)

When BM-SC sends this value, that indicates to GGSN that BM-SC supports only unicast mode (IP multicast packets encapsulated over UDP by IP unicast header).

When GGSN sends this value, that indicates to BM-SC that BM-SC shall send user plane data with unicast mode (IP multicast packets encapsulated over UDP by IP unicast header).

Multicast and Unicast (1)

When BM-SC sends this value, that indicates to GGSN that BM-SC supports both modes of operation.

When GGSN sends this value, that indicates to BM-SC that BM-SC shall send user plane data with multicast mode.

17.7.19 MBMS-GGSN-Address AVP

The MBMS-GGSN-Address AVP (AVP code 916) is of type OctetString, and contains the value of GGSN's Ipv4 address for user plane data. Ipv4 only or dual stack GGSN includes this AVP in case BM-SC requests GGSN's user plane unicast address.

17.7.20 MBMS-GGSN-Ipv6-Address AVP

The MBMS-GGSN-Ipv6-Address AVP (AVP code 917) is of type OctetString, and contains the value of GGSN's Ipv6 address for user plane data. Dual stack GGSN includes this AVP in case BM-SC requests GGSN's user plane unicast address.

17.7.21 MBMS-BMSC-SSM-IP-Address AVP

The MBMS-BMSC-SSM-IP-Address AVP (AVP code 918) is of type OctetString, and contains the value of BM-SC's Ipv4 address for Source Specific Multicasting. Ipv4 only or dual stack BM-SC includes this AVP.

17.7.22 MBMS-BMSC-SSM-Ipv6-Address AVP

The MBMS-BMSC-SSM-Ipv6-Address AVP (AVP code 919) is of type OctetString, and contains the value of BM-SC's Ipv6 address for Source Specific Multicasting. Dual stack BM-SC includes this AVP.

17.7.23 MBMS-Flow-Identifier AVP

The MBMS-Flow-Identifier AVP (AVP code 920) is of type OctetString. Its length is two octets. It represents a location dependent subflow of a broadcast MBMS bearer service. When present, the MBMS-Flow-Identifier together with the TMGI uniquely identify an MBMS Bearer Context.

17.7.24 CN-IP-Multicast-Distribution AVP

CN-IP-Multicast-Distribution AVP (AVP code 921) is of type Enumerated. It represents an indication if IP multicast distribution to UTRAN should be used for the MBMS user plane data. The following values are supported:

NO-IP-MULTICAST (0)

Value 0 indicates that IP multicast distribution of MBMS user plane data to UTRAN shall not be used.

IP-MULTICAST (1)

Value 1 indicates that MBMS user plane data to UTRAN should be delivered by IP multicast mechanism.

17.7.25 MBMS-HC-Indicator AVP

MBMS-HC-Indicator AVP (AVP code 922) is of type Enumerated. It represents an indication if header compression is used by BM-SC when sending for MBMS user plane data. The enumeration values are defined in 3GPP TS 25.413 [92].

17.7a Gmb re-used AVPs

Table 17.7a.1 lists the Diameter AVPs re-used by the Gmb reference point from other existing Diameter Application, reference to their respective specifications and short description of their usage witin the Gmb reference point. Other AVPs from existing Diameter Applications, except for the AVPs from Diameter base protocol, do not need to be supported. The AVPs from Diameter base protocol are not included in table 17.7a.1, but they are re-used for the Gmb reference point. Unless otherwise stated, re-used AVPs shall maintain their 'M', 'P' and 'V' flag settings. Where RADIUS VSAs are re-used, they shall be translated to Diameter AVPs as described in IETF RFC 4005 [67] with the exception that the 'M' flag shall be set and the 'P' flag may be set.

Table 17.7a.1: Gmb re-used Diameter AVPs

Attribute Name	Reference	Description
MBMS-GW-UDP-Port	Clause 20.5a.5	A transport layer UDP port allocated at the GGSN to receive multicast datagrams encapsulated in unicast IP/UDP encapsulation.

17.8 Gmb specific Experimental-Result-Code AVP values

17.8.0 General

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 IETF RFC 6733 [111] specific procedures. Application errors, on the other hand, generally occur due to a problem with a function specified in a Diameter application.

Diameter Base IETF RFC 6733 [111] 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 IETF RFC 6733 [111], 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 IETF RFC 6733 [111] 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 IETF RFC 6733 [111] are applicable. Also the following specific Gmb Experimental-Result-Code values are defined for permanent failures:

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.

17.8.3 Transient Failures

Errors that fall within the transient failures category are used to inform a peer that a request could not be satisfied at the time it was received, but it may be satisfied in the future.

The Result-Code AVP values defined in Diameter Base IETF RFC 6733 [111] are applicable. Also the following specific Gmb Experimental-Result-Code value is defined for transient failures:

DIAMETER_ERROR_OUT_OF_RESOURCES (4121)

This error covers the case when a MBMS Session Start procedure could not be performed due to a temporary resource shortage in the GGSN. The BM-SC may re-try later.

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.

19 Usage of Diameter on Mz interface

19.1 Introduction

3GPP TS 23.246 [65] specifies that when MBMS bearers are used to provide MBMS user services to roaming users, three specific scenarios are used.

One uses a GGSN in the Home PLMN, which is not related to Mz interface. The other two are enabled by use of the Mz interface for multicast services and are further described below.

Mz is the roaming variant of the Gmb reference point with the same functionality as decribed under Gmb, i.e. with MBMS bearer and user specific signalling. The support of Mz with in BM-SC is needed for MBMS roaming scenario. Mz interface is defined between the visited BM-SC and the home BM-SC.

MBMS bearer and user specific Mz signalling is used between a BM-SC in the visited PLMN and a BM-SC in the home PLMN when MBMS services from the home PLMN are offered by the visited PLMN.

User specific signalling is used between a BM-SC in the visited PLMN and a BM-SC in the home PLMN when the visited PLMN offers MBMS user service to roaming users. This user specifice Mz signalling provides home PLMN authorisation for MBMS user service that are provided by the visited PLMN.

Mz may use proxy capabilities as described for Gmb, e.g. to proxy signalling between BM-SCs.

19.2 Call flows in roaming scenarios

The procedures described in clause 17 of the present specification: Session Start procedure (clause 17.5.2), Session Stop procedure (clause 17.5.3), Registration procedure (clause 17.5.4), De-registration procedure (GGSN initiated) (clause 17.5.5), De-registration procedure (BM-SC initiated) (clause 17.5.6), Trace Session Activation procedure (clause 17.5.8), Trace Session Deactivation procedure (clause 17.5.9), MBMS UE Context Modification procedure (clause 17.5.10), and Session Update procedure (clause 17.5.11) work exactly the same in roaming scenarios, i.e when the GGSN is in a visited PLMN and the BM-SC is in the home PLMN, and they are Gmb procedures only and are not needed over Mz interface.

Service activation procedures and Service deactivation procedures are the only procedures over Mz interface, and are described in detail in the following subclauses.

19.2.1 Service activation

19.2.1.1 Service Provided by the BM-SC in Home PLMN

A visited PLMN may offer to roaming users MBMS user services from their home PLMN. For this case, the PDP connection, which will be used for the JOIN step, may be from the UE to the visited GGSN due to operator policy or routing optimization. Then the authorization is done in the BM-SC in visited PLMN with the authorization information retrieved from the BM-SC in home PLMN.

Whether GGSN of home or visited PLMN would be used is based on the operator policy, or agreement between PLMNs.

The MBMS user traffic is provided by the BM-SC in home PLMN and proxyed.

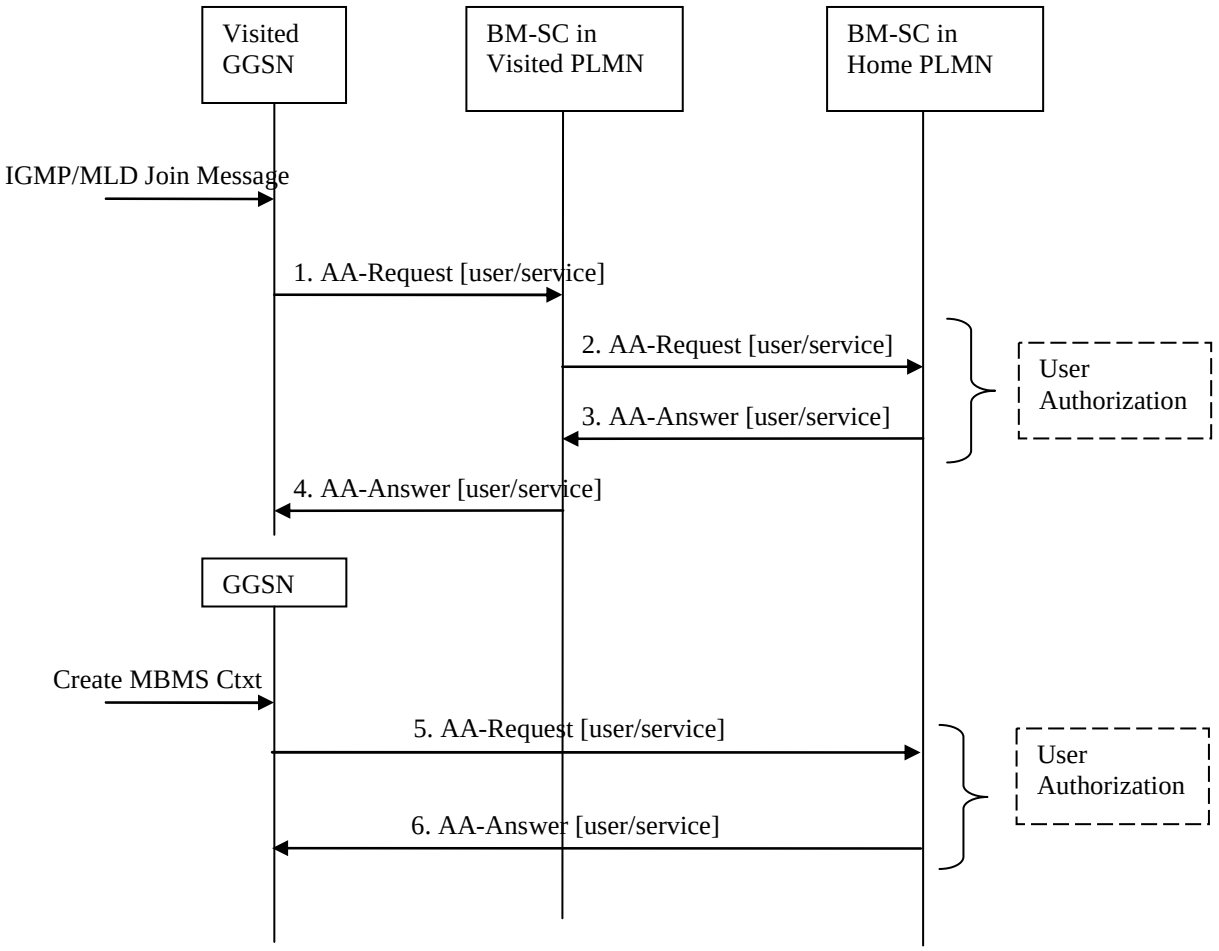


Figure 28: Activation of an MBMS multicast service in roaming scenario with service provided in the home PLMN

1. The GGSN sends an AAR to the BM-SC in visited PLMN seeking authorizationt for the activating roaming UE to receive data from a particular service.

2. The BM-SC in visited PLMN finds the BM-SC in home PLMN which will serve the roaming UE based on the multicast IP address, and identity of the user, and sends the AAR to it for the roaming UE to receive data from a 148orrection service.

3. The authorization decision is provided from BM-SC in home PLMN in the AAA to BM-SC in visited PLMN. An APN may be included in the signalling between BM-SCs, which indicates a GGSN in home PLMN which will serve the UE for the specific MBMS service. The BM-SC in the visit network may modify the APN based on the operator policy or agreement between PLMNs.

4. The authorization decision, as received from BM-SC in home PLMN, is provided in the AAA to GGSN together with the APN to be used for creation of the MBMS UE Context If the AAA indicates that the roaming UE is not authorized to receive the MBMS data the process terminates with no additional message exchange.

   Whether GGSN of home or visited PLMN would be used is based on the operator policy, or agreement between PLMNs, for example, the visited BM-SC may modify the APN from the home BM-SC according to configuration of operator policy.

5. The GGSN sends an AAR seeking authorization for the activating UE to BM-SC in home PLMN. This GGSN may be different from the GGSN that receives IGMP join message.

6. The authorization decision is provided in the AAA to GGSN.

19.2.1.2 Service Provided by the BM-SC in visited PLMN

When visited and home PLMN support the same classes of MBMS user services, a visited PLMN may offer its own MBMS user services to roaming users. In this case, the authorization is done in the BM-SC in visited PLMN with the authorization information retrieved from the BM-SC in home PLMN. Then the MBMS user traffic is provided by the BM-SC in visited PLMN.

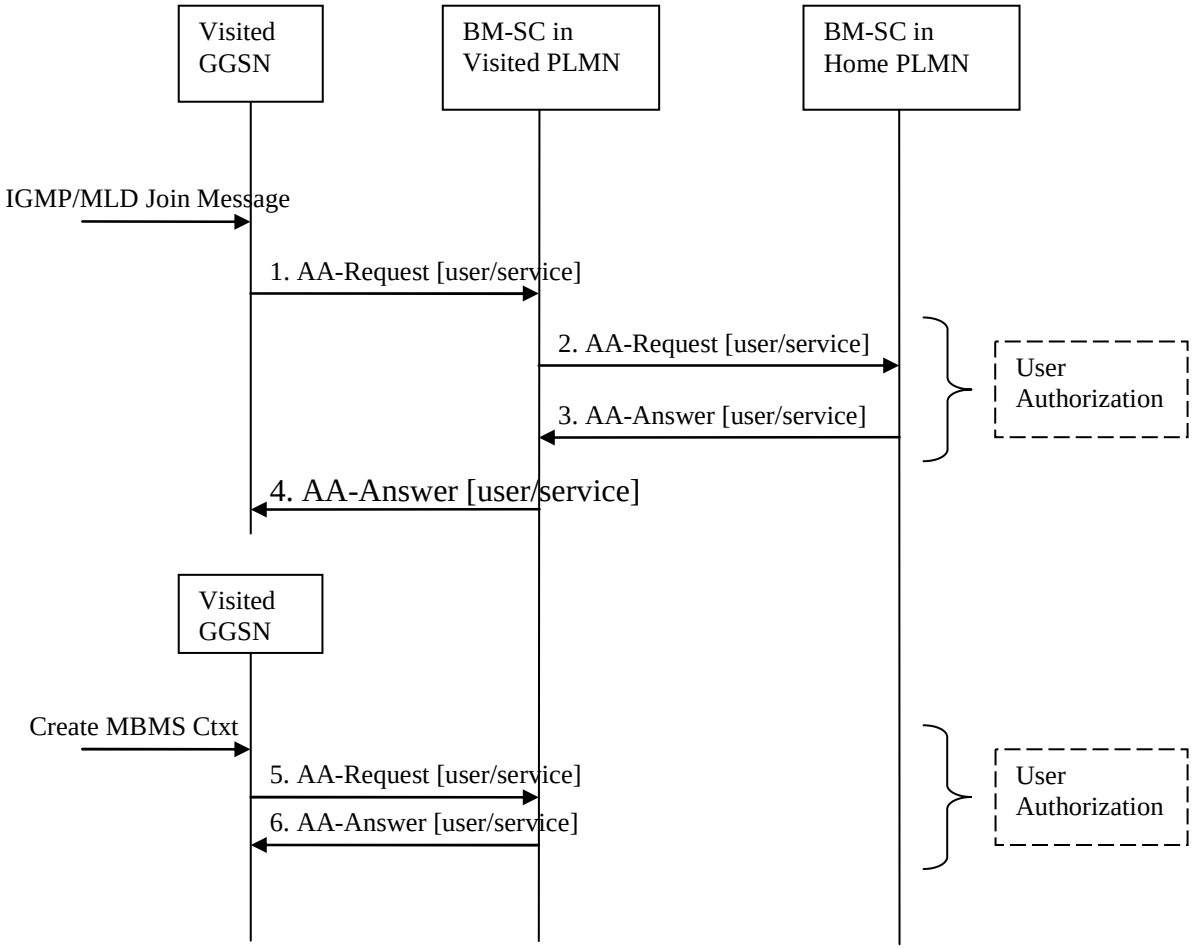


Figure 29: Activation of an MBMS multicast service in roaming scenario with service provided in the visited PLMN

1. The GGSN sends an AAR to the BM-SC in visited PLMN seeking authorizationt information for the activating roaming UE to receive data from a particular service.
2. The BM-SC in visited PLMN finds the BM-SC in home PLMN which have the authorization information for the roaming UE based on the multicast IP address, and identity of the user, and sends the AAR to it for the roaming UE to receive authorization from a 149orrection service.
3. The authorization decision is provided from BM-SC in home PLMN in the AAA to BM-SC in visited PLMN.
4. The authorization decision, as received from BM-SC in home PLMN, is provided in the AAA to GGSN together with the APN to be used for creation of the MBMS UE Context If the AAA indicates that the roaming UE is not authorized to receive the MBMS data the process terminates with no additional message exchange.
5. The GGSN sends an AAR seeking authorization for the activating UE to BM-SC in visited PLMN. This GGSN may be different from the GGSN that receives IGMP join message.
6. The authorization decision is provided in the AAA to GGSN.

19.2.2 Service deactivation

19.2.2.1 Service Provided by the BM-SC in home PLMN

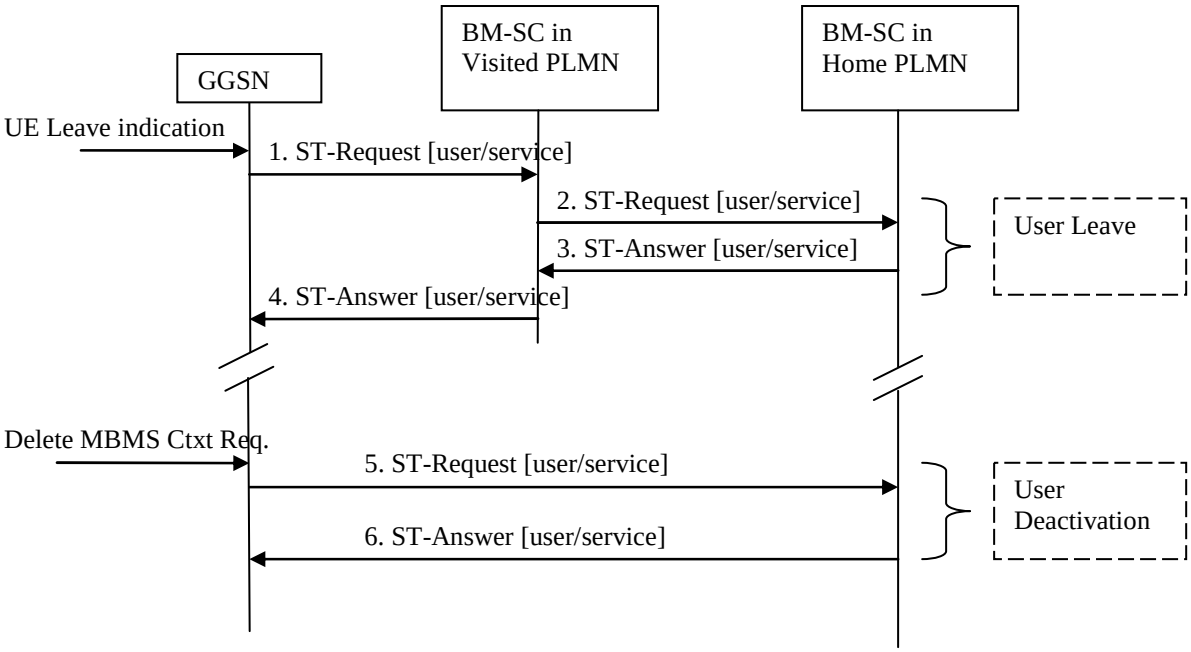


Figure 30: Deactivation of an MBMS multicast service in roaming scenario with service provided in the home PLMN

1. Upon receiving the leave indication, the GGSN sends an STR to the BM-SC in visited PLMN, indicating that the roaming UE is requesting to leave the multicast service. The session to be terminate is uniquely identified by the Diameter session-id.

2. Upon reception of the STR, the BM-SC in visited PLMN finds the BM-SC in home PLMN which serves the roaming UE, and sends an STR to it for the roaming UE to deactivate a particular service.

3. Upon reception of the STR, the BM-SC in home PLMN verifies that the IP multicast address corresponds to a valid MBMS bearer service and responds the BM-SC in visited PLMN with an ST-Answer. The APN shall be the same that was provided during service activation.

4. Upon reception of the STA, the BM-SC in visited PLMN sends an STA to the GGSN that orignated the Leave Indication.

5. The GGSN which is used to establish the MBMS bearer service deletes the MBMS UE Context and sends an STR to the BM-SC in home PLMN to confirm the successful deactivation of the MBMS UE Context.

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

19.2.2.2 Service Provided by the BM-SC in visited PLMN

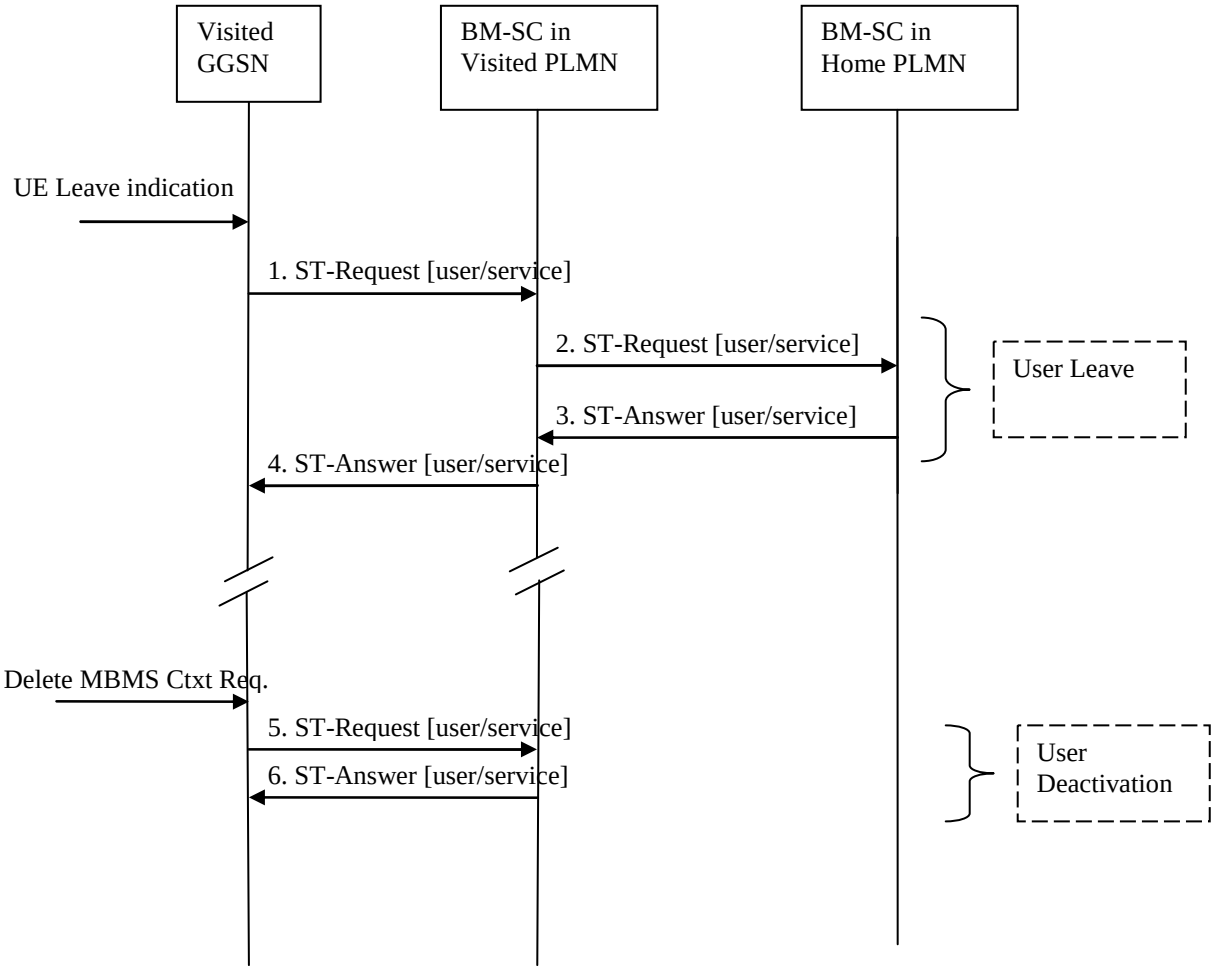


Figure 31: Deactivation of an MBMS multicast service in roaming scenario with service provided in the visited PLMN

1. Upon receiving the leave indication, the GGSN sends an STR to the BM-SC in visited PLMN, indicating that the roaming UE is requesting to leave the multicast service. The session to be terminate is uniquely identified by the Diameter session-id.

2. Upon reception of the STR, the BM-SC in visited PLMN verifies that the IP multicast address corresponds to a valid MBMS bearer service and sends an STR to the BM-SC in home PLMN.

3. The BM-SC in home PLMN responds the BM-SC in visited PLMN with an ST-Answer.

4. Upon reception of the STA, the BM-SC in visited PLMN sends an STA to the GGSN that orignated the Leave Indication. The APN shall be the same that was provided during service activation.

5. The GGSN deletes the MBMS UE Context and sends an STR to the BM-SC in visited PLMN to confirm the successful deactivation of the MBMS UE Context.

6. The BM-SC in visited PLMN, then, delets the MBMS UE Context and sends a confirmation to the GGSN in an STA message.

19.2.2.3 BM-SC in the home PLMN initiated multicast service deactivation

This section defines the BM-SC in the home PLMN initiated multicast service deactivation procedure.

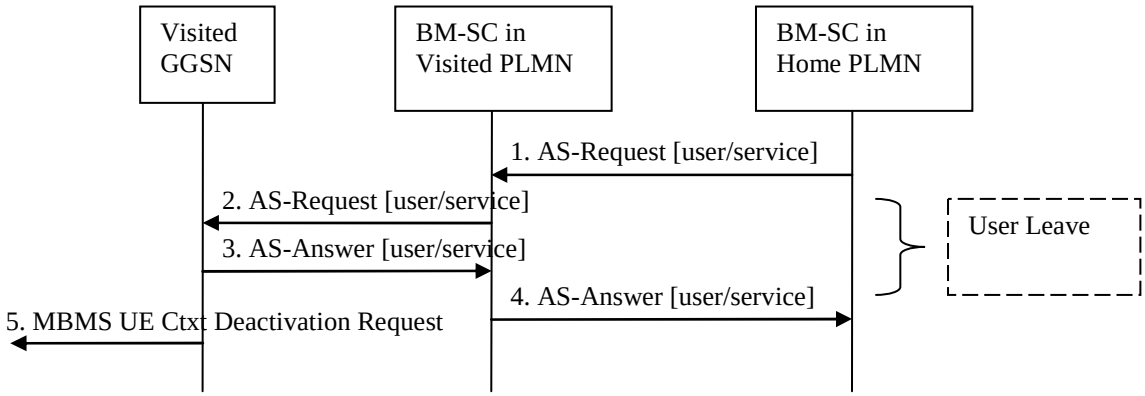


Figure 32: BM-SC in the home PLMN initiated MBMS multicast service deactivation procedure

1. The BM-SC in home PLMN sends an ASR to the BM-SC in visited PLMN, indicating that the UE shall be removed from a specific multicast service. The session to be terminated is uniquely identified by the Diameter session-id.
2. The BM-SC in the visited PLMN 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.
3. Upon reception of the ASR, the GGSN sends an ASA to the BM-SC in visited PLMN.
4. Upon reception of the ASA, the BM-SC in visited PLMN sends an ASA to the BM-SC in home PLMN.
5. Upon reception of the ASR in step 3, 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 5 and 6 of Figure 30 in section 19.2.2.1 follows in roaming scenarios where service was provided in the home PLMN.

Steps 5 and 6 of Figure 31 in section 19.2.2.2 follows in roaming scenarios where service was provided in the visited PLMN.

19.3 Mz messages

This clause defines the Mz interface Diameter messages.

The Diameter messages used in the Mz protocol, are the same as specified for Gmb interface described in Clause 17 of the present specification: AAR Command (clause 17.6.1), AAA Command (clause 17.6.2), STR Command (clause 17.6.3), STA Command (clause 17.6.4), Abort-Session-Request Command (clause 17.6.7) and Abort-Session-Answer Command (17.6.8).

To route Diameter messages from the visited PLMN to the home PLMN, the BM-SC in the visited PLMN shall derive the realm of the home PLMN from the user's IMSI. The way to derive the realm of the home PLMN from IMSI is specified in 3GPP TS 23.003 [40] subclause 15.4.

The derived realm of the home PLMN shall be filled in the Destination-Realm AVP of messages sent from the visited PLMN to the home PLMN, i.e. AAR command, STR command.

19.4 Mz specific AVPs

The Mz specific AVPs are the same as specified in Table 10 and Table 11. The Vendor-Id header of all Mz specific AVPs defined in the present specification shall be set to 3GPP (10415).

19.5 Mz 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 IETF RFC 6733 [111] specific procedures. Application errors, on the other hand, generally occur due to a problem with a function specified in a Diameter application.

Diameter Base IETF RFC 6733 [111] 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.

Note that according to IETF RFC 6733 [111], 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.

19.5.1 Success

The success result codes specified in clause 17.8.1 of the present specification are applicable for Mz.

19.5.2 Permanent Failures

The Result-Code AVP values defined in Diameter Base IETF RFC 6733 [111] are applicable. Also the following specific Gmb Experimental-Result-Code value defined in clause 17.8.2 is applicable for Mz:

DIAMETER_ERROR_UNKNOWN_MBMS_BEARER_SERVICE (5122)

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

19.5.3 Transient Failures

Errors that fall within the transient failures category are used to inform a peer that a request could not be satisfied at the time it was received, but it may be satisfied in the future.

The Result-Code AVP values defined in Diameter Base IETF RFC 6733 [111] are applicable.

20 Usage of Diameter on SGmb interface

20.1 General

Signalling between MBMS GW and BM-SC is exchanged at SGmb reference point.

The MBMS GW uses the SGmb interface:

- to receive indication of session start, session update and session stop messages, which shall cause the MBMS GW, MME/SGSN and E-UTRAN/UTRAN to set up/tear down the appropriate resources for the service. For further details, see 3GPP TS 23.246 [65];
- to enable the BM-SC and MBMS GW to detect an SGmb path failure or the restart of the peer MBMS node. For further details, see 3GPP TS 23.007 [104].
- to enable the BM-SC to transfer the M1 interface information of local MBMS information. For further details, see 3GPP TS 23.285 [112].

NOTE: The localized MBMS architecture refers to Annex B of 3GPP TS 23.285 [112].

The SGmb 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 SGmb application identifier value assigned by IANA is 16777292.

The SGmb application identifier value shall be included in the Auth-Application-Id AVP.

The BM-SC and the MBMS GW shall advertise the support of the SGmb 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 IETF RFC 6733 [111], 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.

20.2 MBMS session start / update/ 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, MBMS service area, or MBMS-Cell-List) to every MBMS GW that will deliver the MBMS bearer service.

The MBMS session update shall be used by the BM-SC to trigger the update of MBMS session attributes in the affected MBMS GWs. The attributes that can be modified are the MBMS service area, the MBMS-Cell-List and the list of MBMS control plane nodes (MMEs, SGSNs).

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 MBMS GW that has been delivering the MBMS bearer service.

20.2A MBMS heartbeat

The MBMS heartbeat procedure enables the BM-SC and MBMS GW to detect an SGmb path failure or the restart of the peer MBMS node, as specified in 3GPP TS 23.007 [104].

The use of this procedure shall be negotiated between the BM-SC and MBMS GW upon contacting the peer node for the first time.

NOTE: The MBMS Heartbeat procedure however applies per (BM-SC, MBMS GW) pair, i.e. not per MBMS session.

When this procedure is applied, the BM-SC and MBMS GW shall detect an SGmb path failure or the restart of the peer MBMS node as specified in clause 29 of 3GPP TS 23.007 [104].

The BM-SC and MBMS GW shall maintain a local restart counter which shall be incremented monotonically whenever the MBMS node restarts with loss of previous states.

The MBMS heartbeat message shall include the Restart Counter AVP set to the local restart counter of the sending node. The Restart-Counter AVP may also be included in any other SGmb messages e.g. if contacting the peer node for the first time or if the local restart counter has been incremented.

20.3 Message flows

20.3.1 Session start procedure

The BM-SC initiates the MBMS session start procedure when it is ready to send data. This informs the MBMS GW of the imminent start of the transmission and MBMS session attributes are provided to the MBMS GWs included in the list of downstream nodes in BM-SC. The bearer plane is allocated.

BM-SC and MBMS GW shall at least support IP unicast encapsulation of IP multicast datagrams, which shall be default mode of sending user plane data. BM-SC may support IP multicast encapsulation of user plane IP multicast datagrams and MBMS GW also may support this mode of operation.

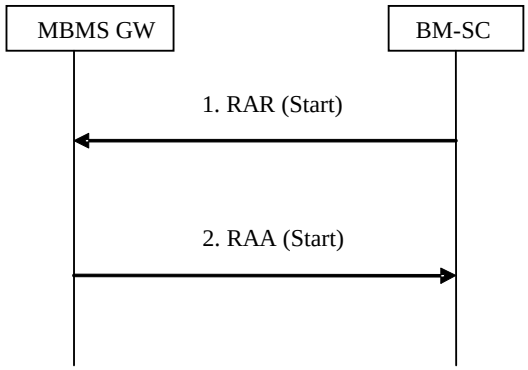


Figure 20.3.1.1: MBMS Session Start procedure

1. The BM-SC sends an RAR message to indicate the impending start of the transmission and to provide the session attributes to the MBMS GWs listed in the "list of downstream nodes" parameter of the corresponding MBMS Bearer Context. BM-SC may indicate to MBMS GW that BM-SC supports sending the user plane IP multicast data without IP unicast encapsulation. In such case BM-SC shall send multicast source address as specified by IETF RFC 4604 [73] and IETF RFC 4607 [74] and the user plane multicast destination address.

   If IP unicast mode is used, the BM-SC shall also require the MBMS GW to select one UDP port for the reception of the user plane data for the related MBMS service (identified by TMGI and Flow ID).

   The BM-SC may also indicate its intent to use IP multicast encapsulation of IP multicast datagrams across Sgi-mb. In this case, the BM-SC shall specify an Sgi-mb (transport) destination multicast IP address associated with the MBMS bearer context, as well as the source UDP port. The inclusion of these data shall mean IP multicast encapsulation of IP multicast datagram is the only offered multicast mode over Sgi-mb. The destination UDP port for IP multicast transport shall be fixed as port number 927. The BM-SC shall also specify the (transport) multicast source address.

   The BM-SC shall indicate the M1 interface information of local MBMS information as specified in 3GPP TS 23.285 [112] if the BM-SC determines to use the local MBMS information.

2. The MBMS GW creates an MBMS Bearer Context, stores the session attributes in the MBMS Bearer Context, and sends an RAA message to the BM-SC. In case MBMS GW receives BM-SC multicast source address, which indicates BM-SC support for both modes of sending user plane data, MBMS GW decides in which mode MBMS GW shall receive the user plane data. In case MBMS GW decides to receive unicast encapsulated data, then MBMS GW shall send own IP address for user plane to BM-SC and the MBMS GW shall also indicate the UDP port on which the user plane data shall be received. In case MBMS GW decides to receive IP multicast packets, then MBMS GW shall join the multicast group as specified by IETF RFC 4604 [73] and IETF RFC 4607 [74], and indicate to BM-SC about the decision. In case MBMS GW decides to use M1 interface information of local MBMS information, the MBMS GW skips the allocation procedure for IP multicast distribution.

20.3.2 Session update procedure

The BM-SC initiates the MBMS session update procedure when service attributes (e.g. Service Area, MBMS cell list, Access indicator or ARP) for an ongoing MBMS session shall be modified. The MBMS session update procedure update procedure is initiated towards one or more of the MBMS GWs in the list of downstream nodes in the BM-SC, according to the changes in the service area.

NOTE: In addition, when the MBMS Service Area for an ongoing broadcast session is changed in the BM-SC, then MBMS GW(s) may be added to, or removed from, the list of downstream nodes in the BM-SC. The BM-SC will initiate MBMS session start procedures or MBMS session stop procedures towards these MBMS GWs accordingly.

The attributes that can be modified by the RAR message are the MBMS Service Area, the MBMS-Cell-List, the ARP, the Access indicator and the list of MBMS control plane nodes (MMEs, SGSNs).

When a session update message is received, the MBMS GW updates its MBMS Bearer Context accordingly and informs its downstream MMEs/SGSNs of the changed service attributes. If a list of MBMS control plane nodes

(MMEs, SGSNs) is included in the session update message, MBMS GW shall initiate a session start procedure towards the new MMEs/SGSNs, and a session stop procedure towards the MMEs/SGSNs that have been removed from the list.

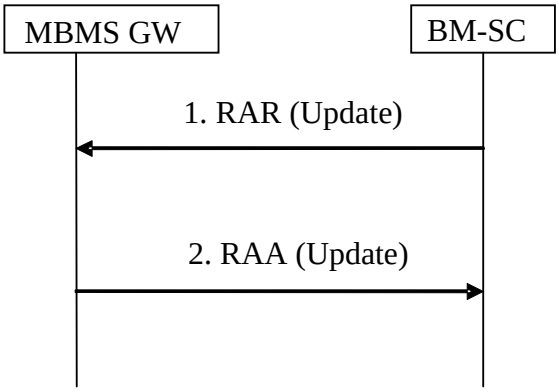


Figure 20.3.2.1: MBMS Session Update procedure

1. The BM-SC sends an RAR message to all MBMS GWs listed in the "list of downstream nodes" parameter of the affected MBMS Bearer Context to indicate that the MBMS session is updated.

2. The MBMS GW stores the new session attributes in the MBMS Bearer Context, initiates session start, session stop or session update procedure towards the MMEs/SGSNs in its list of MBMS control plane nodes and sends an RAA message to the BM-SC. An AAR message is not mandated for the SGmb application in response to an RAR- RAA command exchange.

20.3.3 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.

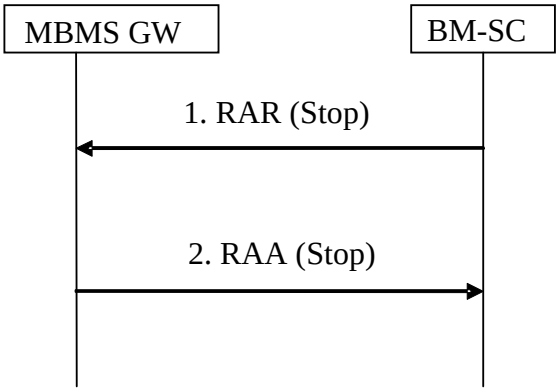


Figure 20.3.3.1: MBMS Session Stop procedure

1. The BM-SC sends an RAR message to all MBMS GWs 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 MBMS GW releases the resources regarding the session and sends an RAA message to the BM-SC. An AAR message is not mandated for the SGmb application in response to an RAR- RAA command exchange.

20.3.4 MBMS session termination (MBMS GW initiated)

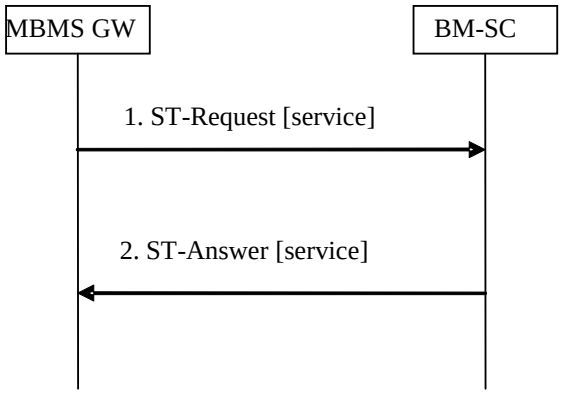


Figure 20.3.4.1: MBMS session termination

1. In exceptional cases (e.g. resource pre-emption or timeout of the MBMS session), the MBMS GW may send an STR command to the BM-SC to initiate the termination of the Diameter session related to an MBMS bearer service. If a bearer plane had been established over SGi-mb for this MBMS bearer service, the bearer plane is released. If the MBMS GW detects the SGi-mb path failure as specified in subclause 20.3.2.1 of 3GPP TS 23.007 [104], the MBMS GW shall set the Termination-Cause to "DIAMETER_LINK_BROKEN" (see IETF RFC 6733 [111]) and shall include the Diagnostic-Info AVP set to "User Plane Failure" if it tears down the MBMS session as a result of detecting an SGi-mb path failure.

2. The BM-SC removes the Diameter session and confirms the operation by sending an STA message to the MBMS GW.

20.3.5 MBMS heartbeat procedure

The BM-SC initiates the MBMS heartbeat procedure to detect a SGmb path failure or the restart of the MBMS GW as specified in 3GPP TS 23.007 [104].

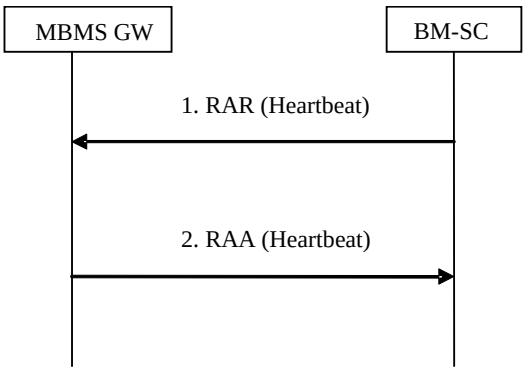


Figure 20.3.5.1: MBMS Heartbeat procedure initiated by the BM-SC

1. The BM-SC sends an RAR message to the MBMS GW and indicates this is a heartbeart request. The BM-SC also includes the Restart-Counter AVP set to its local restart counter.

2. The MBMS GW sends an RAA message to the BM-SC to acknowledge the heartbeat request. The MBMS GW also includes the Restart-Counter AVP set to its local restart counter.

The MBMS GW initiates the MBMS heartbeat procedure to detect a SGmb path failure or the restart of the BM-SC as specified in 3GPP TS 23.007 [104].

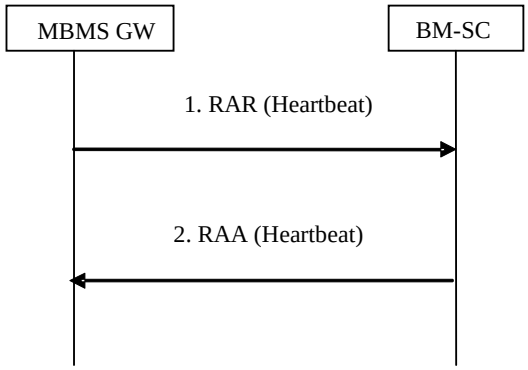


Figure 20.3.5.2: MBMS Heartbeat procedure initiated by the MBMS GW

1. The MBMS GW sends an RAR message to the BM-SC and indicates this is a heartbeart request. The MBMS GW also includes the Restart-Counter AVP set to its local restart counter.

2. The BM-SC sends an RAA message to the MBMS GW to acknowledge the heartbeat request. The BM-SC also includes the Restart-Counter AVP set to its local restart counter.

In the context of this procedure, the Diameter session shall be implicitly terminated, i.e. the client (server) shall behave as if the Auth-Session-State AVP was set to the value NO_STATE_MAINTAINED (1), as described in IETF RFC 6733 [111]. As a consequence, the server shall not maintain any state information about this session and the client shall not send any session termination request.

NOTE: The Auth-Session-State AVP is not included in the RAR/RAA message as this is not permitted by the Diameter base protocol. See IETF RFC 6733 [111].

20.4 SGmb Messages

This clause defines the SGmb interface Diameter message.

The relevant AVPs that are of use for the SGmb 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 SGmb specific AVPs for SGmb are needed to be compliant to the SGmb interface unless otherwise stated.

20.4.1 Re-Auth-Request Command

The Re-Auth-Request (RAR) command, defined in IETF RFC 6733 (DIAMETER BASE) [111], 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 SGmb interface are detailed in the ABNF description below. Other valid AVPs for this command are not used for SGmb 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 SGmb, 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-Access-Indicator ]
```

```
    [ MBMS-StartStop-Indication ]
    [ MBMS-Service-Area ]
    [ QoS-Information ]
    [ MBMS-Session-Duration ]
    [ MBMS-Session-Identity ]
    [ MBMS-Session-Repetition-number ]
    [ TMGI ]
*   [ 3GPP-SGSN-Address ]
*   [ 3GPP-SGSN-Ipv6-Address ]
    [ MBMS-Time-To-Data-Transfer ]
    [ MBMS-Data-Transfer-Start ]
    [ MBMS-Data-Transfer-Stop ]
    [ MBMS-Flags ]
    [ MBMS-User-Data-Mode-Indication ]
    [ MBMS-BMSC-SSM-IP-Address ]
    [ MBMS-BMSC-SSM-Ipv6-Address ]
    [ MBMS-Flow-Identifier ]
    [ CN-IP-Multicast-Distribution ]
    [ MBMS-HC-Indicator ]
    [ MBMS-GW-UDP-Port-Indicator]   ; for IP unicast encapsulated user data
    [ MBMS-GW-SSM-IP-Address ]      ; for IP multicast encapsulated user data
    [ MBMS-GW-SSM-Ipv6-Address ]    ; for IP multicast encapsulated user data
    [ MBMS-BMSC-SSM-UDP-Port ]      ; for IP multicast encapsulated user data
    [ MBMS-Cell-List ]
    [ Local-M1-Information ]
    [ Origin-State-Id ]
*   [ Proxy-Info ]
*   [ Route-Record ]
*   [ Supported-Features ]
    [ Restart-Counter ]
```

For the MBMS Session Start procedure, RAR is sent by the BM-SC to the MBMS GW(s) that will deliver the MBMS 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. The RAR message contains either an Ipv4 address included in 3GPP-SGSN-Address AVP or an Ipv6 address included in 3GPP-SGSN-Ipv6-Address AVP for each participating MBMS control plane nodes (MMEs, SGSNs). The MBMS-Time-to-Data-Transfer AVP shall be included to indicate the expected time between the reception of the MBMS Session Start and the transmission of MBMS data flows. For E-UTRAN access, the RAR message may also contain the MBMS-Data-Transfer-Start AVP containing the absolute time stamp of the data delivery start. The RAR message shall also contain the MBMS-Service-Area AVP. If the MBMS Cell List feature is supported, or if the BM-SC does not yet know whether the MBMS-GW supports this feature, the RAR may contain the MBMS-Cell-List AVP. For the distributed MCE architectures, i.e. when the MCE is part of eNB as described in clause 15.1.1 in TS 36.300 [98], the MBMS-Data-Transfer-Start AVP should be used at MBSFN operation mode to ensure synchronized session control and to facilitate a graceful reallocation of resources for the MBSFN when needed. The RAR message shall also contain the Local-M1-Information AVP if the BM-SC determines to use the local MBMS information as specified in 3GPP TS 23.285 [112].

The MBMS-Flags AVP may provide specific control indications in relation to MBMS, e.g. whether the MBMS Session Start procedure is used to re-establish an MBMS session.

For the MBMS Session Update procedure, RAR is sent by the BM-SC in order for the MBMS GW(s) to update their session attributes. If the MBMS service area or the MBMS cell list needs to be changed, the MBMS-Service-Area AVP shall be included in the RAR. If the MBMS Cell List feature is supported and the MBMS cell list needs to be changed, the MBMS-Cell-List AVP shall also be included. If the MBMS-Service-Area AVP but no MBMS-Cell-List AVP is included, this shall indicate that any MBMS Cell List included in a previous RAR does no longer apply. If the Access indicator needs to be updated, it shall be included in the MBMS-Access-Indicator AVP. For E-UTRAN access, the RAR message may also contain the MBMS-Data-Transfer-Start AVP containing the absolute time stamp of the data delivery start. For the distributed MCE architectures, i.e. when the MCE is part of eNB as described in clause 15.1.1 in TS 36.300 [98], the MBMS-Data-Transfer-Start AVP should be used at MBSFN operation mode to ensure synchronized session control and to facilitate a graceful reallocation of resources for the MBSFN when needed. The MBMS-StartStop-Indication AVP with the value UPDATE shall be included. The MBMS-Time-To-Data-Transfer with AVP the value set to 0 shall be included. The MBMS-Session-Duration AVP shall be included to indicate the duration of the remaining part of the MBMS session. The 3GPP-SGSN-Address AVP and the 3GPP-SGSN-Ipv6-Address AVP shall be included if the related lists of MBMS control plane nodes (MMEs, SGSNs) in the MBMS GW(s) have changed. The other bold marked AVPs shall be included as given by the previous, corresponding MBMS Session Start procedure.

For the MBMS Session Stop procedure, RAR is sent by the BM-SC to the MBMS GW(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. For E-UTRAN access, the RAR message may also contain the MBMS-Data-Transfer-Stop AVP containing the absolute time

stamp of the data delivery stop. The MBMS-Flags AVP may provide specific control indications, e.g. whether the MBMS Session Stop procedure is used to release the MBMS bearer context locally.

For the MBMS Session Start procedure, the Qos-Information AVP indicates the QoS that is required for the MBMS bearer service for the actual MBMS session. Only the QoS-Class-Identifier AVP, Max-Requested-Bandwidth-DL AVP, Guaranteed-Bitrate-DL AVP and Allocation-Retention-Priority AVP within the QoS-Information AVP are applicable for the MBMS bearer service. The MBMS-Service-Area AVP is passed from BM-SC transparently through MBMS GW to the MMEs/SGSN(s) that are relevant for the actual MBMS bearer service. The MBMS-Cell-List AVP is also passed transparently through MBMS GW to the MMEs. The MBMS-Access-Indicator AVP indicates in which radio access types the MBMS bearer service shall be broadcasted, i.e UTRAN, or E-UTRAN, or both.

The usage of MBMS-StartStop-Indication AVP, Session-Id AVP, Framed-IP-Address AVP, Framed-Ipv6-Prefix AVP, Framed-Interface-Id AVP, Called-Station-Id AVP and MBMS-Flow-Identifier AVP can refer to Gmb interface as described in clause 17.6.5.

If unicast mode is used, the MBMS GW shall select an IP unicast address and a destination UDP port that is unique within the MBMS GW or that IP unicast address.

If IP multicast encapsulation of application IP multicast datagram is used over Sgi-mb, the BM-SC shall select a source UDP port that is unique within the BM-SC for that IP multicast address.

For the MBMS Heartbeat procedure, RAR is sent by the BM-SC to the MBMS GW, or vice-versa. The RAR message shall contain the following AVPs:

- the MBMS-StartStop-Indication AVP set to the value "heartbeat";
- the Restart-Counter AVP set to the local restart counter of the sender.

20.4.2 RE-Auth-Answer Command

The Re-Auth-Answer (RAA) command, defined in IETF RFC 6733 (DIAMETER BASE) [111], 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 SGmb interface are detailed in the ABNF description below. Other valid AVPs for this command are not used for SGmb 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 SGmb, or modified existing AVPs.

Message Format:

```
<RAA>  ::= < Diameter Header: 258, PXY >
             < Session-Id >
             { Origin-Host }
             { Origin-Realm }
             [ Result-Code ]
             [ Experimental-Result ]
             [ MBMS-StartStop-Indication ]
             [ MBMS-GGSN-Address ]             ; for unicast encapsulated user data
             [ MBMS-GGSN-Ipv6-Address ]        ; for unicast encapsulated user data
             [ MBMS-User-Data-Mode-Indication ]
             [ MBMS-GW-UDP-Port]               ; for unicast encapsulated user data
             [ Origin-State-Id ]
             [ Error-Message ]
             [ Error-Reporting-Host ]
             [ Failed-AVP ]
           *  [ Redirected-Host ]
             [ Redirected-Host-Usage ]
             [ Redirected-Host-Cache-Time ]
             [ Proxy-Info ]
           *  [ Supported-Features ]
             [ Restart-Counter ]
```

For the MBMS Heartbeat procedure, RAA is sent by the BM-SC to the MBMS GW, or vice-versa. The RAA message shall contain the following AVPs:

- the MBMS-StartStop-Indication AVP set to the value "heartbeat";

- the Restart-Counter AVP set to the local restart counter of the sender.

20.4.3 Session-Termination-Request Command

A DIAMETER session may be terminated by the MBMS GW in exceptional cases.

The relevant AVPs that are of use for the SGmb interface are detailed in the ABNF description below. Other valid AVPs for this command are not used for SGmb 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 ]
                       [ Diagnostic-Info ]
                       [ Restart-Counter ]
```

20.4.4 Session-Termination-Answer Command

The STA command, defined in IETF RFC 6733 (DIAMETER BASE) [111], 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.

The relevant AVPs that are of use for the SGmb interface are detailed in the ABNF description below. Other valid AVPs for this command are not used for SGmb 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 ]
                       [ Restart-Counter ]
```

20.4.5 Abort-Session-Request Command

The Abort-Session-Request (ASR) command, defined in IETF RFC 6733 (DIAMETER BASE) [111], is indicated by the Command-Code set to 274 and the message flags' 'R' bit set, is sent by the BM-SC to the MBMS GW to request that the session identified by the Session-Id be stopped.

The relevant AVPs that are of use for the SGmb interface are detailed in the ABNF description below. Other valid AVPs for this command are not used for SGmb 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 ]
                  [ Restart-Counter ]
```

20.4.6 Abort-Session-Answer Command

The Abort-Session-Answer (ASA) command, defined in IETF RFC 6733 (DIAMETER BASE) [111], 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 SGmb interface are detailed in the ABNF description below. Other valid AVPs for this command are not used for SGmb 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 ]
                  [ Restart-Counter ]
```

20.5 SGmb re-used AVPs

Table 20.5.1 lists the Diameter AVPs re-used by the SGmb reference point from the Gmb reference point and other existing Diameter Application, reference to their respective specifications and short description of their usage witin the SGmb reference point. When reused from Gmb reference point, the specific clause in the present specification is referred. Other AVPs from existing Diameter Applications, except for the AVPs from Diameter base protocol, do not need to be supported. The AVPs from Diameter base protocol are not included in table 20.5.1, but they are re-used for the SGmb reference point. Where RADIUS VSAs are re-used, they shall be translated to Diameter AVPs as described in RFC 4005 [67] with the exception that the 'M' flag shall be set and the 'P' flag may be set.

Table 20.5.1 : SGmb re-used Diameter AVPs

Attribute Name	Reference	Description
TMGI	17.7.2	Contains the Temporary Mobile Group Identity allocated to a particular MBMS bearer service.
MBMS-StartStop-Indication	17.7.5	Indicates the type of MBMS Session procedure.
MBMS-Service-Area	17.7.6	Indicates the area over which the MBMS bearer service has to be distributed.
MBMS-Session-Duration	17.7.7	Indicates the estimated session duration (MBMS Service data transmission).
MBMS-Session-Identity	17.7.11	Together with TMGI it identifies a transmission of a specific MBMS session.
MBMS-Time-To-Data-Transfer	17.7.14	Indicates the expected time between reception of the MBMS Session Start (RAR (Start) command) or the MBMS Session Update (RAR (Update) command) and the commencement of the MBMS Data flow. A value of 0 (1 sec.) shall be used in the Session Update.
MBMS-Session-Repetition-Number	17.7.15	Contains the session identity repetition number of the MBMS transmission session on the SGmb interface.
MBMS-User-Data-Mode-Indication	17.7.18	When sent from the BM-SC to the MBMS GW, it indicates the mode that BM-SC supports. When sent from the MBMS GW to the BM-SC, it indicates the mode that BM-SC shall send user plane data with. Two modes apply: • Unicast mode: IP multicast packets over UDP encapsulated by IP unicast header. • Multicast mode: IP multicast packetsencapsulated over UDP by IP multicast header.
MBMS-GGSN-Address	17.7.19	Contains the value of MBMS GW's Ipv4 address for user plane data.
MBMS-GGSN-Ipv6-Address	17.7.20	Contains the valus of MBMS GW's Ipv6 address for user plane data.
MBMS-BMSC-SSM-IP-Address	17.7.21	Contains the value of BM-SC's Ipv4 address of Source Specific Multicasting.
MBMS-BMSC-SSM-Ipv6-Address	17.7.22	Contains the value of BM-SC's Ipv6 address of Source Specific Multicasting.
MBMS-Flow-Identifier	17.7.23	Represents a location dependent subflow of an MBMS bearer service.
CN-IP-Multicast-Distribution	17.7.24	Indicates if IP multicast distribution to UTRAN should be used for the MBMS user plane data.
MBMS-HC-Indicator	17.7.25	Indicates if header compression is used by BM-SC when sending for MBMS user plane data.(NOTE 1)
3GPP-SGSN-Address	16.4.7	Represents the SGSN or MME's Ipv4 address that is used by the GTP control plane for the handling of control messages.
3GPP-SGSN-Ipv6-Address	16.4.7	Represents the SGSN or MME's Ipv6 address that is used by the GTP control plane for the handling of control messages.
Called-Station-Id	NASREQ, IETF RFC 4005 [67]	Contains the Access Point Name (APN) for which the MBMS bearer service is defined
Framed-Interface-Id	NASREQ, IETF RFC 4005 [67]	Contains the Ipv6 interface identifier of the multicast address
Framed-IP-Address	NASREQ, IETF RFC 4005 [67]	Contains the Ipv4 multicast address.
Framed-Ipv6-Prefix	NASREQ, IETF RFC 4005 [67]	Contains the Ipv6 prefix of the multicast address.
Local-M1-Information	3GPP TS 29.468 [113]	Contains the M1 interface information of the local MBMS information, i.e., transport network IP Multicast Address, IP address of multicast source and C-TEID.
QoS-Information	3GPP TS 29.212 [75]	Contains the QoS that is required for the MBMS bearer service for the MBMS session. Only the QoS-Class-Identifier AVP, Max-Requested-Bandwidth-DL, Guaranteed-Bitrate-DL AVP and Allocation-Retention-Priority AVP within the QoS-Information AVP are applicable for the MBMS bearer service.
Supported-Features	3GPP TS 29.229 [105]	If present, this AVP informs the destination host about the features that the origin host requires to successfully complete this command exchange
NOTE 1: Header Compression only supported for UTRAN for this Release.		

20.5a SGmb specific AVPs

Table 20.5a.1 describes the SGmb specific Diameter AVPs. The Vendor-Id header of all SGmb specific AVPs defined in the present specification shall be set to 3GPP (10415).

The SGmb specific AVPs require to be supported to be compliant with the present specification. All AVPs in table 20.5a.1 are mandatory within SGmb interface unless otherwise stated.

Table 20.5a.1: SGmb specific AVPs

				AVP Flag rules					
Attribute Name	**AVP Code**	**Section defined**	**Value Type**	**Must**	**May**	**Should not**	**Must not**	**May Encr.**	**Applicability (NOTE)**
MBMS-Access-Indicator	923	20.5a.1	Enumerated	M.V	P			Y	
MBMS-GW-SSM-IP-Address	924	20.5a.2	OctetString	V	P		M	Y	
MBMS-GW-SSM-Ipv6-Address	925	20.5a.3	OctetString	V	P		M	Y	
MBMS-BMSC-SSM-UDP-Port	926	20.5a.4	OctetString	V	P		M	Y	
MBMS-GW-UDP-Port	927	20.5a.5	OctetString	V	P		M	Y	
MBMS-GW-UDP-Port-Indicator	928	20.5a.6	Enumerated	V	P		M	Y	
MBMS-Data-Transfer-Start	929	20.5a.7	Unsigned64	V	P		M	Y	
MBMS-Data-Transfer-Stop	930	20.5a.8	Unsigned64	V	P		M	Y	
MBMS-Flag	931	20.5a.9	Unsigned32	V	P		M	Y	
Restart-Counter	932	20.5a.10	Unsigned32	V	P		M	Y	MBMS Heartbeat
Diagnostic-Info	933	20.5a.11	Unsigned32	V	P		M	Y	
MBMS-Cell-List	934	20.5a.12	OctetString	V	P		M	Y	MBMS Cell List
NOTE: AVPs marked with a supported feature are applicable as described in subclause 20.7.									

20.5a.1 MBMS-Access-Indicator AVP

The MBMS-Access-Indicator AVP (AVP code 923) is of type Enumerated. It indicates whether the MBMS bearer service will be delivered in UTRAN-only, E-UTRAN-only or both coverage areas. The following values are supported:

UTRAN (0)

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

E-UTRAN (1)

The MBMS bearer service shall only be delivered in E-UTRAN only coverage areas.

UTRAN-AND-E-UTRAN (2)

The MBMS bearer service shall be delivered both in UTRAN and E-UTRAN coverage areas.

20.5a.2 MBMS-GW-SSM-IP-Address AVP

The MBMS-GW-SSM-IP-Address AVP (AVP code 924) is of type OctetString and contains the Sgi-mb (transport) plane Ipv4 destination multicast address used by BM-SC for IP multicast encapsulation of application IP multicast datagrams.

20.5a.3 MBMS-GW-SSM-Ipv6-Address AVP

The MBMS-GW-SSM-Ipv6-Address AVP (AVP code 925) is of type OctetString and contains the Sgi-mb (transport) plane Ipv6 prefix of the destination multicast address used by BM-SC for IP multicast encapsulation of application IP multicast datagrams.

20.5a.4 MBMS-BMSC-SSM-UDP-Port AVP

The MBMS-BMSC-SSM-UDP-Port AVP (AVP code 926) is of type OctetString and contains the Sgi-mb (transport) plane source UDP port number at the BM-SC for IP multicast encapsulation of IP multicast datagrams.

20.5a.5 MBMS-GW-UDP-Port AVP

The MBMS-GW-UDP-Port AVP (AVP code 927) is of type OctetString, and contains the value of the UDP port from which the user plane data will be received in the MBMS-GW.

20.5a.6 MBMS-GW-UDP-Port-Indicator AVP

MBMS-GW-UDP-Port-Indicator AVP (AVP code 928) is of type Enumerated. It indicates that the payload related to the MBMS service is required to be delivered in the MBMS UDP Port assigned by the MBMS-GW.

UDP-PORT-REQUIRED (1)

Value 1 indicates that the user plane data corresponding to the MBMS service shall be delivered on the UDP Port provided by the MBMS-GW.

20.5a.7 MBMS-Data-Transfer-Start AVP

The MBMS-Data-Transfer-Start AVP (AVP code 929) is of type Unsigned64.

This value indicates the time in seconds for the radio resources set up relative to 00:00:00 on 1 January 1900 (calculated as continuous time without leap seconds and traceable to a common time reference) where binary encoding of the integer part is in the first 32 bits and binary encoding of the fraction part in the last 32 bits. The fraction part is expressed with a granularity of 1 /2**32 second.

This AVP is only valid for E-UTRAN access type.

20.5a.8 MBMS-Data-Transfer-Stop AVP

The MBMS-Data-Transfer-Stop AVP (AVP code 930) is of type Unsigned64.

This value indicates the time in seconds for the release of resources relative to 00:00:00 on 1 January 1900 (calculated as continuous time without leap seconds and traceable to a common time reference) where binary encoding of the integer part is in the first 32 bits and binary encoding of the fraction part in the last 32 bits. The fraction part is expressed with a granularity of 1 /2**32 second.

This AVP is only valid for E-UTRAN access type.

20.5a.9 MBMS-Flags AVP

The MBMS-Flags AVP (AVP coce 931) is of type Unsigned32. It provides control indications.

It shall contain a bit mask. The meaning of the bits shall be as defined in table 20.5a.9.1:

Table 20.5a.9.1 : MBMS-Flags

Bit	Name	Description
0	MSRI	MBMS Session Re-establishment Indication : This bit, when set, indicates that the MBMS Session Start Request message is used to re-establish an MBMS session (see 3GPP TS 23.007 [104]).
1	LMBCRI	Local MBMS Bearer Context Release Indication : This bit, when set, indicates that the MBMS Session Stop Request message is used to locally release the MBMS bearer context in the MBMS-GW and in the associated MME/SGSNs (see3GPP TS 23.007 [104]
NOTE:	Bits not defined in this table shall be cleared by the sending BM-SC and ignored by the receiving MBMS GW.	

20.5a.10 Restart-Counter AVP

The Restart-Conter AVP (AVP coce 932) is of type Unsigned32. This is a monotonically increasing value that is advanced whenever the MBMS entity restarts with loss of previous state, for example upon restart. The Restart-Counter AVP may be included in any Diameter message over the SGmb reference point, including CER/CEA.

20.5a.11 Diagnostic-Info AVP

The Diagnostic-Info AVP (AVP code 933) is of type Unsigned32.

It shall contain a bit mask. The meaning of the bits shall be as defined in table 20.5a.11.1:

Table 20.5a.11.1 : Diagnostic-Info

Bit	Name	Description
0	UPFAIL	User Plane Failure: This bit, when set, indicates the detection of a User Plane Failure by the MBMS GW (see subclause 20.3.2.1 of 3GPP TS 23.007 [104]).
NOTE:	Bits not defined in this table shall be cleared by the sending MBMS GW and ignored by the receiving BM-SC.	

20.5a.12 MBMS-Cell-List AVP

The MBMS-Cell-List AVP (AVP code 934) is of type OctetString. It contains the MBMS Cell Listthat the E-UTRAN uses to determine a set of radio resources to be used for the broadcast. Based on the cell ID list, the set of radio resources selected may be reduced from the full set of resources defined by the MBMS service area.

The AVP shall consist of two octets indicating the number of cell identifiers in the list, followed by a sequence of maximum 4096 cell identifiers, coded as E-CGIs.

Bits	
1-16	Number N of ECGI codes coded as: 1 binary value is ‘0000 0000 0000 0000’ 4096 binary value is '0000 1111 1111 1111'
17-(56*N+16)	A consecutive list of N ECGI codes, each encoded according to subclause 8.21.5 of 3GPP TS 29.274 [81].

The ECGI and its semantics are defined in subclause 19.6 of 3GPP TS 23.003 [40].

20.6 SGmb specific Experimental-Result-Code AVP values

The same codes specified in clause 17.8 apply here except
DIAMETER_ERROR_UNKNOWN_MBMS_BEARER_SERVICE (5122)

20.7 Use of the Supported-Features AVP on the SGmb reference point

The Supported-Features AVP is used during session establishment to inform the destination host about the required and optional features that the origin host supports. The client shall, in the first request in a Diameter session indicate the set of supported features. The server shall, in the first answer within the Diameter session indicate the set of features that it has in common with the client and that the server shall support within the same Diameter session. Any further command messages shall always be compliant with the list of supported features indicated in the Supported-Features AVPs during session establishment. Features that are not advertised as supported shall not be used to construct the command messages for that Diameter session. Unless otherwise stated, the use of the Supported-Features AVP on the SGmb reference point shall be compliant with the requirements for dynamic discovery of supported features and associated error handling on the Cx reference point as defined in clause 7.2.1 of 3GPP TS 29.229 [105].

The base functionality for the SGmb reference point is the 3GPP Rel-11 standard and a feature is an extension to that functionality. If the origin host does not support any features beyond the base functionality, the Supported-Features AVP may be absent from the SGmb commands. As defined in clause 7.1.1 of 3GPP TS 29.229 [105], when extending the application by adding new AVPs for a feature, the new AVPs shall have the M bit cleared and the AVP shall not be defined mandatory in the command ABNF.

As defined in 3GPP TS 29.229 [105], the Supported-Features AVP is of type grouped and contains the Vendor-Id, Feature-List-ID and Feature-List AVPs. On the SGmb reference point, the Supported-Features AVP is used to identify features that have been defined by 3GPP and hence, for features defined in this document, the Vendor-Id AVP shall contain the vendor ID of 3GPP (10415). If there are multiple feature lists defined for the SGmb reference point, the Feature-List-ID AVP shall differentiate those lists from one another.

On receiving an initial request application message, the destination host shall act as defined in clause 7.2.1 of 3GPP TS 29.229 [105]. The following exceptions apply to the initial RAR/RAA command pair:

- If the BM-SC supporting post-Rel-11 SGmb functionality is able to interoperate with a MBMS GW supporting Rel-11, the RAR shall include the features supported by the BM-SC within Supported-Features AVP(s) with the ‘M’ bit cleared. Otherwise, the RAR shall include the supported features within the Supported-Features AVP(s) with the M-bit set.

NOTE 1: One instance of Supported-Features AVP is needed per Feature-List-ID.

- If the RAR command does not contain any Supported-Features AVP(s) and the MBMS GW supports Rel-11 SGmb functionality, the RAA command shall not include the Supported-Features AVP. In this case, both BM-SC and MBMS GW shall behave as specified in the Rel-11 version of this document.

- If the RAR command contains the Supported-Features AVP, the MBMS GW shall include the Supported-Features AVP in the RAA command, with the ‘M’ bit cleared, indicating only the features that both the BM-SC and MBMS GW support.

NOTE 2: The client will always declare all features that are supported according to table 20.7.1. When more than one feature identifying a release is supported by both BM-SC and MBMS GW, the BM-SC will work according to the latest common supported release.

Once the BM-SC and MBMS GW have negotiated the set of supported features during session establishment, the set of common features shall be used during the lifetime of the Diameter session.

The table below defines the features applicable to the SGmb interface for the feature list with a Feature-List-ID of 1.

Table 20.7.1: Features of Feature-List-ID 1 used in SGmb

Feature bit	Feature	M/O	Description
0	MBMS Heartbeat	O	This feature indicates the support of the MBMS Heartbeat functionality, including the AVPs and corresponding procedures.
1	MBMS Cell List	O	This feature indicates the support of providing a MBMS-Cell-List AVP in the MBMS Session Start and MBMS Session Update procedures. For deployments with E-UTRAN access, this feature shall be supported.
Feature bit: The order number of the bit within the Feature-List AVP where the least significant bit is assigned number "0". Feature: A short name that can be used to refer to the bit and to the feature, e.g. "EPS". M/O: Defines if the implementation of the feature is mandatory ("M") or optional ("O") in this 3GPP Release. Description: A clear textual description of the feature.			

Annex A (informative): Interworking PCS1900 with PSDNs

Void.

Annex B (normative): Rate control related to Cellular Internet Of Things (CIoT) optimisations

B.1 General

The present annex defines specific requirements for rate control related to CIoT optimisations.

B.2 Support of rate control of user data

B.2.0 General

The rate of user data sent to and from a UE (e.g. a UE using CIoT EPS Optimizations) can be controlled in two different ways:

- Serving PLMN rate control
- APN rate control

Serving PLMN rate control is further described in 3GPP TS 23.401 [77].

The APN rate control parameters are a part of the configuration data stored in the GGSN/PGW and is configured on per APN basis.

APN rate control allows HPLMN operators on per APN and user to control the amount of user data sent DL and UL. This is done with help of policing user data on a maximum number of user data packets per time unit both DL and UL. APN rate control DL policing is done in the GGSN/PGW or the SCEF and the APN rate control policing UL is done in the UE. The GGSN/PGW or SCEF can also do APN rate control UL policing.
For further information on APN rate control UL in the UE, see 3GPP TS 24.301 [84].
For further information on APN rate control in the SCEF, see 3GPP TS 29.128 [110].

NOTE: Existing AMBR mechanisms are not suitable for such a service since, for radio efficiency and UE battery life reasons, an AMBR of e.g. > 100kbit/s is desirable and such an AMBR translates to a potentially large daily data volume.

B.2.1 APN Rate Control in the PGW

To enable APN rate control it shall be configured in the PGW per APN.

The APN rate control parameters, if configured, shall consist of:

- the maximum number of DL user data packets per time unit,
- the maximum number of UL user data packets per time unit,
- an indication whether the UE is allowed to send additional exception reports when the limit for the UL APN rate control has been reached , and
- if UE supports it, the maximum number of additional UL exception reports per time unit.

Possible time units shall be, minute, hour, day or week.

If the UE does not indicate APN rate control support, the GGSN/PGW may refrain from providing APN rate control information to the UE.

NOTE 1: The UE indicates support for APN rate control with help of an indicator in the Protocol Configuration Options IE (PCO IE) or the Extended Protocol Configuration Options IE (ePCO IE), see 3GPP TS 24.008 [54] or 3GPP TS 24.301 [84] for IE definition. The APN rate control indicator within the PCO/ePCO IE is received at IP-CAN session establishment.

NOTE 2: The UE and network support of the ePCO IE, is indicated with help of the Indication IE. The ePCO support indication within the Indication IE can be received at IP-CAN session establishment or at IP-CAN session modification. See 3GPP TS 29.274 [81] for IE definition.

If the APN rate control is supported by the UE and the Indication IE is received indicating support of ePCO IE at the IP-CAN session establishment request and the PGW supports the ePCO IE, the PGW shall in the reply, if configured for the APN used, include APN UL rate control parameters in the ePCO IE, see 3GPP TS 24.008 [54] for IE definition.
If the ePCO IE is not supported the PGW shall use the PCO IE.
The GGSN shall use the PCO IE.

If the APN rate control UL parameter(s) is modified and the ePCO IE is supported, the PGW shall initiate an IP-CAN session modification procedure and include the APN UL rate control parameters in the ePCO IE.
If the ePCO IE is not supported the PGW shall use the PCO IE.
The GGSN shall use the PCO IE.

The GGSN/PGW shall enforce the APN rate control per UE and APN according to the configuration for DL and may enforce APN rate control for UL, e.g. when the PGW have indicated to the UE that the UE is not allowed to send exception reports when the limit for the UL APN rate control has been reached.

NOTE 3: The UE locally enforces this uplink APN rate control instruction. The UE considers this APN rate control instruction as valid until it receives a new one from the GGSN/PGW.

B.2.2 Serving PLMN Rate Control information handling in the PGW

If Serving PLMN rate control information is received in the Serving PLMN Rate Control IE from the MME, the PGW shall store this information and use that for rate control enforcement DL for this UE.
If the PGW previously have received Serving PLMN rate control information, the PGW shall behave as follows:

- If the PGW receives new Serving PLMN rate control information in the Serving PLMN Rate Control IE from the MME, the PGW shall replace the old Serving PLMN rate control information with the new Serving PLMN rate control information and use that for rate control enforcement DL for this UE.

- If the PGW receives no Serving PLMN rate control information in the Serving PLMN Rate Control IE from the MME in an IP-CAN session establishment or an IP-CAN session modification , the PGW shall still consider the latest received Serving PLMN rate control information from the MME as valid.

- If PGW receives an indication that Serving PLMN rate control does not apply in the Serving PLMN Rate Control IE, the PGW shall remove the rate control information based on Serving PLMN rate control information.

See 3GPP TS 29.274 [81] for Serving PLMN Rate Control IE definition.

APN rate control, if configured, also applies for the same IP-CAN session, see subclause B.2.1.

Annex C (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New**
03-2015	CT-67	CP-150126	0444	2		Paging policy differentiation for IMS voice	**13.0.0**
09-2015	CT-69	CP-150464	0450	1	A	Usage of the UDP port for default unicast encapsulation mode at the SGmb interface is required to support SYNC protocol.	13.1.0
09-2015	CT-69	CP-150468	0453	-	A	3GPP Type of RADIUS 3GPP-User-Location-Info-Time sub-attribute	13.1.0
09-2015	CT-69	CP-150472	0455	1	A	Correction of SGmB L4 Transport protocol	13.1.0
12-2015	CT-70	CP-150658	0456	1	B	MBMS bearer establishment and update with cell ID list	13.2.0
12-2015	CT-70	CP-150669	0459	1	A	Transport protocols of Diameter for signalling plane of non transparent case	13.2.0
03-2016	CT-71	CP-160108	0460		B	Support for Non-IP data for CIoT over Sgi	13.3.0
03-2016	CT-71	CP-160089	0465	2	B	Usage of the UDP port for default unicast encapsulation mode at the Gmb interface is required to support SYNC protocol	13.3.0
06-2016	CT-72	CP-160252	0466	1	B	Support of Non-IP delivery data	13.4.0
06-2016	CT-72	CP-160252	0469	-	B	RAT-Type extension for NB-IoT	13.4.0
06-2016	CT-72	CP-160252	0471	1	B	Non-IP Transport	13.4.0
06-2016	CT-72	CP-160277	0472	1	B	Support for rate control of CIoT datat	13.4.0
06-2016	CT-72	CP-160281	0468	1	B	Support of Non-IP delivery data	14.0.0
09-2016	CT-73	CP-160441	0474	1	A	PDP type extension with Non-IP value	14.1.0
09-2016	CT-73	CP-160441	0476	1	A	Support of Exception Reports for CIoT	14.1.0
09-2016	CT-73	CP-160459	0477	-	B	APN rate control support in GPRS	14.1.0
09-2016	CT-73	CP-160441	0479	-	A	APN rate control DL correction	14.1.0
09-2016	CT-73	CP-160452	0480	2	B	Modify the 3GPP-User-Location Info to support eNB ID Information	14.1.0
12-2016	CT-74	CP-160632	0481	1	B	Local MBMS related MBMS data delivery	14.2.0
12-2016	CT-74	CP-160613	0483	1	A	Correction to SGi PtP tunnelling based on UDP/IP	14.2.0
12-2016	CT-74	CP-160616	0484	1	F	Diameter base protocol specification update	14.2.0
03-2017	CT-75	CP-170076	0486	1	F	Handling of Vendor-Specific-Application-Id AVP	14.3.0
03-2017	CT-75	CP-170086	0487	1	F	Support of long and short Macro eNodeB IDs	14.3.0
03-2017	CT-75	CP-170075	0489	2	A	Correction in APN rate control	14.3.0
03-2017	CT-75	CP-170076	0492	1	F	Update instance number for the Failed-AVP in answer commands	14.3.0
12-2017	CT-78	CP-175088	0497	2	F	Rate control for MO exception data	14.4.0

History

Document history		
V14.3.0	April 2017	Publication
V14.4.0	January 2018	Publication