3GPP TSG CN Plenary Meeting #16   **NP-020153**
5th - 7th June 2002. Marco Island, USA.

Title:	**Liaison Statement on "IPv6 update of stage 3 specifications"**
Source:	**CN WG3**
Agenda item:	**5.1**
Document for:	**INFORMATION**

3GPP TSG-CN WG3#22   **Tdoc N3-020361**
Fort Lauderdale, USA. 8th – 12th April 2002

To:	**SA WG2**
Cc:	**TSG CN, CN WG1, CN WG2, SA WG3, SA WG5, TSG T, T WG1 and T WG2,**

Response to: **LS (S2-020910) on "Prefix allocation for IPv6 stateless address autoconfiguration".**

Contact Person:
    Name: Hans Rönneke, Johanna Wild, Jay Iyer
    E-mail Address: hans.ronneke@ericsson.com, johanna.wild@motorola.com, jiyer@cisco.com

Attachments: (N3-020328) CN3 agreed Rel-5 CR 044r2 to 29.061.

1. Description:

CN3 wants to thank SA2 for the Liaison Statement S2-020910 on "Prefix allocation for IPv6 stateless address autoconfiguration".

The attached CR 044r2 (Rel-5) in N3-020328 has been agreed at CN3#22 for update of Rel-5 of stage 3 specification TS 29.061 for IPv6 Stateless Address Autoconfiguration and other IPv6 related changes. However, CN3 has not agreed with the changes for R99/Rel-4, as the changes are significant and not considered necessary to be introduced in R99/Rel-4.

Question 1:
Our first question to SA2 is what are the specific requirements to introduce IPv6 stateless address autoconfiguration changes in R99/Rel-4, as IMS is available only starting in Rel-5?

Question 2:
It is also unclear to CN3 why SA2 has used the work item code "IMS-CCR" for the R99/Rel-4 CRs on 23.060?

Question 3:
Have supporting elements such as RADIUS interface enhancements been considered for use with stateless address autoconfiguration?

Included in the CN3 agreed CR 044r2 was also an update of the stage 3 specification to be aligned with stage 2 on other IPv6 issues like Stateful Address Autoconfiguration and RADIUS interface, and with the latest IETF RFC standards e.g. IPv6 multicast.

Question 4:
CN3 would like SA2 to confirm whether stage 3 update on IPv6 issues like Stateful address autoconfiguration, RADIUS interface and other IPv6 aspects was also intended in the SA2 LS and from what release?

2. Actions:

SA2:
To provide answer on the issues above.

3. Date of Next CN3 Meeting:

CN3 #23   13th – 17th May 2002   Budapest, Hungary

CR-Form-v5

CHANGE REQUEST

| ⌘ | **29.061** CR **044** | ⌘ **rev** | **2** | ⌘ | Current version: | **5.1.0** | ⌘ |

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

Proposed change affects: ⌘   (U)SIM ☐   ME/UE **X**   Radio Access Network ☐   Core Network **X**

Title: ⌘	Address autoconfiguration of IPv6 terminals and IPv6 update	
Source: ⌘	Ericsson, Motorola, Cisco	
Work item code: ⌘	IMS-CCR	***Date:*** ⌘ 2002-04-11

Category: ⌘	**C**	***Release:*** ⌘	REL-5

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

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change: ⌘	Alignment with approved SA2 changes to TS 23.060. See LS S2-020764 from SA2#23 to CN1, CN2, CN3, SA3, SA5, T1 and T2.

The procedures introduced by this CR are in line with the latest updates to the Dynamic IPv6 Stateless Address Allocation described in 23.060, as approved at TSG #15 for R'99 onwards (see 23.060 CR 305r2 in tdoc S2-020760 for R'99, and mirror CRs for R4 and R5 in S2-020761 and S2-020762 respectively).

IPv6 is supported in the user plane since R99, however the stage 3 details of its working have never been defined. IPv6 requires a different behaviour from the MS and the GGSN compared to IPv4. This contribution proposes to introduce the description of the access to an IPv6 PDN, in 29.061. |
Summary of change: ⌘	Subclauses added to clause 11 "Interworking with PDN (IP)" for Stateless and Stateful address autoconfiguratio. Clause 11.3 "Number and Addressing" updated with IPv6 aspects. Clause 11.7 "IP Multicast access" updated to be aligned with IPv6 multicast as specified in RFC 2710. Clause 12 corrected to be protocol independent. An error of a missing PDP Type value for IPv6 is corrected in clause 16.4.7. Clause 2 "References", and clause 3 "Definitions, Abbreviations and Symbols" updated with new IPv6 items. A few updates of old out-dated references are also done in clause 11 and 13.
Consequences if not approved: ⌘	Stage 3 aspects of supporting IPv6 in the user plane would be missing, leading to potential interoperability problems between terminals and core network. Stage 3 will not be aligned with stage 2 (23.060). As identified by the IETF IPng working group, a TE conforming to IETF standards would not always work with an MT conforming to the IPv6 stateless or stateful address autoconfiguration procedures as specified in the current version of this specification. Also the present solution is prone to incompatibilities with future development of IPv6.
Clauses affected: ⌘	2; 3; 11.2.1; 11.3; 11.7; 12; 13; 16

Other specs	⌘	**X**	Other core specifications	⌘	24.008
affected:		**X**	Test specifications		34.123
			O&M Specifications		
Other comments:	⌘				

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at: http://www.3gpp.org/3G_Specs/CRs.htm. Below is a brief summary:

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

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

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

2 References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies.

[1]   Void.

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

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

[4]   Void.

[5]   Void.

[6]   Void.

[7]   Void.

[8]   Void.

[9]   Void.

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

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

[12]   <VOID>

[13]   <VOID>

[14]   <VOID>

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

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

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

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

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

[20]   <VOID>

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[38]   IETF RFC2865 (2000), C. Rigney, S. Willens, A. Rubens, W. Simpson: "Remote Authentication
            Dial In User Service (RADIUS)".

[39]   IETF RFC2866 (2000), C. Rigney, Livingston: " RADIUS Accounting ".

[40]   3GPP TS 23.003: "3rd Generation Partnership Project; Technical Specification Group Core
            Network; Numbering, addressing and identification".

[41]   IETF RFC2882 (2000), D. Mitton: "Extended RADIUS Practices".

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

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

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

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

[46]   IETF Internet-Draft: "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", draft-ietf-dhc-
            dhcpv6-234.txt, work in progress.

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

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

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

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

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

3   Definitions, abbreviations and symbols

3.1   Definitions

For the purposes of the present document, the following terms and definitions given in 3GPP TS 22.060 and 3GPP TS 23.060 and the following apply:

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

A/Gb mode: indicates that the text applies only to a system or sub-system which operate in A/Gb mode of operation, i.e. with a functional division that is in accordance with the use of an A or a Gb interface between the radio access network and the core network

Iu mode: indicates that the text applies only to a system or a sub-system which operates in Iu mode of operation, i.e. with a functional division that is in accordance with the use of an Iu-CS or Iu-PS interface between the radio access network and the core network

3.2   Abbreviations

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

APN	Access Point Name
ATM	Asynchronous Transfer Mode
BG	Border Gateway
CHAP	Challenge Handshake Authentication Protocol
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol version 6
DNS	Domain Name System
DVMRP	Distance Vector Multicast Routing Protocol
GGSN	Gateway GPRS Support Node
GTP-U	GPRS Tunnelling Protocol for user plane
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPCP	IP Control Protocol (PPP NCP for IPv4)
IPV6CP	IPv6 Control Protocol (PPP NCP for IPv6)
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
LAC	L2TP Access Concentrator
LAN	Local Area Network
LNS	L2TP Network Server
MIP	Mobile IP
MLD	Multicast Listener Discovery
MOSPF	Multicast Open Shortest Path First
MS	Mobile Station
MT	Mobile Terminal
MTU	Maximum Transfer Unit
NAI	Network Access Identifier
PAP	Password Authentication Protocol
PDCP	Packet Data Convergence Protocol
PDN	Packet Data Network
PDU	Protocol Data Unit
PIM-SM	Protocol Independant Multicast – Sparse Mode

PPP	Point-to-Point Protocol
PPPv6	IPv6 over Point-to-Point Protocol
PS	Packet Switched
RADIUS	Remote Authentication Dial In User Service
SGSN	Serving GPRS Support Node
SMDS	Switched Multimegabit Data Service
TCP	Transmission Control Protocol
TE	Terminal Equipment
TEID	Tunnel End-point Identifier
UDP	User Datagram Protocol

Next modified section

11.2.1   Access to Internet, Intranet or ISP through Packet Domain

The access to Internet, Intranet or ISP may involve specific functions such as : user authentication, user's authorization, end to end encryption between MS and Intranet/ISP, allocation of a dynamic address belonging to the PLMN/Intranet/ISP addressing space, IPv6 address autoconfiguration, etc.

For this purpose the Packet Domain may offer:

- either direct transparent access to the Internet; or

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

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

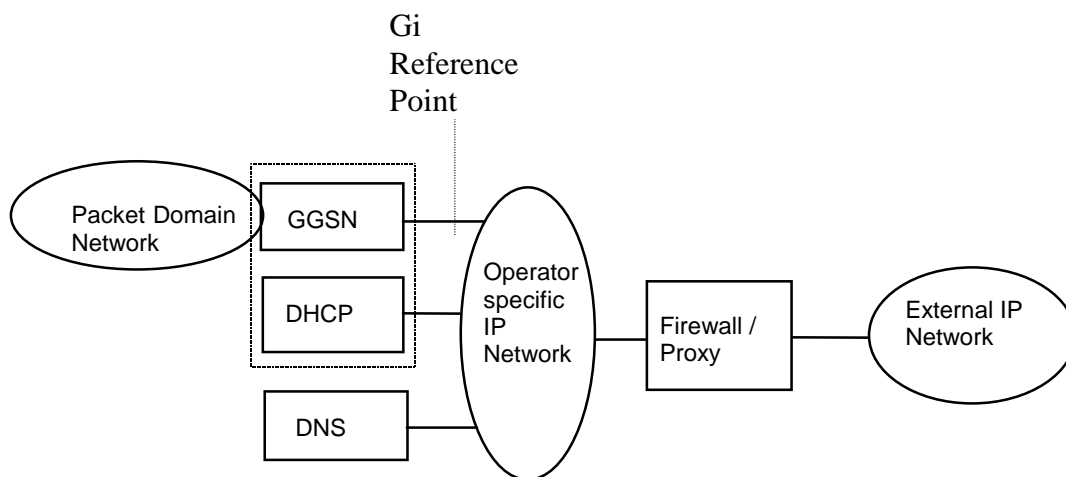### 11.2.1.1   Transparent access to the Internet

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

In this case (see figure 9):

- the MS is given an address or IPv6 Prefix belonging to the operator addressing space. The address or IPv6 Prefix is given either at subscription in which case it is a static address or at PDP context activation in which case it is a dynamic address. This address or IPv6 Prefix is used for packet forwarding between the Internet and the GGSN and within the ~~GGSN~~packet domain. ~~In IPv6, the address given is the link-local address. Thus, for the IPv6~~With IPv6, either Stateless or Stateful Address Autoconfiguration ~~can~~shall ~~it is not necessary to use a DHCP~~

~~implementation for the address allocation, but any unique identifier for the MS in the GGSN is sufficient;~~<u>be used to assign an IPv6 address to the MS. These procedures are as described in the IPv6 non-transparent access case except that the addresses belong to the operator addressing space. The use of stateful or stateless is configured per APN.</u>

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

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

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

- The user level configuration may be carried out between the TE and the intranet, the Packet Domain network is transparent to this procedure.
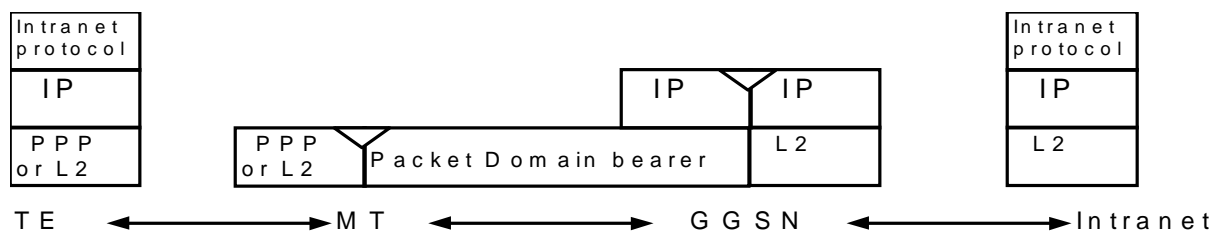
The used protocol stack is depicted in figure 10.

Figure 10: Transparent access to an Intranet

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

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

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

11.2.1.2   <u>IPv4 </u>Non Transparent access to an Intranet or ISP

In this case:

- the MS is given an address belonging to the Intranet/ISP addressing space. The address is given either at subscription in which case it is a static address or at PDP context activation in which case it is a dynamic address. This address is used for packet forwarding within the GGSN and for packet forwarding on the Intranet/ISP. This requires a link between the GGSN and an address allocation server, like ~~Radius~~<u>AAA</u>, DHCP, …, belonging to the Intranet/ISP;

- the MS shall send an authentication request at PDP context activation and the GGSN requests user authentication from a server, like ~~Radius~~<u>AAA</u>, DHCP, …, belonging to the Intranet/ISP;

- the protocol configuration options are retrieved (if requested by the MS at PDP context activation) from some server (~~Radius~~<u>AAA</u> 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.
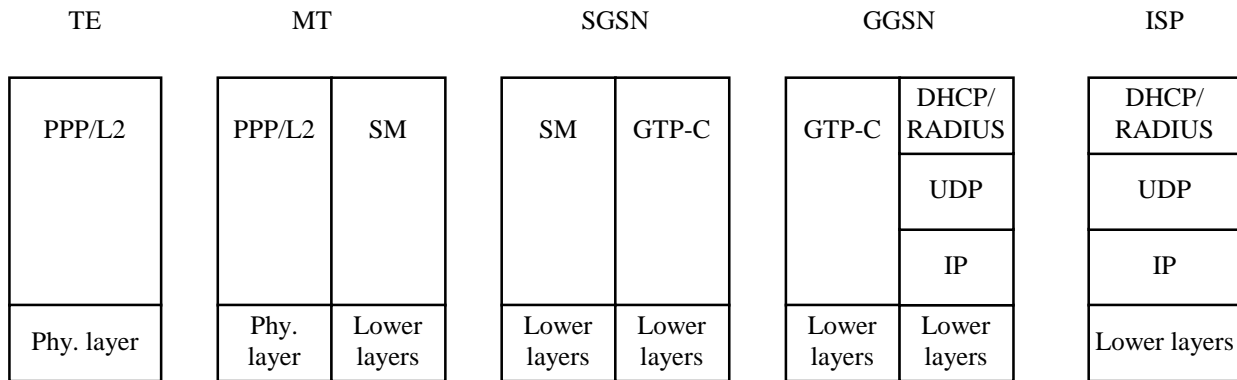
TE	MT		SGSN		GGSN		ISP
PPP/L2	PPP/L2	SM	SM	GTP-C	GTP-C	DHCP/ RADIUS	DHCP/ RADIUS
						UDP	UDP
						IP	IP
Phy. layer	Phy. layer	Lower layers	Lower layers	Lower layers	Lower layers	Lower layers	Lower layers

Figure 11a: Signalling plane of non transparent case

The following description bullet items describe the signal flow.

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

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

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

4) The TE requests IP configuration by sending the IPCP Configure-Request message to the MT indicating either the static IP address that shall be used or that an IP-address shall be dynamically allocated.

5) The MT sends the Activate PDP context request message to the SGSN, including the Protocol Configuration Options. The SGSN sends the Create PDP context req message to the chosen GGSN including the unmodified Protocol Configuration Options.

6) The GGSN deduces from the APN:

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

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

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

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

   - RADIUS for authentication and IP-address allocation~~.~~. The ~~RADIUS~~ 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 ~~RADIUS~~ 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 ~~[20]~~[21] 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.
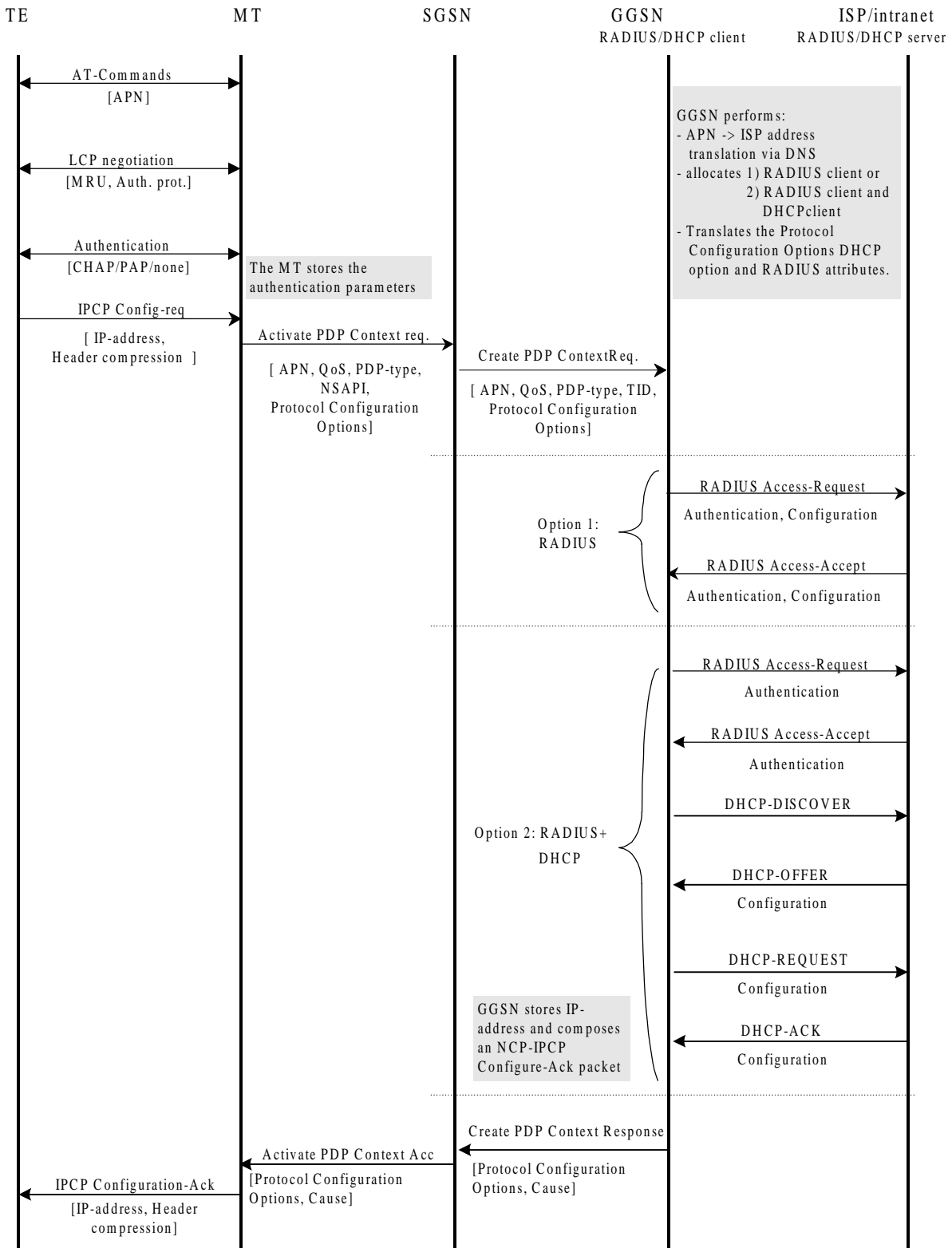
Figure 11b: PDP Context Activation for the IPv4 Non-transparent IP case

11.2.1.3   IPv6 Non Transparent access to an Intranet or ISP

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

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

Whether to use stateless or stateful address autoconfiguration procedure is configured per APN in the GGSN. For APNs configured as stateless, the GGSN ~~must~~shall only use the ~~64 bit~~ Prefix part of the IPv6 address for forwarding of mobile terminated IP packets. The size of the prefix shall be according to the maximum prefix length for a global IPv6 address as specified in the IPv6 Addressing Architecture, see RFC 2373 [28].

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

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

For MS, IPv6 Stateless Address Autoconfiguration is mandatory, and IPv6 Stateful Address Autoconfiguration ~~(DHCPv6)~~ is optional.

11.2.1.3.1   IPv6 PDP Context Activation

In this case:

- The GGSN provides the MS with ~~is given~~ an IPv6 Prefix ~~address~~ belonging to the Intranet/ISP addressing space. A dynamic IPv6 address ~~may~~shall be given using either stateless or stateful address autoconfiguration. This IPv6 address is used for packet forwarding within the packet domain ~~GGSN~~ and for packet forwarding on the Intranet/ISP;

- the MS may send an authentication request at PDP context activation and the GGSN ~~can~~may request user authentication from a server, ~~like~~e.g. ~~Radius,~~ 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. ~~(Radius or~~ 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 ~~must~~shall be assigned by the GGSN. The GGSN ensures the uniqueness of this interface-identifier. The MT ~~must~~shall then enforce the use of this Interface-Identifier by the TE. This is valid for both stateless and stateful address autoconfiguration.

- the communication between the Packet Domain and the Intranet/ISP may be performed over any network, even an insecure e.g. the Internet. In case of an insecure connection between the GGSN and the Intranet/ISP there may be a specific security protocol over the insecure connection~~in between~~. This security protocol is defined by mutual agreement between PLMN operator and Intranet/ISP administrator.

In the following signalling flow example, PPP is used as layer 2 protocol over the R reference point. The MT ~~acts~~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 ~~information~~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 Ccontext Rrequest message to the SGSN, including the Protocol Configuration Options. The Protocol Configuration Options may contain negotiated LCP options such as negotiated Authentication Protocol as well as any authentication data previously stored in the MT. The MS shall for dynamic address allocation leave PDP Address empty and set PDP Type to IPv6. The SGSN sends the Create PDP context request message to the chosen GGSN including the unmodified Protocol Configuration Options.

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

   - IPv6 address allocation type (stateless or stateful);

   - the source of IPv6 Prefixes in the stateless case (GGSN internal prefix pool, or external address allocation server);

   - any server(s) to be used for address allocation, authentication and/or protocol configuration options retrieval (e.g. IMS related configuration, see [47]);

   - the protocol likee.g. RadiusRADIUS, to be used with this / thosethe server(s);

   - the communication and security feature needed to communicatedialogue with this / thosethe 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 RADIUSAAA 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 RADIUSAAA server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the GGSN;

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

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

   The GGSN shall in the PDP Address IE in the Create PDP Context Response return an IPv6 address composed of a 64 bit Prefix and an 64 bit Interface-Identifier. The Interface-Identifier canmay have any value and it does not need to be unique within or across APNs. It mustshall 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 RADIUSAAA server mustshall be globally or site-local unique, if stateless address autoconfiguration is configured on this APN. If, on the other hand, stateful address autoconfiguration is configured on the APN, the Prefix part of the IPv6 address returned in the PDP Address IE shall be set to the link-local prefix (FE80::/64).

   The GGSN shall analyse the requested values of all the protocol options contained in the received Protocol Configurations Options IE. The GGSN response shall be in accordance with the relevant PPP or PPPv6 standards [21] and [48].

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

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

If Protocol Configuration Options are received from the GGSN, the SGSN shall relay those to the MS.

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

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

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

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

In case a link terminate request packet was sent to the TE, the TE and MT negotiates for link termination. The MT may then send a final AT-response to inform the TE about the rejected PDP Context activation.

An LCP Terminate-request causes a PDP context deactivation.
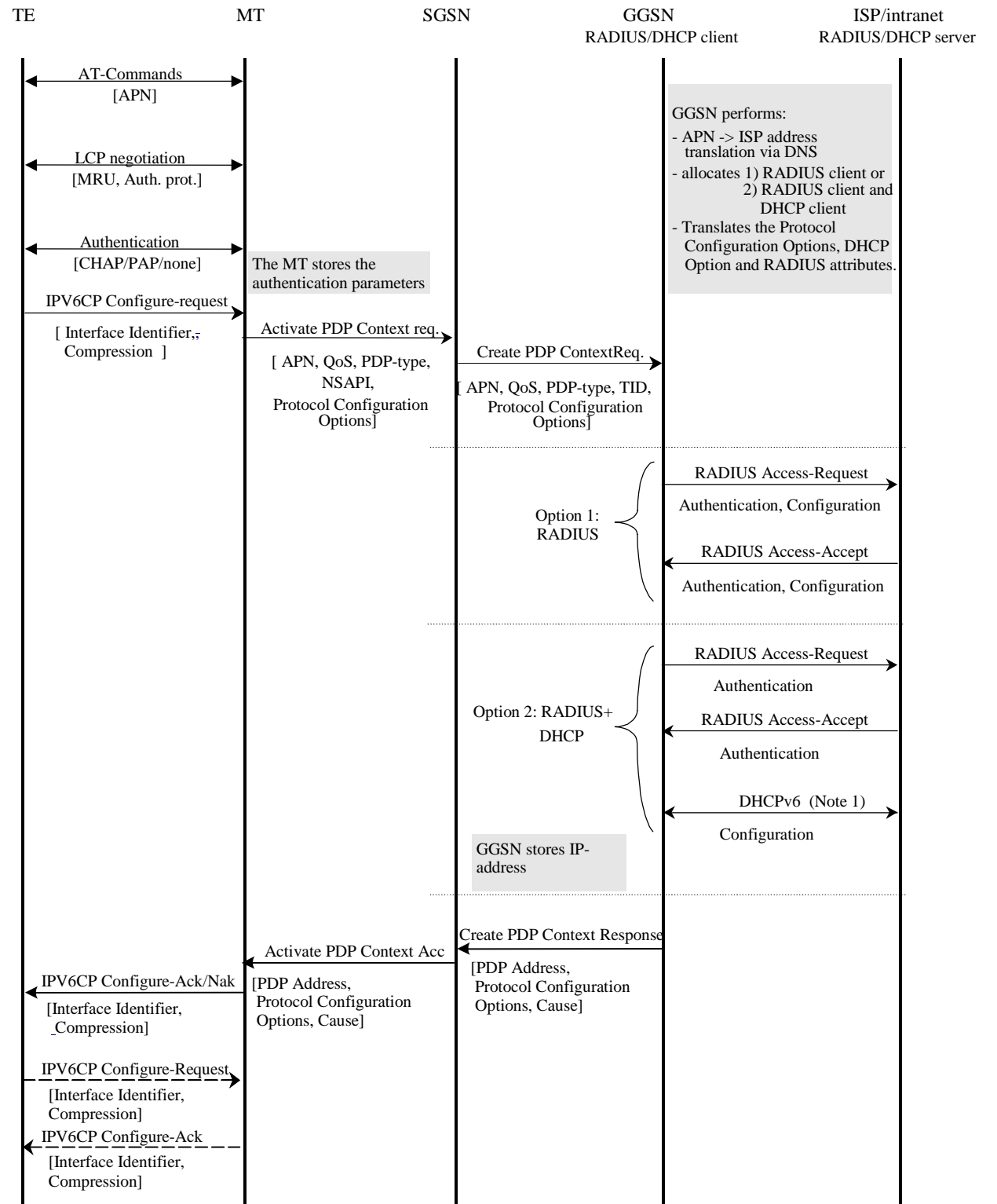
Note 1: DHCPv6 may be used for IPv6 prefix allocation when an appropriate RFC becomes available.

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

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

11.2.1.3.2   IPv6 Stateless Address Autoconfiguration

As described in 3GPP TS 23.060 [3], a PDP Context of PDP type IPv6 activated by means of the IPv6 Stateless Address Autoconfiguration Procedure is uniquely identified by the prefix part of the IPv6 address only. The MS canmay select any value for the Interface-Identifier part of the address. The only exception is the Interface-Identifier for the link-local address used by the MS (see RFC 2373 [28]). This Interface-Identifier mustshall 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 For APNs configured to use Stateless Address Autoconfiguration, the procedure can for example look like themay be as follows following:

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

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

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

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

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

    -The Prefix sent in the Router Advertisements shall have a length of 64 bits and shall be identical to the Prefix returned in the Create PDP Context Response. The Prefix is contained in the Prefix Information Option of the Router Advertisements and shall have the A-flag set ("Autonomous address configuration flag") and the L-flag cleared (i.e. the prefix should not be used for on-link determination). The lifetime of the prefix shall be set to infinity. In practice, the lifetime of a Prefix will be the lifetime of its PDP Context. There shall be exactly one Prefix included in the Router Advertisements.

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

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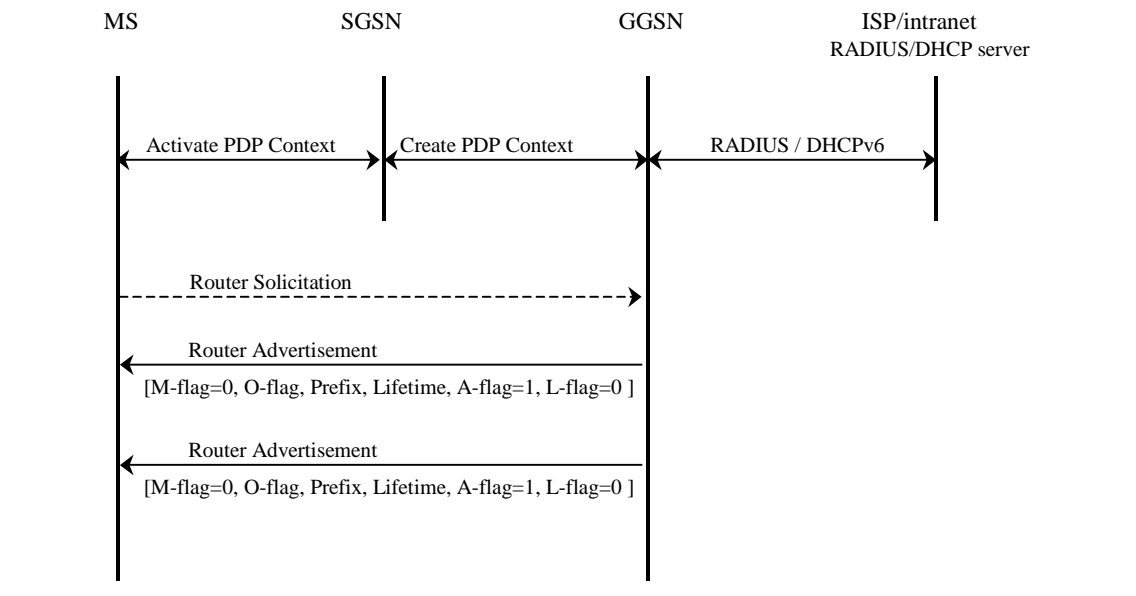
MS   SGSN   GGSN   ISP/intranet
                                                           RADIUS/DHCP server

Activate PDP Context   Create PDP Context   RADIUS / DHCPv6

Router Solicitation

Router Advertisement

[M-flag=0, O-flag, Prefix, Lifetime, A-flag=1, L-flag=0]

Router Advertisement

[M-flag=0, O-flag, Prefix, Lifetime, A-flag=1, L-flag=0]

Figure 11bbd: IPv6 Stateless Address Autoconfiguration

11.2.1.3.3   IPv6 Stateful Address Autoconfiguration

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

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

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

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

3) When the MS has received a Router Advertisement with the M-flag set, it shall start a DHCPv6 configuration as described in subclause "Address allocation using DHCPv6" including a request for an IPv6 address.
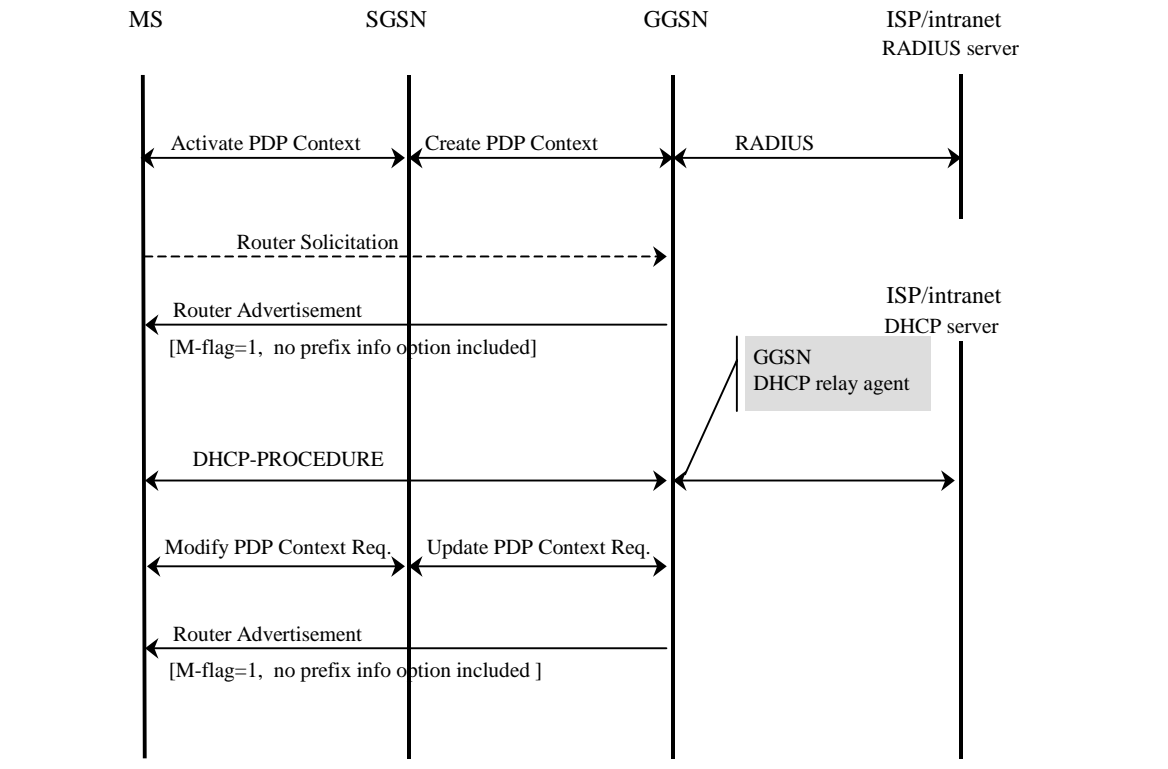
Figure 11bc: IPv6 Stateful Address Autoconfiguration

11.2.1.3.4~~3~~   IPv6 Router Configuration Variables in the GGSN

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

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

MaxRtrAdvInterval
>	Shall have a default value of 21600 seconds (6 h).

MinRtrAdvInterval
>	Shall have a default value of 0.75* MaxRtrAdvInterval i.e.16200 seconds (4.5 h).

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

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

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

MAX_INITIAL_RTR_ADVERT_INTERVAL
>	This constant may be a variable within GPRS. It ~~can~~may have a value that gradually increases (exponentially or by some other means) with the number of initial Router Advertisements sent. This

will enable a fast set-up of the MS-GGSN link in most cases, while still allowing the MS to receive a
Router Advertisement within the initial phase, even in case of bad radio conditions or slow response
time, without having to send a large number of initial Router Advertisements.

MAX_INITIAL_RTR_ADVERTISEMENTS

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

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

~~11.2.1.3~~11.2.1.4   Access to Internet, Intranet or ISP with Mobile IPv4

> **Rest of subclause unchanged**

> **Next modified section**

11.3   Numbering and Addressing

In the case of interworking with public IP networks (such as the Internet), the PLMN operator shall use public network
addresses. These public addresses can be reserved from the responsible IP numbering body, or from an ISP with which
the PLMN operator has an agreement. In case of IPv6, a global IPv6 prefix can be obtained from the same sources.

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

1. the GPRS operator manages internally the subnetwork addresses or IPv6 prefixes. Each private network is
   assigned a unique subnetwork address or range of IPv6 prefixes. Normal routing functions are used to route
   packets to the appropriate private network;

2. each private network manages its own addressing. In general this will result in different private networks having
   overlapping address ranges. A logically separate connection (e.g. an IP in IP tunnel or layer 2 virtual circuit) is
   used between the GGSN and each private network. In this case the IP address alone is not necessarily unique.
   The pair of values, Access Point Name (APN) and IP address or IPv6 Prefix, is unique.

Note: In IPv6 "site-local addresses" replace "private addresses" in IPv4, see RFC 2373 [28]. Site-local
                 addresses ~~can~~may be used when a site (e.g. a corporate network) requires local administration of its
                 address space. ~~In IPv6 there are no "private" addresses as in IPv4. Site-local addresses can be used
                 instead when a site (e.g. a corporate network) requires local administration of its address space, since
                 there are enough addresses to always use global addresses. There are "site-local" addresses though, but
                 which have a slightly different intention, see RFC 2373 [28].~~

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

-    The PLMN operator allocates a static IP address (IPv4 or IPv6) when the subscription record is built. The IP
     address is reserved from a pool of free IP addresses. Each external network has its own pool of addresses.

~~-~~The PLMN operator allocates (either on its own or in conjunction with the external network) a dynamic IP
     ~~address~~(IPv4 or IPv6) address or ~~64-bit~~ IPv6 prefix ~~when the MS performs the PDP Context Activation
     procedure with dynamic address allocation~~ as described in 3GPP TS 23.060.

11.7   IP Multicast access

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

In order for the Packet Core Network to support Multicast traffic that will allow the MS to subscribe to multicast groups from outside the PLMN, the GGSN shall support IGMP (IPv4) and/or MLD (IPv6) and one or more Inter-Router Multicast protocols, such as DVMRP, MOSPF, or PIM-SM.

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

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

The IP-Multicast proxy will perform the following tasks:

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

- maintain a list of mobiles that joined one or more Multicast groups. This list is built/updated each time the GGSN receives an IGMP Join ~~Message~~ or MLD Report message from the mobile;

- send, based on this maintained list of mobiles, multicast routing information to the routers attached to the Packet Domain, allowing them to route multicast packets;

- upon reception by the GGSN of multicast packets, make and send a copy as Point-to-Point packets, to each mobile of the group.

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

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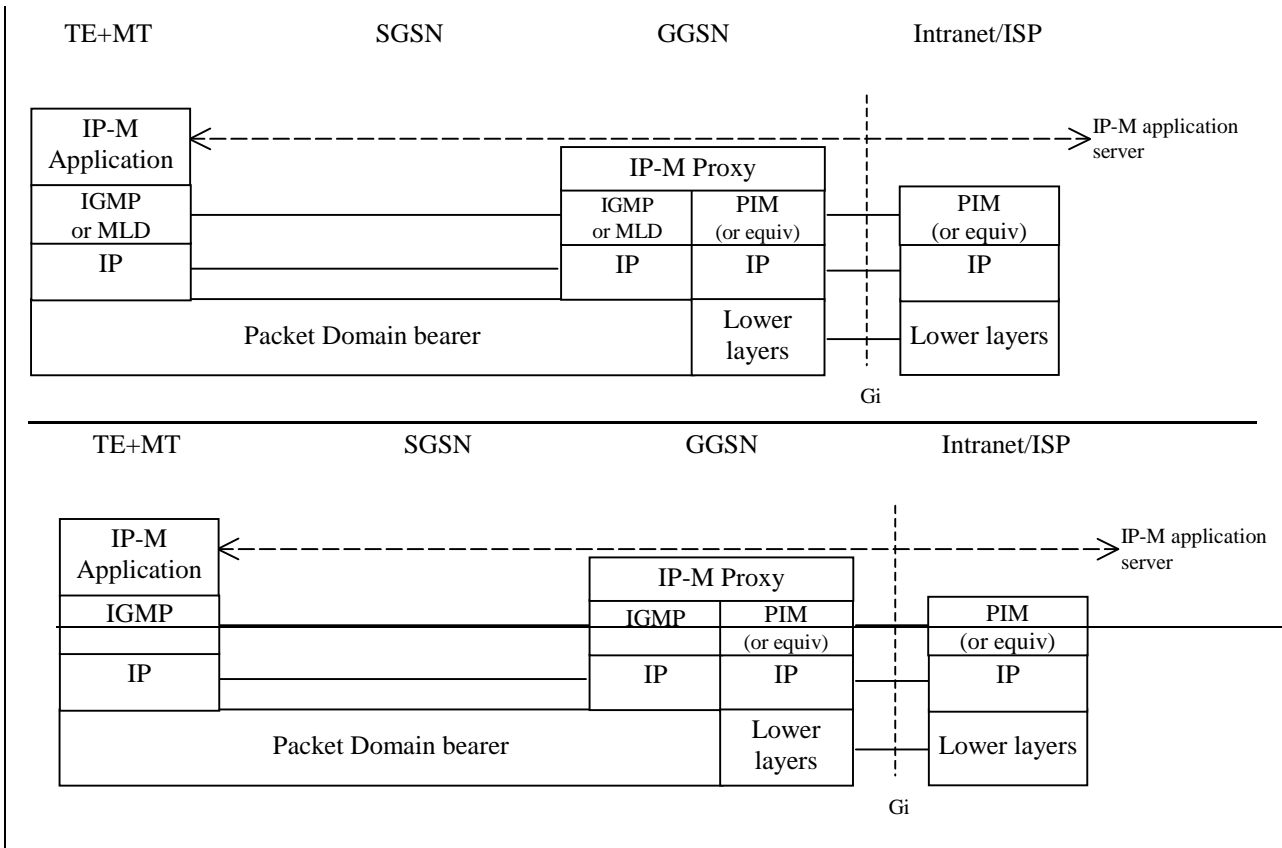
Figure 12: Protocol configuration for IP-Multicast handling (control plane)

12 Interworking with PDN (PPP)

12.1 General

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

12.2 PDN Interworking Model

The interworking point is at the Gi reference point. The GGSN for interworking with the ISP/PDN is the access point of the Packet Domain (see figure 13). The GGSN will either terminate the PPP connection towards the MS or may further relay PPP frames to the PDN. The PPP frames may be tunnelled in e.g. L2TP.
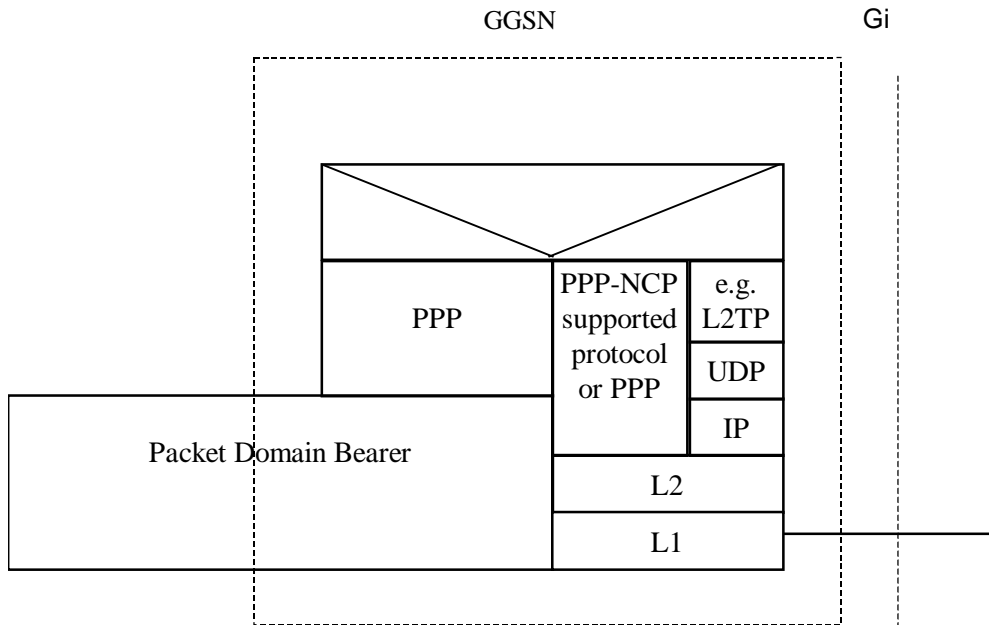
Figure 13: The protocol stacks for the Gi PPP reference point

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

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

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

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

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

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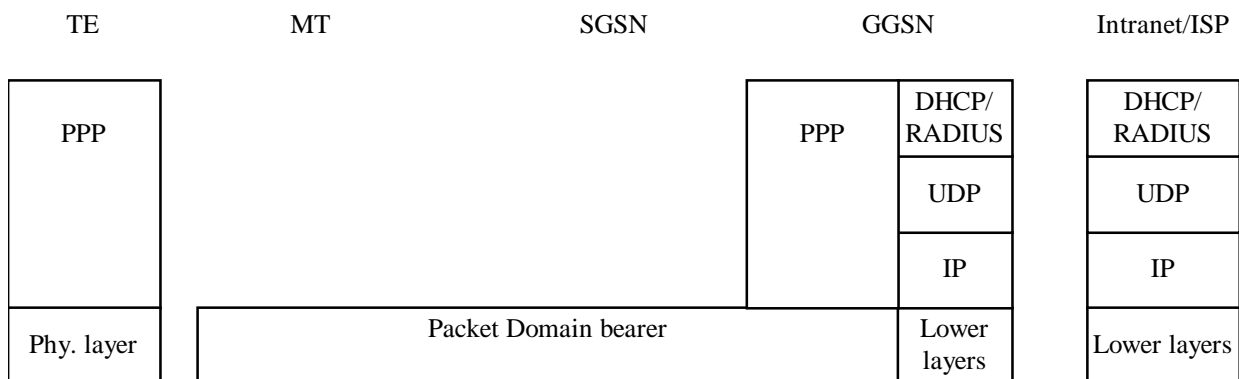

Figure 14: Protocol stack for direct access to IP-based Intranets/ISPs

- virtual dial-up access to a PDN with PPP frame tunnelling as depicted in figure 15.
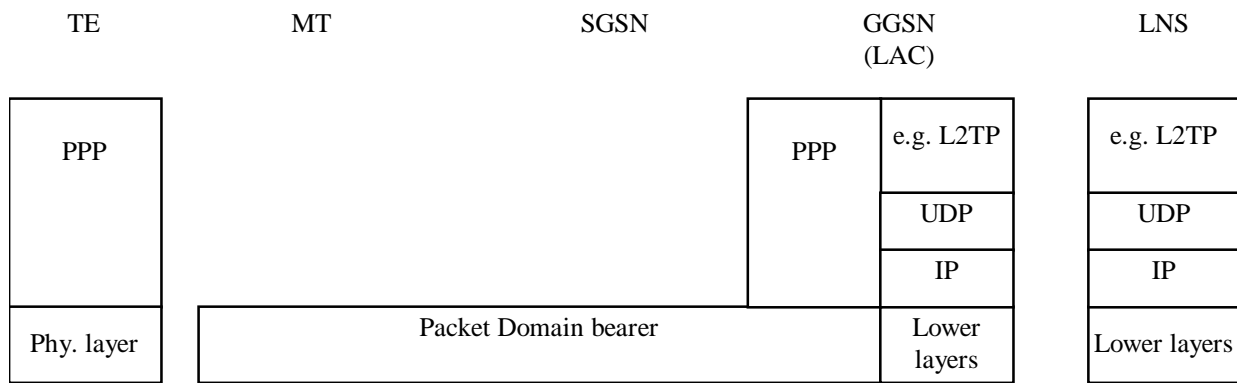
TE	MT	SGSN	GGSN (LAC)	LNS

PPP			PPP	e.g. L2TP	e.g. L2TP
				UDP	UDP
				IP	IP
Phy. layer		Packet Domain bearer		Lower layers	Lower layers

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

12.2.1.1   Procedural description

In this case:

- the MS is given an address belonging to the Intranet/ISP addressing space. The address is given either at subscription in which case it is a static address or at PDP context activation in which case it is a dynamic address. This address is used for packet forwarding within the GGSN and for packet forwarding on the Intranet/ISP. This requires a link between the GGSN and an address allocation server, such as ~~Radius~~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~~RADIUS, DHCP or L2TP to be used with this / those server(s);

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

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

- RADIUS for authentication and IP-address allocation. The ~~RADIUS~~ 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 ~~RADIUS~~ 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 ~~IPCP (in case of IP)~~ negotiations are then carried out. During these negotiations the GGSN may acknowledge values, for any LCP options related to 'L2' framing (e.g. 'ACCM', 'ACFC' and 'FCS-Alternatives'), as proposed by the MT, which itself is forwarding these negotiations from the TE.

NOTE: With the <PDP Type>"PPP" the MT may provide a PPP relay (or proxy) function between the TE and GGSN. This gives the opportunity for the MT to intercept the 'L2' framing end to end negotiations.

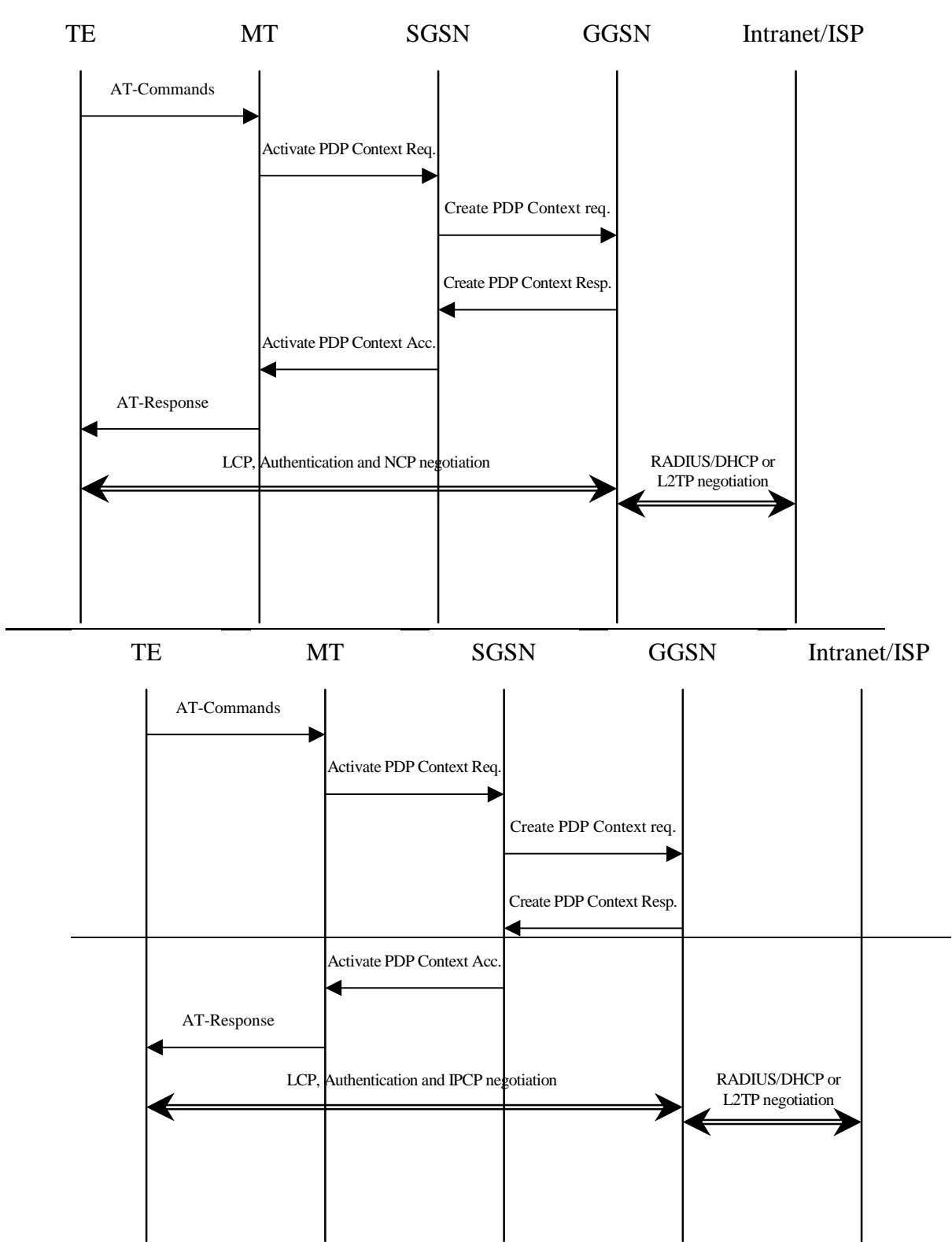EXAMPLE: In the following example the successful PDP context activation is shown.

Figure 16a

13 Interworking with PDN (DHCP)

13.1 General

In current LAN environments the most commonly used configuration protocol is DHCP (Dynamic Host Configuration Protocol, [20]).[26]) and DHCPv6 when it becomes an RFC standard [46]. It provides a mechanism for passing a large set of configuration parameters to hosts connected to a TCP/IP network (IP address, sub-net mask, domain name, MTU, etc.) in an automatic manner. Moreover DHCP may assign IP addresses to clients for a finite lease time, allowing for sequential reassignment of addresses to different users.

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

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

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

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

- if the DHCP lease expires

- if the DHCP renewal is rejected by the DHCP server

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

13.2 PDN Interworking Model for DHCP

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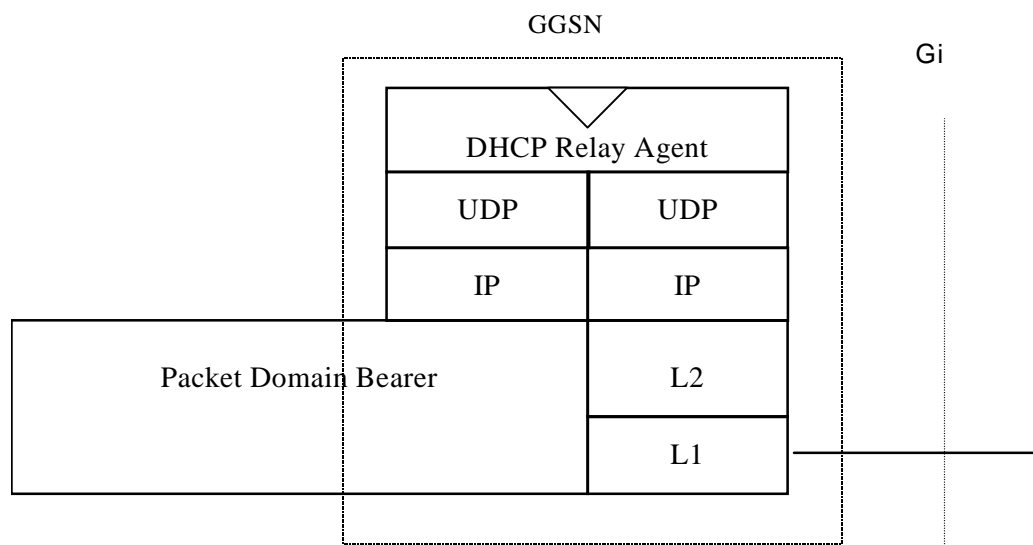

Figure 16b: The protocol stacks for the Gi IP reference point for DHCP

The DHCP relay agent relays the requests received from the DHCP client to the DHCP server(s), and the replies received from the server(s) to the corresponding client. The DHCP relay agent allows for the replies from DHCP servers to be delivered to the correct terminal, as the logical connection from the MT terminates in the GGSN, and consequently only the GGSN holds enough information to locate the DHCP client. How the DHCP relay agent identifies the MT based on the DHCP messages is out of the scope of 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 ~~(DHCP authentication is currently described in an Internet Draft).~~(see RFC 3118 [45]).

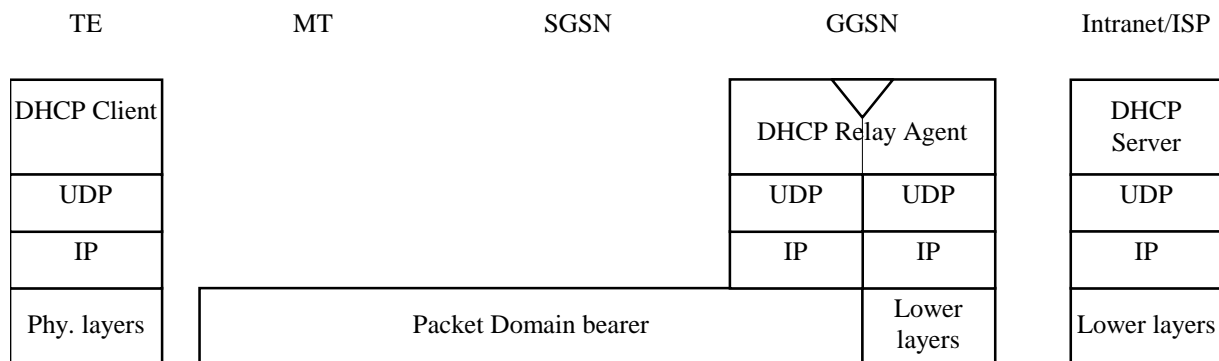The protocol configuration options are retrieved from the DHCP server belonging to the Intranet/ISP.

TE	MT	SGSN	GGSN	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 [26], [27]. The end-to-end protocol configuration is depicted in figure 16c.

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

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

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

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

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

6) The TE sends a DHCPDISCOVER message with the IP destination address set to the limited broadcast address (all 1s). The GGSN will pass the DHCPDISCOVER to the DHCP relay agent which will relay the request to the DHCP server configured for the APN of the PDP context. If more than one DHCP server is configured for a given APN, the request will be sent to all of them. The DHCP relay agent will add enough information to the DHCPDISCOVER message to be able to relay the replies back to the MS. How this is done is out of the scope of 3GPP standardisation.

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

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

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

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

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

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

EXAMPLE: In the following example a successful PDP context activation with use of DHCP from end to end is shown.
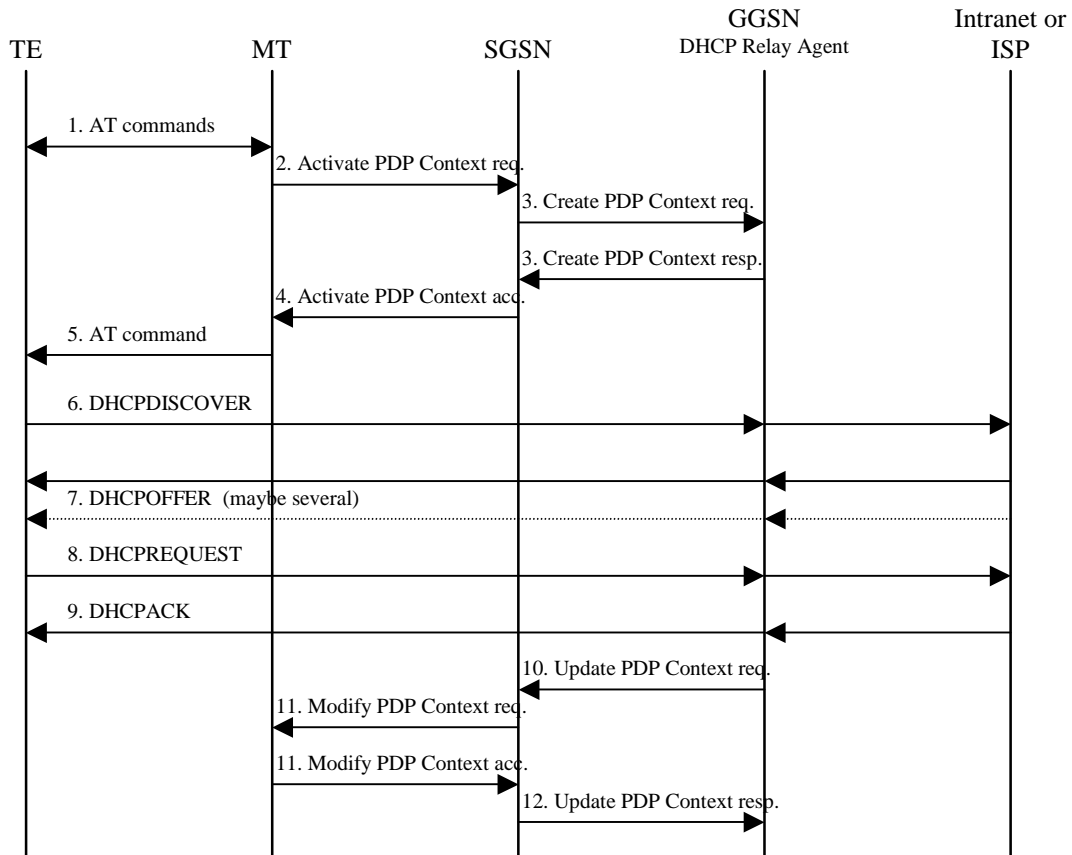
Figure16d: DHCPv4 signal flow

13.2.1.2 Address allocation using DHCPv6

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

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

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

2) The GGSN creates a RELAY-FORWARD message. The "Client-Message" option shall include the entire SOLICIT message. The GGSN sends the message to the DHCP server(s) configured for the APN using unicast addresses or the All_DHCP_Servers multicast address. More details on the parameters for the RELAY-FORWARD are found in [46]. Note that tThe GGSN canmay store a PDP Context ID in the Interface-Id option if this aids it in handling the Relay-Reply (the DHCP server will echo the Interface-Id option).

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

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

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

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

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

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

9) The GGSN initiates a PDP context modification procedure by sending an Update PDP Context Request to the appropriate SGSN with the End User Address information element set to the allocated IPv6 address.

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

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

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

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

EXAMPLE: In the following example a successful PDP context activation with use of DHCPv6 from end to end is shown.
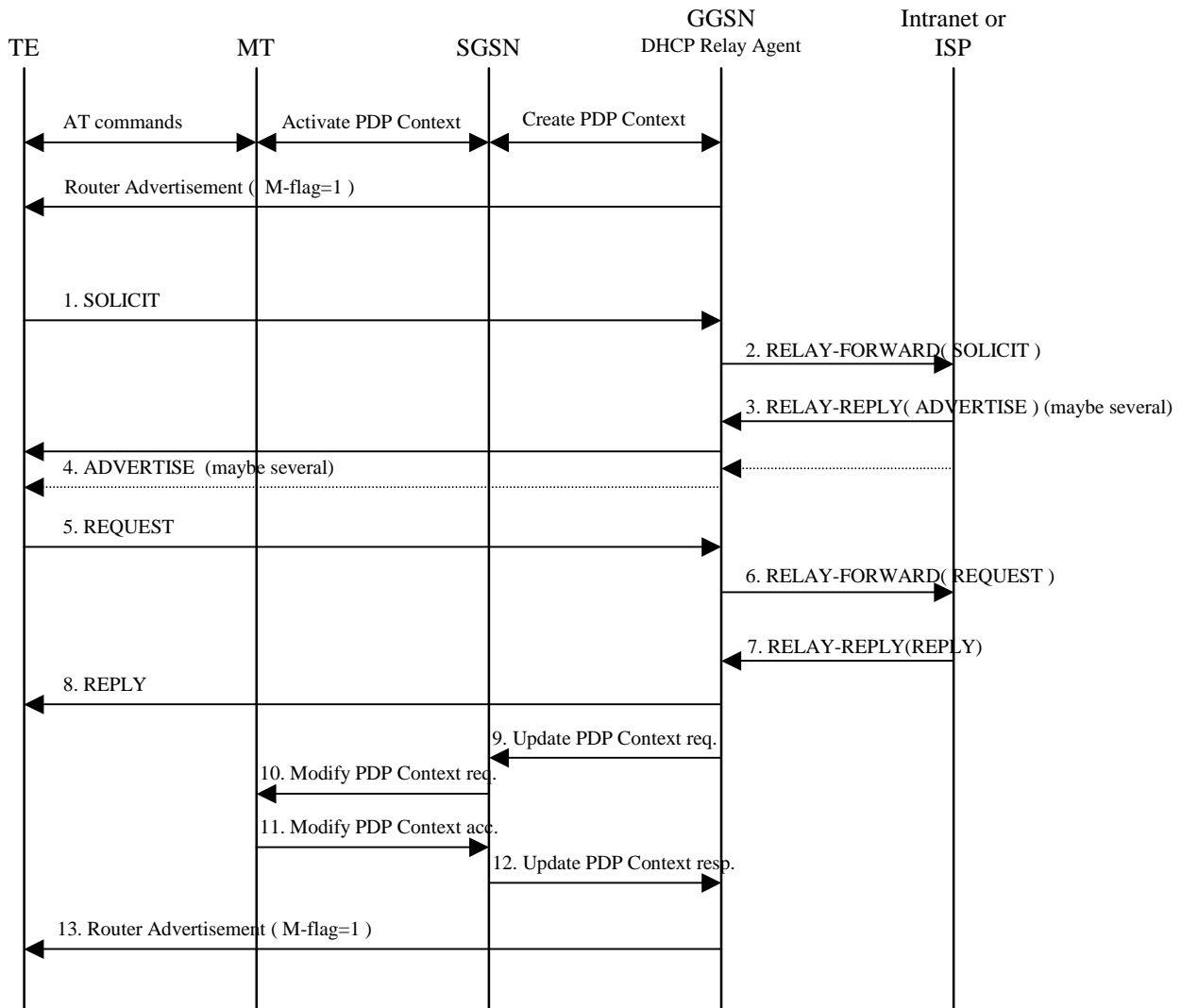
Figure 16e: DHCPv6 signal flow

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

When using IPv6, in some situations the MS may need additional configuration information from the Intranet or ISP besides the IP address. It canmay 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 willshall 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 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 [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_Servers multicast address defined in DHCPv6 [46]. The source address is the global or site-local address of the MS. GGSN forwards this message as normal IP payload, i.e. no DHCP relay agent is required.

3) DHCP servers receiving the INFORMATION-REQUEST message, reply by sending 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.
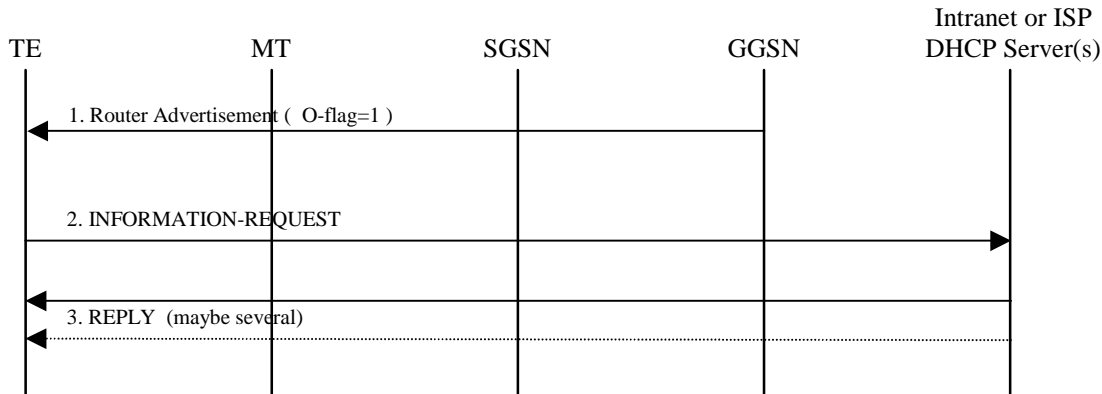
Figure 16f: DHCPv6 Other configuration signal flow

Next modified section

16   Usage of RADIUS on Gi interface

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

16.1   RADIUS Authentication

RADIUS Authentication shall be used according to RFC2865 [38] and RFC 3162 [50].

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

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

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

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

16.2   RADIUS Accounting

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

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

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

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

If the AAA server is used for IP address or IPv6 prefix assignment, then, upon reception of a RADIUS Accounting-Request STOP message for all PDP contexts associated to a session defined by APN and IMSI or MSISDN, the AAA server may make the associated IP address or IPv6 prefix available for assignment.
In order to avoid race conditions, the GGSN shall include a 3GPP Vendor-Specific sub-attribute "Session Stop indicator" when it sends the Accounting-Request STOP for the last PDP context of a PDP session and the PDP session is terminated (i.e. the IP address or IPv6 prefix and all GTP tunnels can be released). The AAA server shall not assume the PDP session terminated until an Accounting-Request STOP with the Session Stop indicator is received.

16.3 Authentication and accounting message flows

16.3.1 IP PDP type

The figure 22 represents the RADIUS message flows between a GGSN and an Authentication, Authorization and Accounting (AAA) server.
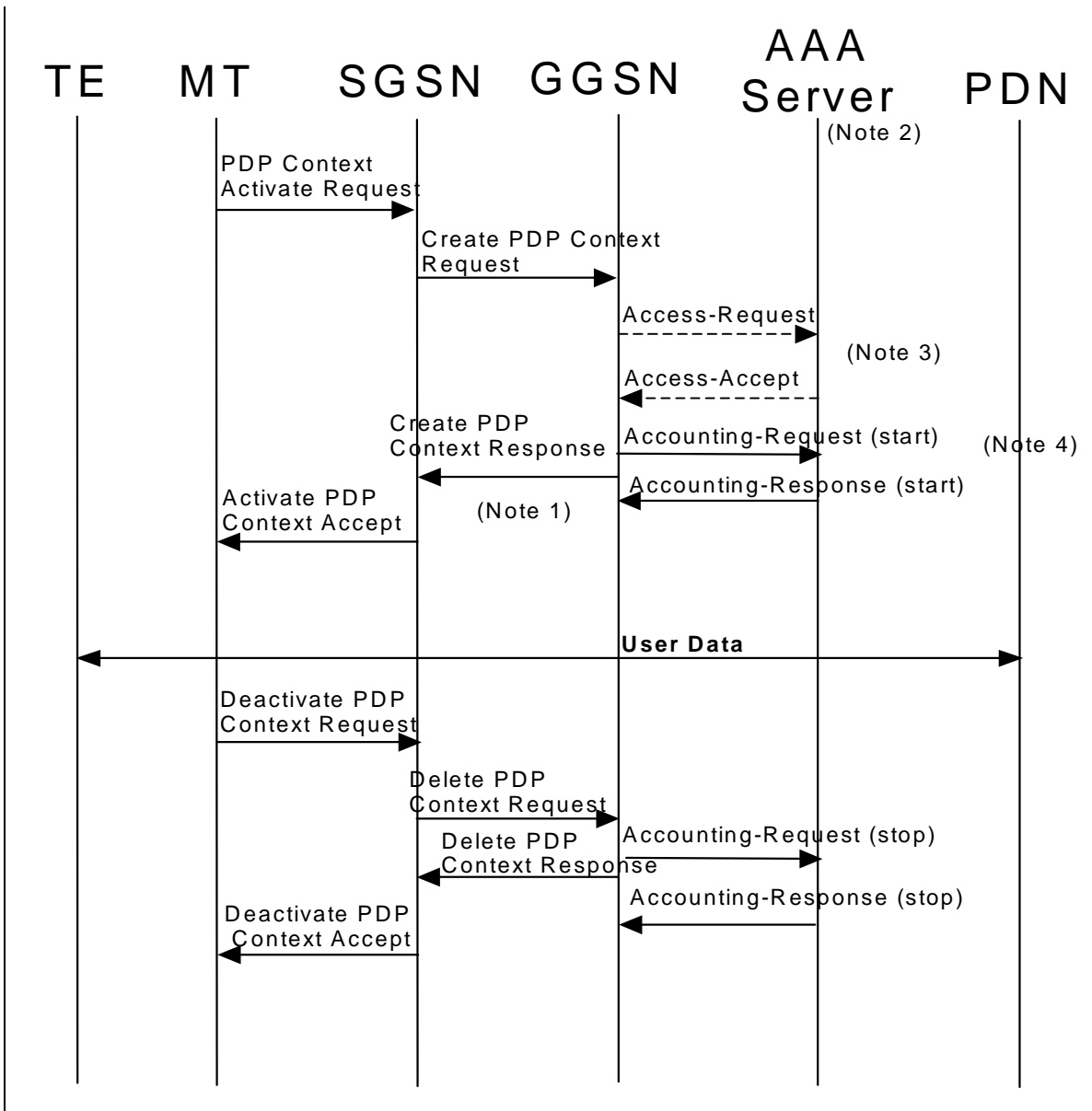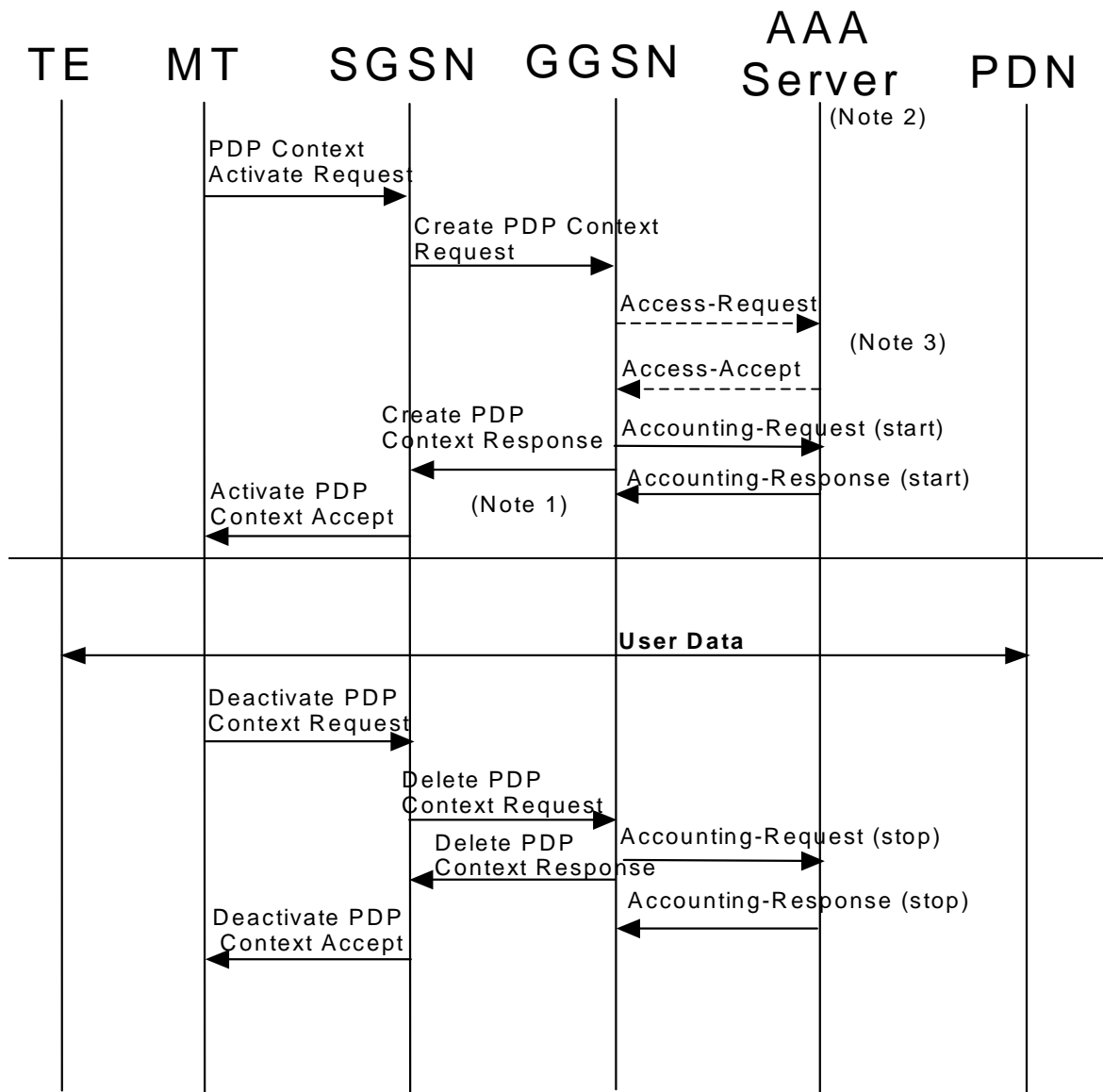
NOTE 1: If some external applications require RADIUS Accounting request (Start) information before they can process user packets, then the selected APN (GGSN) may be configured in such a way that the GGSN drops user data until the Accounting Response (START) is received from the AAA server. Both Authentication and Accounting servers may be optional and separately configured for each APN.

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

NOTE 3: The Access-Request message shall be used for primary PDP context only.

NOTE 4: The Accounting-Request (Start) message may be sent at a later stage, e.g. after IPv6 address has been assigned and PDP Context updated, in case of a stateful address autoconfiguration.

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

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

Even if the GGSN was not involved in user authentication (e.g. transparent network access mode), it may send a RADIUS Accounting-Request START message to an AAA server. This message contains parameters, e.g. the tuple which includes the user-id and IP address or IPv6 prefix, to be used by application servers (e.g. WAP gateway) in order to identify the user. This message also indicates to the AAA server that the user session has started. User data forwarding at the GGSN may not be allowed before the Accounting Response START is received. If this is the case, the GGSN drops user data until the Accounting Response START is received. This is configurable per APN.

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

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

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

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

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

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

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

16.3.2   PPP PDP type

The figure 23 describes the RADIUS message flows between a GGSN and an Authentication, Authorization and Accounting (AAA) server for the case where PPP is terminated at the GGSN. The case where PPP is relayed to an LNS is beyond the scope of this specification.
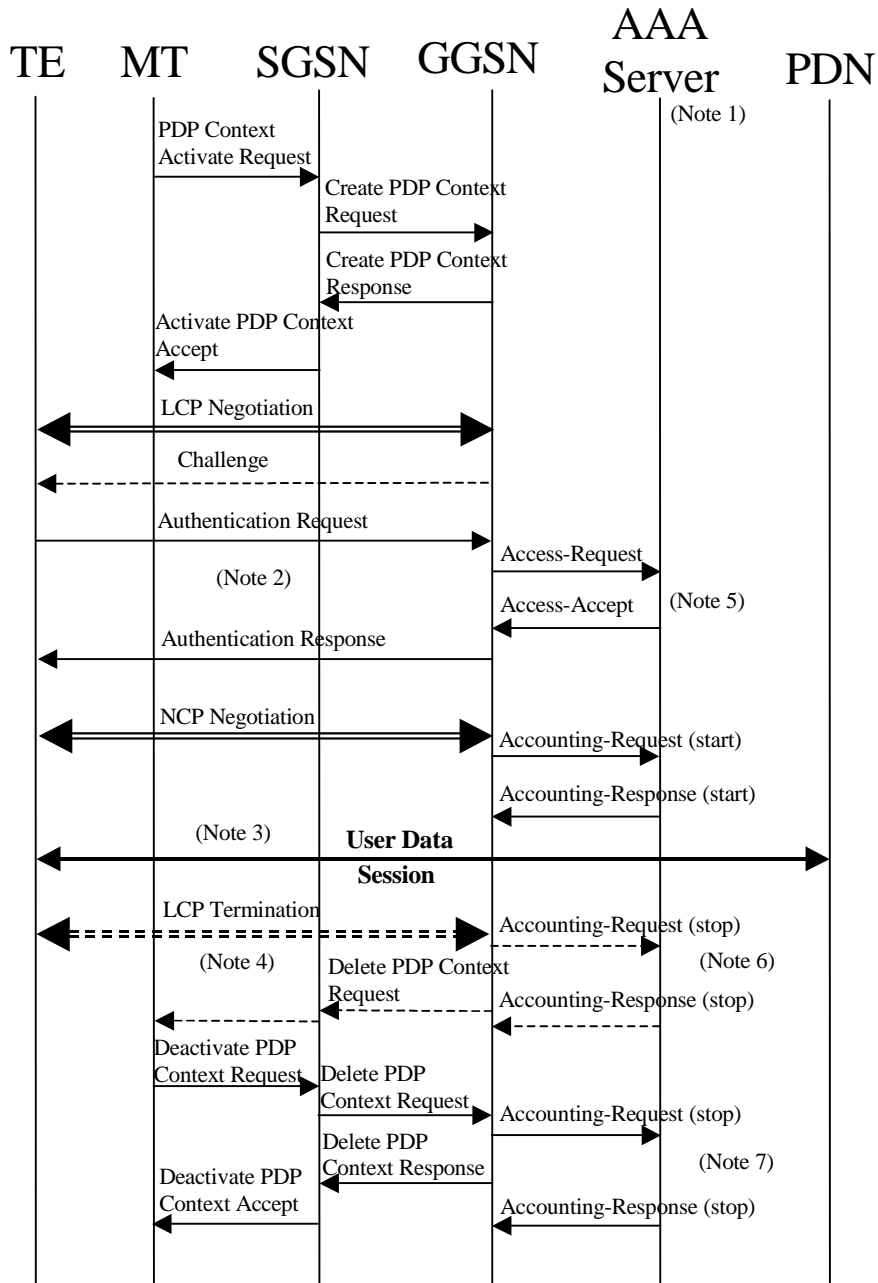
NOTE 1: Separate accounting and Authentication servers may be used.

NOTE 2: Actual messages depend on the used authentication protocol (e.g. PAP, CHAP)

NOTE 3: User data may not be allowed before the Accounting Response (START) is received. If this is the case, the GGSN drops user data until the Accounting Response (START) is 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.

User data forwarding at the GGSN may not be allowed before the Accounting Response START is received. If this is the case, the GGSN drops user data until the Accounting Response START is received. This is configurable per 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 [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).
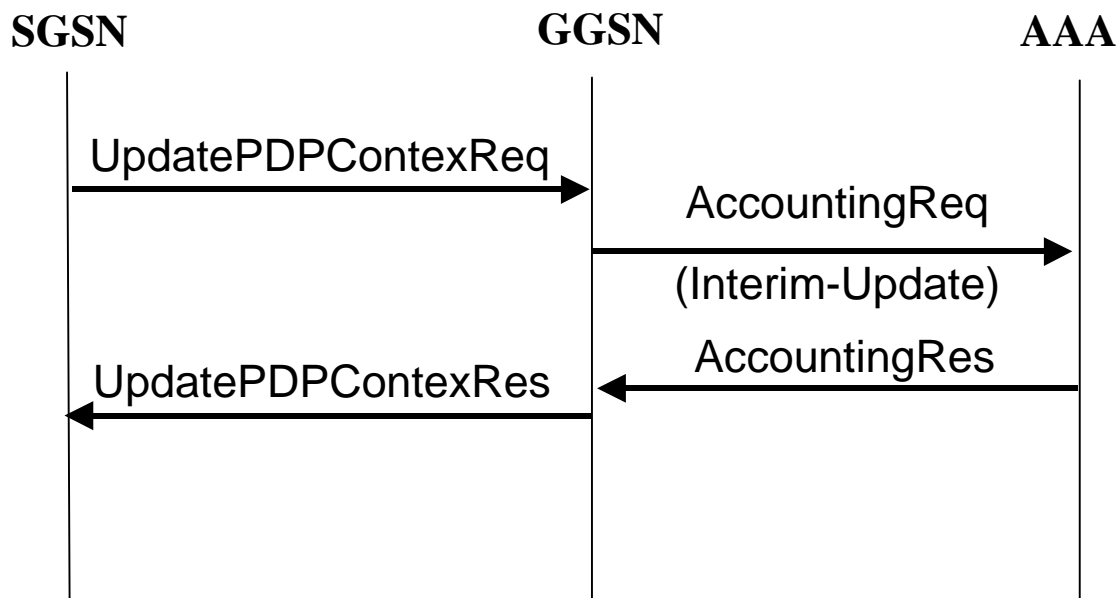
Figure 24: RADIUS for PDP context Update

16.3.4   AAA-Initiated PDP context termination

RADIUS is used as the protocol between the GGSN and a AAA server or proxy for applications (e.g. MMS) to deliver information related to GPRS user session. However some IP applications could need to interwork with the GGSN to terminate a particular PDP context. For this purpose, the AAA server or proxy may send a RADIUS Disconnect Request to the GGSN. As depicted in Figure 25, the GGSN may react by deleting the corresponding PDP context or silently discard the Disconnect Request message. For more information on RADIUS Disconnect, see [41θ].
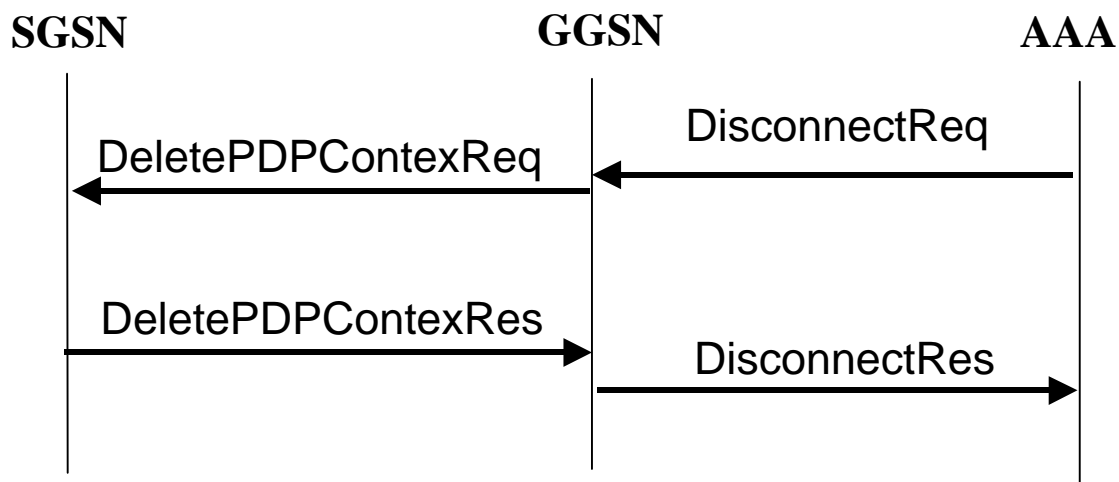
Figure 25: PDP Context deletion with RADIUS

16.4   List of RADIUS attributes

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

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

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

Table 1: The attributes of the Access-Request message

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

NOTE 1: Shall be present if PAP is used.

NOTE 2: Shall be present if CHAP is used.

NOTE 3: Either NAS-IP-Address or NAS-Identifier shall be present.

NOTE 5: Either IPv4 or IPv6 address/prefix attribute shall be present. ~~Note that~~The IP protocol version for end-user and network ~~can~~may be different.

NOTE 6: Included if the prefix alone is not unique for the user. This may be the case, for example, if address is assigned using stateful address autoconfiguration or if a static IPv6 address.

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

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

Table 2: The attributes of the Access-Accept message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username received in the Access-Request message or a substitute username provided by the AAA server. If the User-Name has been received in the Access-Accept message, this user-name shall be used in preference to the above	String	Optional
6	Service-Type	Indicates the type of service for this user	Framed	Optional
7	Framed-Protocol	Indicates the type of protocol for this user	7 (GPRS PDP Context)	Optional
8	Framed-IP-Address	IP address allocated for this user, if the AAA server is used to allocate IP address.	IPv4	Conditional Note 5
9	Framed-IP-Netmask	Netmask for the user IP address, if the AAA server is used to allocate IP netmask.	IPv4	Conditional Note 5
97	Framed-IPv6-Prefix	IPv6 address prefix allocated for this user, if the AAA server is used to allocate IP address prefixes.	IPv6	Conditional Note 5
100	Framed-IPv6-Pool	Name of the prefix pool for the specific APN	IPv6	Optional Note 5
12	Framed-IP-MTU	MTU for the user towards this particular APN, MTU shall be less or equal to 1500	String	Optional
25	Class	Identifier to be used in all subsequent accounting messages.	String	Optional (NOTE 4)
27	Session-Timeout	Indicates the timeout value (in seconds) for the user session	32 bit unsigned Integer	Optional
28	Idle-Timeout	Indicates the timeout value (in seconds) for idle user session	32 bit unsigned Integer	Optional
26/311	MS-P~~ primary~~-DNS-server	Contains the primary DNS server address for this APN	IP~~p~~v4	Optional Note 7
26/311	MS-Secondary-DNS-Server	Contains the secondary DNS server address for this APN	IPv4	Optional Note 7
26/311	MS-Primary-NBNS-Server	Contains the primary NetBios name server address for this APN	IPv4	Optional Note 7
26/311	MS-Secondary-NBNS-Server	Contains the secondary NetBios server address for this APN	IPv4	Optional Note 7
26/10415	3GPP Vendor-Specific	Sub-attributes according sub-clause 16.4.7	See sub-clause 16.4.7	Optional Note 7
NOTE 4: The presence of this attribute is conditional upon this attribute being received in the Access-Accept message				
NOTE 5: Either IPv4 or IPv6 address/prefix attribute shall be present. ~~Note that~~The IP protocol version for end-user and network ~~can~~may be different.				
NOTE 7: Either IPv4 or IPv6 address attribute shall be present				

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

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

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

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username provided by the user (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used). If no username is available a generic username, configurable on a per APN basis, shall be present. If the User-Name has been received in the Access-Accept message,	String	Optional

		this user-name shall be used in preference to the above		
4	NAS-IP-Address	GGSN IP address for communication with the AAA server.	IPv4	Conditional Note 3, 5
95	NAS-IPv6-Address	GGSN IPv6 address for communication with the AAA server.	IPv6	Conditional Note 3, 5
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 3
6	Service-Type	Indicates the type of service for this user	Framed	Optional
7	Framed Protocol	Indicates the type of protocol for this user	7 (GPRS PDP Context)	Optional
8	Framed-IP-Address	User IP address	IPv4	~~Mandatory~~Conditional Note 5
97	Framed-IPv6-Prefix	User IPv6 Prefix	IPv6	Conditional Note 5
96	Framed-Interface-Id	User IPv6 Interface Identifier	IPv6	Conditional Note 5, 6
25	Class	Received in the access accept	String	Conditional (NOTE 4)
30	Called-Station-Id	Identifier for the target network	APN (UTF-8 encoded)	Mandatory
31	Calling-Station-Id	This attribute is the identifier for the MS, and it shall be configurable on a per APN basis.	MSISDN in international format according to 3GPP TS 23.003, UTF-8 encoded decimal. Note that there are no leading characters in front of the country code.	Optional
40	Acct-Status-Type	Type of accounting message	START	Mandatory
41	Acct-Delay-Time	Indicates how many seconds the GGSN has been trying to send this record for, and can be subtracted from the time of arrival on the AAA server to find the approximate time (in seconds) of the event generating this Accounting-Request.	32 unsigned integer	Optional
44	Acct-Session-Id	User session identifier.	GGSN IP address (IPv4 or IPv6) and Charging-ID concatenated in a UTF-8 encoded hexadecimal. NOTE: The GGSN IP address is the same as that used in the GCDRs.	Mandatory
45	Acct-Authentic	Authentication method	RADIUS or LOCAL	Optional
61	NAS-Port-Type	Port type for the GGSN	As per RFC 2865	Optional
26/10415	3GPP Vendor-Specific	Sub-attributes according sub-clause 16.4.7.	See sub-clause 16.4.7	Optional except sub-attribute 3 which is conditional

NOTE 3:	Either NAS-IP-Address or NAS-Identifier shall be present.
NOTE 4:	The presence of this attribute is conditional upon this attribute being received in the Access-Accept message
NOTE 5:	Either IPv4 or IPv6 address/prefix attribute shall be present. ~~Note that~~The IP protocol version for end-user and network ~~can~~ may be different.
NOTE 6:	Included if the prefix alone is not unique for the user. This may be the case, for example, if address is assigned using stateful address autoconfiguration or if a static IPv6 address.

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

The table 4 describes the attributes of the Accounting-Request STOP message.

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

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

43	Acct-Output-Octets	GGSN counted number of octets received by the user for the PDP context	integer 32 bit unsigned integer	Optional
44	Acct-Session-Id	User session identifier.	GGSN IP address (IPv4 or IPv6) and Charging-ID concatenated in a UTF-8 encoded hexadecimal. NOTE: The GGSN IP address is the same as that used in the GCDRs.	Mandatory
45	Acct-Authentic	Authentication method	RADIUS or LOCAL	Optional
46	Acct-Session-Time	Duration of the session	Second	Optional
47	Acct-Input-Packets	GGSN counted number of packets sent by the user	Packet	Optional
48	Acct-Output-Packets	GGSN counted number of packets received by the user	Packet	Optional
49	Acct-Terminate-Cause	Indicate how the session was terminated	See RFC 2866	Optional
61	NAS-Port-Type	Port type for the GGSN	As per RFC 2865	Optional
26/10415	3GPP Vendor-Specific	Sub-attributes according to sub-clause 16.4.7.	See sub-clause 16.4.7	Optional except sub-attribute 3 which is conditional

NOTE 3: Either NAS-IP-Address or NAS-Identifier shall be present.

NOTE 4: The presence of this attribute is conditional upon this attribute being received in the Access-Accept message

NOTE 5: Either IPv4 or IPv6 address/prefix attribute shall be present. Note thatThe IP protocol version for end-user and network can may be different.

NOTE 6: Included if the prefix alone is not unique for the user. This may be the case, for example, if address is assigned using stateful address autoconfiguration or if a static IPv6 address.

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

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

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

Attr #	Attribute Name	Description	Content	Presence Requirement
4	NAS-IP-Address	IP address of the GGSN for communication with the AAA server.	IPv4	Conditional Note 3, 7
95	NAS-IPv6-Address	IP address of the GGSN for communication with the AAA server.	IPv6	Conditional Note 3, 7
30	Called-Station-ID	Identifier for the target network.	APN (UTF-8 encoded)	Optional
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 3

NOTE 3: Either NAS-IP-Address or NAS-Identifier shall be present.

NOTE 7: Either IPv4 or IPv6 address attribute shall be present

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

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

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

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

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

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

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

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

9	3GPP-GGSN- MCC-MNC	MCC-MNC of the network the GGSN belongs to.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
10	3GPP-NSAPI	Identifies a particular PDP context for the associated PDN and MSISDN/IMSI from creation to deletion.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP Accounting-Request Interim-Update
11	3GPP- Session-Stop-Indicator	Indicates to the AAA server that the last PDP context of a session is released and that the PDP session has been terminated.	Optional	Accounting Request STOP
12	3GPP- Selection-Mode	Contains the Selection mode for this PDP Context received in the Create PDP Context Request Message	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
13	3GPP-Charging-Characteristics	Contains the charging characteristics for this PDP Context received in the Create PDP Context Request Message (only available in R99 and later releases)	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
14	3GPP-CG-IPv6-Address	Charging Gateway IPv6 address	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
15	3GPP-SGSN-IPv6-Address	SGSN IPv6 address that is used by the GTP control plane for the handling of control messages. It may be used to identify the PLMN to which the user is attached.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
16	3GPP-GGSN-IPv6-Address	GGSN IPv6 address that is used by the GTP control plane for the context establishment.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
17	3GPP-Primary-IPv6-DNS-Server	IPv6 address of the primary Domain Name Server (DNS) server for an APN	Optional	Access-Accept
18	3GPP-Secondary-IPv6-	IPv6 address of	Optional	Access-Accept

		DNS-Server	the secondary Domain Name Server (DNS) server for an APN		
19		3GPP-Primary-IPv6-NBNS-Server	IPv6 address of the primary NetBIOS Name Server (NBNS) server for an APN	Optional	Access-Accept
20		3GPP-Secondary-IPv6-NBNS-Server	IPv6 address of the secondary NetBIOS Name Server (NBNS) server for an APN	Optional	Access-Accept

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

Bits

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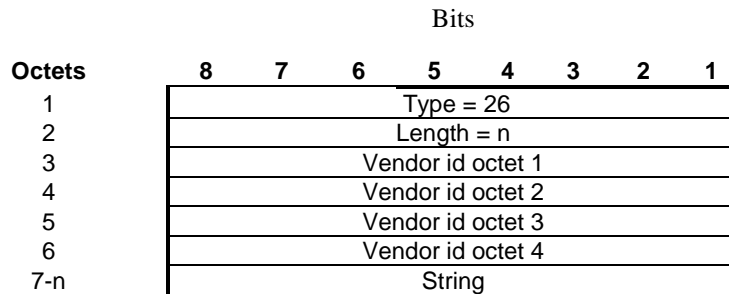
$n >= 7$

3GPP Vendor Id = 10415

The string part is encoded as follows:

Bits

Octets	8	7	6	5	4	3	2	1
1				3GPP type =				
2				3GPP Length = m				
3 –m				3GPP value				
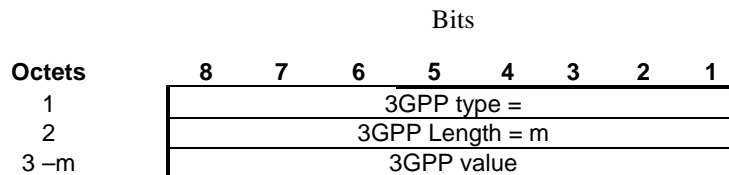
$m >= 2$ and $m <= 248$

The 3GPP specific attributes encoding is clarified below.

1 - 3GPP-*IMSI*

Bits

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

3GPP Type: 1

n <=15

Length: m =17

IMSI value: Text:

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

2 - 3GPP-*Charging ID*

Bits

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

3GPP Type: 2

Length: 6

Charging ID value: 32 bits unsigned integer

3- 3GPP-*PDP type*

Bits

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

3GPP Type: 3

Length: 6

PDP type value: Unsigned 32 bits integer

PDP type octet possible values:

0 = IP_v4_

1 = PPP

2 = IPv6

4 - 3GPP-*Charging Gateway address*

Bits

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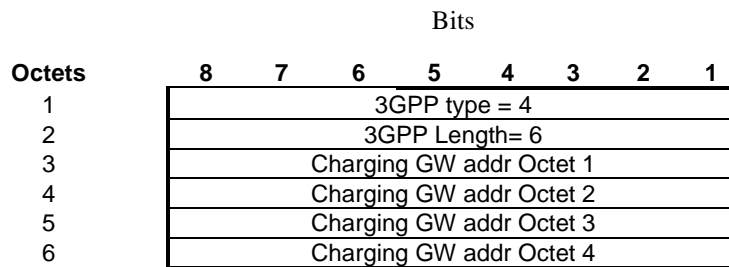
3GPP Type: 4

Length: 6

Charging GW address value: Address

5 - 3GPP-*GPRS 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							
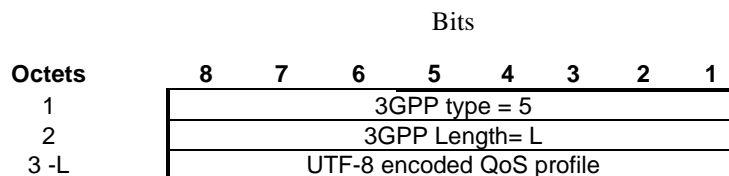
3GPP Type: 5

Length: 24 (release 99) or 8 (release 98)

QoS profile value: Text

UTF-8 encoded QoS profile syntax:

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

<Release indicator> = UTF-8 encoded number :

"98" = Release 98

"99"= Release 99

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

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

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

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

6 - 3GPP-*SGSN address*

<div align="center">Bits</div>

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

3GPP Type: 6

Length: 6

SGSN address value: Address

7 - 3GPP-*GGSN address*

<div align="center">Bits</div>

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

3GPP Type: 7

Length: 6

GGSN address value: Address

8 - 3GPP-*IMSI MCC-MNC*

<div align="center">Bits</div>

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

3GPP Type: 8

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

MS address value: text

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

9 - 3GPP-*GGSN MCC-MNC*

Bits

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

3GPP Type: 9

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

GGSN address value: text

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

10 - 3GPP-*NSAPI*

Bits

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

3GPP Type: 10

Length: 3

NSAPI value: text

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

11 - 3GPP-*Session Stop Indicator*

Bits

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

3GPP Type: 11

Length: 2

There is no value field for this Vendor Specific Attribute.

12 - 3GPP-Selection-Mode

Bits

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

3GPP Type: 12

Length: 3

Selection mode value: Text

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

13 - 3GPP-*Charging-Characteristics*

Bits

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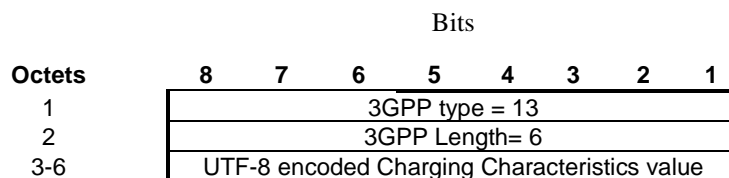
3GPP Type: 13

Length: 6

Charging characteristics value: Text

The charging characteristics is value is the value of the 2 octets value field taken from the GTP IE described in 29.060section 7.7.23.

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

14 - 3GPP-*Charging Gateway IPv6 address*

Bits

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

3GPP Type: 14

Length: 18

Charging GW IPv6 address value: IPv6 Address

15 - 3GPP-*SGSN IPv6 address*

Bits

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

3GPP Type: 15

Length: 18

SGSN IPv6 address value: IPv6 Address

16 - 3GPP-*GGSN IPv6 address*

<div align="center">

Bits

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

</div>

3GPP Type: 16

Length: 18

GGSN IPv6 address value: IPv6 Address

17 - 3GPP-*Primary-IPv6-DNS-Server*

<div align="center">

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 17							
2	3GPP Length= 18							
3	GGSN IPv6 addr Octet 1							
4	GGSN IPv6 addr Octet 2							
5-18	GGSN IPv6 addr Octet 3-16							

</div>

3GPP Type: 17

Length: 18

Primary IPv6 DNS Server value: IPv6 Address

The 3GPP-Primary-IPv6-DNS-Server Attribute is used to indicate the IPv6 address of the primary Domain Name Server (DNS) server for an APN. It may be included in Access-Accept packets.

18 - 3GPP-*Secondary-IPv6-DNS-Server*

<div align="center">

Bits

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

</div>

3GPP Type: 18

Length: 18

Secondary IPv6 DNS Server value: IPv6 Address

The 3GPP-Secondary-IPv6-DNS-Server Attribute is used to indicate the IPv6 address of the secondary Domain Name Server (DNS) server for an APN. It may be included in Access-Accept packets.

19 - 3GPP-Primary-IPv6-NBNS-Server

<div align="center">Bits</div>

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 19							
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: 19

Length: 18

Primary IPv6 NBNS Server value: IPv6 Address

The 3GPP-Primary-IPv6-NBNS-Server Attribute is used to indicate the IPv6 address of the primary NetBIOS Name Server (NBNS) server for an APN. It may be included in Access-Accept packets.

20 - 3GPP-Secondary-IPv6-NBNS-Server

<div align="center">Bits</div>

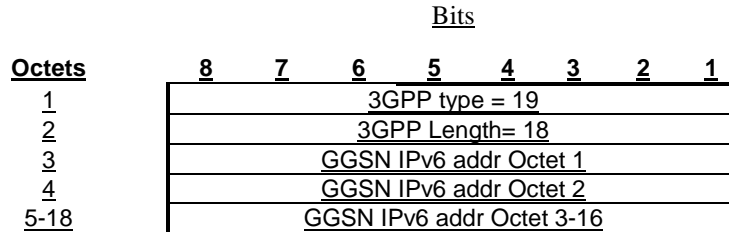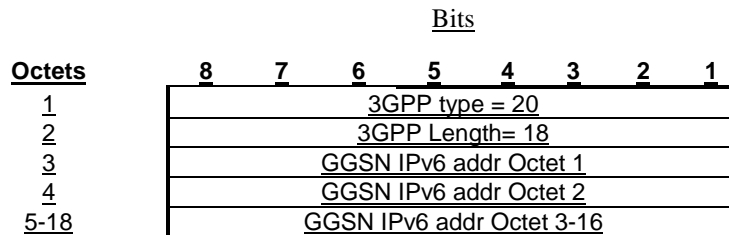| Octets	8	7	6	5	4	3	2	1
1	3GPP type = 20							
2	3GPP Length= 18							
3	GGSN IPv6 addr Octet 1							
4	GGSN IPv6 addr Octet 2							
5-18	GGSN IPv6 addr Octet 3-16							

3GPP Type: 20

Length: 18

Secondary IPv6 NBNS Server value: IPv6 Address

The 3GPP-Secondary-IPv6-NBNS-Server Attribute is used to indicate the IPv6 address of the secondary NetBIOS Name Server (NBNS) server for an APN. It may be included in Access-Accept packets.

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

The table 8 describes the attributes of the Accounting-Request Interim-Update message.

<div align="center">**Table 8: The attributes of the Accounting-Request Interim-Update message**</div>

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username provided by the user (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP	String	Optional

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

		user		
61	NAS-Port-Type	Port type for the GGSN	As per RFC 2865	Optional
26/10415	3GPP Vendor-Specific	Sub-attributes according to sub-clause 16.4.7.	See sub-clause 16.4.7	Optional except sub-attribute 3 which is conditional

NOTE 3: Either NAS-IP-Address or NAS-Identifier shall be present.

NOTE 4: The presence of this attribute is conditional upon this attribute being received in the Access-Accept message

NOTE 5: Either IPv4 or IPv6 address/prefix attribute shall be present. ~~Note that~~The IP protocol version for end-user and network ~~can~~ may be different.

NOTE 6: Included if the prefix alone is not unique for the user. This may be the case, for example, if address is assigned using stateful address autoconfiguration or if a static IPv6 address.

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

The table 9 describes the attributes of the Disconnect-Request message.

Table 9: The attributes of the Disconnect-Request message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username provided by the user (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used). If no username is available a generic username, configurable on a per APN basis, shall be present. If the User-Name has been sent in the Access-Accept message, this user-name shall be used in preference to the above	String	Optional
8	Framed-IP-Address	User IP address	IPv4	~~Mandatory~~Conditional Note 8
97	Framed-IPv6-Prefix	User IPv6 address	IPv6	Conditional Note 8
96	Framed-Interface-Id	User IPv6 Interface Identifier	IPv6	Conditional Note 6, 8
44	Acct-Session-Id	User session identifier.	GGSN IP address (IPv4 or IPv6) and Charging-ID concatenated in a UTF-8 encoded hexadecimal. NOTE: The GGSN IP address is the same as that used in the GCDRs.	Mandatory

NOTE 6: Included if the prefix alone is not unique for the user. This may be the case, for example, if address is assigned using stateful address autoconfiguration or if a static IPv6 address.

NOTE 8: Either IPv4 or IPv6 address/prefix attribute shall be present.

End of modified sections