ETSI TS 129 060 V4.1.0 (2001-06)

Technical Specification

Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
General Packet Radio Service (GPRS);
GPRS Tunnelling Protocol (GTP)
across the Gn and Gp Interface
(3GPP TS 29.060 version 4.1.0 Release 4)

Reference
RTS/TSGN-0429060Uv4R1

Keywords
GSM, UMTS

ETSI

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

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

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

Intellectual Property Rights

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

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

Foreword

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

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

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under www.etsi.org/key .

Contents

Foreword

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

The present document defines the Gn and Gp interfaces for the General Packet Radio Service (GPRS) within the 3GPP system.

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document defines the second version of GTP used on:

- the Gn and Gp interfaces of the General Packet Radio Service (GPRS);
- the Iu, Gn and Gp interfaces of the UMTS system.

NOTE: The version number used in the message headers is 0 for the first version of GTP described in GSM 09.60, and 1 for the second version in 3GPP TS 29.060.

2 References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "3G Vocabulary".

[2] 3GPP TS 23.003: "Numbering, addressing and identification".

[3] 3GPP TS 23.007: "Restoration Procedures".

[4] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service Description; Stage 2".

[5] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols-Stage 3".

[6] 3GPP TS 29.002: "Mobile Application Part (MAP) specification".

[7] 3GPP TS 25.413: "UTRAN Iu interface RANAP signalling".

[8] 3GPP TS 33.102: "Security Architecture".

[9] GSM 03.20: "Digital cellular telecommunications system (Phase 2+); Security related network functions".

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

[11] GSM 04.64: "Digital cellular telecommunications system (Phase 2+); Mobile Station - Serving GPRS Support Node (MS-SGSN) Logical Link Control (LLC) Layer Specification".

[12] STD 0005: "Internet Protocol", J. Postel.

[13] STD 0006: "User Datagram Protocol", J. Postel.

[14] RFC 1700: "Assigned Numbers", J. Reynolds and J. Postel.

[15] RFC 2181: "Clarifications to the DNS Specification", R. Elz and R. Bush.

[16] 3GPP TS 23.007: "Restoration Procedures".

[17] 3GPP TS 23.121: "Architectural Requirements for Release 1999".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

Conditional: When the presence requirement for the information element is conditional, the receiving protocol level can check the presence or absence of an IE based on the received information.

G-PDU: A G-PDU is a user data message. It consists of a T-PDU plus a GTP header.

GTP Tunnel: A GTP tunnel in the GTP-U plane is defined for each PDP Context in the GSNs and/or each RAB in the RNC. A GTP tunnel in the GTP-C plane is defined for all PDP Contexts with the same PDP address and APN (for Tunnel Management messages) or for each MS (for messages not related to Tunnel Management). A GTP tunnel is identified in each node with a TEID, an IP address and a UDP port number. A GTP tunnel is necessary to forward packets between an external packet data network and an MS user.

MM Context: Information sets held in MS and GSNs for a GPRS subscriber related to mobility management (MM) (please refer to the MM Context Information Element).

NSAPI: Network Service Access Point Identifier. An integer value in the range [0; 15], identifying a certain PDP Context. It identifies a PDP context belonging to a specific MM Context ID.

Path: UDP/IP path is used to multiplex GTP tunnels.

Path Protocol: Path Protocol is the protocol used as a bearer of GTP between GSNs or between a GSN and a RNC.

PDP: Packet Data Protocol (PDP) is a network protocol used by an external packet data network interfacing to GPRS.

PDP Context: Information sets held in MS and GSNs for a PDP address (please refer to the PDP Context Information Element).

Quality of Service: Quality of Service may be applicable for the GPRS backbone and the Iu interface if the path media supports it. Separate paths with different priorities may be defined between a GSN pair or between a GSN and an RNC.

GTP-C Message: GTP-C or control plane messages are exchanged between GSN/RNC pairs in a path. The control plane messages are used to transfer GSN capability information between GSN pairs, to create, update and delete GTP tunnels and for path management.

GTP-U Message: GTP-U or user plane messages are exchanged between GSN pairs or GSN/RNC pairs in a path. The user plane messages are used to carry user data packets, and signalling messages for path management and error indication.

GTP-PDU: A GTP Protocol Data Unit is either a GTP-C message or a GTP-U message.

Signalling Message: Any GTP-PDU except the G-PDU.

T-PDU: Original packet, for example an IP datagram, from an MS or a network node in an external packet data network. A T-PDU is the payload that is tunnelled in the GTP-U tunnel.

Traffic Flow Template: TFTs are used by GGSN to distinguish between different user payload packets and transmit packets with different QoS requirements via different PDP context but to the same PDP address.

Tunnel Endpoint IDentifier (TEID): The TEID unambiguously identifies a tunnel endpoint in the receiving GTP-U or GTP-C protocol entity. The receiving end side of a GTP tunnel locally assigns the TEID value the transmitting side has to use. The TEID values are exchanged between tunnel endpoints using GTP-C (or RANAP, over the Iu) messages.

UDP/IP Path: UDP/IP path is a connection-less unidirectional or bidirectional path defined by two end-points. An IP address and a UDP port number define an end-point. A UDP/IP path carries GTP messages between GSN nodes, and between GSN and RNC nodes related to one or more GTP tunnels.

3.2 Abbreviations

Abbreviations used in the present document are listed in GSM 01.04.

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

BB	Backbone Bearer
DF	Don't Fragment
FFS	For Further Study
GTP	GPRS Tunnelling Protocol
GTP-C	GTP Control
GTP-U	GTP User
IANA	Internet Assigned Number Authority
ICMP	Internet Control Message Protocol
IE	Information Element
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
MTU	Maximum Transmission Unit
QoS	Quality of Service
RANAP	Radio Access Network Application Part
RNC	Radio Network Controller
TEID	Tunnel Endpoint IDentifier
TFT	Traffic Flow Template
UDP	User Datagram Protocol
UTRAN	UMTS Terrestrial Radio Access Network
Gn interface	Interface between GPRS Support Nodes (GSNs) within a PLMN
Gp interface	Interface between GPRS Support Nodes (GSNs) in different PLMNs

4 General

The present document defines the GPRS Tunnelling Protocol (GTP), i.e. the protocol between GPRS Support Nodes (GSNs) in the UMTS/GPRS backbone network. It includes both the GTP control plane (GTP-C) and data transfer (GTP-U) procedures. GTP also lists the messages and information elements used by the GTP based charging protocol GTP', which is described in GSM 12.15.

GTP (GTP-C and GTP-U) is defined for the Gn interface, i.e. the interface between GSNs within a PLMN, and for the Gp interface between GSNs in different PLMNs. Only GTP-U is defined for the Iu interface between Serving GPRS Support Node (SGSN) and the UMTS Terrestrial Radio Access Network (UTRAN).

On the Iu interface, the Radio Access Network Application Part (RANAP) protocol and signalling part of GTP-U are performing the control function for user plane (GTP-U).

GTP' is defined for the interface between CDR generating functional network elements and Charging Gateway(s) within a PLMN. Charging Gateway(s) and GTP' protocol are optional, as the Charging Gateway Functionality may either be located in separate network elements (Charging Gateways), or alternatively be embedded into the CDR generating network elements (GSNs) when the GSN-CGF interface is not necessarily visible outside the network element. These interfaces relevant to GTP are between the grey boxes shown in Figure 1.

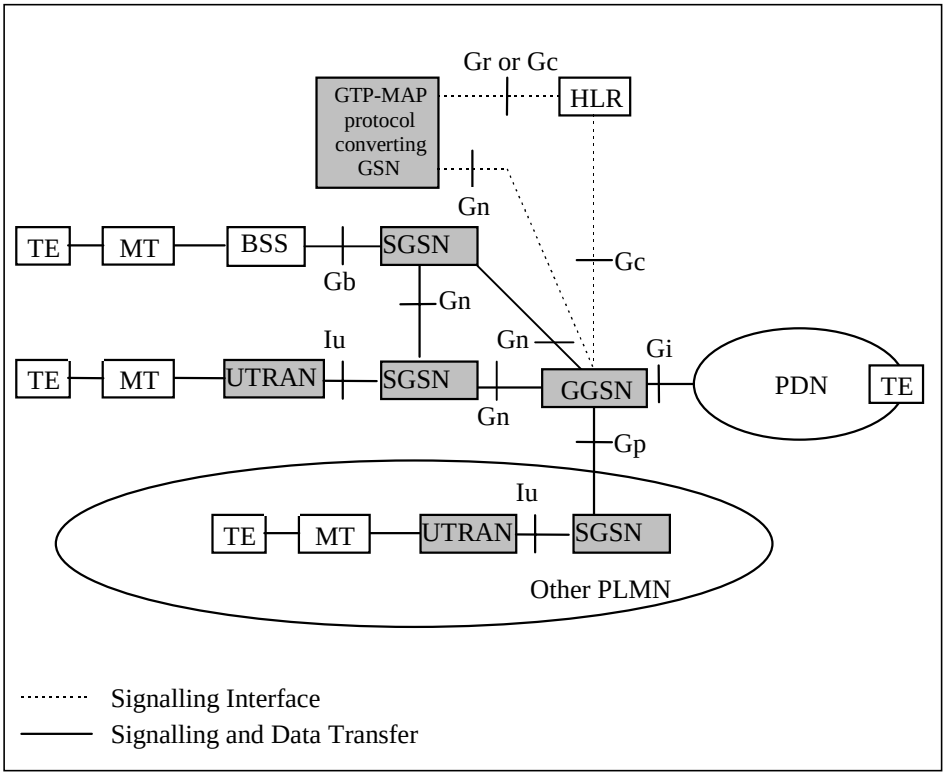


Figure 1: GPRS Logical Architecture with interface name denotations

GTP allows multi-protocol packets to be tunnelled through the UMTS/GPRS Backbone between GSNs and between SGSN and UTRAN.

In the control plane, GTP specifies a tunnel control and management protocol (GTP-C) which allows the SGSN to provide packet data network access for an MS. Control Plane signalling is used to create, modify and delete tunnels.

In the user plane, GTP uses a tunnelling mechanism (GTP-U) to provide a service for carrying user data packets.

The GTP-U protocol is implemented by SGSNs and GGSNs in the UMTS/GPRS Backbone and by Radio Network Controllers (RNCs) in the UTRAN. SGSNs and GGSNs in the UMTS/GPRS Backbone implement the GTP-C protocol. No other systems need to be aware of GTP. UMTS/GPRS MSs are connected to an SGSN without being aware of GTP.

It is assumed that there will be a many-to-many relationship between SGSNs and GGSNs. A SGSN may provide service to many GGSNs. A single GGSN may associate with many SGSNs to deliver traffic to a large number of geographically diverse mobile stations.

SGSN and GGSN implementing GTP protocol version 1 should be able to fallback to GTP protocol version 0. All GSNs should be able to support all earlier GTP versions.

5 Transmission Order and Bit Definitions

The messages in this document shall be transmitted in network octet order starting with octet 1. Where information elements are repeated within a message the order shall be determined by the order of appearance in the table defining the information elements in the message.

The most significant bit of an octet in a GTP message is bit 8. If a value in a GTP message spans several octets and nothing else is stated, the most significant bit is bit 8 of the octet with the lowest number.

6 GTP Header

The GTP header is a variable length header used for both the GTP-C and the GTP-U protocols. The minimum length of the GTP header is 8 bytes. There are three flags that are used to signal the presence of additional optional fields: the PN flag, the S flag and the E flag. The PN flag is used to signal the presence of N-PDU Numbers. The S flag is used to signal the presence of the GTP Sequence Number field. The E flag is used to signal the presence of the Extension Header field, used to enable future extensions of the GTP header defined in this document, without the need to use another version number. If any of these three flags are set, the length of the header is at least 12 octets and the fields corresponding to the flags that are set shall be evaluated by the receiver. The sender shall set all the bits of the unused fields to zero. The receiver shall not evaluate the unused fields.

The GTP-C and the GTP-U use some of the fields in the GTP header differently. The different use of such fields is described in the sections related to GTP-C and to GTP-U.

Always present fields:

- Version field: This field is used to determine the version of the GTP protocol. For the treatment of other versions, see subclause 11.1.1, "Different GTP versions". The version number shall be set to '1'.

- Protocol Type (PT): This bit is used as a protocol discriminator between GTP (when PT is '1') and GTP' (when PT is '0'). GTP is described in this document and the GTP' protocol in GSM 12.15. Note that the interpretation of the header fields may be different in GTP' than in GTP.

- Extension Header flag (E): This flag indicates the presence of the Next Extension Header field when it is set to '1'. When it is set to' 0', the Next Extension Header field either is not present or, if present, must not be interpreted.

- Sequence number flag (S): This flag indicates the presence of the Sequence Number field when it is set to '1'. When it is set to '0', the Sequence Number field either is not present or, if present, must not be interpreted. The S flag shall be set to '1' in GTP-C messages and in GTP-U/GTP signalling type of messages.

- N-PDU Number flag (PN): This flag indicates the presence of the N-PDU Number field when it is set to '1'. When it is set to '0', the N-PDU Number field either is not present, or, if present, must not be interpreted. This flag is significant only for GTP-U. As such, this flag is unused by GTP-C and it shall be ignored by a GTP-C receiving entity.

- Message Type: This field indicates the type of GTP message. The valid values of the message type are defined in subclause 7.1 for both GTP-C and GTP-U.

- Length: This field indicates the length in octets of the payload, i.e. the rest of the packet following the mandatory part of the GTP header (that is the first 8 octets). The Sequence Number, the N-PDU Number or any Extension headers shall be considered to be part of the payload, i.e. included in the length count.

- Tunnel Endpoint Identifier (TEID): This field unambiguously identifies a tunnel endpoint in the receiving GTP-U or GTP-C protocol entity. The receiving end side of a GTP tunnel locally assigns the TEID value the transmitting side has to use. The TEID values are exchanged between tunnel endpoints using GTP-C (or RANAP, over the Iu) messages.

Optional fields:

- Sequence Number: This field is an optional field in G -PDUs. It is used as a transaction identity for signalling messages having a response message defined for a request message, that is the Sequence Number value is copied from the request to the response message header. In the user plane, an increasing sequence number for T-PDUs is transmitted via GTP-U tunnels, when transmission order must be preserved.

- N-PDU Number: This field is used at the Inter SGSN Routeing Area Update procedure and some inter-system handover procedures (e.g. between 2G and 3G radio access networks). This field is used to co-ordinate the data transmission for acknowledged mode of communication between the MS and the SGSN. The exact meaning of this field depends upon the scenario. (For example, for GSM/GPRS to GSM/GPRS, the SNDCP N-PDU number is present in this field).

- Next Extension Header Type: This field defines the type of Extension Header that follows this field in the GTP-PDU.

Bits

Octets	8	7	6	5	4	3	2	1
1	Version			PT	(*)	E	S	PN
2	Message Type							
3	Length (1st Octet)							
4	Length (2nd Octet)							
5	Tunnel Endpoint Identifier (1st Octet)							
6	Tunnel Endpoint Identifier (2nd Octet)							
7	Tunnel Endpoint Identifier (3rd Octet)							
8	Tunnel Endpoint Identifier (4th Octet)							
9	Sequence Number (1st Octet) 1) 4)							
10	Sequence Number (2nd Octet) 1) 4)							
11	N-PDU Number 2) 4)							
12	Next Extension Header Type 3) 4)							

(*) This bit is a spare bit. It shall be sent as '0'. The receiver shall not evaluate this bit.
1) This field shall only be evaluated when indicated by the S flag.
2) This field shall only be evaluated when indicated by the PN flag.
3) This field shall only be evaluated when indicated by the E flag.
4) This field shall be present when any one or more of the S, PN and E flags are set.

Figure 2: Outline of the GTP Header

The format of GTP Extension Headers is depicted in Figure 2. The Extension Header Length field specifies the length of the particular Extension header in 4 octets units. The Next Extension Header Type field specifies the type of any Extension Header that may follow a particular Extension Header. If no such Header follows, then the value of the Next Extension Header Type shall be 0.

Octets	1	Extension Header Length
	2 - m	Extension Header Content
	m+1	Next Extension Header Type (*)

(*) The value of this field is 0 if no other Extension header follows.

Figure 3: Outline of the Extension Header Format

The length of the Extension header shall be defined in a variable length of 4 octets, i.e. m+1 = n*4 octets, where n is a positive integer.

Bits 7 and 8 of the Next Extension Header Type define how the recipient shall handle unknown Extension Types. The recipient of an extension header of unknown type but marked as 'comprehension not required' for that recipient shall read the 'Next Extension Header Type' field (using the Extension Header Length field to identify its location in the GTP-PDU).

The recipient of an extension header of unknown type but marked as 'comprehension required' for that recipient shall:

- If the message with the unknown extension header was a request, send a response message back with CAUSE set to "unknown mandatory extension header".
- Send a Supported Extension Headers Notification to the originator of the GTP PDU.
- Log an error.

Bits 7 and 8 of the Next Extension Header Type have the following meaning:

Bits 8	Bits 7	Meaning
0	0	Comprehension of this extension header is not required. An Intermediate Node shall forward it to any Receiver Endpoint
0	1	Comprehension of this extension header is not required. An Intermediate Node shall discard the Extension Header Content and not forward it to any Receiver Endpoint. Other extension headers shall be treated independently of this extension header.
1	0	Comprehension of this extension header is required by the Endpoint Receiver but not by an Intermediate Node. An Intermediate Node shall forward the whole field to the Endpoint Receiver.
1	1	Comprehension of this header type is required by recipient (either Endpoint Receiver or Intermediate Node)

Figure 4: Definition of bits 7 and 8 of the Extension Header Type

An Endpoint Receiver is the ultimate receiver of the GTP-PDU (e.g. an RNC or the GGSN for the GTP-U plane). An Intermediate Node is a node that handles GTP but is not the ultimate endpoint (e.g. an SGSN for the GTP-U plane traffic between GGSN and RNC).

Next Extension Header Field Value	Type of Extension Header
0000 0000	No more extension headers
1100 0000	PDCP PDU number

Figure 5: Definition of Extension Header Type

6.1 Extension headers

6.1.1 PDCP PDU Number

This extension header is transmitted, for example, at SRNS relocation time to provide the PDCP sequence number of not yet acknowledged N-PDUs. It is 4 octets long, and therefore the Length field has value 1.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1	1							
2	PDCP PDU number							
3	PDCP PDU number.							
4	Next Extension Header Type (*)							

(*) The value of this field is 0 if no other Extension header follows.

Figure 6: PDCP PDU number Extension Header

7 GTP Messages and Message Formats

7.1 Message Formats

GTP defines a set of messages between two associated GSNs or an SGSN and an RNC. The messages to be used are defined in the table below. The three columns to the right define which parts (GTP-C, GTP-U or GTP') that send or receive the specific message type.

Table 1: Messages in GTP

Message Type value (Decimal)	Message	Reference	GTP-C	GTP-U	GTP'
0	For future use. Shall not be sent. If received, shall be treated as an Unknown message.				
1	Echo Request	7.2.1	X	X	x
2	Echo Response	7.2.2	X	X	x
3	Version Not Supported	7.2.3	X		x
4	Node Alive Request	GSM 12.15			X
5	Node Alive Response	GSM 12.15			X
6	Redirection Request	GSM 12.15			X
7	Redirection Response	GSM 12.15			X
8-15	For future use. Shall not be sent. If received, shall be treated as an Unknown message.				
16	Create PDP Context Request	7.3.1	X		
17	Create PDP Context Response	7.3.2	X		
18	Update PDP Context Request	7.3.3	X		
19	Update PDP Context Response	7.3.4	X		
20	Delete PDP Context Request	7.3.5	X		
21	Delete PDP Context Response	7.3.6	X		
22-25	For future use. Shall not be sent. If received, shall be treated as an Unknown message.				
26	Error Indication	7.3.7		X	
27	PDU Notification Request	7.3.8	X		
28	PDU Notification Response	7.3.9	X		
29	PDU Notification Reject Request	7.3.10	X		
30	PDU Notification Reject Response	7.3.11	X		
31	Supported Extension Headers Notification	7.2.4	X	X	
32	Send Routeing Information for GPRS Request	7.4.1	X		
33	Send Routeing Information for GPRS Response	7.4.2	X		
34	Failure Report Request	7.4.3	X		
35	Failure Report Response	7.4.4	X		
36	Note MS GPRS Present Request	7.4.5	X		
37	Note MS GPRS Present Response	7.4.6	X		
38-47	For future use. Shall not be sent. If received, shall be treated as an Unknown message.				
48	Identification Request	7.5.1	X		
49	Identification Response	7.5.2	X		
50	SGSN Context Request	7.5.3	X		
51	SGSN Context Response	7.5.4	X		
52	SGSN Context Acknowledge	7.5.5	X		
53	Forward Relocation Request	7.5.6	X		
54	Forward Relocation Response	7.5.7	X		
55	Forward Relocation Complete	7.5.8	X		
56	Relocation Cancel Request	7.5.9	X		
57	Relocation Cancel Response	7.5.10	X		
58	Forward SRNS Context	7.5.11	X		
59	Forward Relocation Complete Acknowledge	7.5.x	X		
60	Forward SRNS Context Acknowledge	7.5.x	X		
61-239	For future use. Shall not be sent. If received, shall be treated as an Unknown message.				
240	Data Record Transfer Request	GSM 12.15			X
241	Data Record Transfer Response	GSM 12.15			X
242-254	For future use. Shall not be sent. If received, shall be treated as an Unknown message.				
255	G-PDU	9.3.1		X	

7.2 Path Management Messages

The Path Management messages may be sent between any type of GSN or GSN - RNC pair.

7.2.1 Echo Request

An Echo Request may be sent on a path to another GSN or RNC to find out if the peer GSN or RNC is alive (see section Path Failure). Echo Request messages may be sent for each path in use. A path is considered to be in use if at least one PDP context uses the path to the other GSN. When and how often an Echo Request message may be sent is implementation specific but an Echo Request shall not be sent more often than every 60 seconds on each path.

A GSN or RNC shall be prepared to receive an Echo Request at any time and it shall reply with an Echo Response. A GSN or RNC may optionally send Echo Request messages.

The optional Private Extension contains vendor or operator specific information.

Table 2: Information Elements in an Echo Request

Information element	Presence requirement	Reference
Private Extension	Optional	7.7.44

7.2.2 Echo Response

The message shall be sent as a response to a received Echo Request.

The Recovery information element contains the local Restart Counter (see section Restoration and Recovery) value for the GSN that sends the Echo Response message. For GTP-U the Restart Counter value shall not be used, i.e. it shall be set to zero by the sender and shall be ignored by the receiver.

The GSN that receives an Echo Response from a peer GSN shall compare the Restart Counter value received with the previous Restart Counter value stored for that peer GSN. If no previous value was stored, the Restart Counter value received in the Echo Response shall be stored for the peer GSN.

The value of a Restart Counter previously stored for a peer GSN may differ from the Restart Counter value received in the Echo Response from that peer GSN. In this case, the GSN that sent the Echo Response shall be considered as restarted by the GSN that received the Echo Response. The new Restart Counter value received shall be stored by the receiving entity, replacing the value previously stored for the sending GSN.

If the sending GSN is a GGSN and the receiving GSN is an SGSN, the SGSN shall consider all PDP contexts using the GGSN as inactive. For further actions of the SGSN refer to 3GPP TS 23.007 [16].

If the sending GSN is an SGSN and the receiving GSN is a GGSN, the GGSN shall consider all PDP contexts using the SGSN as inactive. For further actions of the GGSN refer to 3GPP TS 23.007 [16].

The optional Private Extension contains vendor or operator specific information.

Table 3: Information Elements in an Echo Response

Information element	Presence requirement	Reference
Recovery	Mandatory	7.7.11
Private Extension	Optional	7.7.44

7.2.3 Version Not Supported

This message contains only the GTP header and indicates the latest GTP version that the GTP entity on the identified UDP/IP address can support.

7.2.4 Supported Extension Headers Notification

This message indicates a list of supported Extension Headers that the GTP entity on the identified IP address can support. This message is sent only in case a GTP entity was required to interpret a mandatory Extension Header but the GSN or RNC was not yet upgraded to support that extension header. The GTP endpoint at the GSN or RNC sending this message is marked as not enabled to support some extension headers (as derived from the supported extension header list). The GSN may retry to use all the extension headers with that node, in an attempt to verify it has been upgraded. Implementers should avoid repeated attempts to use unknown extension headers with an endpoint that has signalled its inability to interpret them.

Table 4: Information Elements in Supported Extension Headers Notification

Information element	Presence requirement	Reference
Extension Header Type List	Mandatory	7.7.40

7.3 Tunnel Management Messages

7.3.1 Create PDP Context Request

A Create PDP Context Request shall be sent from a SGSN node to a GGSN node as a part of the GPRS PDP Context Activation procedure. After sending the Create PDP Context Request message, the SGSN marks the PDP context as 'waiting for response'. In this state the SGSN shall accept G-PDUs from the GGSN but shall not send these G-PDUs to the MS. A valid request initiates the creation of a tunnel between a PDP Context in a SGSN and a PDP Context in a GGSN. If the procedure is not successfully completed, the SGSN repeats the Create PDP Context Request message to the next GGSN address in the list of IP addresses, if there is one. If the list is exhausted the activation procedure fails.

The Tunnel Endpoint Identifier Data I field specifies a downlink Tunnel Endpoint Identifier for G-PDUs which is chosen by the SGSN. The GGSN shall include this Tunnel Endpoint Identifier in the GTP header of all subsequent downlink G-PDUs which are related to the requested PDP context.

The Tunnel Endpoint Identifier Control Plane field specifies a downlink Tunnel Endpoint Identifier for control plane messages which is chosen by the SGSN. The GGSN shall include this Tunnel Endpoint Identifier in the GTP header of all subsequent downlink control plane messages which are related to the requested PDP context. If the SGSN has already confirmed successful assignment of its Tunnel Endpoint Identifier Control Plane to the peer GGSN, this field shall not be present. The SGSN confirms successful assignment of its Tunnel Endpoint Identifier Control Plane the GGSN when it receives any message with its assigned Tunnel Endpoint Identifier Control Plane in the GTP header from the GGSN.

The MSISDN of the MS is passed to the GGSN inside the Create PDP Context Request; This additional information can be used when a secure access to a remote application residing on a server is needed. The GGSN would be in fact able to provide the user identity (i. e. the MSISDN) to the remote application server, providing it with the level of trust granted to users through successfully performing the GPRS authentication procedures, without having to re-authenticate the user at the application level.

If the MS requests a dynamic PDP address and a dynamic PDP address is allowed, then the PDP Address field in the End User Address information element shall be empty. If the MS requests a static PDP Address then the PDP Address field in the End User Address information element shall contain the static PDP Address. In case the PDP addresses carried in the End User Address and optionally in the Protocol Configuration Option information element contain contradicting information, the PDP address carried in the End User Address information element takes the higher precedence. The Quality of Service Profile information element shall be the QoS values to be negotiated between the MS and the SGSN at PDP Context activation.

The SGSN shall include an SGSN Address for control plane and an SGSN address for user traffic, which may differ from that provided by the underlying network service (e.g. IP). The GGSN shall store these SGSN Addresses and use them when sending control plane on this GTP tunnel or G-PDUs to the SGSN for the MS.

The SGSN shall include a Recovery information element into the Create PDP Context Request if the SGSN is in contact with the GGSN for the very first time or if the SGSN has restarted recently and the new Restart Counter value has not yet been indicated to the GGSN. The GGSN that receives a Recovery information element in the Create PDP Context Request message element shall handle it in the same way as when receiving an Echo Response message. The Create PDP Context Request message shall be considered as a valid activation request for the PDP context included in the message.

The SGSN shall include either the MS provided APN, a subscribed APN or an SGSN selected APN in the message; the Access Point Name may be used by the GGSN to differentiate accesses to different external networks.
The Selection Mode information element shall indicate the origin of the APN in the message.

For contexts created by the Secondary PDP Context Activation Procedure the SGSN shall include the linked NSAPI. Linked NSAPI indicates the NSAPI assigned to any one of the already activated PDP contexts for this PDP address and APN.

The Secondary PDP Context Activation Procedure may be executed without providing a Traffic Flow Template (TFT) to the newly activated PDP context if all other active PDP contexts for this PDP address and APN already have an associated TFT, otherwise a TFT shall be provided. TFT is used for packet filtering in the GGSN.

When using the Secondary PDP Context Activation Procedure, the Selection mode, IMSI, MSISDN, End User Address, Access Point Name and Protocol Configuration Options information elements shall not be included in the message.

The optional Protocol Configuration Options information element is applicable for the end user protocol 'IP' only.

The SGSN shall select one GGSN based on the user provided or SGSN selected APN. The GGSN may have a logical name that is converted to an address. The conversion may be performed with any name-to-address function. The converted address shall be stored in the "GGSN Address in Use" field in the PDP context and be used during the entire lifetime of the PDP context.

NOTE: A DNS query may be used as the name-to-IP address mapping of the GGSN. The IP address returned in the DNS response is then stored in the "GGSN Address in Use" field in the PDP context.

The IMSI information element together with the NSAPI information element uniquely identifies the PDP context to be created.

The SGSN may send a Create PDP Context Request even if the PDP context is already active.

The GGSN shall check if the PDP context already exists for the MS. The existing parameters in the PDP context shall then be replaced with the parameters in the Create PDP Context Request message. If a dynamic PDP address has already been allocated for the existing context, this address should be used and copied to the Create PDP Context Response message.

If the GGSN uses the MNRG flag and the flag is set, the GGSN should treat the Create PDP Context Request as a Note MS Present Request and clear the MNRG flag.

The SGSN shall determine Charging Characteristics from the Subscribed Charging Characteristics and/or PDP Context Charging Characteristics depending on the presence of the information in the Packet Domain Subscription Data as defined in 3GPP TS 23.060 [4].

The SGSN shall include Trace Reference, Trace Type, Trigger Id, and OMC Identity in the message if GGSN trace is activated. The SGSN shall copy Trace Reference, Trace Type, and OMC Identity from the trace request received from the HLR or OMC.

The optional Private Extension contains vendor or operator specific information.

Table 5: Information Elements in a Create PDP Context Request

Information element	Presence requirement	Reference
IMSI	Conditional	7.7.2
Recovery	Optional	7.7.11
Selection mode	Conditional	7.7.12
Tunnel Endpoint Identifier Data I	Mandatory	7.7.13
Tunnel Endpoint Identifier Control Plane	Conditional	7.7.14
NSAPI	Mandatory	7.7.17
Linked NSAPI	Conditional	7.7.17
Charging Characteristics	Optional	7.7.23
Trace Reference	Optional	7.7.24
Trace Type	Optional	7.7.25
End User Address	Conditional	7.7.27
Access Point Name	Conditional	7.7.30
Protocol Configuration Options	Conditional	7.7.31
SGSN Address for signalling	Mandatory	GSN Address 7.7.32
SGSN Address for user traffic	Mandatory	GSN Address 7.7.32
MSISDN	Conditional	7.7.33
Quality of Service Profile	Mandatory	7.7.34
TFT	Conditional	7.7.36
Trigger Id	Optional	7.7.41
OMC Identity	Optional	7.7.42
Private Extension	Optional	7.7.44

7.3.2 Create PDP Context Response

The message shall be sent from a GGSN node to a SGSN node as a response of a Create PDP Context Request. When the SGSN receives a Create PDP Context Response with the Cause value indicating 'Request Accepted', the SGSN activates the PDP context and may start to forward T-PDUs to/from the MS from/to the external data network.

The Cause value indicates if a PDP context has been created in the GGSN or not. A PDP context has not been created in the GGSN if the Cause differs from 'Request accepted'. Possible Cause values are:

- "Request Accepted".
- "No resources available".
- "All dynamic PDP addresses are occupied".
- "No memory is available".
- "Missing or unknown APN".
- "Unknown PDP address or PDP type".
- "User authentication failed".
- "System failure".
- "Semantic error in the TFT operation".
- "Syntactic error in the TFT operation".
- "Semantic errors in packet filter(s)".
- "Syntactic errors in packet filters(s)".
- "Mandatory IE incorrect".
- "Mandatory IE missing".
- "Optional IE incorrect".
- "Invalid message format".

'No resources available' indicates e.g. that all dynamic PDP addresses are occupied or no memory is available. 'Missing or unknown APN' indicates e.g. when the GGSN does not support the Access Point Name. 'Unknown PDP address or PDP type' indicates e.g. when the GGSN does not support the PDP type or the PDP address. 'User authentication failed' indicates that the external packet network has rejected the service requested by the user.

Only the Cause information element, optionally Protocol Configuration Options and optionally the Recovery information element shall be included in the response if the Cause contains another value than 'Request accepted'.

All information elements, except Recovery, Protocol Configuration Options, Charging Gateway Address and Private Extension, are mandatory if the Cause contains the value 'Request accepted'.

The Tunnel Endpoint Identifier for Data (I) field specifies an uplink Tunnel Endpoint Identifier for G-PDUs that is chosen by the GGSN. The SGSN shall include this Tunnel Endpoint Identifier in the GTP header of all subsequent uplink G-PDUs which are related to the requested PDP context.

The Tunnel Endpoint Identifier Control Plane field specifies an uplink Tunnel Endpoint Identifier for control plane messages, which is chosen by the GGSN. The SGSN shall include this Tunnel Endpoint Identifier in the GTP header of all subsequent uplink-control plane messages, which are related to the requested PDP context. If the GGSN has already confirmed successful assignment of its Tunnel Endpoint Identifier Control Plane to the peer SGSN, this field shall not be present. The GGSN confirms successful assignment of its Tunnel Endpoint Identifier Control Plane to the SGSN when it receives any message with its assigned Tunnel Endpoint Identifier Control Plane in the GTP header from the SGSN.

The GGSN shall include a GGSN Address for control plane and a GGSN address for user traffic, which may differ from that provided by the underlying network service (e.g. IP). The SGSN shall store these GGSN Addresses and use them when sending control plane on this GTP tunnel or G-PDUs to the GGSN for the MS.

If the MS requests a dynamic PDP address with the PDP Type IPv4 or IPv6 and a dynamic PDP address is allowed, then the End User Address information element shall be included and the PDP Address field in the End User Address information element shall contain the dynamic PDP Address allocated by the GGSN. If the MS requests a static PDP address with the PDP Type IPv4 or IPv6, or a PDP address is specified with PDP Type PPP, then the End User Address information element shall not be included. In case the PDP addresses carried in the End User Address and optionally in the Protocol Configuration Option information element contain contradicting information, the PDP address carried in the End User Address information element takes the higher precedence.

The QoS values supplied in the Create PDP Context Request may be negotiated downwards by the GGSN. The negotiated values or the original values from SGSN are inserted in the Quality of Service Profile information element of the Create PDP Context Response message.

The GGSN may start to forward T-PDUs after the Create PDP Context Response has been sent. The SGSN may start to forward T-PDUs when the Create PDP Context Response has been received. In this case the SGSN shall also be prepared to receive T-PDUs from the GGSN after it has sent a Create PDP Context Request but before a Create PDP Context Response has been received.

The Reordering Required value supplied in the Create PDP Context Response indicates whether the end user protocol benefits from packet in sequence delivery and whether the SGSN and the GGSN therefore shall perform reordering or not. In other words, if reordering is required by the GGSN, the SGSN and the GGSN shall perform reordering of incoming T-PDUs on this path. When the Quality of Service (QoS) Profile is Release 99 the receiving entity shall ignore the Reordering Required.

The GGSN shall include the Recovery information element into the Create PDP Context Response if the GGSN is in contact with the SGSN for the first time or the GGSN has restarted recently and the new Restart Counter value has not yet been indicated to the SGSN. The SGSN receiving the Recovery information element shall handle it as when an Echo Response message is received but shall consider the PDP context being created as active if the response indicates successful context activation at the GGSN.

The Charging ID is used to identify all charging records produced in SGSN(s) and the GGSN for this PDP context. The Charging ID is generated by the GGSN and shall be unique within the GGSN.

The Charging Gateway Address is the IP address of the recommended Charging Gateway Functionality to which the SGSN should transfer the Charging Detail Records (CDR) for this PDP Context.

The optional Private Extension contains vendor or operator specific information.

Table 6: Information Elements in a Create PDP Context Response

Information element	Presence requirement	Reference
Cause	Mandatory	7.7.1
Reordering required	Conditional	7.7.6
Recovery	Optional	7.7.11
Tunnel Endpoint Identifier Data I	Conditional	7.7.13
Tunnel Endpoint Identifier Control Plane	Conditional	7.7.14
Charging ID	Conditional	7.7.26
End User Address	Conditional	7.7.27
Protocol Configuration Options	Optional	7.7.31
GGSN Address for Control Plane	Conditional	GSN Address 7.7.32
GGSN Address for user traffic	Conditional	GSN Address 7.7.32
Quality of Service Profile	Conditional	7.7.34
Charging Gateway Address	Optional	7.7.43
Private Extension	Optional	7.7.44

7.3.3 Update PDP Context Request

An Update PDP Context Request message shall be sent from a SGSN to a GGSN as part of the GPRS Inter SGSN Routeing Update procedure or the PDP Context Modification procedure or to redistribute contexts due to load sharing.

It shall be used to change the QoS and the path. In addition it shall be used if it is neccessary to change the GTP version of a tunnel to a GGSN from GTP v0 to GTP v1. The message shall be sent by the new SGSN at the Inter SGSN Routeing Update procedure.

The NSAPI information element together with the Tunnel Endpoint Identifier in the GTP header unambiguously identifies a PDP Context in the GGSN.

The IMSI shall be included if the message is sent during an Inter SGSN change when changing the GTP version from GTP v0 to GTP v1; this is required, as the TEID in the header of the message is set to all zeros in this case.

The Tunnel Endpoint Identifier Data field specifies a downlink Tunnel Endpoint Identifier for G-PDUs which is chosen by the SGSN. The GGSN shall include this Tunnel Endpoint Identifier in the GTP header of all subsequent downlink G-PDUs that are related to the requested PDP context.

The Tunnel Endpoint Identifier Control Plane field specifies a downlink Tunnel Endpoint Identifier Control Plane messages which is chosen by the SGSN. The GGSN shall include this Tunnel Endpoint Identifier in the GTP header of all subsequent downlink control plane messages that are related to the requested PDP context. If the SGSN has already confirmed successful assignment of its Tunnel Endpoint Identifier Control Plane to the peer GGSN, this field shall not be present. The SGSN confirms successful assignment of its Tunnel Endpoint Identifier Control Plane to the GGSN when it receives any message with its assigned Tunnel Endpoint Identifier Control Plane in the GTP header from the GGSN.

The Quality of Service Profile information element shall include the QoS negotiated between the MS and SGSN at PDP Context activation or the new QoS negotiated in the PDP Context Modification procedure.

The SGSN shall include an SGSN Address for control plane and an SGSN address for user traffic, which may differ from that provided by the underlying network service (e.g. IP). The GGSN shall store these SGSN Addresses and use them when sending subsequent control plane on this GTP tunnel or G-PDUs to the SGSN for the MS. When active contexts are being redistributed due to load sharing, G-PDUs that are in transit across the Gn-interface are in an undetermined state and may be lost.

The SGSN shall include a Recovery information element into the Update PDP Context Request if the SGSN is in contact with the GGSN for the very first time or if the SGSN has restarted recently and the new Restart Counter value has not yet been indicated to the GGSN. The GGSN that receives a Recovery information element in the Update PDP Context Request message element shall handle it in the same way as when receiving an Echo Response message. The Update PDP Context Request message shall be considered as a valid update request for the PDP context indicated in the message.

The Traffic Flow Template (TFT) is used to distinguish between different user traffic flows.

The SGSN shall include Trace Reference, Trace Type, Trigger Id, and OMC Identity in the message if GGSN trace is activated while the PDP context is active. The SGSN shall copy Trace Reference, Trace Type, and OMC Identity from the trace request received from the HLR or OMC.

The optional Private Extension contains vendor or operator specific information.

Table 7: Information Elements in an SGSN-Initiated Update PDP Context Request

Information element	Presence requirement	Reference
IMSI	Conditional	7.7.2
Recovery	Optional	7.7.11
Tunnel Endpoint Identifier Data I	Mandatory	7.7.13
Tunnel Endpoint Identifier Control Plane	Conditional	7.7.14
NSAPI	Mandatory	7.7.17
Trace Reference	Optional	7.7.24
Trace Type	Optional	7.7.25
SGSN Address for Control Plane	Mandatory	GSN Address 7.7.32
SGSN Address for User Traffic	Mandatory	GSN Address 7.7.32
Quality of Service Profile	Mandatory	7.7.34
TFT	Optional	7.7.36
Trigger Id	Optional	7.7.41
OMC Identity	Optional	7.7.42
Private Extension	Optional	7.7.44

An Update PDP Context Request may also be sent from a GGSN to a SGSN to re-negotiate the QoS of a PDP context. This GGSN-initiated Update PDP Context Request can also be used to provide a PDP address to the SGSN (and MS). The latter shall be used by GGSN when it acts as a DHCP Relay Agent or Mobil IP Foreign Agent.

The Quality of Service Profile information element shall include the GGSN requested QoS.

The End User Address information element shall contain a valid IPv4 or IPv6 address.

The GGSN shall include a Recovery information element into the Update PDP Context Request if the GGSN has restarted recently and the new Restart Counter value has not yet been indicated to the SGSN. The SGSN that receives a Recovery information element in the Update PDP Context Request message element shall handle it in the same way as when receiving an Echo Response message. The Update PDP Context Request message shall be considered as a valid update request for the PDP context indicated in the message.

The NSAPI information element together with the Tunnel Endpoint Identifier in the GTP header unambiguously identifies a PDP Context in the SGSN.

The optional Private Extension contains vendor or operator specific information.

Table 8: Information Elements in a GGSN-Initiated Update PDP Context Request

Information element	Presence requirement	Reference
Recovery	Optional	7.7.11
NSAPI	Mandatory	7.7.17
End User Address	Optional	7.7.27
Quality of Service Profile	Optional	7.7.34
Private Extension	Optional	7.7.44

7.3.4 Update PDP Context Response

The message shall be sent from a GGSN node to a SGSN node as a response of an Update PDP Context Request.

If the SGSN receives an Update PDP Context Response with a Cause value other than ‘Request accepted’, it shall abort the update of the PDP context.

Only the Cause information element and optionally the Recovery information element shall be included in the response if the Cause contains another value than ‘Request accepted’.

Possible Cause values are:

- ‘Request Accepted’.
- ‘Non-existent’.
- ‘Service not supported’.
- ‘System failure’.
- ‘Semantic error in the TFT operation’.
- ‘Syntactic error in the TFT operation’.
- ‘Semantic errors in packet filter(s)’.
- ‘Syntactic errors in packet filters(s)’.
- ‘Mandatory IE incorrect’.
- ‘Mandatory IE missing’.
- ‘Optional IE incorrect’.
- ‘Invalid message format’.

The Tunnel Endpoint Identifier Data field specifies an uplink Tunnel Endpoint Identifier for G-PDUs that is chosen by the GGSN. The SGSN shall include this Tunnel Endpoint Identifier in the GTP header of all subsequent uplink G-PDUs that are related to the requested PDP context. This information element shall be included if the Cause contains the value 'Request accepted'.

The Tunnel Endpoint Identifier Control Plane field specifies an uplink Tunnel Endpoint Identifier Control Plane messages which is chosen by the GGSN. The SGSN shall include this Tunnel Endpoint Identifier in the GTP header of all subsequent uplink control plane messages which are related to the requested PDP context. If the GGSN has already confirmed successful assignment of its Tunnel Endpoint Identifier Control Plane to the peer SGSN, this field shall not be present. The GGSN confirms successful assignment of its Tunnel Endpoint Identifier Control Plane to the SGSN when it receives any message with its assigned Tunnel Endpoint Identifier Control Plane in the GTP header from the SGSN.

The QoS values supplied in the Update PDP Context Request may be negotiated downwards by the GGSN. The negotiated values or the original value from SGSN is inserted in the Quality of Service Profile information element. This information element shall be included if the Cause contains the value 'Request accepted'.

The GGSN may start to forward T-PDUs after the Update PDP Context Response has been sent. The SGSN may start to forward T-PDUs when the Update PDP Context Response has been received. In this case the SGSN shall also be prepared to receive T-PDUs from the GGSN after it has sent an Update PDP Context Request but before an Update PDP Context Response has been received.

The GGSN shall include a GGSN Address for control plane and an GGSN address for user traffic, which may differ from that provided by the underlying network service (e.g. IP). The SGSN shall store these GGSN Addresses and use them when sending subsequent control plane on this GTP tunnel or G-PDUs to the GGSN for the MS. When active contexts are being redistributed due to load sharing, G-PDUs that are in transit across the Gn-interface are in an undetermined state and may be lost. The GGSN Address for control plane and the GGSN Address for user traffic shall be included if the Cause contains the value 'Request accepted'.

The GGSN shall include the Recovery information element into the Update PDP Context Response if the GGSN is in contact with the SGSN for the first time or if the GGSN has restarted recently and the new Restart Counter value has not yet been indicated to the SGSN. The SGSN receiving the Recovery information element shall handle it as when an Echo Response message is received but shall consider the PDP context as updated and active if the response cause indicates a successful operation at the GGSN.

The Charging ID is used to identify all charging records produced in SGSN(s) and the GGSN for this PDP context. The Charging ID has been previously generated by the GGSN and is unique for this PDP context. If an inter-SGSN routing area update occurs, it is transferred to the new SGSN as part of each active PDP context. This information element shall be included if the Cause contains the value 'Request accepted'.

The Charging Gateway Address is the IP address of the recommended Charging Gateway Functionality to which the SGSN should transfer the Charging Detail Records (CDR) for this PDP Context.

The optional Private Extension contains vendor or operator specific information.

Table 9: Information Elements in an Update PDP Context Response sent by a GGSN

Information element	Presence requirement	Reference
Cause	Mandatory	7.7.1
Recovery	Optional	7.7.11
Tunnel Endpoint Identifier Data I	Conditional	7.7.13
Tunnel Endpoint Identifier Control Plane	Conditional	7.7.14
Charging ID	Conditional	7.7.26
GGSN Address for Control Plane	Conditional	GSN Address 7.7.32
GGSN Address for User Traffic	Conditional	GSN Address 7.7.32
Quality of Service Profile	Conditional	7.7.34
Charging Gateway Address	Optional	7.7.43
Private Extension	Optional	7.7.44

The message can also be sent from a SGSN node to a GGSN node as a response of a GGSN-initiated Update PDP Context Request.

If the GGSN receives an Update PDP Context Response with a Cause value other than 'Request accepted', it shall abort the update of the PDP context if the associated Update PDP Context Request was sent only to re-negotiate the QoS of a PDP context. Furthermore if the associated Update PDP Context Request included an 'End User Address' information element the GGSN shall delete the PDP context using the Delete PDP Context procedure and may notify the Operation and Maintenance network element.

Only the Cause information element and optionally the Recovery information element shall be included in the response if the Cause contains another value than 'Request accepted'.

Possible Cause values are the same as for the Update PDP Context Response sent by a GGSN.

The QoS values supplied in the Update PDP Context Request may be negotiated downwards by the SGSN. The negotiated values or the original value from GGSN is inserted in the Quality of Service Profile information element. This information element shall be included if the Cause contains the value 'Request accepted' and a QoS information element was supplied in the corresponding request message.

The SGSN shall include the Recovery information element into the Update PDP Context Response if the SGSN has restarted recently and the new Restart Counter value has not yet been indicated to the GGSN. The GGSN receiving the Recovery information element shall handle it as when an Echo Response message is received but shall consider the PDP context as updated and active if the response cause indicates a successful operation at the SGSN.

Table 10: Information Elements in an Update PDP Context Response sent by a SGSN

Information element	Presence requirement	Reference
Cause	Mandatory	7.7.1
Recovery	Optional	7.7.11
Quality of Service Profile	Conditional	7.7.34
Private Extension	Optional	7.7.44

7.3.5 Delete PDP Context Request

A Delete PDP Context Request shall be sent from a SGSN node to a GGSN node as part of the GPRS Detach procedure or the GPRS PDP Context Deactivation procedure or from a GGSN node to a SGSN node as part of the PDP Context Deactivation Initiated by GGSN procedure. A request shall be used to deactivate an activated PDP Context or an activated set of PDP contexts associated to a PDP address assigned to a single MS.

A GSN shall be prepared to receive a Delete PDP Context Request at any time and shall always reply regardless if the PDP context exists or not (as per the Delete PDP Context Response message description section), except in cases described below.

If any collision occurs, the Delete PDP Context Request takes precedence over any other Tunnel Management message.

The Teardown Ind is used to indicate that all PDP contexts that share the PDP address with the PDP context identified in the request should also be deactivated. This may trigger the deletion of all the information kept for a MS at a GSN, if no other PDP contexts associated to other PDP addresses are active on the GSN. This information element shall be included by the SGSN if the Deactivate PDP Context Request message from the MS includes the Tear down indicator at PDP Context Deactivation initiated by MS. Otherwise this information element shall be included by the sending GSN when the last PDP context associated to a PDP address is torn down and there are no outstanding Create PDP context requests for other PDP context different from the one being torn down for that PDP address.

If a GSN receives a Delete PDP context without a Teardown Indicator and only that PDP context is active for a PDP address, then the GSN shall ignore the message. (Note: This is symptom of a race condition. The reliable delivery of signalling messages will eventually lead to a consistent situation, allowing the teardown of the PDP context.)The optional Private Extension contains vendor or operator specific information.

Table 11: Information Elements in a Delete PDP Context Request

Information element	Presence requirement	Reference
Teardown Ind	Conditional	7.7.16
NSAPI	Mandatory	7.7.17
Private Extension	Optional	7.7.44

7.3.6 Delete PDP Context Response

The message shall be sent as a response of a Delete PDP Context Request.

A GSN shall ignore a Delete PDP Context Response for a non-existing PDP context.

If a GSN receives a Delete PDP Context Request message for a non existing PDP context, it will send back to the source of the message a Delete PDP Context Response message with cause value "Non existent". The TEID value used in the response message shall be zero.

Possible Cause values are:

- 'Request Accepted'
- 'Mandatory IE incorrect'
- 'Mandatory IE missing'
- 'Optional IE Incorrect'
- 'Invalid message format'.
- 'Non existent'

If the received Delete PDP Context Response contains a cause value other than 'Request accepted' and 'Non Existent', the PDP context shall be kept active.

The optional Private Extension contains vendor or operator specific information.

Table 12: Information Elements in a Delete PDP Context Response

Information element	Presence requirement	Reference
Cause	Mandatory	7.7.1
Private Extension	Optional	7.7.44

7.3.7 Error Indication

A GSN/RNC shall send an Error Indication to the other GSN or RNC if no active PDP context or RAB exists for a received G-PDU.

When an Error Indication is received from a GSN, the receiving GSN shall delete its PDP context and the GSN may notify the Operation and Maintenance network element.

The SGSN shall indicate to the MS when a PDP context has been deleted due to the reception of an Error Indication message from the GGSN. The MS may then request the re-establishment of the PDP context.

The behaviour of the SGSN when it receives an Error Indication from an RNC is specified in TS 23.060.

The behaviour of the RNC when it receives an Error Indication from a SGSN is specified in TS 23.060.

The information element Tunnel Endpoint Identifier Data I shall be the TEID fetched from the G-PDU that triggered this procedure.

The information element GSN Address shall be the destination address (e.g. destination IP address) fetched from the original user data message that triggered this procedure. A GSN Address can be a GGSN, SGSN or RNC address. The TEID and GSN Address together uniquely identify the related PDP context or RAB in the receiving node. The format of the RNC IP address is the same as the GSN address as defined in 3GPP TS 23.003.

The optional Private Extension contains vendor or operator specific information.

Table 13: Information Elements in an Error Indication

Information element	Presence requirement	Reference
Tunnel Endpoint Identifier Data I	Mandatory	7.7.13
GSN Address	Mandatory	7.7.32
Private Extension	Optional	7.7.44

7.3.8 PDU Notification Request

When receiving a T-PDU the GGSN checks if a PDP context is established for that PDP address. If no PDP context has been previously established, the GGSN may try to deliver the T-PDU by initiating the Network-Requested PDP Context Activation procedure. The criteria, used by the GGSN to determine whether trying to deliver the T-PDU to the MS or not, may be based on subscription information in the GGSN and are outside the scope of GPRS standardisation.

As part of the Network-Requested PDP Context Activation procedure the GGSN sends a PDU Notification Request message to the SGSN indicated by the HLR. If the GGSN has an active PDP context with different SGSN from the one indicated by the HLR, then the SGSN information shall be obtained from an active PDP context. When receiving this message, the SGSN shall be responsible for requesting the MS to activate the indicated PDP Context.

The IMSI is inserted in the IMSI information element in the PDU Notification Request message.

The End User Address information element contains the PDP type and PDP address that the SGSN shall request the MS to activate.

The Access Point Name information element identifies the access point of packet data network that wishes to connect to the MS.

The GGSN shall include a GGSN Address for control plane. The SGSN shall store this GGSN Address and use it when sending control plane messages to the GGSN.

The Tunnel Endpoint Identifier Control Plane information element shall be a tunnel endpoint identifier Control Plane selected by the GGSN and shall be used by the SGSN in the GTP header of the corresponding PDU Notification Response or PDU Notification Request Reject message.

If the GGSN receives a Create PDP Context Request before the PDU Notification Response, the GGSN shall handle the Create PDP Context Request as normal context activation and ignore the following PDU Notification Response.

If the SGSN receives a PDU Notification Request after a Create PDP Context Request has been sent but before a Create PDP Context Response has been received, the SGSN shall:

1. send a PDU Notification Response with Cause ‘Request accepted’ without any further processing and then
2. wait for the Create PDP Context Response.

The optional Private Extension contains vendor or operator specific information.

Table 14: Information Elements in a PDU Notification Request

Information element	Presence requirement	Reference
IMSI	Mandatory	7.7.2
Tunnel Endpoint Identifier Control Plane	Mandatory	7.7.14
End User Address	Mandatory	7.7.27
Access Point Name	Mandatory	7.7.30
GGSN Address for Control Plane	Mandatory	7.7.32
Private Extension	Optional	7.7.44

7.3.9 PDU Notification Response

The message is sent by a SGSN to GGSN as a response of a PDU Notification Request.

The Cause value ‘Request accepted’ indicates if the PDP context activation will proceed. The PDP context activation procedure will not proceed for other Cause values.

Possible Cause values are:

- 'Request Accepted'.
- 'No resources available'.
- 'Service not supported'.
- 'System failure'.
- 'IMSI not known'.
- 'MS is GPRS Detached'.
- 'GPRS connection suspended'.
- 'Mandatory IE incorrect'.
- 'Mandatory IE missing'.
- 'Optional IE incorrect'.
- 'Invalid message format'.
- 'Roaming restriction'.

After an unsuccessful activation attempt the GSNs may perform some actions to prevent unnecessary enquires to the HLR as described in the section Unsuccessful Network-Requested PDP Context Activation procedure in 3GPP TS 23.060.

The optional Private Extension contains vendor or operator specific information.

Table 15: Information Elements in a PDU Notification Response

Information element	Presence requirement	Reference
Cause	Mandatory	7.7.1
Private Extension	Optional	7.7.44

7.3.10 PDU Notification Reject Request

If the PDP context activation proceeds after the PDU Notification Response, but the PDP context was not established, the SGSN sends a PDU Notification Reject Request message. The Cause value indicates the reason why the PDP Context could not be established:

- 'MS Not GPRS Responding'.
- 'MS Refuses'.

When receiving the PDU Notification Reject Request message the GGSN may reject or discard the stored T-PDU(s) depending on the PDP type.

After an unsuccessful activation attempt the GSNs may perform some actions to prevent unnecessary enquiries to the HLR as described in the section Unsuccessful Network-Requested PDP Context Activation procedure in 3GPP TS 23.060.

The Tunnel Endpoint Identifier in the GTP header of the PDU Notification Reject Request message shall be the same as the Tunnel Endpoint Identifier Control Plane information element of the PDU Notification Request that triggered the reject.

The Tunnel Endpoint Identifier Control Plane information element shall be a tunnel endpoint identifier Control Plane selected by the SGSN and shall be used by the GGSN in the GTP header of the corresponding PDU Notification Reject Response message.

The End User Address information element contains the PDP type and PDP address of the PDP context that could not be activated.

The Access Point Name shall be the same as the Access Point Name of the received PDU Notification Request message that triggered the reject.

The optional Private Extension contains vendor or operator specific information.

Table 16: Information Elements in a PDU Notification Reject Request

Information element	Presence requirement	Reference
Cause	Mandatory	7.7.1
Tunnel Endpoint Identifier Control Plane	Mandatory	7.7.14
End User Address	Mandatory	7.7.27
Access Point Name	Mandatory	7.7.30
Private Extension	Optional	7.7.44

7.3.11 PDU Notification Reject Response

The message is sent by a GGSN to SGSN as a response of a PDU Notification Reject Request.

Possible Cause values are:

- 'Request Accepted'.
- 'Mandatory IE incorrect'.
- 'Mandatory IE missing'.
- 'Optional IE incorrect'.
- 'Invalid message format'.

The optional Private Extension contains vendor or operator specific information.

Table 17: Information Elements in a PDU Notification Reject Response

Information element	Presence requirement	Reference
Cause	Mandatory	7.7.1
Private Extension	Optional	7.7.44

7.4 Location Management Messages

The optional Location Management messages are defined to support the case when Network-Requested PDP Context Activation procedures are used and a GGSN does not have a SS7 MAP interface, i.e. a Gc interface. GTP is then used to transfer control plane messages between the GGSN and a GTP-MAP protocol-converting GSN in the GPRS backbone network. The GTP-MAP protocol-converting GSN converts the control plane messages described in this section between GTP and MAP. The MAP messages are sent to and received from the HLR. The GTP-MAP protocol-converting function is described in 3GPP TS 23.060.The MAP protocol describing the corresponding procedures and messages is described in 3GPP TS 29.002. This alternative method is illustrated in Figure 7

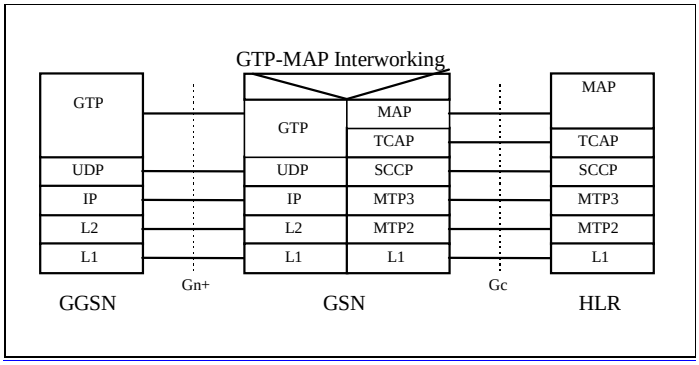


Figure 7: GGSN - HLR Signalling via a GTP-MAP Protocol-Converter in a GSN

When receiving a T-PDU the GGSN checks if a PDP Context is established for that PDP address. If no PDP context has been previously established the GGSN may store the T-PDU, try to initiate the Network-Requested PDP Context Activation procedure and, when the activation procedure is completed, deliver the T-PDU.

To support Network-Requested PDP Context Activation the GGSN has to have static PDP information about the PDP address.

7.4.1 Send Routeing Information for GPRS Request

The GGSN may send a Send Routeing Information for GPRS Request message to a GTP-MAP protocol-converting GSN, to obtain the IP address of the SGSN where the MS is located, when no PDP context is established.

The IMSI information element contains the IMSI to be used as a key to get the IP address of the SGSN.

If the GGSN receives a Create PDP Context Request after a Send Routeing Information for GPRS Request has been sent but before a Send Routeing Information for GPRS Response has been received, the GGSN shall:

1. handle the Create PDP Context Request as a normal context activation and
2. ignore the following Send Routeing Information for GPRS Response.

The optional Private Extension contains vendor or operator specific information.

Table 18: Information Elements in a Send Routeing Information for GPRS Request

Information element	Presence requirement	Reference
IMSI	Mandatory	7.7.2
Private Extension	Optional	7.7.44

7.4.2 Send Routeing Information for GPRS Response

The GTP-MAP protocol-converting GSN sends a Send Routeing Information for GPRS Response message as a response to the Send Routeing Information for GPRS Request message to the GGSN that sent the request.

The Cause value indicates if the GTP-MAP protocol-converting GSN accepted the request or not.

Possible Cause values are:

- 'Request Accepted'.
- 'No resources available'.
- 'Service not supported'.

- 'System failure'.
- 'Mandatory IE incorrect'.
- 'Mandatory IE missing'.
- 'Optional IE incorrect'.
- 'Invalid message format'.

The MAP Cause information element contains the MAP error code received from the HLR and shall not be included if the Cause contains another value than 'Request accepted'.

The GSN Address information element contains the IP address of the SGSN and shall not be included if the Cause contains another value than 'Request accepted'.

It is an implementation issue what to do if the Cause or MAP Cause indicates that no location information is available. The MS not Reachable Reason information element indicates the reason for the setting of the Mobile station Not Reachable for GPRS (MNRG) flag and shall not be included if the Cause contains another value than 'Request accepted'.

The optional Private Extension contains vendor or operator specific information.

Table 19: Information Elements in a Send Routeing Information for GPRS Response

Information element	Presence requirement	Reference
Cause	Mandatory	7.7.1
IMSI	Mandatory	7.7.2
MAP Cause	Optional	7.7.8
MS not Reachable Reason	Optional	7.7.25A
GSN Address	Optional	7.7.32
Private Extension	Optional	7.7.44

7.4.3 Failure Report Request

The GGSN may send this message to the GTP-MAP protocol-converting GSN to set the MNRG flag for the IMSI in the HLR.

The IMSI information element contains the IMSI for which the MNRG shall be set.

The optional Private Extension contains vendor or operator specific information.

Table 20: Information Elements in a Failure Report Request

Information element	Presence requirement	Reference
IMSI	Mandatory	7.7.2
Private Extension	Optional	7.7.44

7.4.4 Failure Report Response

The GTP-MAP protocol-converting GSN sends a Failure Report Response message as a response to the Failure Report Request message to the GGSN that sent the request.

The Cause value indicates if the GTP-MAP protocol-converting GSN accepted the request or not.

Possible Cause values are:

- 'Request Accepted'.
- 'No resources available'.
- 'Service not supported'.

- 'System failure'.
- 'Mandatory IE incorrect'.
- 'Mandatory IE missing'.
- 'Optional IE incorrect'.
- 'Invalid message format'.

The MAP Cause information element contains the MAP error code received from the HLR and shall not be included if the Cause contains another value than 'Request accepted'.

It is an implementation issue what to do if the Cause or MAP Cause indicates that the HLR has not received the request or rejected the request.

The optional Private Extension contains vendor or operator specific information.

Table 21: Information Elements in a Failure Report Response

Information element	Presence requirement	Reference
Cause	Mandatory	7.7.1
MAP Cause	Optional	7.7.8
Private Extension	Optional	7.7.44

7.4.5 Note MS GPRS Present Request

The GTP-MAP protocol-converting GSN sends a Note MS GPRS Present message to notify that an MS should be reachable for GPRS again.

The GGSN shall use the IMSI in the request and find all PDP contexts for the IMSI. The MNRG shall be cleared and the SGSN IP address from the request shall be stored in each found PDP context.

The IMSI information element contains the IMSI for the PDP contexts.

The GSN Address information element contains the IP address of the SGSN.

The optional Private Extension contains vendor or operator specific information.

Table 22: Information Elements in a Note MS Present Request

Information element	Presence requirement	Reference
IMSI	Mandatory	7.7.2
GSN Address	Mandatory	7.7.32
Private Extension	Optional	7.7.44

7.4.6 Note MS GPRS Present Response

The GGSN sends a Note MS GPRS Present Response message to the GTP-MAP protocol converting GSN as a response to the Note MS GPRS Present Request.

Possible Cause values are:

- 'Request Accepted'.
- 'Mandatory IE incorrect'.
- 'Mandatory IE missing'.
- 'Optional IE incorrect'.
- 'Invalid message format'.

The optional Private Extension contains vendor or operator specific information.

Table 23: Information Elements in a Note MS Present Response

Information element	Presence requirement	Reference
Cause	Mandatory	7.7.1
Private Extension	Optional	7.7.44

7.5 Mobility Management Messages

The Mobility Management messages are the control plane messages, defined in 3GPP TS 23.060 and 3GPP TS 24.008, that are sent between SGSNs at the GPRS Attach and Inter SGSN Routeing Update procedures. The new SGSN derives the address of the old SGSN from the old routeing area identity. The address translation mechanism is implementation specific. Some possible translation mechanisms are found in Annex C in 3GPP TS 23.003.

Generally, the purpose of the control plane is to transfer data associated with the MS from the old SGSN to the new SGSN.

7.5.1 Identification Request

If the MS, at GPRS Attach, identifies itself with P-TMSI and it has changed SGSN since detach, the new SGSN shall send an Identification Request message to the old SGSN to request the IMSI.

The P-TMSI and RAI is a P-TMSI and an RAI in the old SGSN. The P-TMSI Signature is conditionally provided by the MS to the new SGSN for identification checking purposes as defined in GSM 3GPP TS 23.060and 3GPP TS 24.008. If the MS has provided the P-TMSI Signature, the new SGSN shall include this parameter in the Identification Request message.

The optional Private Extension contains vendor or operator specific information.

Table 24: Information Elements in an Identification Request

Information element	Presence requirement	Reference
Routeing Area Identity (RAI)	Mandatory	7.7.3
Packet TMSI	Mandatory	7.7.5
P-TMSI Signature	Conditional	7.7.9
Private Extension	Optional	7.7.44

7.5.2 Identification Response

The old SGSN shall send an Identification Response to the new SGSN as a response to a previous Identification Request.

Possible Cause values are:

- ‘Request Accepted’.
- ‘IMSI not known’.
- ‘System failure’.
- ‘Mandatory IE incorrect’.
- ‘Mandatory IE missing’.
- ‘Optional IE incorrect’.
- ‘Invalid message format’.
- ‘P-TMSI Signature mismatch’.

Only the Cause information element shall be included in the response if the Cause contains another value than ‘Request accepted’.

The IMSI information element is mandatory if the Cause contains the value ‘Request accepted’.

One or several Authentication Triplet information elements or up to 5 Authentication Quintuplet information elements may be included in the message if the Cause contains the value 'Request accepted'.

The optional Private Extension contains vendor or operator specific information.

Table 25: Information Elements in an Identification Response

Information element	Presence requirement	Reference
Cause	Mandatory	7.7.1
IMSI	Conditional	7.7.2
Authentication Triplet	Conditional	7.7.7
Authentication Quintuplet	Conditional	7.7.35
Private Extension	Optional	7.7.44

7.5.3 SGSN Context Request

The new SGSN shall send an SGSN Context Request to the old SGSN to get the MM and PDP Contexts for the MS. The MS is identified by its old RAI and old TLLI/old P-TMSI values. The TLLI/P-TMSI and RAI is a TLLI/P-TMSI and an RAI in the old SGSN. One of the TLLI or P-TMSI information fields must be present unless IMSI is present.

The old SGSN responds with an SGSN Context Response.

The new SGSN shall include a SGSN Address for control plane. The old SGSN shall store this SGSN Address and use it when sending control plane messages for the MS to the new SGSN in the SGSN context transfer procedure.

The Tunnel Endpoint Identifier Control Plane field specifies a Tunnel Endpoint Identifier for control plane messages, which is chosen by the new SGSN. The old SGSN shall include this Tunnel Endpoint Identifier in the GTP header of all subsequent control plane messages that are sent from the old SGSN to the new SGSN and related to the PDP context(s) requested.

The MS Validated indicates that the new SGSN has successfully authenticated the MS. IMSI shall be included if MS Validated indicates 'Yes'.

The P-TMSI Signature is conditionally provided by the MS to the new SGSN for identification checking purposes as defined in GSM 3GPP TS 23.060 and 3GPP TS 24.008. If the MS has provided the P-TMSI Signature, the new SGSN shall include this parameter in the SGSN Context Request message.

The optional Private Extension contains vendor or operator specific information.

Table 26: Information Elements in a SGSN Context Request

Information element	Presence requirement	Reference
IMSI	Conditional	7.7.2
Routeing Area Identity (RAI)	Mandatory	7.7.3
Temporary Logical Link Identifier (TLLI)	Conditional	7.7.4
Packet TMSI (P-TMSI)	Conditional	7.7.5
P-TMSI Signature	Conditional	7.7.9
MS Validated	Optional	7.7.10
Tunnel Endpoint Identifier Control Plane	Mandatory	7.7.14
SGSN Address for Control Plane	Mandatory	7.7.32
Private Extension	Optional	7.7.44

7.5.4 SGSN Context Response

The old SGSN shall send an SGSN Context Response to the new SGSN as a response to a previous SGSN Context Request.

Possible Cause values are:

- 'Request Accepted'.
- 'IMSI not known'.

- 'System failure'.
- 'Mandatory IE incorrect'.
- 'Mandatory IE missing'.
- 'Optional IE incorrect'.
- 'Invalid message format'.
- 'P-TMSI Signature mismatch'.

If the Cause contains the value 'Request accepted', all information elements are mandatory, except PDP Context and Private Extension.

If the Cause contains the value 'P-TMSI Signature mismatch' the IMSI information element shall be included in the response, otherwise only the Cause information element shall be included in the response.

The old SGSN shall include a SGSN Address for control plane. The new SGSN shall store this SGSN Address and use it when sending control plane messages for the MS to the old SGSN in the SGSN context transfer procedure.

The Tunnel Endpoint Identifier Control Plane field specifies a Tunnel Endpoint Identifier, which is chosen by the old SGSN. The new SGSN shall include this Tunnel Endpoint Identifier in the GTP header of all subsequent control plane messages, which are sent from the new SGSN to the old SGSN and related to the PDP context(s) requested.

The IMSI information element contains the IMSI matching the TLLI or P-TMSI (for GSM or UMTS respectively) and RAI in the SGSN Context Request.

The MM Context contains necessary mobility management and security parameters.

All active PDP contexts in the old SGSN shall be included as PDP Context information elements.

If there is at least one active PDP context, the old SGSN shall start the T3-TUNNEL timer and store the address of the new SGSN in the "New SGSN Address" field of the MM context. The old SGSN shall wait for SGSN Context Acknowledge before sending T-PDUs to the new SGSN. If the old SGSN has one or more active PDP contexts for the subscriber and an SGSN Context Acknowledge message is not received within a time defined by T3-RESPONSE, the old SGSN shall retransmit the SGSN Context Response to the new SGSN as long as the total number of attempts is less than N3-REQUESTS. After N3-REQUESTS unsuccessfully attempts, the old SGSN shall proceed as described in section 'Reliable delivery of signalling messages' in case the transmission of a control plane message fails N3-REQUESTS times.

Radio Priority SMS contains the radio priority level for MO SMS transmission, and shall be included if a valid Radio Priority SMS value exists for the MS in the old SGSN.

Radio Priority is the radio priority level that the MS uses when accessing the network for the transmission of uplink user data for a particular PDP context. One Radio Priority IE shall be included per PDP context that has a valid radio priority value assigned to it in the old SGSN.

Packet Flow Id is the packet flow identifier assigned to the PDP context. One Packet Flow Id IE shall be included per PDP context that has a valid packet flow identifier value assigned to it in the old SGSN.

The optional Private Extension contains vendor or operator specific information.

Table 27: Information Elements in a SGSN Context Response

Information element	Presence requirement	Reference
Cause	Mandatory	7.7.1
IMSI	Conditional	7.7.2
Tunnel Endpoint Identifier Control Plane	Conditional	7.7.14
Radio Priority SMS	Optional	7.7.20
Radio Priority	Optional	7.7.21
Packet Flow Id	Optional	7.7.22
MM Context	Conditional	7.7.28
PDP Context	Conditional	7.7.29
SGSN Address for Control Plane	Conditional	7.7.32
Private Extension	Optional	7.7.44

7.5.5 SGSN Context Acknowledge

The new SGSN shall send an SGSN Context Acknowledge message to the old SGSN as a response to the SGSN Context Response message. Only after receiving the SGSN Context Acknowledge message, shall the old SGSN start to forward user data packets. SGSN Context Acknowledge indicates to the old SGSN that the new SGSN has correctly received PDP Context information and is ready to receive user data packets identified by the corresponding Tunnel Endpoint Identifier values. This message shall not be sent if no PDP contexts are active for the MS (that is no PDP context information was transferred in the SGSN context response message) or the SGSN Context Request was rejected.

Possible cause values are:

- 'Request accepted'.
- 'System failure'.
- 'Mandatory IE incorrect'.
- 'Mandatory IE missing'.
- 'Optional IE incorrect'.
- 'No resources available'.
- 'Invalid message format'.
- 'Authentication failure'.

Only the Cause information element shall be included in the acknowledgement if the Cause contains a value other than 'Request accepted'.

For each active PDP context the new SGSN shall include a Tunnel Endpoint Identifier Data II information element. The Tunnel Endpoint Identifier Data II field specifies a Tunnel Endpoint Identifier which is chosen by the new SGSN for a particular PDP context. The old SGSN shall include this Tunnel Endpoint Identifier in the GTP header of all subsequent G-PDUs which are sent from the old SGSN to the new SGSN and related to the particular PDP context. When active PDP context(s) exist, this information element shall be included if the Cause contains the value 'Request accepted'.

The new SGSN shall include an SGSN Address for user traffic, which may differ from that provided by the underlying network service (e.g. IP). The old SGSN shall store this SGSN Address and use it when sending G-PDUs to the new SGSN for the MS. When active PDP context(s) exist, this information element shall be included if the Cause contains the value 'Request accepted'.

The optional Private Extension contains vendor or operator specific information.

Table 28: Information Elements in a SGSN Context Acknowledge

Information element	Presence requirement	Reference
Cause	Mandatory	7.7.1
Tunnel Endpoint Identifier Data II	Conditional	7.7.15
SGSN Address for user traffic	Conditional	GSN Address 7.7.32
Private Extension	Optional	7.7.44

7.5.6 Forward Relocation Request

The old SGSN shall send a Forward Relocation Request to the new SGSN to convey necessary information to perform the SRNS Relocation procedure between new SGSN and Target RNC.

All information elements are mandatory, except PDP Context and Private Extension.

The IMSI information element contains the IMSI of the target MS for SRNS Relocation procedure.

The old SGSN shall include a SGSN Address for control plane. The new SGSN shall store this SGSN Address and use it when sending control plane messages for the MS to the old SGSN in the SRNS Relocation procedure.

The Tunnel Endpoint Identifier Control Plane field specifies a tunnel endpoint identifier, which is chosen by the old SGSN. The new SGSN shall include this Tunnel Endpoint Identifier Control Plane in the GTP header of all subsequent control plane messages, which are sent from the new SGSN to the old SGSN.

The MM Context contains necessary mobility management and security parameters.

All active PDP contexts in the old SGSN shall be included as PDP Context information elements. In case no PDP context is active, this IE shall not be included.

UTRAN transparent container, Target identification and RANAP Cause are information from the source RNC in the old SGSN.

The optional Private Extension contains vendor or operator specific information.

Table 29: Information Elements in a Forward Relocation Request

Information element	Presence requirement	Reference
IMSI	Mandatory	7.7.2
Tunnel Endpoint Identifier Control Plane	Mandatory	7.7.14
RANAP Cause	Mandatory	7.7.18
MM Context	Mandatory	7.7.28
PDP Context	Conditional	7.7.29
SGSN Address for Control plane	Mandatory	7.7.32
Target Identification	Mandatory	7.7.37
UTRAN transparent container	Mandatory	7.7.38
Private Extension	Optional	7.7.44

7.5.7 Forward Relocation Response

The new SGSN shall send a Forward Relocation Response to the old SGSN as a response to a previous Forward Relocation Request.

Possible Cause values is:

- ‘Request Accepted’.
- ‘System failure’.
- ‘Mandatory IE incorrect’.
- ‘Mandatory IE missing’.
- ‘Optional IE incorrect’.

- 'No resources available'.
- 'Invalid message format'.
- 'Relocation failure'.

RANAP Cause is mandatory if cause value is contained in RANAP message.

RAB Setup Information, UTRAN transparent container and RANAP Cause are information from the target RNC in the new SGSN.

One or more RAB Setup Information parameters shall be set in this message. This information element shall be included if the Cause contains the value 'Request accepted'.

The new SGSN shall include a SGSN Address for control plane. The old SGSN shall store this SGSN Address and use it when sending control plane messages for the MS to the new SGSN in the SRNS Relocation Procedure.

The Tunnel Endpoint Identifier Control Plane field specifies a Tunnel Endpoint Identifier that is chosen by the new SGSN. The old SGSN shall include this Tunnel Endpoint Identifier in the GTP header of all subsequent signalling messages that are sent from the old SGSN to the new SGSN. This information element shall be included if the Cause contains the value 'Request accepted'.

The optional Private Extension contains vendor or operator specific information.

Table 30: Information Elements in a Forward Relocation Response

Information element	Presence requirement	Reference
Cause	Mandatory	7.7.1
Tunnel Endpoint Identifier Control Plane	Conditional	7.7.14
RANAP Cause	Conditional	7.7.18
SGSN Address for Control plane	Conditional	7.7.32
UTRAN transparent container	Optional	7.7.38
RAB Setup Information	Conditional	7.7.39
Private Extension	Optional	7.7.44

7.5.8 Forward Relocation Complete

The new SGSN shall send a Forward Relocation Complete to the old SGSN to indicate that the SRNS relocation procedure has been successfully finished.

The optional Private Extension contains vendor or operator specific information.

Table 31: Information Elements in a Forward Relocation Complete

Information element	Presence requirement	Reference
Private Extension	Optional	7.7.44

7.5.9 Relocation Cancel Request

The Relocation Cancel Request message is sent from the old SGSN to the new SGSN when the old SGSN is requested to cancel the relocation procedure by the source RNC by means of RANAP message.

The optional Private Extension contains vendor or operator specific information.

Table 32: Information Elements in a Relocation Cancel Request

Information element	Presence requirement	Reference
IMSI	Mandatory	7.7.2
Private Extension	Optional	7.7.44

7.5.10 Relocation Cancel Response

The Relocation Cancel Response message is sent from the new SGSN to the old SGSN when the relocation procedure has been cancelled in the old SGSN. This message is used as the response to the Relocation Cancel Request message.

Possible Cause values are:

- 'Request Accepted'
- 'IMSI not known'
- 'Mandatory IE incorrect'
- 'Mandatory IE missing'
- 'Optional IE incorrect'
- 'Invalid message format'

The optional Private Extension contains vendor or operator specific information.

Table 33: Information Elements in a Relocation Cancel Response

Information element	Presence requirement	Reference
Cause	Mandatory	7.7.1
Private Extension	Optional	7.7.44

7.5.11 Forward Relocation Complete Acknowledge

The old SGSN sends a Forward Relocation Complete Acknowledge message to the new SGSN as a response to Forward Relocation Complete.

Possible Cause Values are:

- 'Request Accepted'
- 'Optional IE incorrect'
- 'Invalid message format'

The optional Private Extension contains vendor or operator specific information.

Table 34: Information elements in a Forward Relocation Complete Acknowledge

Information element	Presence requirement	Reference
Cause	Mandatory	7.7.1
Private Extension	Optional	7.7.26

7.5.12 Forward SRNS Context Acknowledge

The new SGSN sends a Forward SRNS Context Acknowledge message to the old SGSN as a response to Forward SRNS Context.

Possible Cause values are:

- 'Request Accepted'

- 'Mandatory IE incorrect'
- 'Mandatory IE missing'
- 'Optional IE incorrect'
- 'Invalid message format'

Table 35: Information elements in a Forward SRNS Context Acknowledge

Information element	Presence requirement	Reference
Cause	Mandatory	7.7.1
Private Extension	Optional	7.7.26

7.5.13 Forward SRNS Context

The Forward SRNS Context message is used in case of hard handover with switch in CN. When the old SGSN receives the RANAP message Forward SRNS Context, the old SGSN shall send a Forward SRNS Context message to the new SGSN. The new SGSN shall forward the message to the target RNC using the corresponding RANAP message.

For each RAB context in the received RANAP message, the old SGSN shall include a RAB Context IE in the GTP-C Forward SRNS Context message.

Table 36: Information Elements in a Forward SRNS Context

Information element	Presence requirement	Reference
RAB Context	Mandatory	7.7.19
Private Extension	Optional	7.7.44

7.6 Reliable Delivery of Signalling Messages

Each path maintains a queue with signalling messages to be sent to the peer. The message at the front of the queue, if it is a request for which a response has been defined, shall be sent with a Sequence Number, and shall be held in a path list until a response is received. Each path has its own list. The Sequence Number shall be unique for each outstanding request message sourced from the same IP/UDP endpoint. A GSN or RNC may have several outstanding requests while waiting for responses.

The T3-RESPONSE timer shall be started when a signalling request message (for which a response has been defined) is sent. A signalling message request or response has probably been lost if a response has not been received before the T3-RESPONSE timer expires. The request is then retransmitted if the total number of request attempts is less than N3-REQUESTS times. The timer shall be implemented in the control plane application as well as user plane application for Echo Request / Echo Response. The wait time for a response (T3-RESPONSE timer value) and the number of retries (N3-REQUESTS) shall be configurable per procedure. The total wait time shall be shorter than the MS wait time between retries of Attach and RA Update messages.

All received request messages shall be responded to and all response messages associated with a certain request shall always include the same information. Duplicated response messages shall be discarded, and, for the SGSN Context Response case, the SGSN Context Acknowledge message shall be sent depending on the content of the received response message. A response message without a matching outstanding request should be considered as a duplicate.

The Forward Relocation Complete and Forward SRNS Context messages shall be treated as signalling request messages. The SGSN Context Acknowledge, Forward Relocation Complete Acknowledge and Forward SRNS Context Acknowledge messages shall be treated as response messages.

The SGSN Context Response message needs special treatment by the old SGSN and New SGSN:

The New SGSN must consider this as a regular response to the outstanding SGSN Context Request message, but also copy the sequence number in the header of the SGSN Context Acknowledge it shall send back to the old SGSN depending on the content of the received response message.The Old SGSN, when it expects the new SGSN to send back a SGSN Context Acknowledge in response to a SGSN Context Response, shall keep track of the SGSN Context Response message sequence number and apply to this message the rules valid for a Request message too.If a GSN or RNC is not successful with the transfer of a signalling message, e.g. a Create PDP Context Request message, it shall inform the upper layer of the unsuccessful transfer so that the controlling upper entity may take the necessary measures.

7.7 Information Elements

A GTP Signalling message may contain several information elements. The TLV (Type, Length, Value) or TV (Type, Value) encoding format shall be used for the GTP information elements. The information elements shall be sorted, with the Type fields in ascending order, in the signalling messages. The Length field contains the length of the information element excluding the Type and Length field.

For all the length fields, bit 8 of the lowest numbered octet is the most significant bit and bit 1 of the highest numbered octet is the least significant bit.

Within information elements, certain fields may be described as spare. These bits shall be transmitted with the value defined for them. To allow for future features, the receiver shall not evaluate these bits.

The most significant bit in the Type field is set to 0 when the TV format is used and set to 1 for the TLV format.

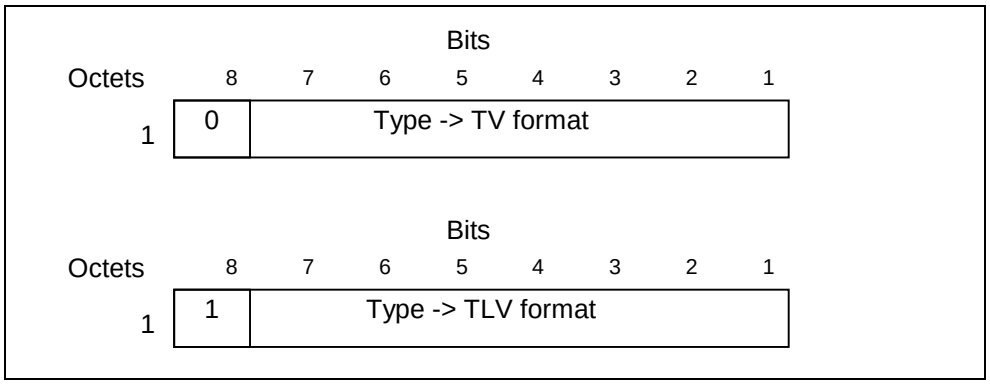


Figure 8: Type field for TV and TLV format

Table 37: Information Elements

IE Type Value	Format	Information Element	Reference
1	TV	Cause	7.7.1
2	"	International Mobile Subscriber Identity (IMSI)	7.7.2
3	"	Routeing Area Identity (RAI)	7.7.3
4	"	Temporary Logical Link Identity (TLLI)	7.7.4
5	"	Packet TMSI (P-TMSI)	7.7.5
6-7	Spare		
8	"	Reordering Required	7.7.6
9	"	Authentication Triplet	7.7.7
10	Spare		
11	"	MAP Cause	7.7.8
12	"	P-TMSI Signature	7.7.9
13	"	MS Validated	7.7.10
14	"	Recovery	7.7.11
15	"	Selection Mode	7.7.12
16	"	Tunnel Endpoint Identifier Data I	7.7.13
17	"	Tunnel Endpoint Identifier Control Plane	7.7.14
18	"	Tunnel Endpoint Identifier Data II	7.7.15
19	"	Teardown Ind	7.7.16
20	"	NSAPI	7.7.17
21	"	RANAP Cause	7.7.18
22	"	RAB Context	7.7.19
23	"	Radio Priority SMS	7.7.20
24	"	Radio Priority	7.7.21
25	"	Packet Flow Id	7.7.22
26	"	Charging Characteristics	7.7.23
27	"	Trace Reference	7.7.24
28	"	Trace Type	7.7.25
29	"	MS Not Reachable Reason	7.7.25A
117-126	Reserved for the GPRS charging protocol (see GTP' in GSM 12.15)		
127	"	Charging ID	7.7.26
128	TLV	End User Address	7.7.27
129	"	MM Context	7.7.28
130	"	PDP Context	7.7.29
131	"	Access Point Name	7.7.30
132	"	Protocol Configuration Options	7.7.31
133	"	GSN Address	7.7.32
134	"	MS International PSTN/ISDN Number (MSISDN)	7.7.33
135	"	Quality of Service Profile	7.7.34
136	"	Authentication Quintuplet	7.7.35
137	"	Traffic Flow Template	7.7.36
138	"	Target Identification	7.7.37
139	"	UTRAN Transparent Container	7.7.38
140	"	RAB Setup Information	7.7.39
141	"	Extension Header Type List	7.7.40
142	"	Trigger Id	7.7.41
143	"	OMC Identity	7.7.42
239-250	Reserved for the GPRS charging protocol (see GTP' in GSM 12.15)		
251	"	Charging Gateway Address	7.7.43
252-254	Reserved for the GPRS charging protocol (see GTP' in GSM 12.15)		
255	"	Private Extension	7.7.44

7.7.1 Cause

In a request, the Cause Value indicates the reason for the request. The Cause shall be included in the request message.

In a response, the Cause Value indicates the acceptance or the rejection of the corresponding request. In addition, the Cause Value may indicate what was the reason for the corresponding request. The Cause value shall be included in the response message.

'Request accepted' is returned when a GSN has accepted a control plane request.

'Non-existent' indicates a non-existent or an inactive PDP context.

'IMSI not known' indicates a non-existent MM context.

'MS is GPRS Detached' indicates an idle MM context.

'MS is not GPRS Responding' and 'MS Refuses' may be used by SGSN to reject a Network-Requested PDP Context Activation.

'Version not supported' is returned when the recipient does not recognise the version number in the request message.

'Request IMSI', 'Request IMEI', 'Request IMSI and IMEI' and 'No identity needed' are used by GGSN to notify SGSN what to do.

'No resources available' is a generic temporary error condition e.g. all dynamic PDP addresses occupied or no memory available.

'Service not supported' is a generic error indicated that the GSN do not support the requested service.

'User authentication failed' indicates that the external packet network has rejected the user's service request.

'System failure' is a generic permanent error condition.

'Roaming restriction' indicates that the SGSN cannot activate the requested PDP context because of the roaming restrictions.

'P-TMSI Signature mismatch' is returned if either:

- the P-TMSI Signature stored in the old SGSN does not match the value sent by the MS via the new SGSN
- or the MS does not provide the P-TMSI Signature to the new SGSN while the old SGSN has stored the P-TMSI Signature for that MS.

'Semantic error in the TFT operation', 'Syntactic error in the TFT operation', 'Semantic errors in packet filter(s)' and 'Syntactic errors in packet filters(s) are indications of abnormal cases involving TFTs. The abnormal TFT cases and the use of the cause codes are defined in 3GPP TS 24.008.

'Invalid message format', 'Mandatory IE incorrect', 'Mandatory IE missing' and 'Optional IE incorrect' are indications of protocol errors described in the section Error handling.

'GPRS connection suspended' indicates that the GPRS activities of the mobile station are suspended.

'Authentication failure' indicates that the user authentication failed in the new SGSN.

'Context not found' indicates that the PDP Context referenced in an Active Secondary Context Request message was not found in the receiving GGSN.

'Relocation failure' indicates that the SRNS relocation failed in the new SGSN side.

'Unknown mandatory extension header' signals in a response message that the corresponding request included an extension header for which comprehension was required but unknown to the receiving end.

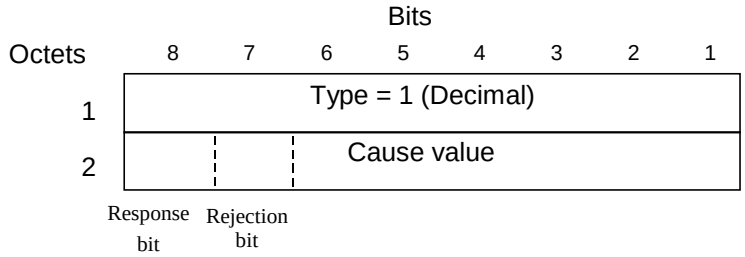


Figure 9: Cause information element

Table 38: Cause Values

Cause			Value (Decimal)
request		Request IMSI	0
		Request IMEI	1
		Request IMSI and IMEI	2
		No identity needed	3
		MS Refuses	4
		MS is not GPRS Responding	5
		For future use	6-48
		Cause values reserved for GPRS charging protocol use (see GTP' in GSM 12.15)	49-63
For future use			64-127
response	acc	Request accepted	128
		For future use	129-176
		Cause values reserved for GPRS charging protocol use (see GTP' in GSM 12.15)	177-191
	rej	Non-existent	192
		Invalid message format	193
		IMSI not known	194
		MS is GPRS Detached	195
		MS is not GPRS Responding	196
		MS Refuses	197
		For future use	198
		No resources available	199
		Service not supported	200
		Mandatory IE incorrect	201
		Mandatory IE missing	202
		Optional IE incorrect	203
		System failure	204
		Roaming restriction	205
		P-TMSI Signature mismatch	206
		GPRS connection suspended	207
		Authentication failure	208
		User authentication failed	209
		Context not found	210
		All dynamic PDP addresses are occupied	211
		No memory is available	212
		Relocation failure	213
		Unknown mandatory extension header	214
		Semantic error in the TFT operation	215
		Syntactic error in the TFT operation	216
		Semantic errors in packet filter(s)	217
		Syntactic errors in packet filter(s)	218
		Missing or unknown APN	219
		Unknown PDP address or PDP type	220
		For future use	221-240
		Cause values reserved for GPRS charging protocol use (see GTP' in GSM 12.15)	241-255

NOTE: With this coding, bits 8 and 7 of the Cause Value respectively indicate whether the message was a request or a response, and whether the request was accepted or rejected.

Table 39: Use of the Cause Values

Cause 8	value bits 7	Result
0	0	Request
0	1	For future use (Note)
1	0	Acceptance
1	1	Rejection

NOTE: The value '01' is for future use and shall not be sent. If received in a response, it shall be treated as a rejection.

7.7.2 International Mobile Subscriber Identity (IMSI)

The IMSI shall be the subscriber identity of the MS. The IMSI is defined in 3GPP TS 23.003.

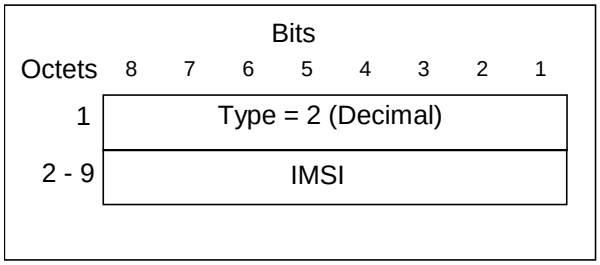


Figure 10: IMSI Information Element

The IMSI is TBCD-coded with a fixed length of 8 octets. Bits 8765 of octet n+1 encodes digit 2n, bits 4321 of octet n+1 encodes digit 2n-1. Unused half octets shall be coded as binary "1 1 1 1". Digits are packed contiguously with no internal padding.

7.7.3 Routeing Area Identity (RAI)

The RAI information element is given by:

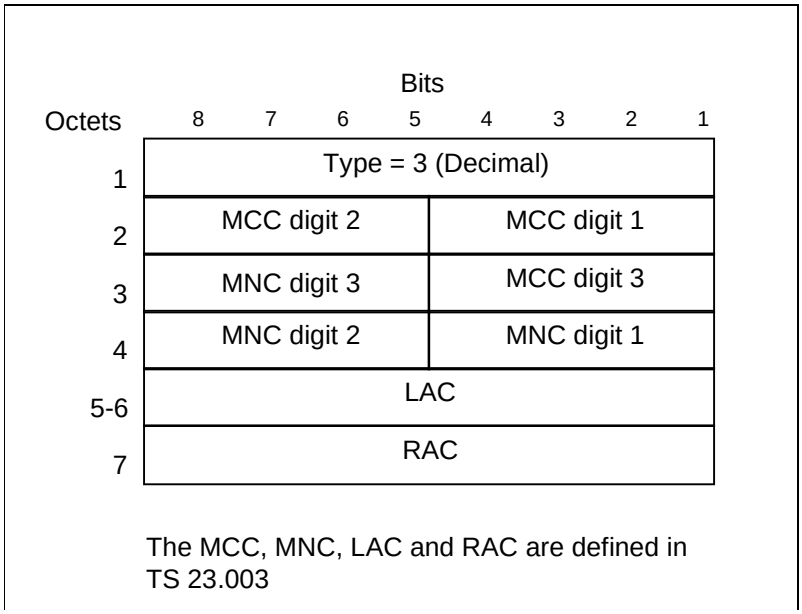


Figure 11: RAI Information Element

If an Administration decides to include only two digits in the MNC, then bits 5 to 8 of octet 3 are coded as "1111".

7.7.4 Temporary Logical Link Identity (TLLI)

The information element of the TLLI associated with a given MS and routeing area is given by:

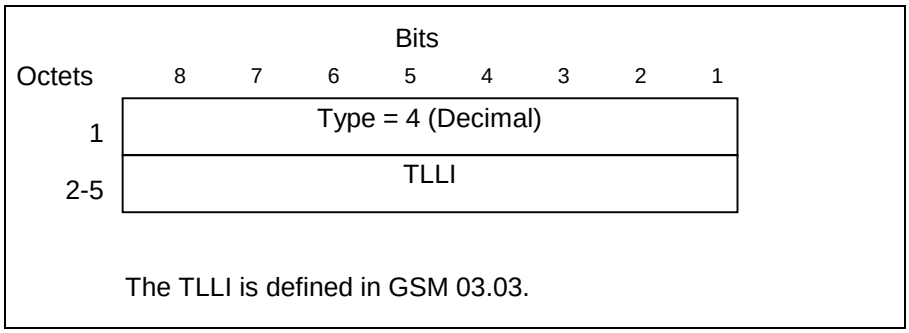


Figure 12: TLLI Information Element

7.7.5 Packet TMSI (P-TMSI)

The Packet TMSI, unambiguously associated with a given MS and routeing area, is given by:

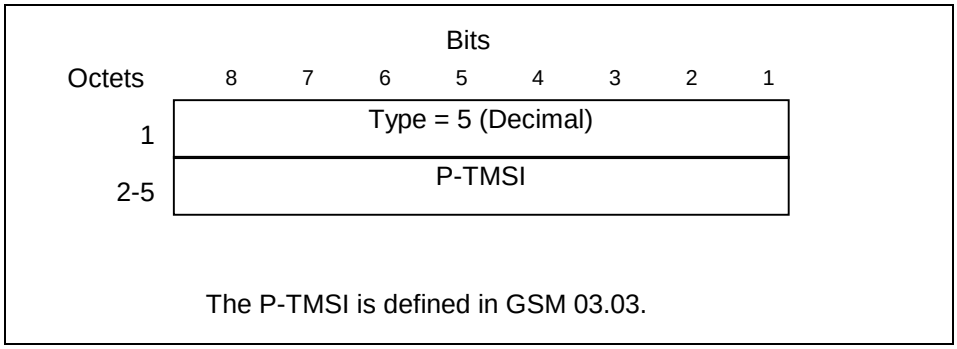


Figure 13: The Packet TMSI Information Element

7.7.6 Reordering Required

The Reordering Required information element states whether reordering by GTP is required or not.

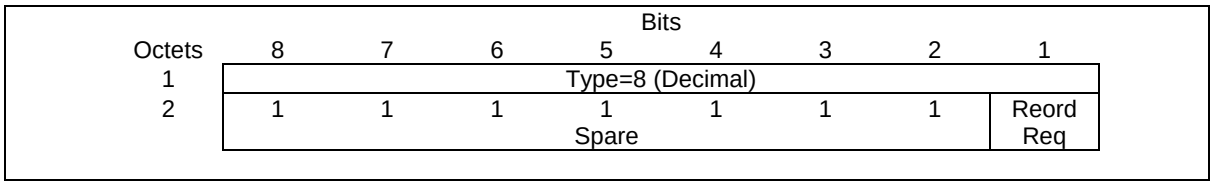


Figure 14: Reordering Required Information Element

Table 40: Reordering Required Values

Reordering required	Value (Decimal)
No	0
Yes	1

7.7.7 Authentication Triplet

An Authentication triplet consists of a random string (RAND), a signed response (SRES) and a ciphering key (Kc) (see GSM 03.20).

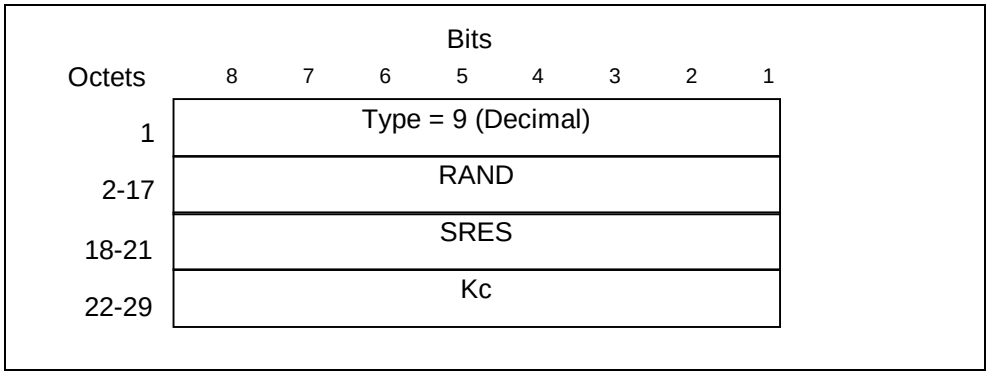


Figure 15: Authentication Triplet Information Element

7.7.8 MAP Cause

The MAP Cause is a value that the GTP-MAP protocol-converting GSN relays transparently from HLR to the GGSN. The possible MAP Cause values for the appropriate messages are described in 3GPP TS 29.002.

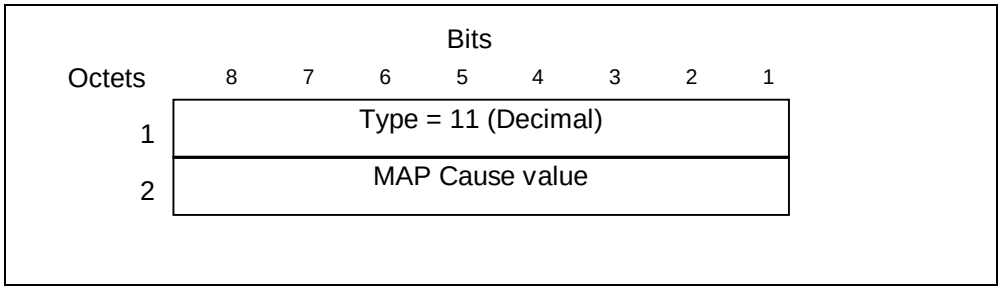


Figure 16: MAP Cause Information Element

7.7.9 P-TMSI Signature

The P-TMSI Signature information element is provided by the MS in the Routing Area Update Request and Attach Request messages to the SGSN for identification checking purposes. The content and the coding of the P-TMSI Signature information element are defined in 3GPP TS 24.008.

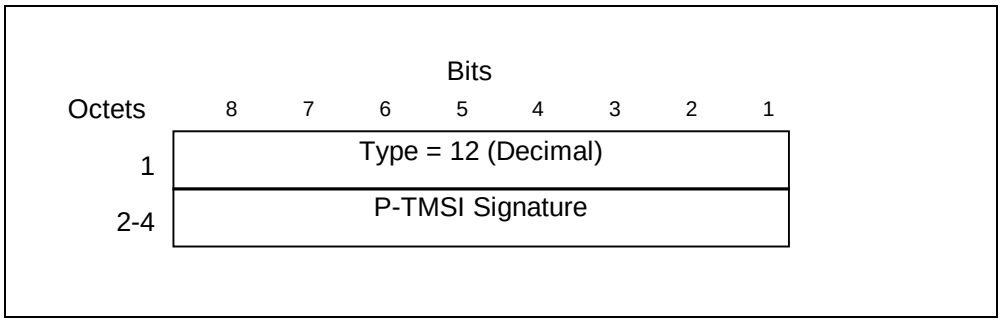


Figure 17: P-TMSI Signature Information Element

7.7.10 MS Validated

The MS Validated information element indicates whether the new SGSN has successfully authenticated the MS.

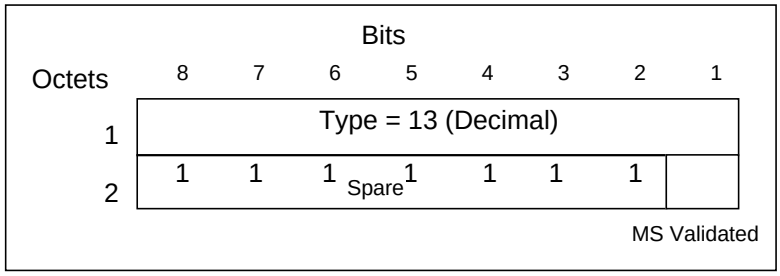


Figure 18: MS Validated Information Element

Table 41: MS Validated Values

MS Validated	Value
No	0
Yes	1

7.7.11 Recovery

The Recovery information element indicates if the peer GSN has restarted. The Restart Counter shall be the value described in the section Restoration and Recovery.

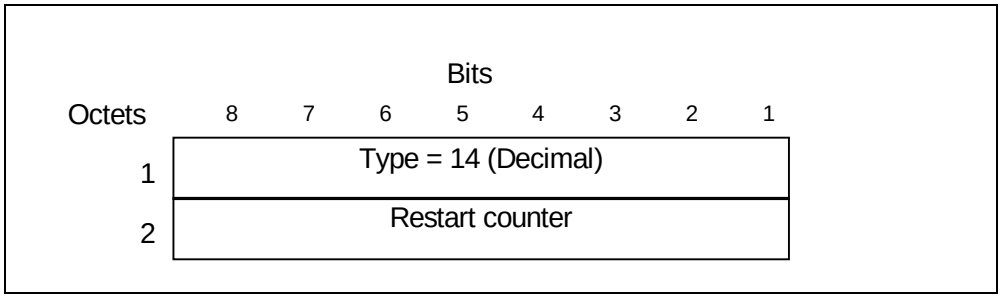


Figure 19: Restart Counter Information Element

7.7.12 Selection Mode

The Selection mode information element indicates the origin of the APN in the message.

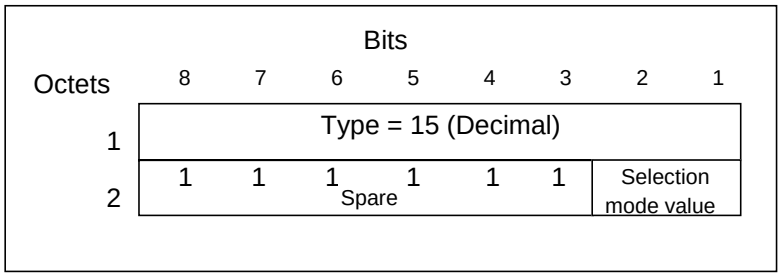


Figure 20: Selection Mode Information Element

Table 42: Selection Mode Values

Selection mode value	Value (Decimal)
MS or network provided APN, subscribed verified	0
MS provided APN, subscription not verified	1
Network provided APN, subscription not verified	2
For future use. Shall not be sent. If received, shall be interpreted as the value '2'.	3

7.7.13 Tunnel Endpoint Identifier Data I

The Tunnel Endpoint Identifier Data I information element contains the Tunnel Endpoint Identifier for data transmission requested by the receiver of the flow.

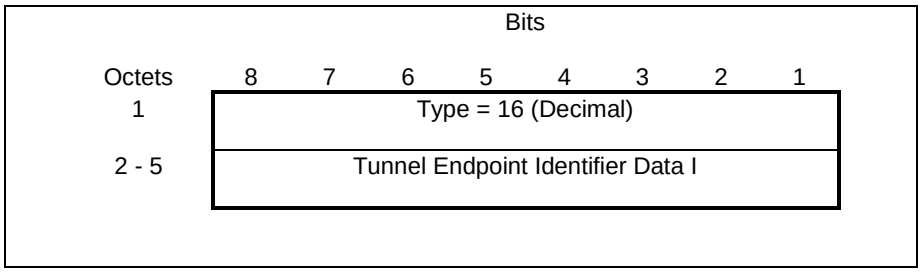


Figure 21: Tunnel Endpoint Identifier Data I Information Element

7.7.14 Tunnel Endpoint Identifier Control Plane

The Tunnel Endpoint Identifier Control Plane information element contains the Tunnel Endpoint Identifier for the control plane; it is assigned by the receiver of the flow. It distinguishes the tunnel from other tunnels between the same pair of entities.

If the receiver has not yet assigned a TEID for this tunnel, it shall assign an unused value to the TEID.

If the receiver has already assigned a Tunnel Endpoint Identifier Control Plane to the tunnel, but has not yet received confirmation of successful assignment from the transmitter, this information element shall take the same value as was sent before for this tunnel.

The receiver receives confirmation of successful assignment of its Tunnel Endpoint Identifier Control Plane from the transmitter when it receives any message with its assigned Tunnel Endpoint Identifier Control Plane in the GTP header from the transmitter.

If the Tunnel Endpoint Identifier Control Plane is received from the transmitter, this information element shall be stored.

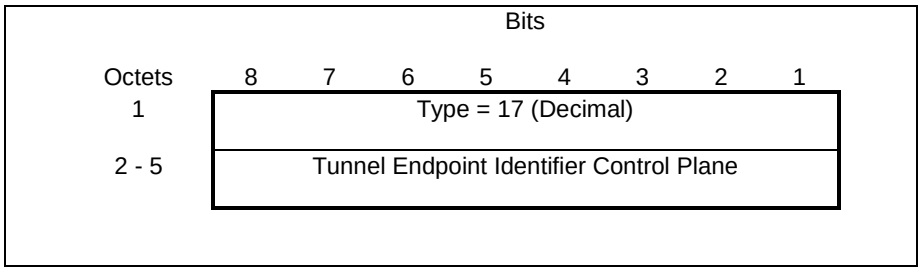


Figure 22: Tunnel Endpoint Identifier Control Plane Information Element

7.7.15 Tunnel Endpoint Identifier Data II

The Tunnel Endpoint Identifier Data II information element contains the Tunnel Endpoint Identifier for data transmission between old and new SGSN for a particular PDP context and is requested by the new SGSN.

The spare bits x indicate unused bits, which shall be set to 0 by the sending side and which shall not be evaluated by the receiving side.

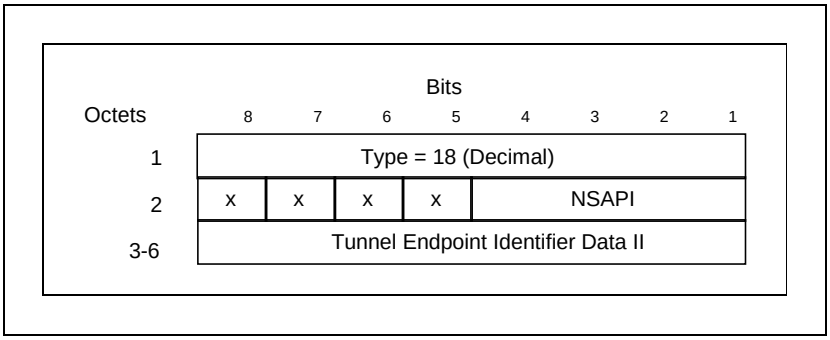


Figure 23: Tunnel Endpoint Identifier Data II Information Element

7.7.16 Teardown Ind

The Teardown Ind information element, when included in the Delete PDP Context Request, indicate that the message applies to all PDP contexts that share the same PDP address.

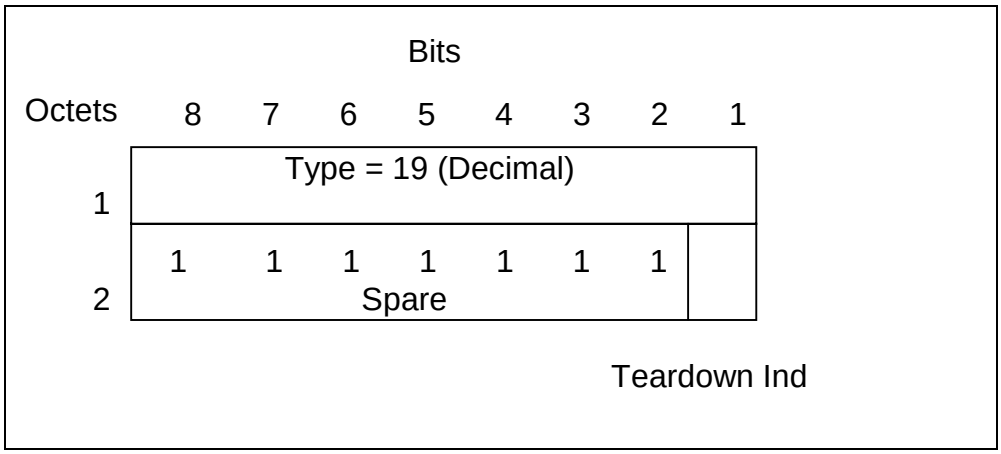


Figure 24: Teardown Ind Information Element

Table 43: Teardown Ind

Teardown Ind	Value
No	0
Yes	1

7.7.17 NSAPI

The NSAPI information element contains an NSAPI identifying a PDP Context in a mobility management context specified by the Tunnel Endpoint Identifier Control Plane.

The spare bits x indicate unused bits, which shall be set to 0 by the sending side, and the sending side shall not evaluate them.

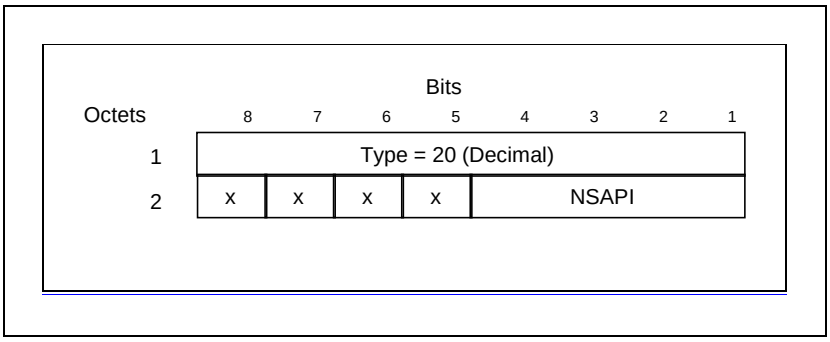


Figure 25: NSAPI Information Element

7.7.18 RANAP Cause

The RANAP Cause information element contains the cause as defined in 3GPP TS 25.413.

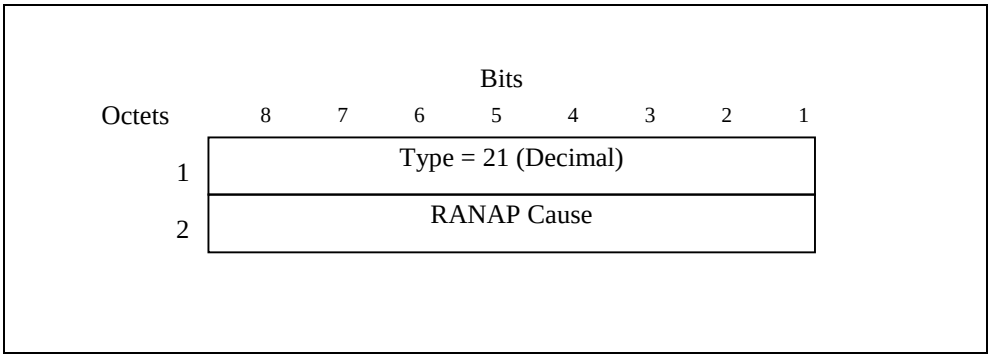


Figure 26: RANAP Cause Information Element

7.7.19 RAB Context

The RAB context information element contains sequence number status for one RAB in RNC, which corresponds to one PDP context in CN. The RAB contexts are transferred between the RNCs via the SGSNs at inter SGSN hard handover.

NSAPI identifies the PDP context and the associated RAB for which the RAB context IE is intended.

DL GTP-U Sequence Number is the number for the next downlink GTP-U T-PDU to be sent to the MS.

UL GTP-U Sequence Number is the number for the next uplink GTP-U T-PDU to be tunnelled to the GGSN.

DL PDCP Sequence Number is the number for the next downlink PDCP-PDU to be sent to the MS.

UL PDCP Sequence Number is the number for the next uplink PDCP-PDU to be received from the MS.

1	Type = 22 (Decimal)
2	Spare (0 0 0 0) | NSAPI
3-4	DL GTP-U Sequence Number
5-6	UL GTP-U Sequence Number
7	DL PDCP Sequence Number
8	UL PDCP Sequence Number

Figure 27: RAB Context Information Element

7.7.20 Radio Priority SMS

The Radio Priority SMS information element contains the radio priority level for MO SMS transmission.

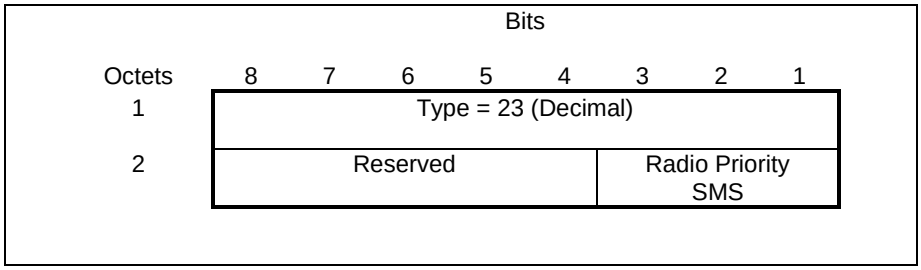


Figure 28: Radio Priority SMS Information Element

7.7.21 Radio Priority

The Radio Priority information element contains the radio priority level that the MS uses when accessing the network for the transmission of uplink user data for a PDP context as identified by NSAPI.

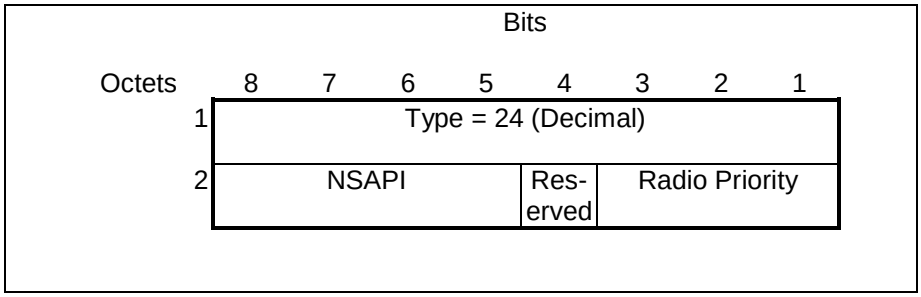


Figure 29: Radio Priority Information Element

7.7.22 Packet Flow Id

The Packet Flow Id information element contains the packet flow identifier assigned to a PDP context as identified by NSAPI.

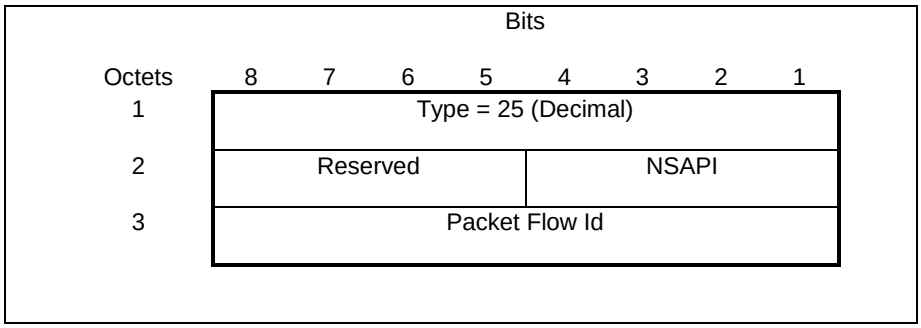


Figure 30: Packet Flow Id Information Element

7.7.23 Charging Characteristics

The charging characteristics information element is a way of informing both the SGSN and GGSN of the rules for producing charging information based on operator configured triggers. For the encoding of this information element see TS 3G 32.015.

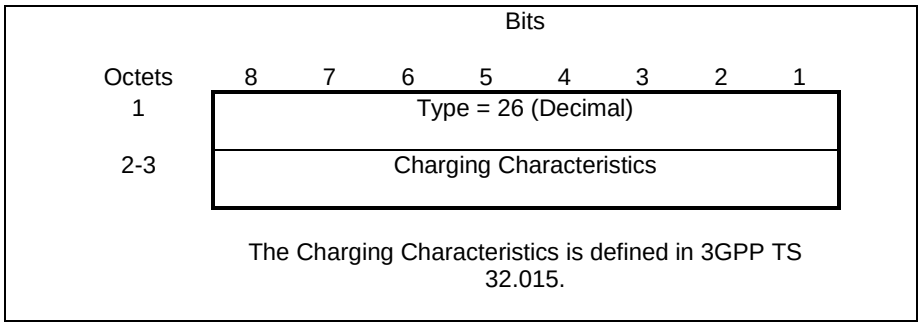


Figure 31: Charging Characteristics Information Element

7.7.24 Trace Reference

The Trace Reference information element identifies a record or a collection of records for a particular trace. The Trace Reference is allocated by the triggering entity.

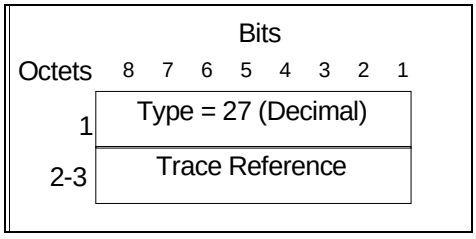


Figure 32: Trace Reference Information Element

7.7.25 Trace Type

The Trace Type information element indicates the type of the trace.

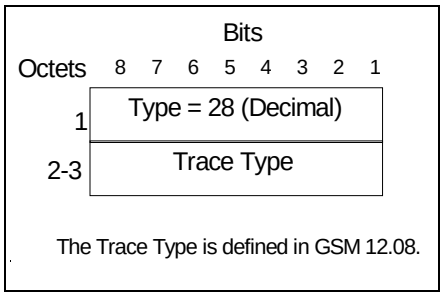


Figure 33: Trace Type Information Element

The Trace Type value 0 (Decimal) and the Trace Type value which is not understood by the receiver shall be treated as a basic trace type.

7.7.25A MS Not Reachable Reason

The MS Not Reachable Reason indicates the reason for the setting of the MNRG flag.

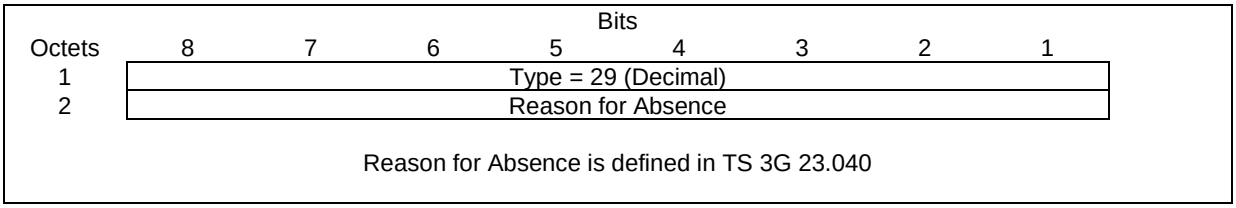


Figure 33A: MS Not Reachable Reason Information Element

7.7.26 Charging ID

The Charging ID is a unique four-octet value generated by the GGSN when a PDP context is activated. A Charging ID is generated for each activated context. The Charging ID value 0 is reserved and shall not be assigned by the GGSN.

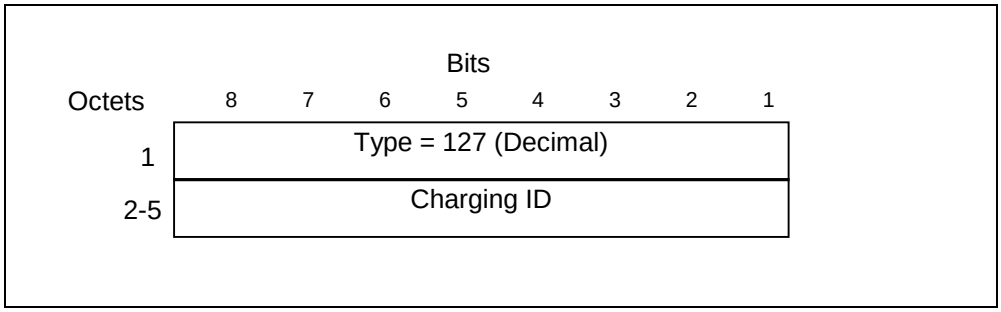


Figure 34: Charging ID Information Element

7.7.27 End User Address

The purpose of the End User Address information element shall be to supply protocol specific information of the external packet data network accessed by the GPRS subscriber.

The Length field value shall be 2 in an End User Address information element with an empty PDP Address.

The PDP Type defines the end user protocol to be used between the external packet data network and the MS and is divided into an Organisation field and a Number field.

The PDP Type Organisation is the organisation that is responsible for the PDP Type Number field and the PDP Address format.

For PPP the PDP Type Organisation is ETSI and the PDP Type Number is 1 and there shall be no address in the End User Address IE. In this case the address is negotiated later as part of the PPP protocol.

If the PDP Type Organisation is IETF, the PDP Type Number is a compressed number (i.e. the most significant HEX(00) is skipped) in the "Assigned PPP DLL Protocol Numbers" list in the most recent "Assigned Numbers" RFC (RFC 1700 or later). The most recent "Assigned PPP DLL Protocol Numbers" can also be found using the URL = ftp://ftp.isi.edu/in-notes/iana/assignments/ppp-numbers.

The PDP Address shall be the address that this PDP context of the MS is identified with from the external packet data network.

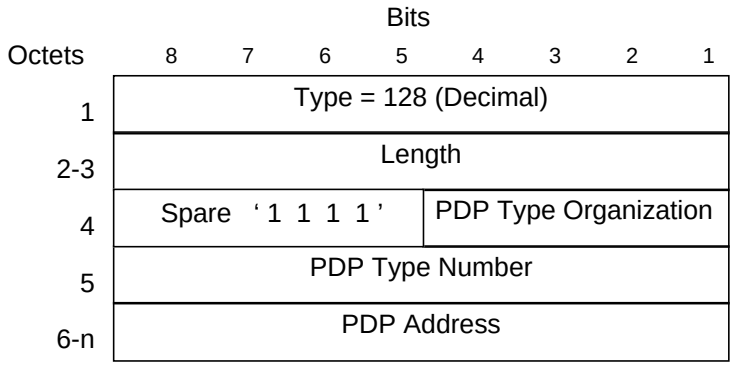


Figure 35: End User Address Information Element

Table 44: PDP Type Organisation Values

PDP Type Organisation	Value (Decimal)
ETSI	0
IETF	1
All other values are reserved	

Table 45: ETSI defined PDP Type Values

PDP Type Number	Value (Decimal)
PPP	1
All other values are reserved	

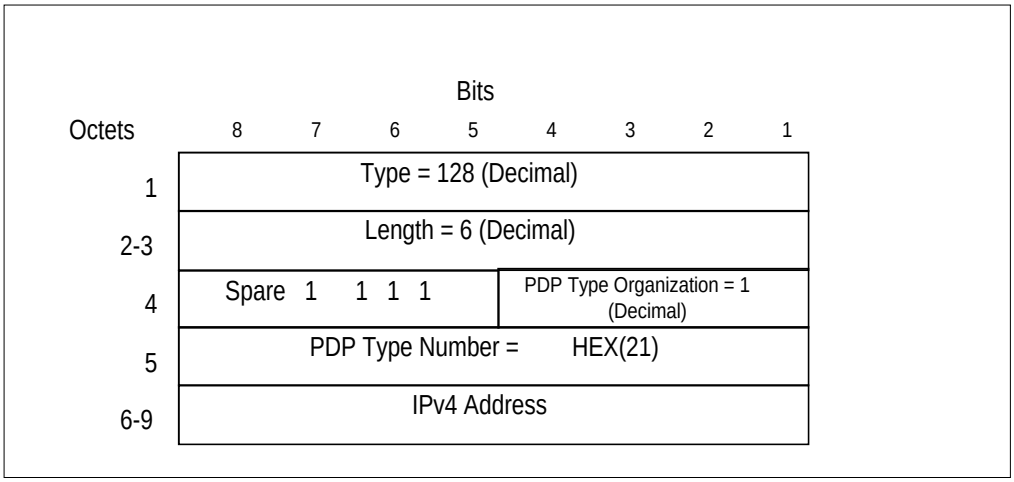


Figure 36: End User Address Information Element for IPv4

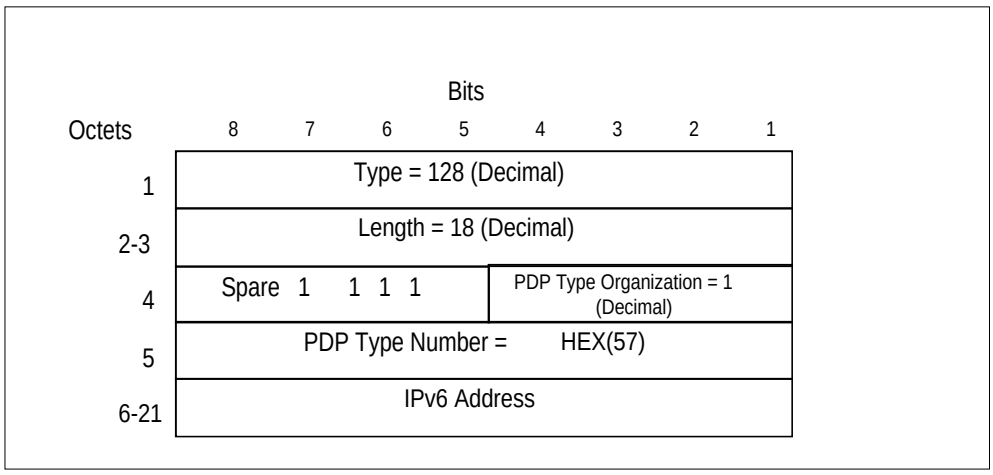


Figure 37: End User Address Information Element for IPv6

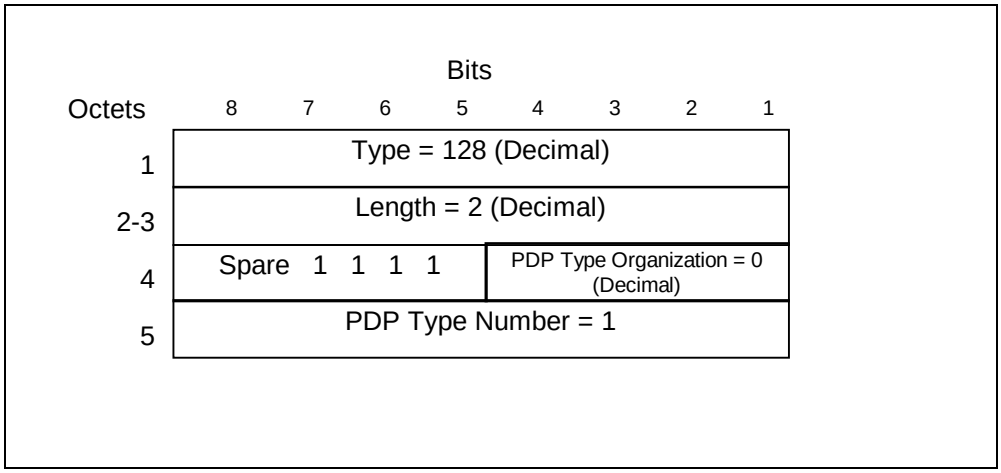


Figure 38: End User Address Information Element for PPP

7.7.28 MM Context

The MM Context information element contains the Mobility Management, MS and security parameters that are necessary to transfer between SGSNs at the Inter SGSN Routeing Area Update procedure.

Security Mode indicates the type of security keys (GSM/UMTS) and Authentication Vectors (quintuplets/triplets) that are passed to the new SGSN.

Ciphering Key Sequence Number (CKSN) is described in 3GPP TS 24.008. Possible values are integers in the range [0; 6]. The value 7 is reserved. CKSN identifies Kc. During the Intersystem Change to 3G-SGSN, the KSI shall be assigned the value of CKSN.

Key Set Identifier (KSI) identifies CK and IK. During the Intersystem Change to 2G-SGSN, the CKSN shall be assigned the value of KSI.

Used Cipher indicates the GSM ciphering algorithm that is in use.

Kc is the GSM ciphering key currently used by the old SGSN. Kc shall be present if GSM key is indicated in the Security Mode.

CK is the UMTS ciphering key currently used by the old SGSN. CK shall be present if UMTS keys are indicated in the Security Mode.

IK is the UMTS integrity key currently used by the old SGSN. IK shall be present if UMTS keys are indicated in the Security Mode.

The Triplet array contains triplets encoded as the value in the Authentication Triplet information element The Triplet array shall be present if indicated in the Security Mode.

The Quintuplet array contains Quintuplets encoded as the value in the Authentication Quintuplet information element. The Quintuplet shall be present if indicated in the Security Mode.

DRX parameter indicates whether the MS uses DRX mode or not.

MS Network Capability provides the network with information concerning aspects of the MS related to GPRS. MS Network Capability and MS Network Capability Length are coded as in the value part described in 3GPP TS 24.008.

DRX parameter is coded as described in 3GPP TS 24.008, the value part only.

The two octets Container Length holds the length of the Container, excluding the Container Length octets.

Container contains one or several optional information elements as described in the sub-clause ‘Overview’, from the clause ‘General message format and information elements coding’ in 3GPP TS 24.008.

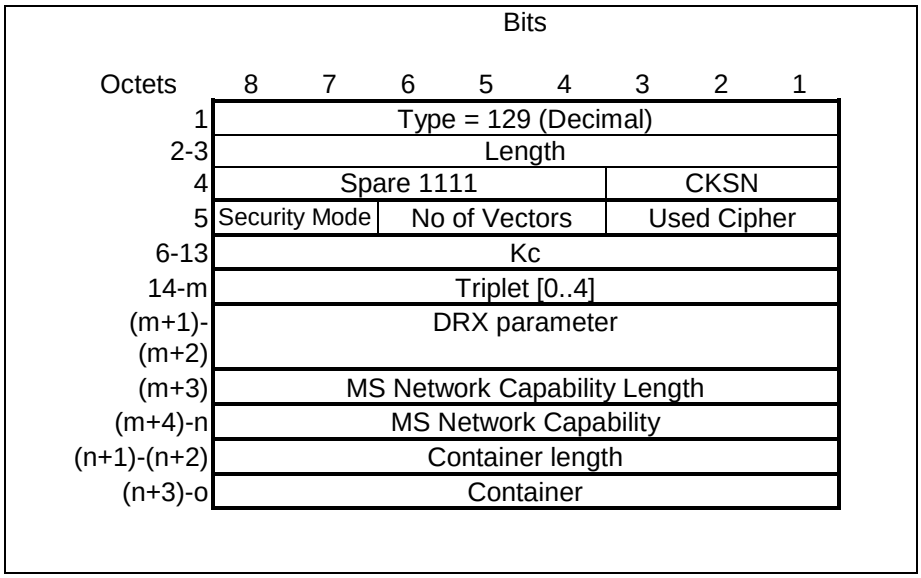


Figure 40: MM Context Information Element with GSM Key and Triplets

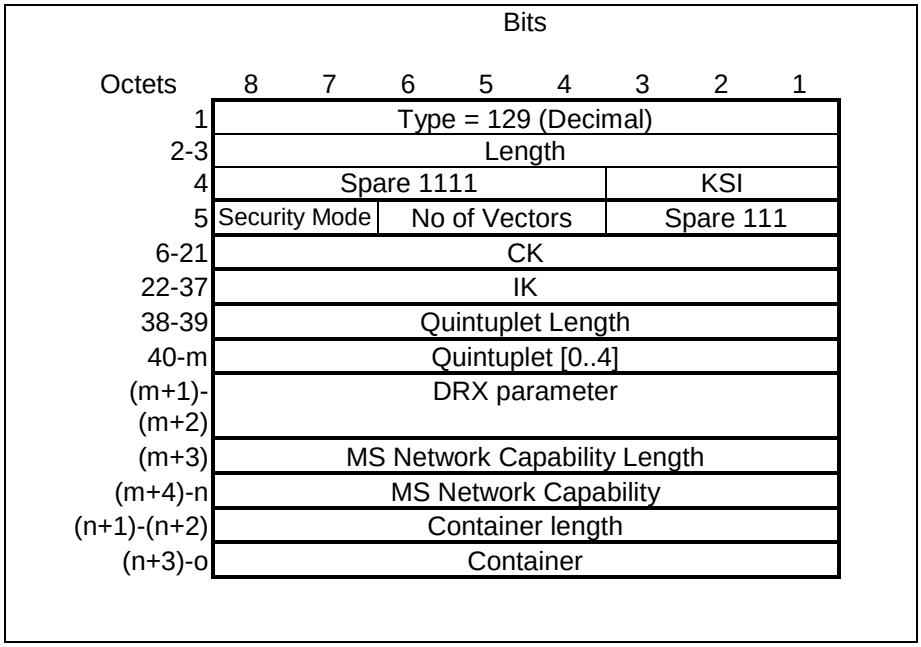
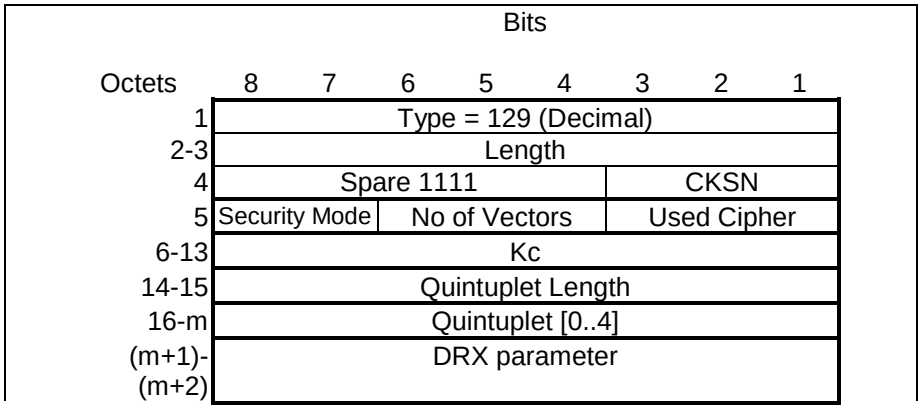


Figure 41: MM Context Information Element with UMTS Keys and Quintuplets



(m+3)	MS Network Capability Length
(m+4)-n	MS Network Capability
n+1-n+2	Container length
n+3-o	Container

Figure 42: MM Context Information Element with GSM Keys and UMTS Quintuplets

Bits

Octets	8	7	6	5	4	3	2	1
1	Type = 129 (Decimal)							
2-3	Length							
4	Spare 1111					CKSN/KSI		
5	Security Mode		No of Vectors			Used Cipher		
6-21	CK							
22-37	IK							
38-39	Quintuplet Length							
40-m	Quintuplet [0..4]							
(m+1)-(m+2)	DRX parameter							
(m+3)	MS Network Capability length							
(m+4)-n	MS Network Capability							
(n+1)-(n+2)	Container length							
(n+3)-n	Container							

Figure 42A: MM Context Information Element with Used Cipher value, UMTS Keys and Quintuplets

Table 46: Used Cipher Values

Cipher Algorithm	Value (Decimal)
No ciphering	0
GEA/1	1
GEA/2	2
GEA/3	3
GEA/4	4
GEA/5	5
GEA/6	6
GEA/7	7

Table 47: Security Mode Values

Security Type	Value (Decimal)
GSM key and triplets	1
GSM key and quintuplets	3
UMTS key and quintuplets	2
Used cipher value, UMTS Keys and Quintuplets	0

7.7.29 PDP Context

The PDP Context information element contains the Session Management parameters, defined for an external packet data network address, that are necessary to transfer between SGSNs at the Inter SGSN Routeing Area Update procedure.

NSAPI is an integer value in the range [0; 15].

The NSAPI points out the affected PDP context.

The SAPI indicates the LLC SAPI that is associated with the NSAPI.

The Transaction Identifier is the 4 or 12 bit Transaction Identifier used in the 3GPP TS 24.008 Session Management messages which control this PDP Context. If the length of the Transaction Identifier is 4 bit, the second octet shall be set to all zeros. The encoding is defined in 3GPP TS 24.007. The latest Transaction Identifier sent from SGSN to MS is stored in the PDP context IE.

Reordering Required (Order) indicates whether the SGSN shall reorder T-PDUs before delivering the T-PDUs to the MS. When the Quality of Service Negotiated (QoS Neg) is Release 99, the Reordering Required (Order) shall be ignored by receiving entity.

The VPLMN Address Allowed (VAA) indicates whether the MS is allowed to use the APN in the domain of the HPLMN only or additionally the APN in the domain of the VPLMN.

The QoS Sub Length, QoS Req Length and QoS Neg Length represent respectively the lengths of the QoS Sub, QoS Req and QoS Neg fields, excluding the QoS Length octet.

The Quality of Service Subscribed (QoS Sub), Quality of Service Requested (QoS Req) and Quality of Service Negotiated (QoS Neg) are encoded as described in section ‘Quality of Service (QoS) Profile’. Their minimum length is 4 octets; their maximum length may be 255 octets.

The Sequence Number Down is the number of the next T-PDU that shall be sent from the new SGSN to the MS. The number is associated to the Sequence Number from the GTP Header of an encapsulated T-PDU.

The Sequence Number Up is the number that new SGSN shall use as the Sequence Number in the GTP Header for the next encapsulated T-PDU from the MS to the GGSN.

The Send N-PDU Number is used only when acknowledged peer-to-peer LLC operation is used for the PDP context. Send N-PDU Number is the N-PDU number to be assigned by SNDCP to the next down link N-PDU received from the GGSN. It shall be set to 255 if unacknowledged peer-to-peer LLC operation is used for the PDP context.

The Receive N-PDU Number is used only when acknowledged peer-to-peer LLC operation is used for the PDP context. The Receive N-PDU Number is the N-PDU number expected by SNDCP from the next up link N-PDU to be received from the MS. It shall be set to 255 if unacknowledged peer-to-peer LLC operation is used for the PDP context.

The Uplink Tunnel Endpoint Identifier Control Plane is the Tunnel Endpoint Identifier used between the old SGSN and the GGSN in up link direction for control plane purpose. It shall be used by the new SGSN within the GTP header of the Update PDP Context Request message.

The GGSN Address for User Traffic and the UplinkTunnel Endpoint Identifier Data I are the GGSN address and the Tunnel Endpoint Identifier used between the old SGSN and the GGSN in uplink direction for user plane traffic on a PDP context. They shall be used by the new SGSN to send uplink user plane PDU to the GGSN

The PDP Context Identifier is used to identify a PDP context for the subscriber.

The PDP Type Organisation and PDP Type Number are encoded as in the End User Address information element.

The PDP Address Length represents the length of the PDP Address field, excluding the PDP Address Length octet.

The PDP Address is an octet array with a format dependent on the PDP Type. The PDP Address is encoded as in the End User Address information element if the PDP Type is IPv4 or IPv6.

The GGSN Address Length represents the length of the GGSN Address field, excluding the GGSN Address Length octet.

The old SGSN includes the GGSN Address for control plane that it has received from GGSN at PDP context activation or update.

The APN is the Access Point Name in use in the old SGSN. I.e. the APN sent in the Create PDP Context request message.

The spare bits x indicate unused bits that shall be set to 0 by the sending side and which shall not be evaluated by the receiving side.

1	Type = 130 (Decimal)				
2-3	Length				
4	Res-erved	VAA	Res-erved	Order	NSAPI
5	X	X	X	X	SAPI
6	QoS Sub Length				
7 - (q+6)	QoS Sub [4..255]				
q+7	QoS Req Length				
(q+8)-(2q+7)	QoS Req [4..255]				
2q+8	QoS Neg. Length				
(2q+9)-(3q+8)	QoS Neg [4..255]				
(3q+9)-(3q+10)	Sequence Number Down (SND) 1)				
(3q+11)-(3q+12)	Sequence Number Up (SNU) 1)				
3q+13	Send N-PDU Number 1)				
3q+14	Receive N-PDU Number 1)				
(3q+15)-(3q+18)	Uplink Tunnel Endpoint Identifier Control Plane				
(3q+19)-(3q+22)	UplinkTunnel Endpoint Identifier Data I				
3q+23	PDP Context Identifier				
3q+24	Spare 1 1 1 1				PDP Type Organisation
3q+25	PDP Type Number				
3q+26	PDP Address Length				
(3q+27)-m	PDP Address [1..63]				
m+1	GGSN Address for control plane Length				
(m+2)-n	GGSN Address for control plane [4..16]				
n+1	GGSN Address for User Traffic Length				
(n+2)-o	GGSN Address for User Traffic [4..16]				
o+1	APN length				
(o+2)-p	APN				
p+1	Spare (sent as 0 0 0 0)				Transaction Identifier
p+2	Transaction Identifier				

Figure 43: PDP Context Information Element

1) This field shall not be evaluated when the PDP context is received during UMTS intra system handover/relocation.

Table 48: Reordering Required Values

Reordering Required	Value (Decimal)
No	0
Yes	1

Table 49: VPLMN Address Allowed Values

VPLMN Address Allowed	Value (Decimal)
No	0
Yes	1

7.7.30 Access Point Name

The Access Point Name is sent from the GGSN in the Network-requested PDP Context Activation procedure that is used to identify the access point of the packet data network that wishes to connect to the MS.

The Access Point Name is information from the MS or SGSN that may be used by the GGSN to differentiate between accesses to different external packet data networks using the same PDP Type.

The Access Point Name contains a logical name that is the APN Network Identifier (see 3GPP TS 23.060). It is coded as in the value part defined in 3GPP TS 24.008 (i.e. the 3GPP TS 24.008 IEI and 3GPP TS 24.008 octet length indicator are not included).

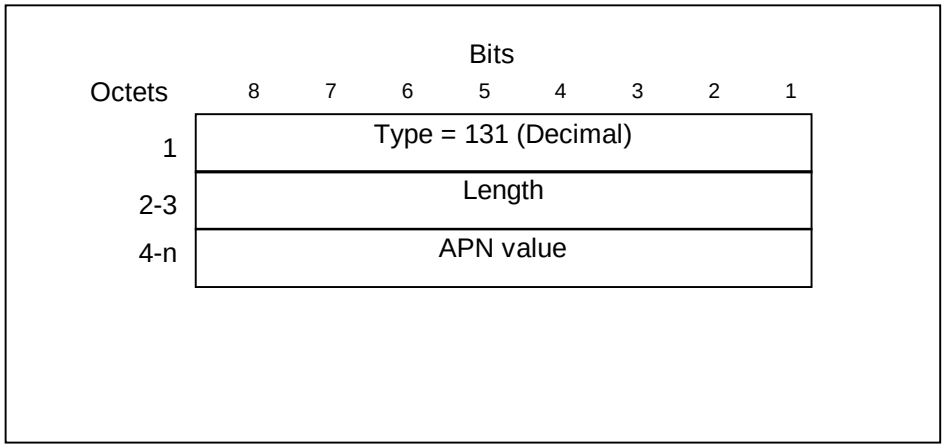


Figure 44: Access Point Name Information Element

7.7.31 Protocol Configuration Options

The Protocol Configuration Options contains external network protocol options that may be necessary to transfer between the GGSN and the MS. The content and the coding of the Protocol Configuration are defined in octet 3-z of the Protocol Configuration Options in3GPP TS 24.008.

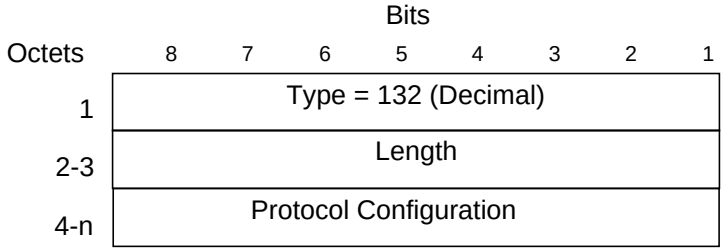


Figure 45: Protocol Configuration Options Information Element

7.7.32 GSN Address

The GSN Address information element contains the address of a GSN as defined in 3GPP TS 23.003. The Address Type and Address Length fields from 23.003 are not included in the GSN Address field.

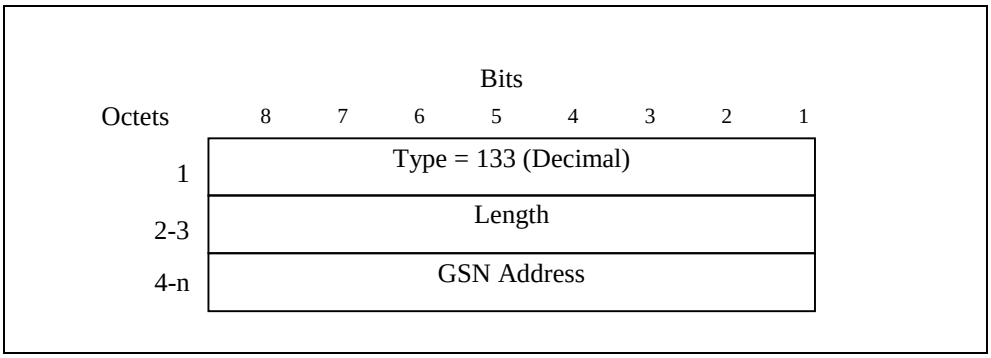


Figure 46: GSN Address Information Element

7.7.33 MS International PSTN/ISDN Number (MSISDN)

The MS international ISDN numbers are allocated from the CCITT Recommendation E.164 numbering plan, see 3GPP TS 23.003. The MSISDN is coded according to the contents of ISDN-AddressString data type defined in 3GPP TS 29.002. The MSISDN shall be in international format and the “nature of address indicator” shall indicate “international number”.

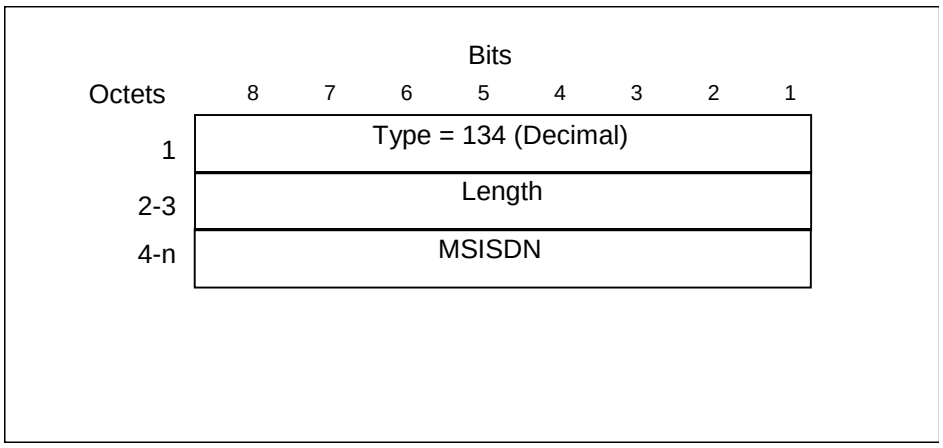


Figure 47: MSISDN Information Element

7.7.34 Quality of Service (QoS) Profile

The Quality of Service (QoS) Profile shall include the values of the defined QoS parameters. Octet 4 carries the allocation/retention priority octet that is defined in 3GPP TS 23.107. The allocation/retention priority octet encodes each priority level defined in 23.107 as the binary value of the priority level. Octets 5 – n are coded according to 3GPP TS 24.008 Quality of Service IE, octets 3 - 13. If a pre-Release '99 only capable terminal is served, octets 5 - n are coded according to GSM 04.08 Quality of Service IE, octets 3 - 5. The minimum length of the field QoS Profile Data is 3 octets; the maximum length may be up to 254 octets.

The allocation/retention priority shall be ignored if the QoS profile is pre-Release '99 or the QoS profile is present in Quality of Service Requested (QoS Req) of the PDP context. A receiving end shall interpret the QoS profile Data field to be coded according to GSM 04.08 (i.e. according to the pre-Release '99 format) if the Length field value is 4.

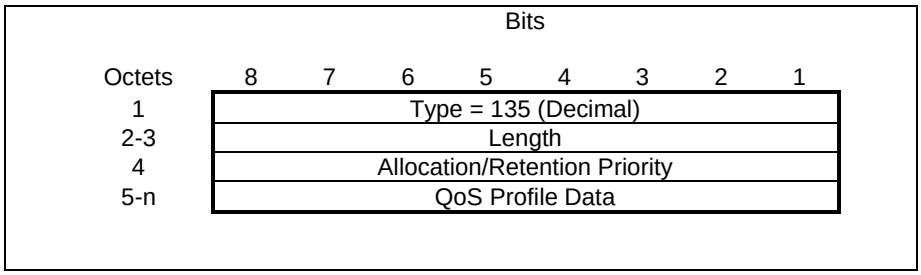


Figure 48: Quality of Service (QoS) Profile Information Element

7.7.35 Authentication Quintuplet

An Authentication Quintuplet consists of a Random challenge (RAND), an Expected user response (XRES), a Cipher key (CK), an Integrity key (IK), an Authentication token (AUTN) (see 3GPP TS 33.102).

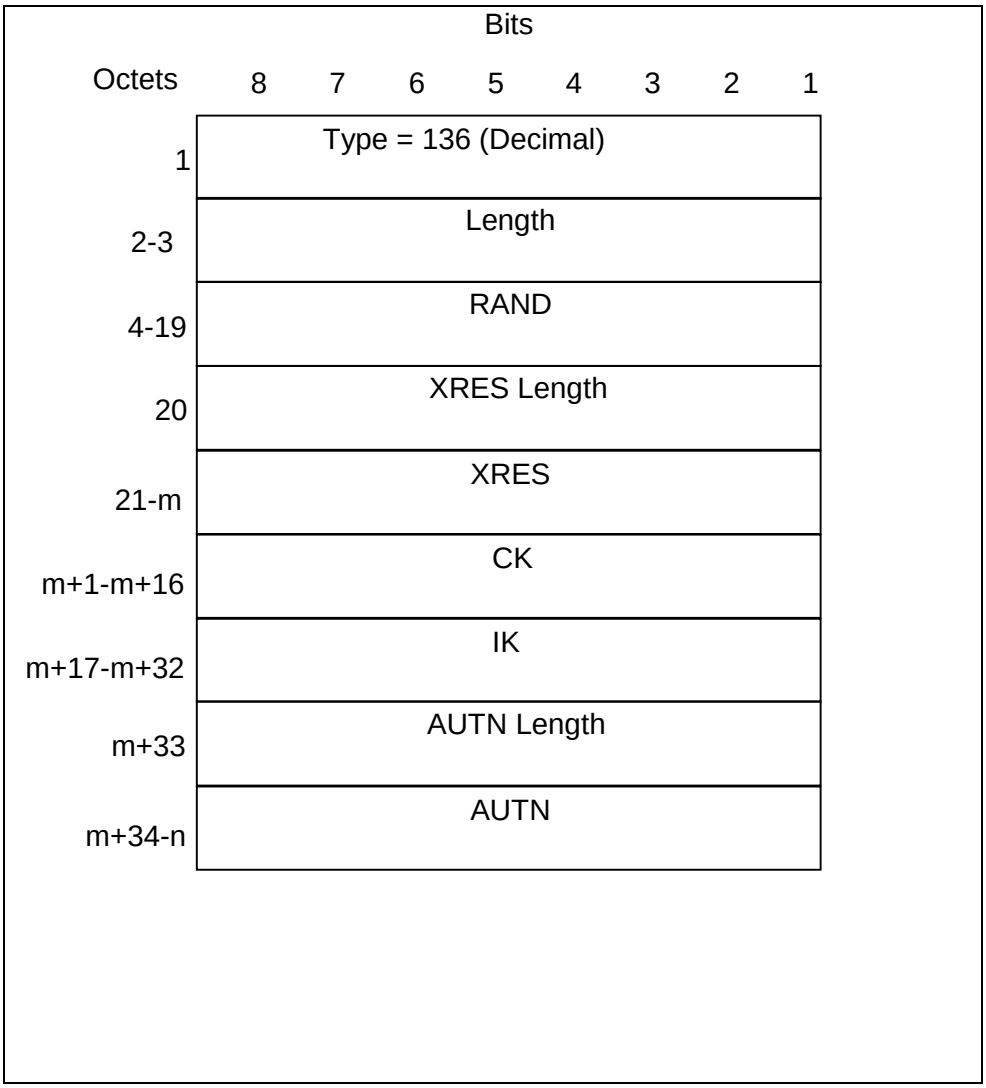


Figure 49: Authentication Quintuplet Information Element

7.7.36 Traffic Flow Template (TFT)

The Traffic Flow Template (TFT) is used to distinguish between different user traffic flows.

The content and the coding of the TFT are defined in 3GPP TS 24.008.

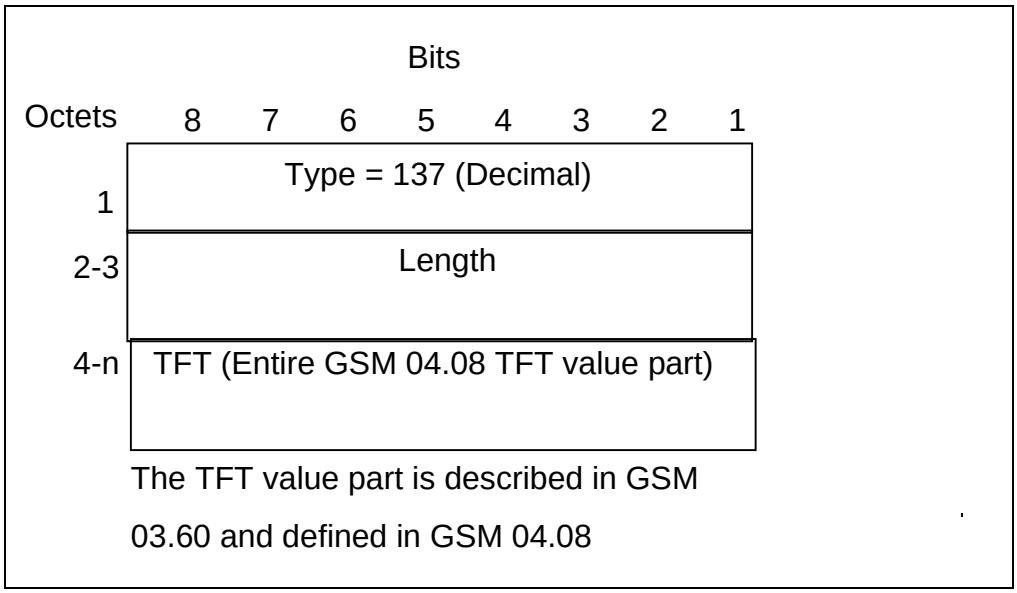


Figure 50: Traffic Flow Template Information Element

7.7.37 Target Identification

The Target Identification information element contains the identification of a target RNC as defined in 3GPP TS 25.413.

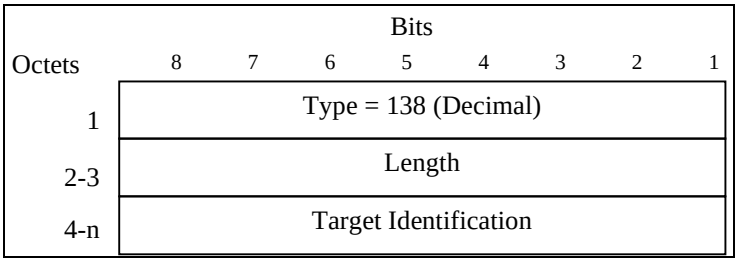


Figure 51: Target Identification Information Element

7.7.38 UTRAN Transparent Container

The UTRAN transparent container information element contains the radio-related information. The contents of this information element are only used by RNC so that GSN does not refer the contents.

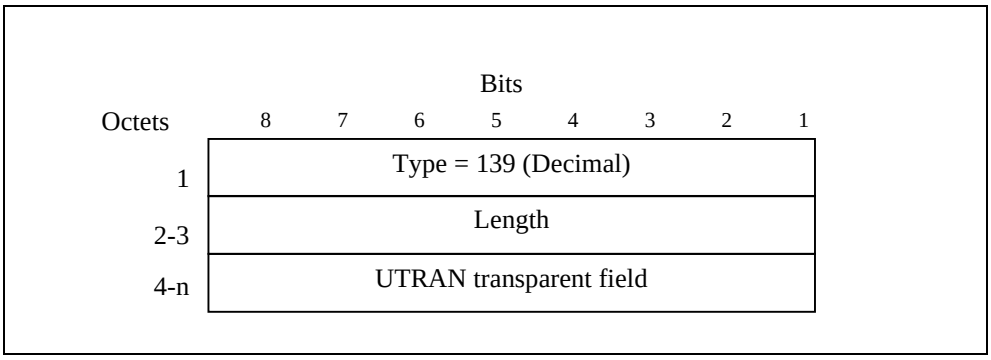


Figure 52: UTRAN Transparent Container Information Element

7.7.39 RAB Setup Information

If the target RNC successfully allocated resources associated with the NSAPI, the RAB Setup Information IE contains the RNC Tunnel Endpoint Identifier and RNC IP address for data forwarding from source RNC to target RNC. If the target RNC or the new SGSN failed to allocate resources the RAB Setup Information IE contains only Length and NSAPI indicating that the source RNC shall release the resources associated with the NSAPI.

The spare bits x indicate unused bits, which shall be set to 0 by the sending side and which shall not be evaluated by the receiving side.

The format of the RNC IP address is the same as the GSN address as defined in 3GPP TS 23.003. The Address Type and Address Length fields from 3GPP TS 23.003 are not included in the RNC IP Address field.

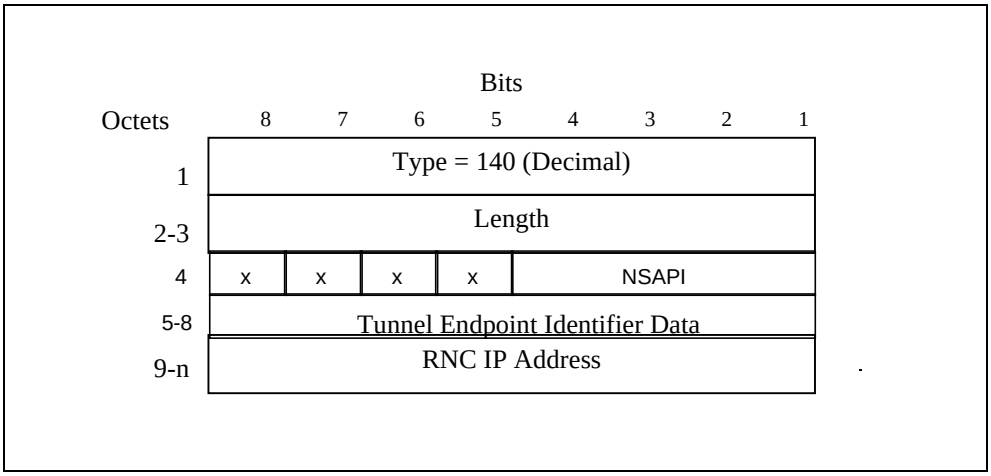


Figure 53: RAB Setup Information IE for data forwarding

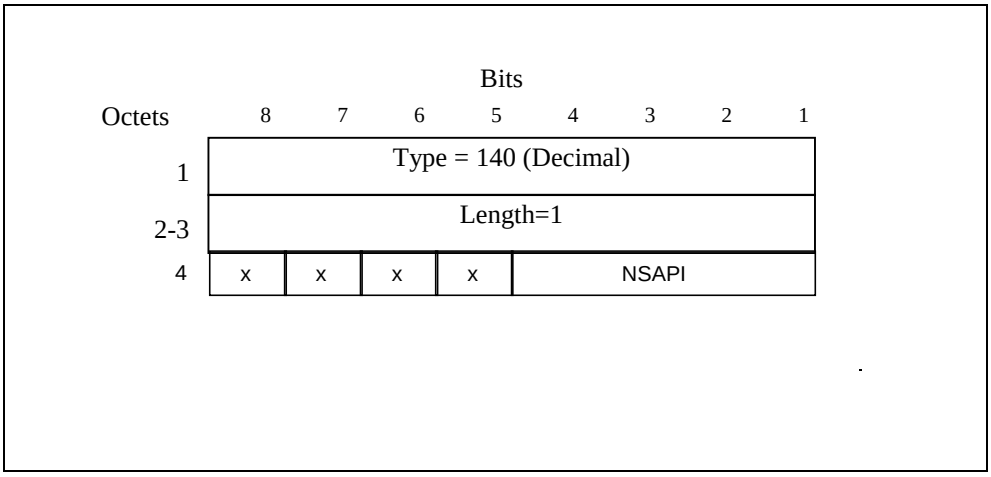


Figure 54: RAB Setup Information IE for release of resources

7.7.40 Extension Header Type List

This information element contains a list of 'n' Extension Header Types. The length field is set to the number of extension header types included.

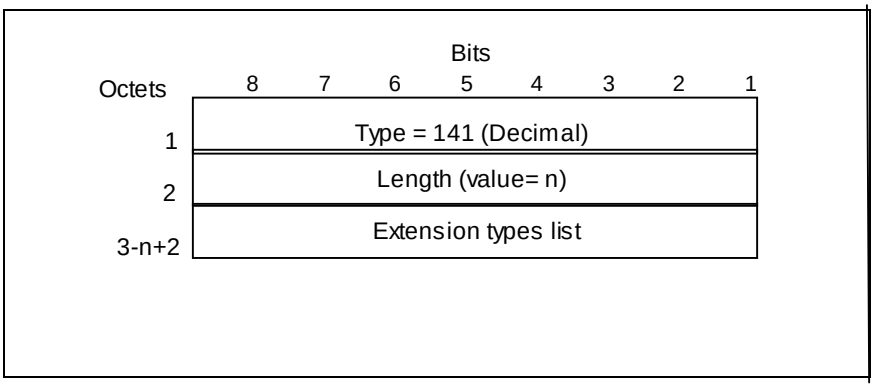


Figure 55: Extension Header Type List Information Element

7.7.41 Trigger Id

The Trigger Id information element identifies the entity that triggered the trace.

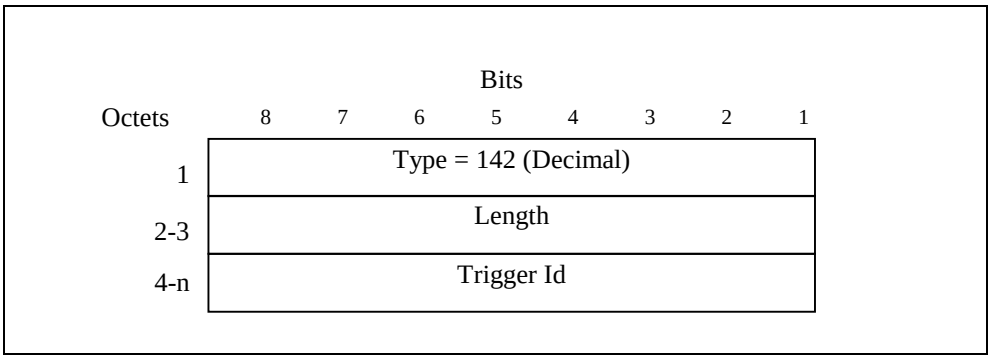


Figure 56: Trigger Id Information Element

7.7.42 OMC Identity

The OMC Identity information element identifies the OMC that shall receive the trace record(s).

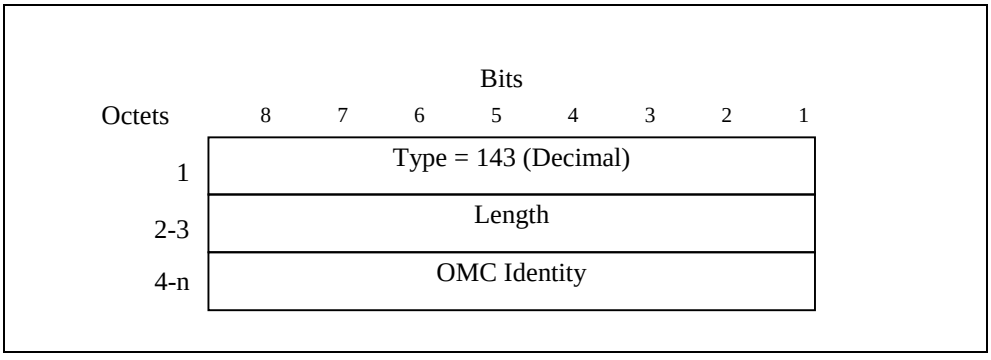


Figure 57: OMC Identity Information Element

7.7.43 Charging Gateway Address

The Charging Gateway Address information element contains an Ipv4 or Ipv6 address of a Charging Gateway.

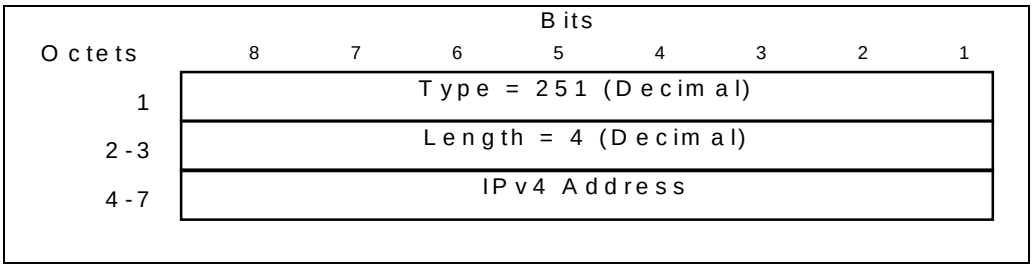


Figure 58a: Ipv4 Charging Gateway Address Information Element

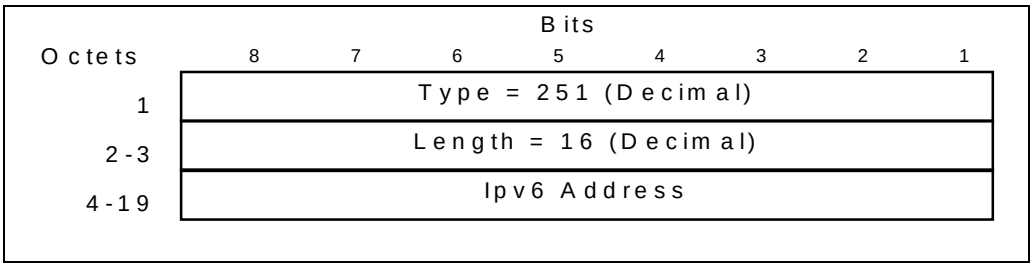


Figure 58b: Ipv6 Charging Gateway Address Information Element

7.7.44 Private Extension

The Private Extension information element contains vendor specific information. The Extension Identifier is a value defined in the Private Enterprise number list in the most recent "Assigned Numbers" RFC (RFC 1700 or later).

This is an optional information element that may be included in any GTP Signalling message. A signalling message may include more than one information element of the Private Extension type.

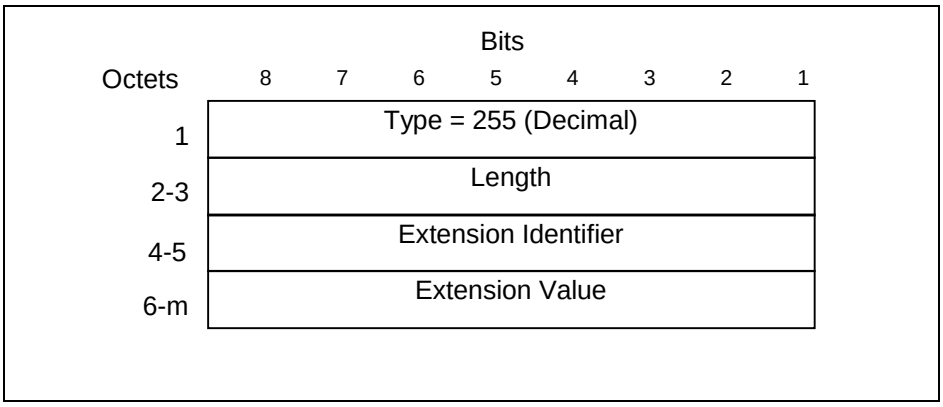


Figure 59: Private Extension Information Element

8 Control Plane (GTP-C)

The control plane in this case relates to GPRS Mobility Management functions like for example GPRS Attach, GPRS Routeing Area Update and Activation of PDP Contexts. The GPRS Tunnelling Protocol-Control plane (GTP-C) shall perform the control plane signalling between GSN nodes.

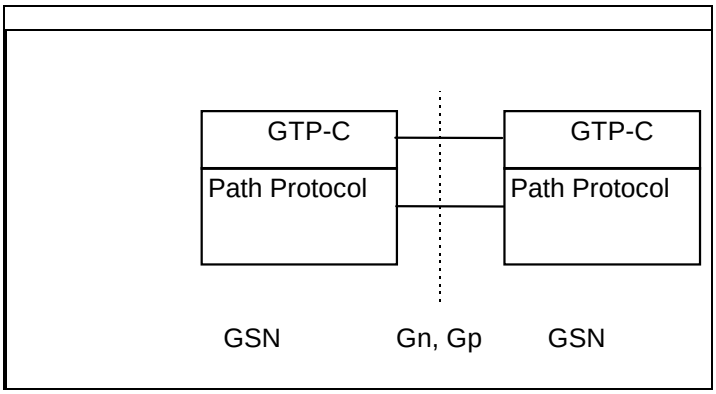


Figure 60: Signalling Plane - Protocol Stack

8.1 Control Plane Protocol

The GTP-C control plane flow shall be logically associated with, but separate from, the GTP-U tunnels. For each GSN-GSN pair one or more paths exist. One or more tunnels may use each path. GTP-C shall be the means by which tunnels are established, used, managed and released. A path may be maintained by keep-alive echo messages. This ensures that a connectivity failure between GSNs can be detected in a timely manner.

8.2 Usage of the GTP-C Header

For control plane messages the GTP header shall be used as follows:

- Version shall be set to decimal 1 (‘001’).
- Protocol Type (PT) shall be set to ‘1’.
- (S) shall be set to ‘1’.
- PN shall be set to ‘0’. A GTP-C receiver shall ignore this flag.
- Message Type shall be set to the unique value that is used for each type of control plane message. Valid message types are marked with an x in the GTP-C column in Table 1.
- Length shall be the length in octets of the payload, i.e. the rest of the packet following the mandatory part of the GTP header (that is the first 8 octets). The Sequence Number, the N-PDU Number or any Extension headers shall be considered to be part of the payload, i.e. included in the length count.
- The Tunnel Endpoint Identifier is set by the sending entity to the value requested by the corresponding entity (SGSN or GGSN); it identifies all the PDP Contexts with the same PDP address and APN (for Tunnel Management messages) or it identifies each MS and its associated context data(for messages not related to Tunnel Management), except for the following cases:
  - The Create PDP Context Request message for a given MS sent to a specific GGSN shall have the Tunnel Endpoint Identifier set to all zeros, if the SGSN has not been assigned a Tunnel Endpoint Identifier Control Plane by the GGSN.
  - The Update PDP Context Request message for a given MS sent to a specific GGSN shall have the Tunnel Endpoint Identifier set to all zeros, if it is used to switch the GTP version of the tunnel to the GGSN from GTP v0 to GTP v1.
  - The Identification Request/Response messages, where the Tunnel Endpoint Identifier shall be set to all zeros.
  - The SGSN Context Request message, where the Tunnel Endpoint Identifier shall be set to all zeros.
  - The Echo Request/Response, Supported Extension Headers notification and the Version Not Supported messages, where the Tunnel Endpoint Identifier shall be set to all zeros.

- The Forward Relocation Request message, where the Tunnel Endpoint Identifier shall be set to all zeros.
- The PDU Notification Request message, where the Tunnel Endpoint Identifier shall be set to all zeros.
-
- The Relocation Cancel Request message where the Tunnel Endpoint Identifier shall be set to all zeros, except for the case where the old SGSN has already been assigned the Tunnel Endpoint Identifier Control Plane of the new SGSN.
- All Location Management messages, where the Tunnel Endpoint Identifier shall be set to all zeros.

The GSN Address for Control Plane set in the request message could be different from the IP Source address of the message. The Tunnel Endpoint Identifier notified in the request message is also used in this case for sending the corresponding response message.

- Sequence Number shall be a message number valid for a path. Within a given set of contiguous Sequence Numbers from 0 to 65535, a given Sequence Number shall, if used, unambiguously define a GTP control plane request message sent on the path (see section Reliable delivery of signalling messages). The Sequence Number in a control plane response message shall be copied from the control plane request message that the GSN is replying to. For GTP-C messages not having a defined response message for a request message, i.e. for messages Version Not Supported and Supported Extension Headers Notification, the Sequence Number shall be ignored by the receiver.
- N-PDU Number shall not be interpreted.

The GTP-C header may be followed by subsequent information elements dependent on the type of control plane message. Only one information element of each type is allowed in a single control plane message, except for the Authentication Triplet, the PDP Context and the Tunnel Endpoint Identifier Data II information element where several occurrences of each type are allowed.

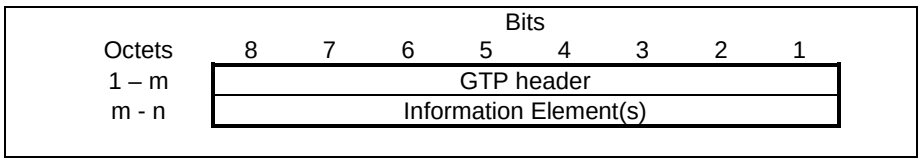


Figure 61: GTP Header followed by subsequent Information Elements

9 GTP-U

GTP-U Tunnels are used to carry encapsulated T-PDUs and signalling messages between a given pair of GTP-U Tunnel Endpoints. The Tunnel Endpoint ID (TEID) which is present in the GTP header shall indicate which tunnel a particular T-PDU belongs to. In this manner, packets are multiplexed and de-multiplexed by GTP-U between a given pair of Tunnel Endpoints. The TEID value to be used in the TEID field shall be negotiated for instance during the GTP-C Create PDP Context and the RAB assignment procedures that take place on the control plane.

The maximum size of a T-PDU that may be transmitted without fragmentation by GGSN or the MS is defined in UMTS 23.060. The GGSN shall fragment, reject or discard T-PDUs, depending on the PDP type and implementation decisions, directed to the MS if the T-PDU size exceeds the maximum size. The decision if the T-PDUs shall be fragmented or discarded is dependent on the external packet data network protocol.

9.1 GTP-U Protocol Entity

The GTP-U protocol entity provides packet transmission and reception services to user plane entities in the GGSN, in the SGSN and, in UMTS systems, in the RNC. The GTP-U protocol entity receives traffic from a number of GTP-U tunnel endpoints and transmits traffic to a number of GTP-U tunnel endpoints. There is a GTP-U protocol entity per IP address.

The TEID in the GTP-U header is used to de-multiplex traffic incoming from remote tunnel endpoints so that it is delivered to the User plane entities in a way that allows multiplexing of different users, different packet protocols and

different QoS levels. Therefore no two remote GTP-U endpoints shall send traffic to a GTP-U protocol entity using the same TEID value except for data forwarding as part of the SRNS relocation or Intersystem Change procedures.

9.1.1 Handling of Sequence Numbers

This functionality is provided only when the S bit is set to 1 in the GTP-U header.

The GTP-U protocol entity must reorder out of sequence T-PDUs when in sequence delivery is required. This is optional at the SGSN in UMTS. The GTP-U protocol entity shall deliver to the user plane entity only in sequence T-PDUs and notify the sequence number associated to each of them. The notification of the sequence number is not necessary at the GGSN, but it is mandatory at the SGSN and RNC. The user plane entity shall provide a sequence number to the GTP-U layer together with T-PDUs to be transmitted in sequence. GTP-U protocol entities at the GGSN may optionally generate autonomously the sequence number, but should be able to use sequence numbers provided by the user plane entity. The sequence number is handled on a per GTP-U Tunnel (that is TEID) basis.

When the sequence number is included in the GTP-U header, a user plane entity acting as a relay of T-PDUs between GTP-U protocol entities, or between PDCP (or SNDCP) protocol entities and GTP-U protocol entities, shall relay the sequence numbers between those entities as well. In this way it is possible to keep consistent values of sequence numbers from the GGSN to the UE (MS in GPRS) by relaying the sequence number across the CN GTP-U bearer, the Iu GTP-U bearer and the Radio bearer (via PDCP or SNDCP N-PDU numbers). This functionality is beneficial during SRNS relocation.

For GTP-U signalling messages having a response message defined for a request message, Sequence Number shall be a message number valid for a path. Within a given set of continuous Sequence Numbers from 0 to 65535, a given Sequence Number shall, if used, unambiguously define a GTP-U signalling request message sent on the path (see section Reliable delivery of signalling messages). The Sequence Number in a signalling response message shall be copied from the signalling request message that the GSN or RNC is replying to. For GTP-U messages not having a defined response message for a request message, i.e. for messages Supported Extension Headers Notification and Error Indication, the Sequence Number shall be ignored by the receiver.

9.2 GTP-U Service Access Points and Primitives

The GTP-U protocol entity offers packet Transmission services between a pair of GTP-U tunnel endpoints. The tunnel between two GTP-U endpoints is established via control plane procedures defined in protocols such as GTP-C and RANAP. The control of GTP-U resource allocation and tunnel set-up takes place via the GTP-U-CONTROL SAP. The GTP-U packet transmission (and packet reception) services are accessed via the GTP-U-UNIT-DATA SAP.

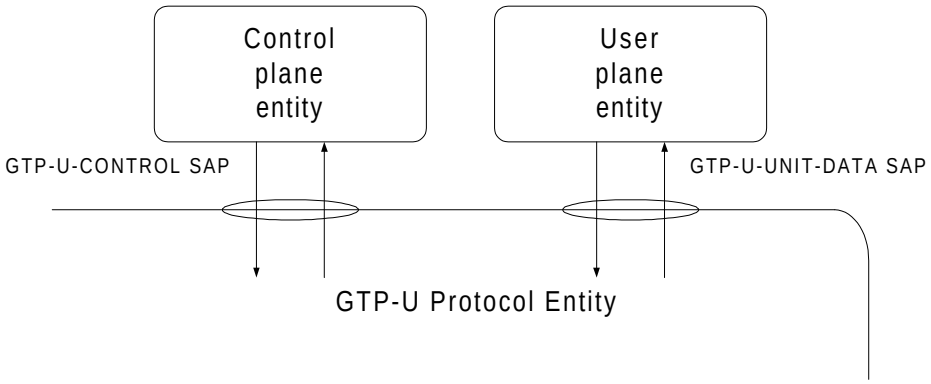


Figure 62: The GTP-U-Control SAP and GTP-U-DATA SAP

9.2.1 GTP-U-CONTROL SAP

The GTP-U-CONTROL SAP is used by a control plane entity to control the allocation of GTP-U resources and associate them to an identifier (the TEID) a user plane entity uses to access them via the GTP-U-UNIT-DATA SAP. It also defines in which way to control tunnel establishment. In particular, it provides means to control the GTP-U packet reception section and the GTP-U packet transmission section. The RX and TX suffix is used in the following to discriminate between primitives used to control the reception section and primitives used to control the transmission section.

9.2.1.1 GTP-U-CONTROL-RX primitives

PRIMITIVE	PARAMETERS	REFERENCE
GTP-U-CONTROL-RX-SETUP.request	QoS info; IP address; TEID	9.2.1.1.1
GTP-U-CONTROL-RX-SETUP.confirm	Result	9.2.1.1.2
GTP-U-CONTROL-RX-RELEASE.request	TEID	9.2.1.1.3
GTP-U-CONTROL-RX-RELEASE.confirm	-	9.2.1.1.4
GTP-U-CONTROL-RX-ERROR.indication	Cause	9.2.1.1.5

9.2.1.1.1 GTP-U-CONTROL-RX-SETUP.request

This primitive is used to allocate packet reception resources according to a QoS profile specified via the 'QoS' parameter. These resources are to be associated to a tunnel endpoint identified via the TEID specified in the 'TEID' parameter. In case this TEID is already being used, this shall be interpreted as a resource modification request.

The 'IP address' parameter is used to identify the IP address of the remote GTP-U protocol entity where the GTP-U tunnel is terminated. This implicitly identifies the path being used. The knowledge of the path being used is necessary in order to send ECHO messages used to detect path failure.

9.2.1.1.2 GTP-U-CONTROL-RX-SETUP.confirm

This primitive acknowledges the corresponding resources set up request. Any information to report is delivered in the parameter 'Result', which may be used to indicate set up failure and the reason of the failure.

9.2.1.1.3 GTP-U-CONTROL-RX-RELEASE.request

This primitive is used to dispose the resources associated to a tunnel identified by TEID.

9.2.1.1.4 GTP-U-CONTROL-RX-RELEASE.confirm

This primitive acknowledges the corresponding resources release request.

9.2.1.1.5 GTP-U-CONTROL-RX-ERROR.indication

This primitive is used to indicate to the controlling entity any error conditions detected on the GTP-U reception section. The error condition is specified in the parameter 'Cause'.

9.2.1.2 GTP-U-CONTROL-TX primitives

PRIMITIVE	PARAMETERS	REFERENCE
GTP-U-CONTROL-TX-SETUP.request	QoS info; IP address; TEID	9.2.1.2.1
GTP-U-CONTROL-TX-SETUP.confirm	Result	9.2.1.2.2
GTP-U-CONTROL-TX-RELEASE.request	TEID; IP address	9.2.1.2.3
GTP-U-CONTROL-TX-RELEASE.confirm	-	9.2.1.2.4
GTP-U-CONTROL-TX-ERROR.indication	Cause	9.2.1.2.5

9.2.1.2.1 GTP-U-CONTROL-TX-SETUP.request

This primitive is used to allocate packet transmission resources according to a QoS profile specified via the 'QoS' parameter. These resources are to be associated to a tunnel endpoint identified via the TEID specified in the 'TEID' parameter. In case this TEID is already being used, this shall be interpreted as a resource modification request.

The 'IP address' parameter is used to identify the IP address of the remote GTP-U protocol entity where the GTP-U tunnel is terminated. This implicitly identifies the path being used. The knowledge of the path being used is necessary in order to send ECHO messages to detect PATH failure.

9.2.1.2.2 GTP-U-CONTROL-TX-SETUP.confirm

This primitive acknowledges the corresponding resources set up request. Any information to report is delivered in the parameter 'Result', which maybe used to indicate set up failure and the reason of the failure.

9.2.1.2.3 GTP-U-CONTROL-TX-RELEASE.request

This primitive is used to dispose the resources associated to a tunnel identified by TEID and the IP address of the remote GTP-U protocol entity where the tunnel is terminated.

9.2.1.2.4 GTP-U-CONTROL-TX-RELEASE.confirm

This primitive acknowledges the corresponding resources release request.

9.2.1.2.5 GTP-U-CONTROL-TX-ERROR.indication

This primitive is used to indicate to the controlling entity any error conditions detected on the GTP-U Transmission section. The error condition is specified in the parameter 'Cause'.

9.2.2 GTP-U-UNIT-DATA SAP and Primitives

The GTP-U-UNIT-DATA SAP is used to send and receive T-PDUs in an unacknowledged mode. Sequence numbers and system dependent info is conditionally passed to the user plane entity using the GTP-U-. This information is identified as *'Other info'* in the following.

PRIMITIVE	PARAMETERS	REFERENCE
GTP-U-UNIT-DATA.request	DATA; TEID; IP address; *Other info**	9.2.2.1
GTP-U- UNIT-DATA.indication	DATA; TEID; *Other info**	9.2.2.2

NOTE *: It is conditionally present (only if the TEID is associated to tunnels providing in sequence delivery, see subclause 9.1.1).

9.2.2.1 GTP-U-UNIT-DATA.request

This primitive is used to send a T-PDU (DATA) by means of a specific GTP-U layer resource (tunnel) identified by the parameter TEID and the IP address where the tunnel is terminated. *Other info* may be conditionally present and transmitted together with T-PDUs.

9.2.2.2 GTP-U- UNIT-DATA.indication

A T-PDU (DATA) is received from a GPT-U peer entity and delivered to a user plane entity. The T-PDU is associated to the to the PDP or RNC context identified by TEID (that is the Tunnel Endpoint ID). *Other info* may be conditionally present and delivered together with T-PDUs.

9.3 Protocol Stack

The GTP-U protocol is used to transmit T-PDUs between GSN pairs (or between an SGSN and an RNC in UMTS), encapsulated in G-PDUs. A G-PDU is a packet including a GTP-U header and a T-PDU. The Path Protocol defines the path and the GTP-U header defines the tunnel. Several tunnels may be multiplexed on a single path. The frames have the following general structure:

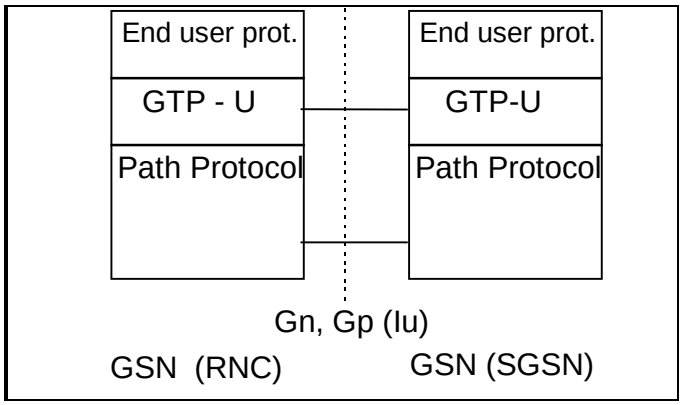


Figure 63: GTP-U - Protocol Stack (GTP-U over the Iu in brackets)

9.3.1 Usage of the GTP-U Header

The GTP-U header shall be used as follows:

- Version shall be set to decimal 1 (‘001’).
- Protocol Type (PT) shall be set to '1’.
- If the S field is set to '1' the sequence number field is present otherwise it is set to '0'.For GTP-U messages Echo Request, Echo Response and Supported Extension Headers Notification, the S field shall be set to ‘1’.
- PN flag: the GTP-U header includes the N-PDU Number field if the PN flag is set to 1.
- Message Type shall be set according to Table 1. The value 255 is used when T-PDUs are transmitted. The value 1 and 2 are used for "Echo" messages. The value 26 is used for “Error Indication” message. The value 31 is used for “Supported Extension Headers Notification” message.
- Length: This field indicates the length in octets of the payload, i.e. the rest of the packet following the mandatory part of the GTP header (that is the first 8 octets). The Sequence Number, the N-PDU Number or any Extension headers shall be considered to be part of the payload, i.e. included in the length count.
- Sequence Number: This field is present only if the S field is set to 1. The handling of this field is specified in subclause 9.1.1. It shall be used in order to decide whether or not to discard a received T-PDU, as specified in sub-clause 9.3.1.1 Usage of the Sequence Number or as a transaction identity for GTP-U signalling messages having a response message defined for a request message. For GTP-U message, Supported Extension Headers Notification and Error Indication the Sequence Number shall be ignored by the receiver.
- N-PDU Number: This field shall be included if and only if the PN flag is set to 1. In this case, the old SGSN (or RNC) uses it, at the Inter SGSN Routeing Area Update procedure (or SRNS relocation), to inform the new SGSN (or RNC) of the N-PDU number assigned to T-PDU. If an N-PDU number was not assigned to the T-PDU by PDCP, or if the T-PDU is to be transferred using unacknowledged peer-to-peer LLC operation, then PN shall be set to 0.
- TEID: Contains the Tunnel Endpoint Identifier for the tunnel to which this T-PDU belongs. The TEID shall be used by the receiving entity to find the PDP context, except for the following cases:
- The Echo Request/Response and Supported Extension Headers notification messages, where the Tunnel Endpoint Identifier shall be set to all zeroes.
- The Error Indication message where the Tunnel Endpoint Identifier shall be set to all zeros.

9.3.1.1 Usage of Sequence Number

The sending GGSN and SRNC shall use 0 for the value of the Sequence Number of the first G-PDU in a tunnel, only during the PDP context activation, and shall increment the Sequence Number for each following G-PDU. The value shall wrap to zero after 65535.

The receiving GGSN and SRNC shall set the content of a counter to zero, only during the PDP context activation. When the receiving GGSN and SRNC receives a valid G-PDU, it shall increment this counter by one. This counter shall wrap to zero after 65535. It defines the 'Expected Sequence Number'.

Based on the received and Expected Sequence Number values, the receiving GGSN and SRNC may decide whether or not to discard the received G-PDU. Annex A (Informative) describes a method to determine whether a received G-PDU is valid.

The receiving GGSN and SRNC shall reorder the incoming T-PDUs in sequence if the Reordering Required flag in the PDP context is set. In this case, if needed, the receiving GGSN and SRNC shall take into account a maximum number of valid received frames and a maximum elapsed time to assume that a G-PDU was lost.

The G-PDU sequence numbers allocated by the GGSN (down-link) and SRNC (uplink) are kept unchanged irrespective of the number of GTP tunnels the PDU is transferred over. Therefore, SGSN shall use on the Iu interface for down-link PDUs the G-PDU sequence number received from the GGSN, and shall use on the Gn interface for uplink PDUs the G-PDU sequence number received from the SRNC. In case of SRNS relocation and intersystem change, the SRNC and SGSN shall tunnel PDUs without changing the G-PDU sequence numbers.

9.4 Tunnelling between SGSNs

T-PDUs, stored in the old SGSN and not yet sent to the MS, shall be tunnelled to the new SGSN as a part of the Inter SGSN Routeing Update procedure described in 3GPP TS 23.060. Some T-PDUs may still be on their way from the GGSN to the old SGSN because they have been sent before the tunnel change. These T-PDUs shall also be tunnelled to the new SGSN.

For intersystem SRNS Relocation, the establishment of the GTP tunnel(s) for the forwarding of G-PDUs is as described in the 3GPP TS 23.121 and in the 3GPP TS 23.060 specifications.

9.5 Tunnelling between Source RNC and Target RNC

For the 3G-3G SRNS Relocation, the establishment of the GTP tunnel for the forwarding of G-PDUs between source and target RNC, is as described in the 3GPP TS 23.121 and in the 3GPP TS 23.060 specifications.

9.6 Tunnelling between GGSNs

GTP shall not specify tunnelling between GGSNs. Transfer of MS-to-MS traffic between GGSNs shall use the Gi interface.

10 Path Protocols

10.1 UDP/IP

UDP/IP is the only path protocol defined to transfer GTP messages in the version 1 of GTP. A User Datagram Protocol (UDP) compliant with STD 0006 shall be used.

10.1.1 UDP Header

10.1.1.1 Request Messages

The UDP Destination Port number for GTP-C request messages is 2123. It is the registered port number for GTP-C.

The UDP Destination Port number for GTP-U request messages is 2152. It is the registered port number for GTP-U.

The UDP Source Port is a locally allocated port number at the sending GSN/RNC.

10.1.1.2 Response Messages

The UDP Destination Port value shall be the value of the UDP Source Port of the corresponding request message.

The UDP Source Port shall be the value from the UDP Destination Port of the corresponding request message.

10.1.1.3 Encapsulated T-PDUs

The UDP Destination Port number shall be 2152. It is the registered port number for GTP-U. The UDP Source Port is a locally allocated port number at the sending GSN/RNC.

10.1.1.4 Error Indication, Version Not Supported and Supported Extension Headers Notification

The UDP destination port for the Error Indication shall be the user plane UDP port (2152).

The UDP destination port for the Version Not Supported message shall be the control plane UDP port (2123)

The UDP destination port for the Supported Extension Headers Notification shall be the UDP port for User plane (2152) if the trigger for it was a user plane message, the control plane port (2123) if the trigger for it was a control plane message.

The UDP source port shall be locally assigned at the sending node.

10.1.2 IP Header

An Internet Protocol (IP) compliant with STD 0005 shall be used.

10.1.2.1 Request Messages and Encapsulated T-PDUs

The IP Source Address shall be an IP address of the source GSN/RNC from which the message is originating.

The IP Destination Address in a GTP request message shall be an IP address of the destination GSN/RNC. The IP Destination Address in an encapsulated T-PDU GTP shall be an IP address of the destination GSN/RNC.

10.1.2.2 Response Messages

The IP Source Address shall be an IP address of the source GSN/RNC from which the message is originating.

The IP Destination Address shall be copied from the IP Source Address of the GTP request message to which this GSN/RNC is replying.

10.1.2.3 Error Indication, Version Not supported and Supported Extension Headers Notification

The IP source address shall be an address of the source GSN/RNC from which the message is originated. In particular, the source Address of the "Version Not Supported" or the "Supported Extension Headers Notification" message, shall be set to the destination address of the message that triggered the GSN/RNC to send the "Version Not Supported" or the "Supported Extension Headers Notification" message.

The IP destination address shall be the source address of the GTP-PDU that is the cause for the GSN/RNC to send one of these messages.

11 Error Handling

11.1 Protocol Errors

A protocol error is defined as a message with unknown, unforeseen or erroneous content. The term silently discarded used in the following sub clauses means that the implementation shall discard the message without further processing and should log the event including the erroneous message and should include the error in a statistical counter.

An information element with 'Mandatory' in the 'Presence requirement' column of a message definition shall always be present in that message.

The conditions for a conditional information element define whether the information element is semantically:

- mandatorily present;
- optionally present;
- mandatorily absent.

An information element, which is semantically mandatorily present but is omitted from the message, is treated as missing data.

An information element, which is semantically mandatorily absent but is present in the message, is treated as unexpected data.

The Error Indication, the Version Not Supported, Supported Extension Headers Notification and the SGSN Context Acknowledge messages shall be considered as Responses for the purpose of this Section.

The sub clauses 11.1.1 to 11.1.13 shall be applied in decreasing priorities.

11.1.1 Different GTP Versions

If a receiving node receives a GTP message of an unsupported version, that node shall return a GTP Version Not Supported message indicating in the Version field of the GTP header the latest GTP version that that node supports. The received GTP-PDU shall then be discarded.

A GTP version '0' only GSN may not be listening on port 2123 and as such it will not be able to send back a Version Not Supported message to a peer trying to establish a dialogue with it using GTP-C. As such, a GSN supporting both version '1' and version '0' shall fall back to version '0' if the attempt to contact a peer using version '1' fails.

It is an implementation option keeping a shortlist of recently contacted version '0' only GSNs, as well of the version supported by those nodes sending back a Version Not Supported message.

11.1.2 GTP Message Too Short

When a GTP message is received, and is too short to contain the GTP header for the GTP version that the sender claims to use, the GTP-PDU message shall be silently discarded.

11.1.3 Unknown GTP Signalling Message

When a message using a Message Type value defining an Unknown GTP signalling message is received, it shall be silently discarded.

11.1.4 Unexpected GTP Signalling Message

When an unexpected GTP control plane message is received, e.g. a Response message for which there is no corresponding outstanding Request, or a GTP control plane message a GSN is not expected to handle (such as a PDU Notification Request received by a GGSN),, it shall be silently discarded.

11.1.5 Missing Mandatorily Present Information Element

The receiver of a GTP signalling Request message with a missing mandatorily present information element shall discard the request, should log the error, and shall send a Response with Cause set to 'Mandatory IE missing'. The receiver of a Response with a missing mandatory information element shall notify the upper layer and should log the error.

11.1.6 Invalid Length

In a received GTP signalling message Request, a mandatory TLV format information element may have a Length different from the Length defined in the version that this message claims to use. In this case, this information element shall be discarded, the error should be logged, and a Response shall be sent with Cause set to 'Mandatory IE incorrect'.

In a received GTP signalling message Response, if a mandatory TLV format information element has a Length different from the Length defined in the version that this message claims to use, then the requesting entity shall treat the GTP signalling procedure as having failed.

11.1.7 Invalid Mandatory Information Element

The receiver of a GTP signalling message Request including a mandatory information element with a Value that is not in the range defined for this information element value shall discard the request, should log the error, and shall send a response with Cause set to 'Mandatory IE incorrect'.

The receiver of a GTP signalling message Response including a mandatory information element with a Value that is not in the range defined for this information element shall notify the upper layer that a message with this sequence number has been received and should log the error.

If a GSN receives an information element with a value which is shown as reserved, it shall treat that information element as not being in the range defined for the information element.

NOTE: The receiver does not check the content of an information element field that is defined as 'spare'.

11.1.8 Invalid Optional Information Element

The receiver of a GTP signalling message including an optional information element with a Value that is not in the range defined for this information element value shall discard this IE, should log the error, and shall treat the rest of the message as if this IE was absent.

If a GSN receives an information element with a value which is shown as reserved, it shall treat that information element as not being in the range defined for the information element.

NOTE: The receiver does not check the content of an information element field that is defined as 'spare'.

11.1.9 Unknown Information Element

An information element with an unknown Type value shall be ignored by the receiver of the message. If this is a TLV element, this information element shall be skipped using its Length value. If this is a TV element, the receiver shall discard the rest of the message.

If the receiving node cannot interpret the rest of the message because of the ignored information element, the receiving node shall discard the message and should log the error. If the message was a Request, it shall, in addition, return a response with Cause set to 'Invalid message format'.

11.1.10 Out of Sequence Information Elements

If two or more information elements are out of sequence in a message, the receiving node shall discard the message and should log the error. In addition, if the message was a Request, the receiving node shall return a Response with Cause set to 'Invalid message format'.

11.1.11 Unexpected Information Element

An information element with a Type value which is defined in GTP but is not expected in the received GTP signalling message shall be ignored (skipped) and the rest of the message processed as if this information element was not present.

11.1.12 Repeated Information Elements

If an information element is repeated in a GTP signalling message in which repetition of the information element is not specified, only the contents of the information element appearing first shall be handled and all subsequent repetitions of the information element shall be ignored. When repetition of information elements is specified, only the contents of specified repeated information elements shall be handled.

11.1.13 Incorrect Optional Information Elements

All optional information elements that are incorrect in a GTP signalling message shall be treated as not present in the message. However, if the receiving node may not handle the message correctly because of the incorrect information element, the receiving node should log the error and shall return a response with Cause set to 'Optional IE incorrect'.

11.2 Path Failure

A path counter shall be reset each time a response is received on the path and incremented when the T3-RESPONSE timer expires for any message sent on the path. The path shall be considered to be down if the counter exceeds N3-REQUESTS. In this case, the GSN or RNC may notify the Operation and Maintenance network element. GTP shall also notify the upper layer of the path failure, so that PDP contexts associated with this path may be deleted.

11.3 MS Detach

When an MS detaches, all ongoing GTP control plane procedures related to this MS shall be aborted. The SGSN shall send Delete PDP Context Request messages for all active PDP contexts to the peer GGSNs.

11.4 Restoration and Recovery

All GSNs shall maintain in non-volatile memory a Restart Counter of local significance. A GSN that restarts shall change the Restart Counter value immediately after the restart procedure has been completed. The value shall be incremented by 1 modulo 256 (see 3GPP TS 23.007).

All GSNs shall also maintain in volatile memory a Restart Counter for each GSN that it is in contact with. The Restart Counters stored for all GSNs that it is in contact with shall be cleared after the restart procedure has been completed (see 3GPP TS 23.007).

12 Inter-PLMN GTP Communication over the Gp Interface

No security is provided in GTP to protect the communication between different GPRS networks. The security is provided, if needed, between the Border Gateways in different GPRS networks by operator agreements. A security mechanism that may be considered is for example IP Security.

13 IP, The Networking Technology used by GTP

13.1 IP Version

The IPv4 (RFC 791) protocol shall be supported, IPv6 (RFC 2460) support is optional.

13.2 IP Fragmentation

Here it is described how the fragmentation mechanism shall work together with GTP, when the GPRS backbone is based on IPv4.

However, fragmentation should be avoided if possible. Examples of fragmentation drawbacks are, e.g.:

- Fragmentation is inefficient, since the complete IP header is duplicated in each fragment.
- If one fragment is lost, the complete packet has to be discarded. The reason is that no selective retransmission of fragments is possible.

By using Path MTU discovery the application may find out the MTU, and thereby utilise more efficient segmentation mechanisms in other protocol layers than IP.

The maximum size of a T-PDU that may be transmitted without fragmentation by GGSN or the MS is defined in GSM 03.60. All backbone links should have MTU values that exceeds the sum of the maximum value plus the size of the tunnel headers (IP header, UDP and GTP header) in order to avoid fragmentation in the backbone.

13.2.1 MO Direction

SGSN: A packet from an MS shall be encapsulated at the SGSN with a GTP header, UDP and IP header. If the resulting IP packet is larger than the MTU of the first link towards the GGSN, fragmentation of the IP packet shall be performed by the SGSN. The SGSN should preferably fragment the IP packet if it is larger than the MTU of any link between SGSN and GGSN.

Backbone router: Any router in the backbone may fragment the GTP packet if needed, according to IPv4.

GGSN: The GGSN shall assemble any IP fragments received from SGSNs, according to IPv4. Note that if any fragment is lost, the whole packet shall be discarded.

13.2.2 MT Direction

GGSN: A packet from an external host shall be encapsulated at the GGSN with a GTP header, UDP and IP header. If the resulting IP packet is larger than the MTU on the first link towards the SGSN, fragmentation of the IP packet shall be performed by the GGSN. The GGSN should preferably fragment the IP packet if it is larger than the MTU of any link between GGSN and SGSN.

Backbone Router: Any router in the backbone may fragment the GTP packet if needed, according to IPv4.

SGSN: The SGSN shall assemble any IP fragments received from the GGSN, according to IPv4. Note that if any fragment is lost, the whole packet shall be discarded.

13.2.3 Tunnelling from old to new SGSN

Old SGSN: A user packet shall be encapsulated with a GTP header, UDP and IP header. If the resulting IP packet is larger than the MTU on the first link towards the new SGSN, fragmentation of the IP packet shall be performed by the old SGSN. The old SGSN should preferably fragment the IP packet if it is larger than the MTU of any link between old and new SGSN.

Backbone router: Any router in the backbone may fragment the GTP packet if needed, according to IPv4.

New SGSN: The new SGSN shall assemble any IP fragments received from the old SGSN, according to IPv4. Note that if any fragment is lost, the whole packet shall be discarded.

14 GTP Parameters

The GTP system parameters defined here and their recommended values shall not be fixed, but shall be possible to configure as described in section ‘Reliable delivery of messages’.

14.1 Timers

The timer T3-RESPONSE holds the maximum wait time for a response of a request message.

The timer T3-TUNNEL holds the time when PDUs shall be forwarded from the old SGSN to the new SGSN. The timer is started in the old SGSN when it receives a GTP SGSN Context Request message and there is at least one active PDP context. GTP shall indicate to the upper layer when the timer has expired. The recommended timer value is 20 seconds.

14.2 Others

The counter N3-REQUESTS holds the maximum number of attempts made by GTP to send a request message. The recommended value is 5.

The N3-BUFFER-SIZE is the size of the receive buffer for G-PDUs and request messages. The recommended value is 8192.

Tables

Figures

Annex A (informative): A method for sequence number checking

This annex describes a method to determine whether or not a received T-PDU is valid, for the Usage of the Sequence Number subclause, 9.3.1.1.

This method deals with two distinct problems.

The first one is the 'drifting' between the Sequence Number value that we expect to receive in the light of the total number of T-PDU received for this tunnel (the Expected value), and the effective received value. The probability that the received T-PDU is not correct because not awaited is higher if the distance between expected and received Sequence Numbers is high than if this distance is low. This leads to Condition 1. Its left part represents the distance between the Expected and received values, in a circular 65536 dimension.

The second one is the duplication of T-PDU frames within a given number of last received frames that have been accepted by the condition 1.

This leads to the following actions:

> This operation shall start when the dialogue is established between the GSNs. When each T-PDU is received during the dialogue, if this T-PDU is valid, its Sequence Number shall be saved. The last 'A' saved Sequence Numbers represent the 'Recorded Sequence Number Set'.

A received T-PDU sequence number is valid only if it satisfies both of the following conditions:

1) Min(Abs(E - r), Abs(r - 65536 - E), Abs(E - 65536 - r)) < 'B' Condition 1
   Where: 'E' is the Expected Sequence Number and 'r' is the received Sequence Number.

2) The received Sequence Number is not a member of the Recorded Sequence Number Set. Condition 2.

'A' and 'B' are parameters. The receiving GSN shall discard a received T-PDU with an invalid Sequence Number.

Abs(X) represents the absolute value of the number X.

Min(X,Y,Z) represents the lowest value taken from the numbers X, Y, and Z.

Annex B (informative): Change history

Change history						
TSG CN #	**Spec**	**Version**	**CR**	**<Phase>**	**New Version**	**Subject/Comment**
Apr 1999	GSM 09.60	7.0.0				Transferred to 3GPP CN1
CN#03	29.060			R99	3.0.0	Approved at CN#03
			001	R99		Replacing the V(R) transfer mechanism with the N-PDU number transfer mechanism in routing area update
CN#4	29.060	3.0.0	002	R99	3.1.0	Clarification of ambiguous/superfluous information
			003	R99		Timer handling in GTP
			005	R99		Mandatory SGSN Context Acknowledge message
			006	R99		Mandatory info in MM Context IE
			007	R99		APN to be transferred in the PDP context at inter SGSN RA update
			008	R99		Consistency on implemented CRs from SMG#28
			009	R99		Removal of changes in PDP context establishment and restoration
			010	R99		MSISDN in the Create PDP Context request
CN#05	29.060	3.1.0	014r2	R99	3.2.0	Specification of the MSISDN Information Element in GSM 09.60
CN#06	29.060	3.2.1	017r4	R99	3.3.0	QoS enhancements
CN#06	29.060	3.2.1	031	R99	3.3.0	Merged CRs on GTP Enhancements
CN#07	29.060	3.3.0	033r2	R99	3.4.0	Addition of Radio Priority to the SGSN Context Response
CN#07	29.060	3.3.0	035r2	R99	3.4.0	Addition of Packet Flow Id to the SGSN Context Response
CN#07	29.060	3.3.0	036r1	R99	3.4.0	Change the attribution of the PDP Context IE
CN#07	29.060	3.3.0	037	R99	3.4.0	Add new cause value
CN#07	29.060	3.3.0	038	R99	3.4.0	Addition of NSAPI to GGSN-initiated Update PDP Context
CN#07	29.060	3.3.0	040	R99	3.4.0	Improving charging efficiency
CN#07	29.060	3.3.0	041r1	R99	3.4.0	Subscriber and equipment trace for PS domain
CN#07	29.060	3.3.0	042	R99	3.4.0	Necessity of the function of the calculation an SGSN IP address from the target ID
CN#07	29.060	3.3.0	045r1	R99	3.4.0	Removal of Anonymous Access
CN#07	29.060	3.3.0	046r1	R99	3.4.0	Clarification of Authentication Type and Import of Parameters
CN#07	29.060	3.3.0	048	R99	3.4.0	Correction of IE types and order
CN#07	29.060	3.3.0	050r2	R99	3.4.0	Clarification on Protocol Type in GTP Header
CN#07	29.060	3.3.0	051	R99	3.4.0	Clarification of Repeated Information Element Ordering
CN#07	29.060	3.3.0	052r2	R99	3.4.0	Method for GTP extension headers support
CN#07	29.060	3.3.0	053r2	R99	3.4.0	The addition of the conditional description of the GTP parameters
CN#07	29.060	3.3.0	056	R99	3.4.0	Change of naming when referring to primary and secondary contexts
CN#07	29.060	3.3.0	057	R99	3.4.0	Removal of X.25
CN#07	29.060	3.3.0	058r1	R99	3.4.0	Use of 3 Digit MNCs in GTP for R'99
CN#07	29.060	3.3.0	063r2	R99	3.4.0	QoS Profile IE modification
CN#07	29.060	3.3.0	067r1	R99	3.4.0	Distribution of security data
CN#07	29.060	3.3.0	069r1	R99	3.4.0	New cause codes for TFT and packet filter errors

Change history						
TSG CN #	**Spec**	**Version**	**CR**	**<Phase>**	**New Version**	**Subject/Comment**
CN#07	29.060	3.3.0	070	R99	3.4.0	IPv6 support as optional in Iu and Gn
CN#07	29.060	3.3.0	072r4	R99	3.4.0	Clarification on the use of TEID in the GTP header
CN#07	29.060	3.3.0	073	R99	3.4.0	Clarification to the function of the calculation of an SGSN IP address from the target ID
CN#07	29.060	3.3.0	075	R99	3.4.0	Changing references from GSM specifications to 3GPP TS
CN#07	29.060	3.3.0	076	R99	3.4.0	New table for Information Elements
CN#07	29.060	3.3.0	077	R99	3.4.0	Forward SRSN Context
CN#07	29.060	3.3.0	078r1	R99	3.4.0	PDCP sequence numbers in SRNC relocation and inter-system handover
CN#07	29.060	3.3.0	079	R99	3.4.0	Removal of TCP support in the packet domain PLMN backbone network
CN#07	29.060	3.3.0	081	R99	3.4.0	Addition of PDP Context Identifier to PDP Context Information Element
CN#07	29.060	3.3.0	083	R99	3.4.0	Editorial clarification of information elements in the SGSN Context Response
CN#08	29.060	3.4.0	084	R99	3.5.0	16-bit PDCP sequence numbers in GTP header
CN#08	29.060	3.4.0	085	R99	3.5.0	Mandatory inclusion of IMSI in SGSN Context Response if P-TMSI Signature Mismatch
CN#08	29.060	3.4.0	086r1	R99	3.5.0	Encoding of spare IMSI Digits
CN#08	29.060	3.4.0	087r1	R99	3.5.0	Reliable delivery of signalling messages
CN#08	29.060	3.4.0	088	R99	3.5.0	Possible cause codes for Relocation Cancel Response
CN#08	29.060	3,4,0	089	R99	3.5.0	Condition for evaluating the sequence number fields in PDP context
CN#08	29.060	3.4.0	090r1	R99	3.5.0	Target RNC Information
CN#08	29.060	3.4.0	091r1	R99	3.5.0	Change of the length of TI
CN#08	29.060	3.4.0	092r1	R99	3.5.0	Clean up for 29.060
CN#08	29.060	3.4.0	093r2	R99	3.5.0	Clarification on the TEID handling
CN#08	29.060	3.4.0	094r1	R99	3.5.0	QoS Profile IE modification
CN#08	29.060	3.4.0	096	R99	3.5.0	Restart counter in Echo response
CN#08	29.060	3.4.0	097r1	R99	3.5.0	Clarification on the use of TEID in the GTP-C header
CN#08	29.060	3.4.0	098	R99	3.5.0	Add APN IE for PDU Notification Reject Request message
CN#08	29.060	3.4.0	099r1	R99	3.5.0	Addition of response code Delete PDP Context Response
CN#08	29.060	3.4.0	100r1	R99	3.5.0	Introduction of a different port number for GTP-C and GTP-U
CN#08	29.060	3.4.0	101r1	R99	3.5.0	Addition of charging characteristics per PDP context
CN#08	29.060	3.4.0	102	R99	3.5.0	Alignment of text with tables
CN#08	29.060	3.4.0	106	R99	3.5.0	Removal of Connection oriented paths
CN#08	29.060	3.4.0	108	R99	3.5.0	On the use of the Sequence number in GTP-C
CN#08	29.060	3.4.0	109	R99	3.5.0	N-PDU number in GTP-C
CN#08	29.060	3.4.0	110r1	R99	3.5.0	Editorial modifications due to the upgrade from GTPv0 to GTPv1 for R´99
CN#08	29.060	3.4.0	111r1	R99	3.5.0	Editorial modifications concerning GTP-U and GTP-C
CN#08	29.060	3.4.0	112	R99	3.5.0	Introducing Supported Extension Headers Notification to GTP-U
CN#08	29.060	3.4.0	113	R99	3.5.0	Missing IEs in Error Indication
CN#08	29.060	3.4.0	114	R99	3.5.0	Clarification of the Cause of Create PDP Context Response
CN#08	29.060	3.4.0	115	R99	3.5.0	Clarification of the TEID for Signalling
CN#08	29.060	3.4.0	116	R99	3.5.0	Clarification on the TEID for Signalling of the PDU Notification Reject Request

Change history						
TSG CN #	**Spec**	**Version**	**CR**	**<Phase>**	**New Version**	**Subject/Comment**
CN#08	29.060	3.4.0	117r2	R99	3.5.0	Clarification of the conditional information elements
CN#08	29.060	3.4.0	119	R99	3.5.0	Clarification on the use of SGSN address at PDU notification procedure (R99)
CN#09	29.060	3.5.0	105r1	R99	3.6.0	Race Conditions Avoidance
CN#09	29.060	3.5.0	121	R99	3.6.0	Definition of TEID value in GTP-U header
CN#09	29.060	3.5.0	122r3	R99	3.6.0	Solution for race condition of GTP procedures
CN#09	29.060	3.5.0	123r1	R99	3.6.0	Clarifications concerning the use of TEID in the Control Plane
CN#09	29.060	3.5.0	124r1	R99	3.6.0	Editorial modifications concerning TEID Control Plane and TEID Data
CN#09	29.060	3.5.0	126r2	R99	3.6.0	Sequence number in signalling messages
CN#09	29.060	3.5.0	127	R99	3.6.0	Clarification of the conditional information elements
CN#09	29.060	3.5.0	128r1	R99	3.6.0	Enhancement of MS Network capabirity and GPRS Ciphering Algorithm
CN#09	29.060	3.5.0	129	R99	3.6.0	IPv6 support for Charging Gateway Address
CN#09	29.060	3.5.0	130	R99	3.6.0	Signalling messages in GTP
CN#09	29.060	3.5.0	131r1	R99	3.6.0	Security parameter transport in case of 2G-3G interworking
CN#09	29.060	3.5.0	132r1	R99	3.6.0	Encoding of IMSI
CN#09	29.060	3.5.0	133	R99	3.6.0	Removal of IHOSS from GTP
CN#09	29.060	3.5.0	135	R99	3.6.0	Addition of MS Not Reachable Reason to Send Routing Information For GPRS Response
CN#09	29.060	3.5.0	138r1	R99	3.6.0	Coding of TI in PDP Context
CN#09	29.060	3.5.0	139r1	R99	3.6.0	Clarifications on the use of TEID in the Control Plane
CN#09	29.060	3.5.0	140	R99	3.6.0	Correction on the handling of the PDP Context at unsuccessful PDP Context modification
CN#09	29.060	3.5.0	141r2	R99	3.6.0	Categorize Error indication as the GTP-U message
CN#09	29.060	3.5.0	142	R99	3.6.0	Clarifications on the presence condition of TLLI/P-TMSI in SGSN Context request
CN#09	29.060	3.5.0	143r2	R99	3.6.0	Correction on Reliable transmission of signalling messages
CN#09	29.060	3.5.0	144	R99	3.6.0	Alignment of the description of tables for Identification Request and SGSN Context Request
CN#09	29.060	3.5.0	145r1	R99	3.6.0	Correction to the SGSN Context transfer Request and response messages
CN#09	29.060	3.5.0	146r2	R99	3.6.0	Correction to the SGSN Forward relocation Request and Response messages
CN#09	29.060	3.5.0	147	R99	3.6.0	Clarification or the handling of response messages
CN#09	29.060	3.5.0	148	R99	3.6.0	Clarification on SGSN context acknowledge message
CN#10	29.060	3.6.0	136r2	R99	3.7.0	Compatibility GTPv0/GTPv1 in case of SGSN change
CN#10	29.060	3.6.0	149	R99	3.7.0	Clarification on the use of Teardown Indicator
CN#10	29.060	3.6.0	150	R99	3.7.0	Correction to the PDU Notification Request message
CN#10	29.060	3.6.0	151r1	R99	3.7.0	Correction of wrong entry in information table
CN#10	29.060	3.6.0	152	R99	3.7.0	Moving of Annex A to 3GPP TS 23.003
CN#10	29.060	3.6.0	153r2	R99	3.7.0	Selecting GGSN IP address
CN#10	29.060	3.6.0	154r1	R99	3.7.0	Removal of ‘Version not Supported’ for GTP-U

Change history						
TSG CN #	**Spec**	**Version**	**CR**	**<Phase>**	**New Version**	**Subject/Comment**
CN#10	29.060	3.6.0	157	R99	3.7.0	Correction of Security parameters length
CN#10	29.060	3.6.0	159	R99	3.7.0	MS Network Capability in MM Context
CN#10	29.060	3.6.0	161	R99	3.7.0	Clarifications to the usage of CKSN and KSI for security type 0
CN#11	29.060	3.7.0	155r4	R99	3.8.0	Adding Uplink TEID Data I and user plane GGSN address to PDP Context IE
CN#11	29.060	3.7.0	162	R99	3.8.0	Handling of sequence numbers for reliable transmission of control plane messages
CN#11	29.060	3.7.0	163	R99	3.8.0	Re-configure the IEs in the PDU Notification Request to make it in ascending order
CN#11	29.060	3.7.0	166	R99	3.8.0	Corrections to editorwork of 29.060 v 3.7.0
CN#11	29.060	3.7.0	170r2	R99	3.8.0	Clarification on the TEID value of the signalling messages
CN#11	29.060	3.7.0	173r3	R99	3.8.0	Clarifications to the GTP-U protocol
CN#11	29.060	3.7.0	174r1	R99	3.8.0	Essential Correction of the delete PDP context procedure
CN#11	29.060	3.7.0	178	R99	3.8.0	Re-configure the IEs in the Send Routeing Information for GPRS Response message to make it in ascending order
CN#11	29.060	3.7.0	180r1	R99	3.8.0	IMSI Encoding Clarification
CN#11	29.060	3.7.0	181r1	R99	3.8.0	Fix an ambiguous description on the treatment for the PDP Type PPP in PDP context creation procedure
CN#11	29.060	3.7.0	182r2	R99	3.8.0	GSN address in Error Indication
CN#11	29.060	3.7.0	186r1	R99	3.8.0	Clarification of Error Indication
CN#11	29.060	3.7.0	187	R99	3.8.0	Clarification on the handling of sequence numbers in the GTP user plane
CN#11	29.060	3.7.0	188	R99	3.8.0	Clarifications and clean up of the error handling section
CN#11	29.060	3.7.0	191r1	R99	3.8.0	Clarification on the use of the term G-PDU
CN#11	29.060	3.8.0		Rel-4	4.0.0	Version increased from R99 to Rel-4 after CN#11.
CN#12	29.060	4.0.0	194	Rel-4	4.1.0	Correction/Clarification of GGSN handling of Update PDP Context Response
CN#12	29.060	4.0.0	196	Rel-4	4.1.0	Correction due to incorrectly implemented CR on the Error indication message
CN#12	29.060	4.0.0	198	Rel-4	4.1.0	RNC IP Address IE format
CN#12	29.060	4.0.0	208	Rel-4	4.1.0	GTP Message Treatment
CN#12	29.060	4.0.0	220	Rel-4	4.1.0	Clarification of the handling of Version Not Supported; Supported Extension Headers and Error Indication messages
CN#12	29.060	4.0.0	221	Rel-4	4.1.0	Removal of the useless “version not supported” cause code from GTP messages

Change history						
TSG CN #	**Spec**	**Version**	**CR**	**<Phase>**	**New Version**	**Subject/Comment**
CN#12	29.060	4.0.0	222	Rel-4	4.1.0	Ambiguous text description of the Charging Gateway Address IE handling in the GTP create PDP context request message
CN#12	29.060	4.0.0	227	Rel-4	4.1.0	Alignment of the 29.060 with the 23.060 for the SRNS Relocation procedure

History

Document history		
V4.0.0	March 2001	Publication
V4.1.0	June 2001	Publication